

RedCheck

СРЕДСТВО АНАЛИЗА
ЗАЩИЩЕННОСТИ



Руководство
пользователя

АЛМЮ.501410.RC02-01.РП

Версия документа 2.11.ru



Содержание

Перед началом работы.....	5
Сценарии использования RedCheck.....	7
Рабочий процесс в RedCheck	9
Ролевая модель RedCheck	10
Сведения об интегральной оценке по базовым метрикам CVSS	12
1 Группы.....	13
1.1 Создание группы.....	14
1.2 Возможности группы.....	16
2 Хосты	18
2.1 Создание хостов вручную	22
2.2 Импорт из CSV-файла.....	24
2.3 Импорт из AD	27
2.4 Импорт из Host Discovery	30
2.5 Экспорт хостов в CSV.....	32
3 Учетные записи для сканирования	34
3.1 Менеджер учетных записей	36
3.2 Подбор учетных записей для сканирования	38
4 Задания для сканирования.....	41
4.1 Аудит уязвимостей.....	48
4.2 Аудит обновлений.....	52
4.3 Аудит конфигураций	57
4.4 Инвентаризация.....	62
4.5 Фиксация (контроль целостности)	66
4.6 Аудит уязвимостей АСУ ТП.....	70
4.7 Проверка доступности	74
4.8 Обнаружение хостов.....	77
4.9 Аудит в режиме "Пентест"	80
4.10 Аудит уязвимостей Docker / Инвентаризация Docker	86
4.11 Сканирование YARA правил	93
4.12 Настройка расписания для задания	96
4.13 Повторный перезапуск недоступных хостов во время сканирования.....	100
5 Расширенные возможности для заданий сканирования.....	101

5.1 Профили аудитов.....	102
5.1.1 Менеджер профилей.....	106
5.2 Конфигурации	114
5.2.1 Импорт конфигураций.....	118
5.3 OVAL-определения.....	119
5.4 Отслеживание изменений результатов сканирования (Контроль).....	122
5.5 Профили сканирования Altxmap	126
5.6 Импорт скриптов для пентеста	127
5.7 Импорт YARA-правил	132
6 Результаты сканирований	134
6.1 Аудит уязвимостей.....	137
6.2 Аудит обновлений.....	139
6.3 Аудит конфигураций	141
6.4 Инвентаризация.....	147
6.5 Фиксация (контроль целостности)	149
6.6 Аудит уязвимостей АСУ ТП.....	150
6.7 Аудит СУБД	162
6.8 Проверка доступности.....	154
6.9 Обнаружение хостов.....	155
6.10 Аудит в режиме "Пентест"	156
6.11 Аудит уязвимостей Docker / Инвентаризация Docker	159
6.12 Статистика выполненных заданий.....	162
7 Отчеты	168
7.1 Создание простого отчета.....	173
7.1.1 Настройки для разных типов задания.....	178
7.2 Создание дифференциального отчета.....	187
7.2.1 Настройки для разных типов задания.....	190
7.3 Шаблоны отчетов.....	194
7.3.1 Настройки для разных типов задания.....	199
7.4 Просмотр CSV отчетов	207
8 Аналитика	211
8.1 Актуальность сканирования	212
8.2 Недоступность хостов	217
8.3 Анализ уязвимостей	223

8.3.1 Вкладка Уязвимости.....	224
8.3.2 Вкладка Хосты.....	230
8.3.3 Вкладка Хост – Уязвимость	237
8.4 Контроль устранения уязвимостей	243
8.4.1 Вкладка Уязвимости.....	244
8.4.2 Вкладка Хосты.....	252
8.4.3 Вкладка Хост – Уязвимость	260
8.5 Анализ конфигураций	268
8.5.1 Вкладка Статистика	269
8.5.2 Вкладка Правила.....	274
8.5.3 Вкладка Хосты.....	280
8.5.4 Вкладка Хост – Параметр	286
Дополнительные возможности	293
Мониторинг служб сканирования.....	294

Перед началом работы

RedCheck – современное средство анализа защищенности, позволяющее выявлять уязвимости операционных систем и приложений, потенциально опасные настройки, осуществлять оценку соответствия требованиям политик и стандартов, проводить инвентаризацию оборудования и программ, а также формировать детальные отчеты.

Данное руководство пользователя для RedCheck (далее – RedCheck, Система) содержит описание возможностей и функций программы, рекомендации по использованию, условия и порядок работы в RedCheck.

Руководство предназначено для администраторов ИБ. Разработчик может вносить в Руководство изменения, связанные с улучшением Системы.

Актуальная версия документации публикуется в новой редакции Руководства, а также на сайте компании.

Что нового в RedCheck 2.11

- Функция **Ограничения максимального времени выполнения задания** перенесено в настройки расписания
- Аудит СУБД объединен с заданием Аудит конфигураций
- [Добавлена возможность импорта пользовательских скриптов для Аудита в режиме Пентест](#)
- [Добавлено новое задание Сканирование YARA правил](#)
- [Добавлена возможность импорта пользовательских YARA правил](#)

Содержание

- [1 Группы](#)
- [2 Хосты](#)
- [3 Учетные записи для сканирования](#)
- [4 Задания для сканирования](#)
- [5 Расширенные возможности для заданий сканирования](#)
- [6 Результаты сканирований](#)
- [7 Отчеты](#)
- [8 Аналитика](#)

- Дополнительные возможности

Дополнительный материал перед началом работы

- Сценарии использования RedCheck
- Рабочий процесс в RedCheck
- Ролевая модель RedCheck
- Сведения об интегральной оценке по базовым метрикам CVSS

Сценарии использования RedCheck

Сценарий выявления уязвимостей

В данном сценарии сканер RedCheck используется на первых шагах цикла управления уязвимостями, как инструмент их выявления, в условиях слабой стандартизации инфраструктуры и процесса исследования активов со стороны ИБ-администратора или аналитика.

Для обеспечения своевременного обнаружения и выявления уязвимостей согласуется наиболее частый регламент сканирования, который допустим техническим покрытием необходимого количества сканируемых хостов. Например, полный проход сканирования осуществляется каждую неделю. Для исследования могут применяться все необходимые аудиты: в условиях отсутствия прав на хостах – Аудит в режиме «Пентест», а при наличии учетных записей для подключения с полными административными правами – Аудит уязвимостей (а также другие необходимые аудиты «Белого ящика»).

В процессе выявления любых новых уязвимостей, в том числе с учетом любого нового ПО или сканируемых платформ, необходимо обеспечить наличие полных административных полномочий у учетных записей для Аудита уязвимостей (а также других необходимых аудитов «Белого ящика»), иначе возникает риск пропустить критические уязвимости из-за отсутствия полномочий на хосте.

Сценарий контроля устранения уязвимостей

В данном сценарии сканер RedCheck используется на завершающих шагах цикла управления уязвимостями как инструмент контроля устранения уязвимостей, согласно внутреннему регламенту планового обновления со стороны ИТ.

Для обеспечения контроля достаточно проводить сканирование сразу после завершения процесса регламентного обновления. Например, это может происходить один раз в месяц. Для контроля могут применяться все

необходимые аудиты: в условиях отсутствия прав на хостах – Аудит в режиме «Пентест», а при наличии учетных записей для подключения с полными административными правами – Аудит уязвимостей (а также другие необходимые аудиты «Белого ящика»).

В процессе контроля устранения уязвимостей допустимо обеспечить наличие только необходимых полномочий у учетных записей для Аудита уязвимостей (а также других необходимых аудитов «Белого ящика»), слепок которых наиболее правильно собрать в тестовой зоне с использованием расширенного логирования на разных типах исследуемых хостов.

Для возобновления цикла управления уязвимостями и дополнительного выявления уязвимостей на этапе контроля, с учетом поиска «неучтенного ПО», рекомендуется использовать полные административные полномочия для учетных записей, чтобы полноценный поиск RedCheck не оказался за пределами привилегий предоставленных учетных записей.

Рабочий процесс в RedCheck

Рабочий процесс подразумевает под собой взаимодействие с хостами, которые добавляются в RedCheck через Менеджер учетных записей. Ниже предлагается рекомендуемая последовательность работы в Системе.

Алгоритм работы с активами

Этап 1. Интерпретация сканируемой инфраструктуры в объекты RedCheck

На данном этапе производится создание групп ([1 Группы](#)) и добавление в них хостов ([2 Хосты](#)) для дальнейшего сканирования.

Этап 2. Подготовка учетных записей для доступа к сканируемым хостам

Для доступа к хостам во время выполнения задач сканирования используются учетные записи RedCheck, которые добавляются в Систему в Менеджере учетных записей ([3 Учетные записи](#)). На данном этапе создаются учетные записи для каждой сканируемой в дальнейшем платформы.

Этап 3. Создание заданий для сканирования

На данном этапе создаются задания для проведения сканирований инфраструктуры, ранее интерпретированной в объекты RedCheck ([4 Задания](#) / [5 Расширенные возможности для создания заданий](#))

Этап 4. Просмотр результатов сканирования

На данном этапе пользователь может ознакомиться с результатами выполнения ранее созданных заданий ([6 Результаты сканирований](#)), создает отчеты ([7 Отчеты](#)). Результаты сканирований находятся во вкладке **История**. Сформированные отчеты находятся во вкладке **Отчеты**.

Ролевая модель RedCheck

Сегментная ролевая модель

BRedCheck позволяет разбивать инфраструктуру на непересекающиеся между собой сегменты. К каждому сегменту администратор (суперпользователь) привязывает пользователей RedCheck. Каждый пользователь может взаимодействовать с объектами только своего сегмента, а именно:

- группы;
- хосты;
- задания;
- отчеты;
- результаты сканирования.

После установки RedCheck создается сегмент по умолчанию (Default).

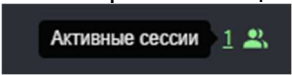
Разграничение прав доступа

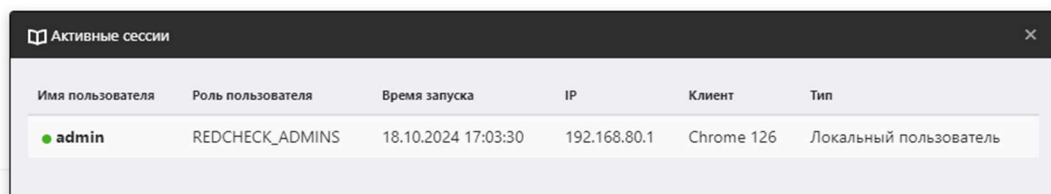
RedCheck для разграничения прав доступа использует ролевую модель. Роль пользователя в Системе определяется его принадлежностью к одной (или нескольким) из четырех групп RedCheck:

- **REDCHECK_ADMINS** – суперпользователь;
- **REDCHECK_ADMINIS** – администратор ИБ;
- **REDCHECK_SYSTEMS** – системный администратор;
- **REDCHECK_USERS** – пользователь ИБ.

Подробную информацию о возможностях каждой из ролей смотрите в [Руководстве администратора \(1.5 Ролевая модель RedCheck\)](#).

Просмотр активных сессий

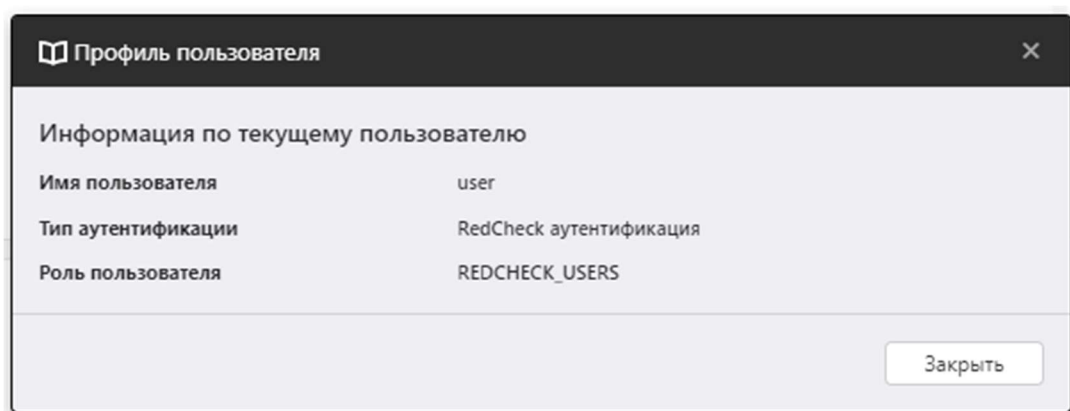
Для просмотра активных сессий (информация о пользователях, работающих с консолью управления на текущий момент) нажмите . В открывшемся окне будет информация: имя и роль пользователя; IP-адрес, с которого выполнен вход; клиент (браузер); время начала сессии; тип авторизации (Локальный пользователь).



Имя пользователя	Роль пользователя	Время запуска	IP	Клиент	Тип
admin	REDCHECK_ADMINS	18.10.2024 17:03:30	192.168.80.1	Chrome 126	Локальный пользователь

Просмотр информации о пользователе

Для просмотра информации о пользователе, под которым вы вошли в консоль управления, нажмите на имя пользователя.



Профиль пользователя

Информация по текущему пользователю

Имя пользователя	user
Тип аутентификации	RedCheck аутентификация
Роль пользователя	REDCHECK_USERS

Закрыть

Сведения об интегральной оценке по базовым метрикам CVSS

Обращаем внимание, что уровень критичности для уязвимости рассчитывается согласно CVSS из самого приоритетного источника. Порядок приоритетов:

- ALTEX-SOFT (экспертная оценка);
- Вендор продукта;
- BDU;
- NKCKI;
- NVD.

Возможно расхождение в уровне критичности, если уязвимость имеет CVSS из источника, более приоритетного, чем NVD. То-есть CVSS из NVD отличается от CVSS из более приоритетного источника настолько сильно, что числовые значения попадают в диапазоны разных уровней критичности.

Если уязвимость имеет статус риска **Недоступно**, но в какой-либо из вышеперечисленных баз уязвимостей есть значение CVSS, это означает, что вендор продукта не предоставил своей оценки уровня критичности для данного продукта.

1 Группы

Группа - это список хостов, которые являются ключевыми объектами для работы в RedCheck. При добавлении хостов в RedCheck обязательно указывается группа, поэтому при начале работы необходимо создать как минимум одну группу.

Группировка позволяет управлять сложной сетью, упрощая процесс работы в RedCheck.

Примеры использования группирования хостов

Ниже представлены самые распространенные варианты объединения хостов.

По платформе (ОС): Если в инфраструктуре сети находятся хосты с разными ОС, целесообразно будет сгруппировать их по этому признаку.

По установленным продуктам: В случае, когда для работы используется несколько серверов, например Nginx и IIS. Объединение хостов в соответствии с установленным на хосте сервером будет правильным решением.

По сетевому расположению: Хосты на предприятии могут находиться в разных подсетях. Полезно разделить их по данному критерию.

По подразделению управления: У каждого сотрудника отдела ИБ может быть своя зона ответственности, поэтому группировка хостов каждого сотрудника в отдельную группу является хорошей практикой.

Реализованный метод группировки **позволяет одному хосту входить в несколько групп**, но не подразумевает **вложенность групп одна в другую**.

Содержание

- [1.1 Создание группы](#)
- [1.2 Возможности группы](#)

1.1 Создание группы

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Чтобы создать пустую группу, выполните следующие шаги.

Шаг 1. Откройте **Инструменты** → **Создать группу**;

Шаг 2. Укажите имя группы и описание при необходимости → **Сохранить**;

Параметры группы хостов

Укажите требуемые параметры для новой или редактируемой группы хостов.

Имя

Описание

Выбранные хосты

ID	IP / DNS	Описание	CPE	
Нет данных для отображения				

Выбрано: 0

Так как в RedCheck хосты могут входить в несколько групп, то при создании новой группы есть возможность добавить в нее уже имеющиеся в других группах хосты.

Нажмите **Добавить хосты** → отметьте необходимые хосты → **Выбрать**;

1.2 Возможности группы

Для того, чтобы отредактировать ранее созданную группу, выполните следующие шаги.

Шаг 1. Перейдите в **Хосты**. Левая таблица будет содержать список групп. При нажатии на строку какой-либо группы в правой таблице появятся хосты, входящие в группу;

Шаг 2. Для редактирования группы выделите ее нажмите **Редактировать**.

Имя	Хосты
FreeBSD group	3
Huawei	1
vCenter	1
vmware	4

RedCheck позволяет изменить имя, описание и состав группы после ее создания.

ID	IP / DNS	Описание	CPE
1	192.168.1.4	1ē2ē12ē1	
2	192.168.1.6		
3	192.168.100.1		
4	192.168.100.2		
5	192.168.99.1		
6	192.168.99.2		
13	10.0.0.159		

Для просмотра результатов сканирования хостов, находящихся в выбранной группе, раскройте выпадающий список ... → **История** ([6 Результаты сканиваний](#))

Сканирования

Интервал

Все

Начало

Завершение

03.02.2025

Быстрый фильтр

Хост

some

Задание

Тип сканирования

Ссылки (CVE, проч.)

Статус

Сканирования

☒ Все

☐ Актуальные

Применить фильтр

№	Хост	Статус	Риск
1263	192.168.80.129	Завершено	
1259	192.168.80.38	Завершено	
1258	192.168.80.8	Завершено	
1256	192.168.80.38	Завершено	
1255	192.168.80.8	Завершено	
1253	192.168.80.129	Завершено	5 48 50 3
1249	192.168.80.38	Завершено	
1247	192.168.80.38	Завершено	
1245	192.168.80.129	Завершено	1 21 36
1244	192.168.80.129	Завершено	4 11 11
1243	192.168.80.129	Завершено	1 21 36
1242	192.168.80.129	Завершено	4 11 11
1238	192.168.80.129	Завершено	44 438 363 13 699
1237	192.168.80.129	Завершено	12
1236	192.168.80.129	Хост недоступен	
1235	192.168.80.129	Завершено	
1231	192.168.80.129	Завершено	
1230	192.168.80.129	Завершено	
1229	9.9.9.9	Хост недоступен	
1228	9.9.9.10	Хост недоступен	

Для проверки доступности к хостам, входящим в выбранную группу, нажмите **Проверка доступности**. Данная функция создаст задание типа **Проверка доступности** ([4.11 Проверка доступности](#)) и автоматически укажет выбранную группу (все входящие в нее хосты) как цель сканирования.

2 Хосты

Хост – объект сканирования RedCheck. Каждый хост в Системе входит в одну или несколько групп.

Перед добавлением хостов в Систему необходимо, чтобы была создана как минимум одна группа, в которой будут состоять новые хосты ([1.1 Создание группы](#)).

При удалении группы возможна ситуация, когда хосты, входящие в нее, перестают относиться к какой-либо группе. Для того, чтобы увидеть такие хосты, перейдите в **Хосты** → отметьте параметр **Показать хосты, не состоящие в группах** в свойствах фильтра. В правой таблице отобразятся хосты.

Способы добавления хостов

Добавить хосты в БД RedCheck можно несколькими способами:

- [2.1 Создание хостов вручную](#)
- [2.2 Импорт из CSV-файла](#)
- [2.3 Импорт из AD](#)
- [2.4 Импорт из Host Discovery](#)
- [2.5 Экспорт хостов в CSV](#)

Редактирование хоста

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Для того, чтобы изменить данные хоста, выполните следующие действия.

Шаг 1. Перейдите в **Хосты** → выберите группу, в которой находятся хосты → выберите хост → нажмите **Редактировать**;

Редактировать Удалить... ... Вид		Хосты Редактировать Удалить... ...	
Имя	Хосты	IP / DNS	
☐ FreeBSD group	3	☐	
☐ Huawei	1	☐	
☐ vCenter	1	☐ win-for-vcenter	
☐ vmware	4		
☐ usergate	4		

При редактировании хоста можно изменить описание и группы, в которые входит хост;

Параметры хоста

ID

5

UUID

Недоступно

Имя хоста

192.168.100.26

Дата модификации

14.11.2024 16:04:29

Описание

Some desc

Группы

Необходимо выбрать как минимум одну группу

☒ 100-сеть
☒ 80-сеть
☒ 10-сеть асу тп

Сохранить

Заккрыть

Шаг 2. Внесите изменения → **Сохранить**.

Просмотр результатов сканирования

Для просмотра результатов сканирования хоста нажмите ... → **История** ([6 Результаты сканирований](#))

Сканирования

Интервал
Все

Начало

Завершение
03.02.2025

Быстрый фильтр

192.168.80.129

Группа

Задание

Тип сканирования

Ссылки (CVE, проч.)

Статус

Сканирования

☒ Все

☐ Актуальные

Применить фильтр

№	Хост	Статус	Риск	К	Задание
1263	192.168.80.129	Завершено			1_23
1253	192.168.80.129	Завершено	5 48 50 3		1_18
1245	192.168.80.129	Завершено	1 21 36		1_12
1244	192.168.80.129	Завершено	4 11 11		1_12
1243	192.168.80.129	Завершено	1 21 36		1_12
1242	192.168.80.129	Завершено	4 11 11		1_12
1238	192.168.80.129	Завершено	44 438 363 13 699		vuln
1237	192.168.80.129	Завершено	12		postgres
1236	192.168.80.129	Хост недоступен			postgres
1235	192.168.80.129	Завершено			проверк
1231	192.168.80.129	Завершено			1_22
1230	192.168.80.129	Завершено			аудит
1203	192.168.80.129	Хост недоступен			postgres
1202	192.168.80.129	Хост недоступен			winrm
1199	192.168.80.129	Завершено	44 434 352 13 4		1_21 - t
1198	192.168.80.129	Завершено	44 434 352 13 4		1_21 - t
1197	192.168.80.129	Завершено	44 434 352 13 4		1_21 - t
1195	192.168.80.129	Завершено	44 434 352 13 4		1_21 - t
1193	192.168.80.129	Завершено	44 434 352 13 4		1_21
1191	192.168.80.129	Завершено	44 434 352 13 4		1_21 - t

Для проверки доступности хоста нажмите **Проверка доступности**. Данная функция создаст задание типа **Проверка доступности** ([4.11 Проверка доступности](#)) и автоматически укажет выбранный хост как цель сканирования.

Удаление хостов

Отметьте в таблице хосты, подлежащие удалению, и нажмите **Удалить**. Запустится операция удаления хостов. Статус удаления можно посмотреть в перечне фоновых задач. Нажмите **Инструменты** → **Фоновые задачи**.

Фоновые задачи					
Запрос	Хосты	Статус	Пользователь	Дата создания	Команды
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:27	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:27	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:27	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Удаление хостов и связанных данных	1	Завершено	admin	04.07.2025, 20:48:26	⚙️
Всего: 101					
			Обновить Закрыть		

2.1 Создание хостов вручную

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Для создания хостов выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Создать хост**;

Шаг 2. Заполните форму → **Сохранить**.

- Хосты – можно указывать IP-адреса, DNS-имена, диапазоны IP-адресов и маски подсети;
- Группы – группы, в которые будут входить добавляемые хосты;

Если среди указанных хостов есть уже существующие в RedCheck, то:

- Описание таких хостов будет обновлено на указанное, если на момент изменения оно было у хоста пустым. Если у существующего хоста уже есть описание, оно обновлено не будет;
- Существующие хосты будут добавлены в указанные группы, если ранее в них не состояли.

Создание хостов

Хосты
DNS-имена или IP-адреса, включая диапазоны и маски.
Например:
server2016, server-2016.domain, 192.168.1.1, 192.168.1.250-192.168.2.10, 192.168.1.1/25

Описание
Указывается по желанию

Группы
Необходимо выбрать как минимум одну группу

☐ 100-сеть
☐ 80-сеть
☐ 10-сеть асу тп

Создать хостыЗаккрыть

При успешном создании хостов будет выведена дополнительная информация:

Создано новых хостов: **1**
Существующих хостов добавлено в новые группы: **1**
Существующим хостам обновлено описание: **1**

Перед добавлением хостов в Систему необходимо, чтобы была создана как минимум одна группа, в которой будут состоять новые хосты ([1.1 Создание группы](#)).

2.2 Импорт из CSV-файла

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

Формат csv – это текстовый файл с разделителями. В первой строке через разделитель «,» указываются названия столбцов. Последующие строки являются записями с информацией о хостах. Значения в строке также указываются через разделитель «,».

Структура csv-файла

Базовая структура csv-файла для импорта хостов в RedCheck должна соответствовать:

Group	GroupDesc	Host	HostDesc	CPE	Action
Название группы	Описание группы	Имя/адрес хоста	Описание хоста	Конфигурация устройства	Определяет действие, выполняемое над хостом Принимает значение Delete

В случае отсутствия первой строки-заголовка информация о хостах будет обрабатываться в соответствии с вышеуказанной структурой столбцов.

Базовая структура может быть переопределена. Например, при заголовке **Group,Host** в строке с информацией о хосте достаточно указать только название группы и имя/адрес хоста.

Файл должен иметь кодировку UTF-8, чтобы избежать проблем с импортом русскоязычных символов.

Сценарии использования

Структура (Group;Host). Создается группа G1 без описания, в которую добавляются хосты H1, H2, H3 без описания, CPE опускается, параметр Action пустой, так как ничего не удаляется.

Код

```
Group,Host  
G1,H1  
G1,H2  
G1,H3
```

Структура (Group;Host;Action). Хосты удаляются из группы G1 и становятся непривязанными к какой-либо группе.

Код

```
Group,Host,Action  
G1,H1,Delete  
G1,H2,Delete  
G1,H3,Delete
```

Структура (Group;Action). Будут удалены все группы, а привязанные хосты станут непривязанными к какой-либо группе.

Код

```
Group,Action  
*,Delete
```

Структура (Group;Host;Action). Хосты удаляются из RedCheck. Также будут удалены все результаты сканирования для этих хостов.

Код

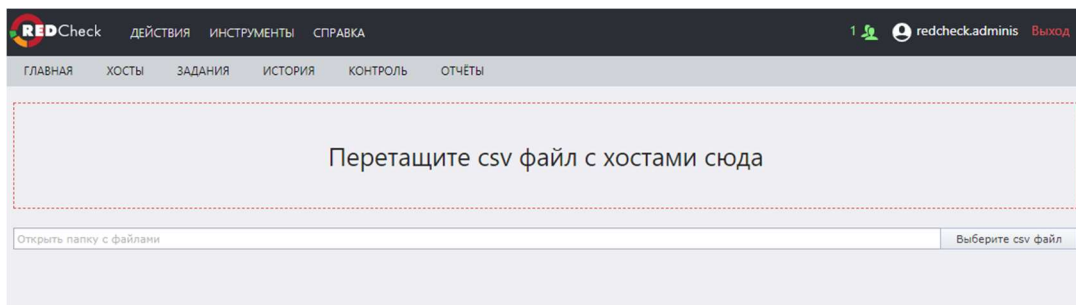
```
Group,Host,Action  
,H1,Delete  
,H2,Delete  
,H3,Delete
```

Импортирование csv-файла

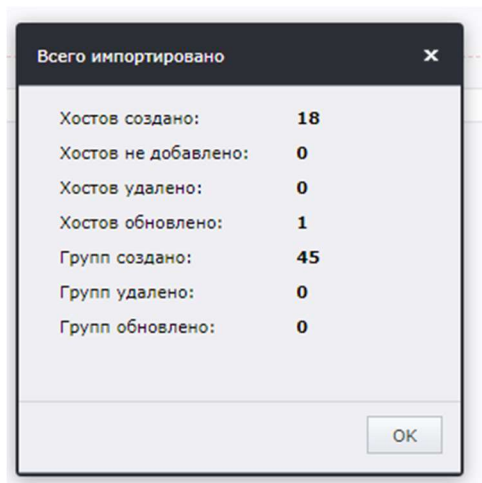
Для добавления хостов с помощью csv-файла выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт хостов** → **Csv file**;

Шаг 2. Перетащите csv-файл в поле или нажмите **Выберите csv файл**;



После завершения импорта появится уведомление с результатом операции.



2.3 Импорт из AD

Для автоматического импорта хостов из Active Directory по расписанию рекомендуется использовать утилиту RedCheck Import AD ([Руководство по импорту хостов из Active Directory в RedCheck](#)).

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Systems

RedCheck предоставляет возможность вручную импортировать хосты, находящиеся в домене. Для этого выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт хостов** → **Active Directory**;

Шаг 2. Заполните форму для поиска → **Искать хосты**;

- Тип протокола – ActiveDirectory, ALD, FreeIPA;
- Адрес контроллера домена – хост контроллера домена, имеющийся в RedCheck, или указанный самостоятельно адрес хоста;
- Профиль – учетная запись RedCheck любого пользователя домена ([создание учетных записей для сканирования](#));
- Группа – группа, в которую будут добавлены импортированные хосты;
- AD путь – путь к хостам в Active Directory (опционально);
- Фильтр – критерий, по которому происходит поиск. Рекомендуется оставить значение по умолчанию;
- Импортировать:
 - Хост – будет импортировано FQDN или IP-адрес хоста;
 - Полное имя хоста – будет импортировано DNS-имя хоста.

Импорт хостов из Active Directory/LDAP

Укажите IP-адрес или DNS-имя контроллера домена, тип протокола, выберите учётную запись, укажите фильтр и получите хосты. Затем выберите необходимые хосты и добавьте их в общий список.

Тип протокола

ActiveDirectory

Адрес контроллера домена

Учетная запись

Группа

AD путь

Фильтр

(&(objectCategory=computer))

Импортировать

Хост

☒ Искать только первые 1000 хостов

Искать хосты

Шаг 3. Отметьте необходимые хосты → Импортировать;

☐	Хост	Полное имя хоста	Операционная система
☐	CL-01	CL-01.STAND.LAB	Windows 7 Корпоративная
☐	DC-01	dc-01.STAND.LAB	Windows Server 2016 Standard
☐	RC-01	rc-01.STAND.LAB	Windows Server 2019 Standard
☐	SQL-01	sql-01.STAND.LAB	Windows Server 2016 Standard
☐	WEB-01	web-01.STAND.LAB	Windows Server 2019 Standard

20 Page 1 of 1 (5 items) 1 Всего

Импортировать

Если хост уже существует в RedCheck, он будет добавлен в указанную группу, если ранее в ней не состоял

Если импорт прошел успешно, появится уведомление с информацией:



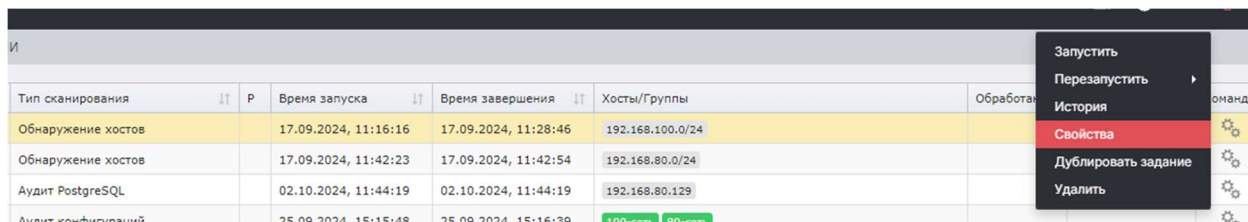
Новых хостов было импортировано: **1**

Существующих хостов добавлено в новые группы: **1**

2.4 Импорт из Host Discovery

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Шаг 1. Перейдите в свойства задания типа Обнаружение хостов, нажав  → **Свойства**;



Тип сканирования	П	Время запуска	Время завершения	Хосты/Группы	Обработка	Команды
Обнаружение хостов		17.09.2024, 11:16:16	17.09.2024, 11:28:46	192.168.100.0/24		
Обнаружение хостов		17.09.2024, 11:42:23	17.09.2024, 11:42:54	192.168.80.0/24		
Аудит PostgreSQL		02.10.2024, 11:44:19	02.10.2024, 11:44:19	192.168.80.129		
Аудит конфигураций		25.09.2024, 15:15:48	25.09.2024, 15:16:39	100-сеть 80-сеть		

Запустить

Перезапустить

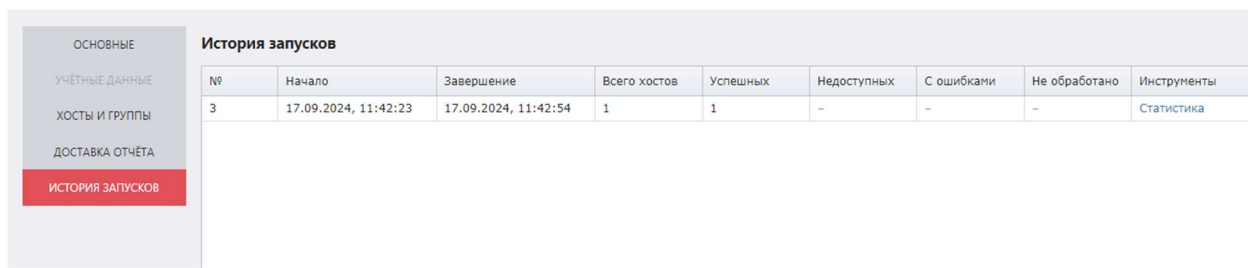
История

Свойства

Дублировать задание

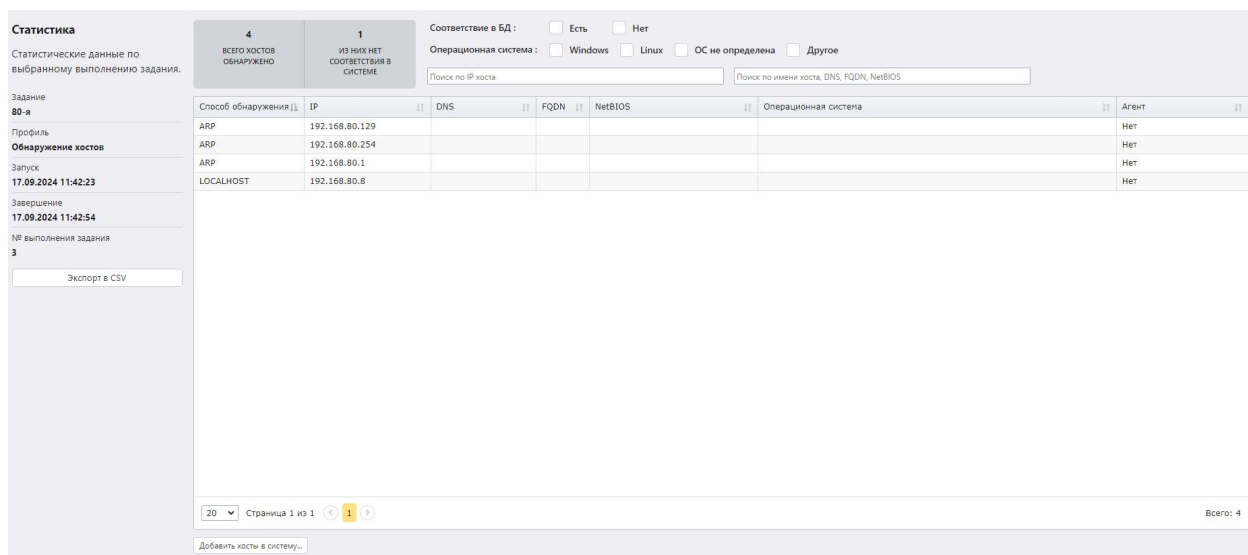
Удалить

Шаг 2. Перейдите во вкладку **История запусков** → нажмите **Статистика** напротив нужного завершённого сканирования;



№	Начало	Завершение	Всего хостов	Успешных	Недоступных	С ошибками	Не обработано	Инструменты
3	17.09.2024, 11:42:23	17.09.2024, 11:42:54	1	1	–	–	–	Статистика

В появившемся окне можно просмотреть все найденные хосты и доступную для них информацию.



Статистика

Статистические данные по выбранному выполнению задания.

Задание: 80-я

Профиль: Обнаружение хостов

Запуск: 17.09.2024 11:42:23

Завершение: 17.09.2024 11:42:54

№ выполнения задания: 3

Экспорт в CSV

4

1

Соответствие в БД: ☐ Есть ☐ Нет

Операционная система: ☐ Windows ☐ Linux ☐ ОС не определена ☐ Другое

Поиск по IP хоста

Поиск по имени хоста, DNS, FQDN, NetBIOS

Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Агент
ARP	192.168.80.129					Нет
ARP	192.168.80.254					Нет
ARP	192.168.80.1					Нет
LOCALHOST	192.168.80.8					Нет

20

Страница 1 из 1

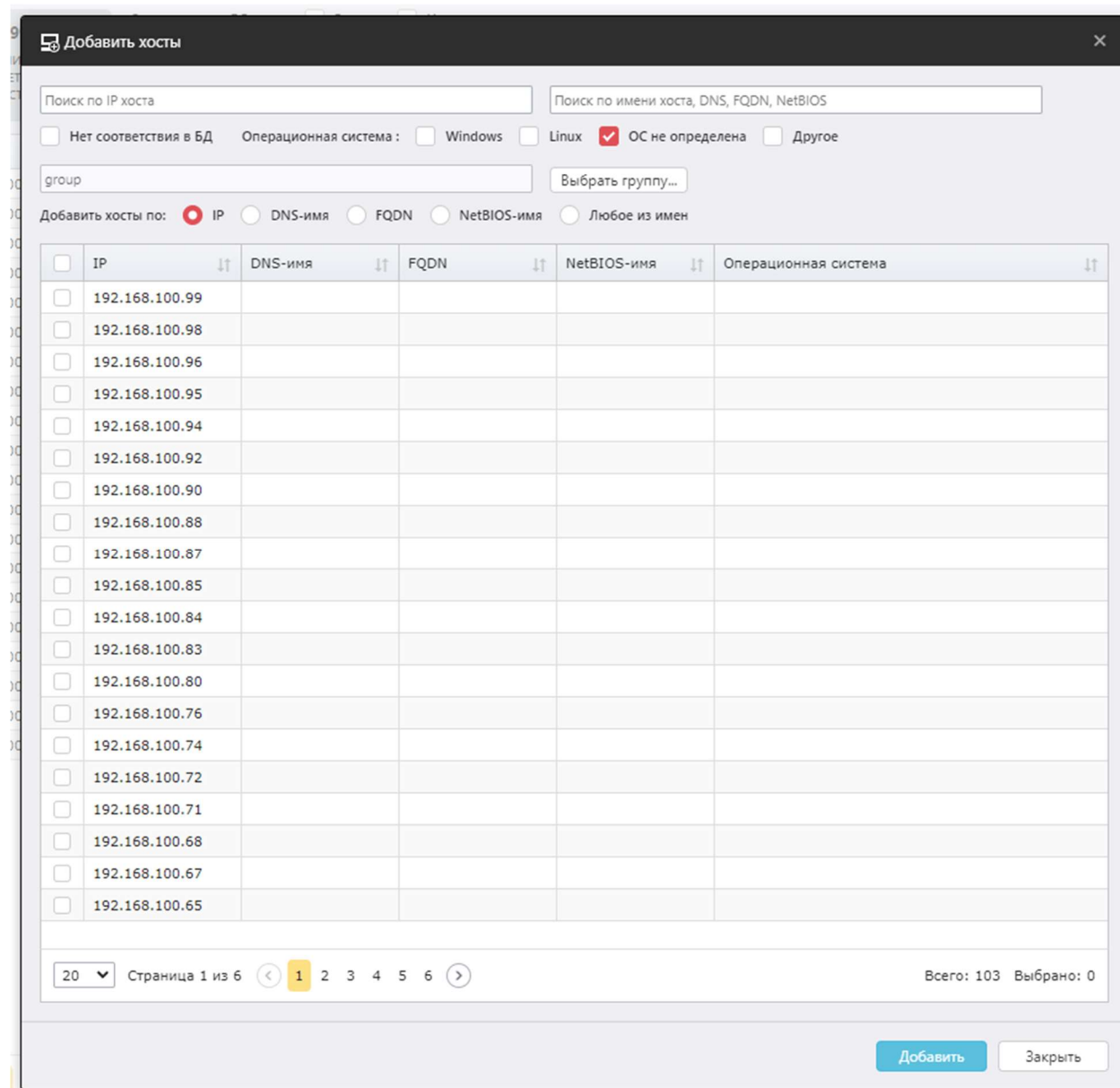
1

Всего: 4

Добавить хосты в систему...

Шаг 3. Нажмите **Добавить хосты в систему** → в появившемся окне отметьте хосты, которые хотите добавить в БД → выберите группу, в которую будут добавлены хосты, нажав **Выбрать группу** → выберите что именно будет

добавлено (IP, DNS, FQDN или NetBIOS), нажав на соответствующий radio-button → нажмите **Добавить**;



Добавить хосты

Поиск по IP хоста

Поиск по имени хоста, DNS, FQDN, NetBIOS

☐ Нет соответствия в БД

Операционная система : ☐ Windows ☐ Linux ☒ ОС не определена ☐ Другое

group

Выбрать группу...

Добавить хосты по: ☒ IP ☐ DNS-имя ☐ FQDN ☐ NetBIOS-имя ☐ Любое из имен

☐	IP	DNS-имя	FQDN	NetBIOS-имя	Операционная система
☐	192.168.100.99				
☐	192.168.100.98				
☐	192.168.100.96				
☐	192.168.100.95				
☐	192.168.100.94				
☐	192.168.100.92				
☐	192.168.100.90				
☐	192.168.100.88				
☐	192.168.100.87				
☐	192.168.100.85				
☐	192.168.100.84				
☐	192.168.100.83				
☐	192.168.100.80				
☐	192.168.100.76				
☐	192.168.100.74				
☐	192.168.100.72				
☐	192.168.100.71				
☐	192.168.100.68				
☐	192.168.100.67				
☐	192.168.100.65				

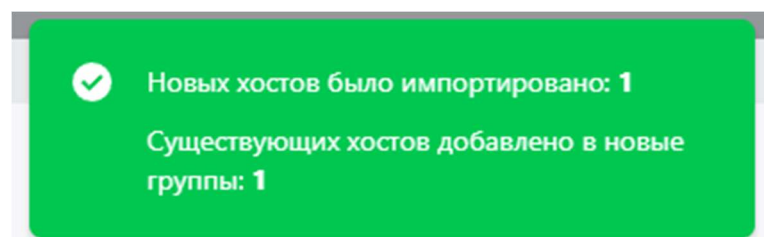
20 Страница 1 из 6 1 2 3 4 5 6

Всего: 103 Выбрано: 0

Добавить Закрыть

Если хост уже существует в RedCheck, он будет добавлен в указанную группу, если ранее в ней не состоял

Если импорт прошел успешно, появится уведомление с информацией:



2.5 Экспорт хостов в CSV

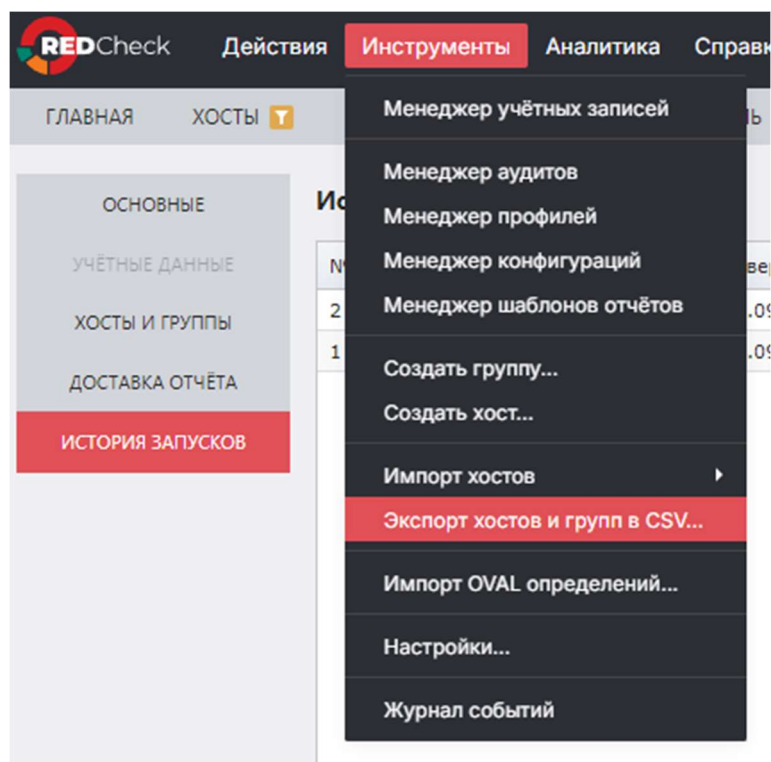
RedCheck позволяет экспортировать имеющуюся в базе данных инфраструктуру в CSV-файл. Получающийся файл можно [импортировать](#) в RedCheck.

Структура csv-файла

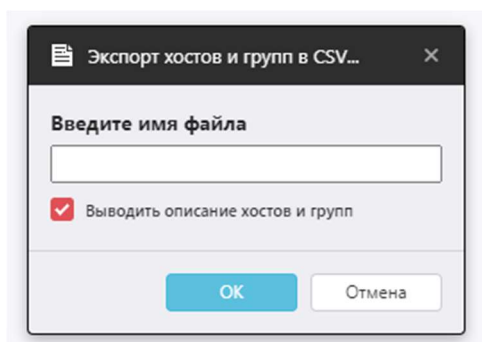
Group	GroupDesc	Host	HostDesc	CPE
Название группы	Описание группы	Имя/адрес хоста	Описание хоста	Конфигурация устройства

Базовая структура может быть переопределена. ([2.2 Импорт из CSV-файла](#)).

Шаг 1. Раскройте **Инструменты** → **Экспорт хостов и групп в CSV**;



Шаг 2. Введите имя файла → отметьте по необходимости опцию **Выводить описание хостов и групп** → **ОК**.



После нажатия **ОК** начнется скачивание файла.

3 Учетные записи для сканирования

Учетная запись – объект RedCheck, необходимый для доступа к хостам во время выполнения сканирования. Учетная запись состоит из данных для подключения к сканируемому хосту (учетные данные пользователя, порты для протоколов доступа), настроек привилегий и других параметров. Управление учетными записями для сканирования производится через Менеджер учетных записей ([3.1 Менеджер учетных записей](#))

Задания Аудит в режиме Пентест, Обнаружение хостов и Аудит АСУ ТП не требуют создания учетных записей для сканирования.

RedCheck позволяет сканировать следующие платформы:

- Windows;
- Linux-системы;
- Сетевое оборудование;
- Системы виртуализации и контейнеризации;
- СУБД;
- Контролеры и протоколы АСУ ТП.

В Системе реализовано два режима доступа к сканируемому хосту:

- Режим черного ящика – сетевое сканирование без привилегий;
- Режим белого ящика:
 - сканирование с использованием непривилегированной учетной записи и агента сканирования RedCheck;
 - сканирование с использованием привилегированной учетной записи без использования агента сканирования;

С подробным перечнем платформ и доступных для них режимов сканирования можно ознакомиться в [Руководстве администратора \(1.9 Перечень поддерживаемых платформ\)](#).

Типы учетных записей

RedCheck предлагает следующие типы учетных записей для соответствующих платформ:

- Windows;
- SSH;

- SQL:
 - Microsoft SQL Server;
 - MySQL;
 - Oracle;
 - PostgreSQL;
- Cisco:
 - Cisco IOS;
 - Cisco NX-OS;
- Huawei VRP;
- VMware:
 - VMware ESXi;
 - VMware vCenter;
 - VMware NSX;
- Solaris;
- FreeBSD;
- Eltex серии ESR / MES
- Check Point (GAiA);
- Fortinet FortiOS;
- UserGate NGFW.

3.1 Менеджер учетных записей

Создание учетной записи для сканирования

Необходимая роль: RedCheck_Admins / RedCheck_Systems

Для создания учетной записи выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Менеджер учетных записей** → **Добавить учетные данные**;

Менеджер учётных записей							
ID	Тип	Подтип	Имя профиля	Дата создания	Дата модификации	X	Команды
> 1	Windows		windows	29.11.2022, 16:03:01	23.01.2023, 10:04:59		⚙
> 2	Sql	MsSql	ms	05.12.2022, 13:47:10	05.12.2022, 13:47:10		⚙
> 3	Linux		linux	05.12.2022, 17:05:22	27.01.2023, 12:38:59	🖨	⚙
> 4	Cisco	Ios	cisco-ios	07.12.2022, 09:59:50	07.12.2022, 09:59:50		⚙
> 5	Cisco	Nxos	cisco-nxos	07.12.2022, 11:19:43	07.12.2022, 11:19:43		⚙
> 6	Huawei		huawei	07.12.2022, 11:54:18	07.12.2022, 11:54:18		⚙
> 7	VMware	ESXi	vm-esxi	07.12.2022, 11:55:15	07.12.2022, 11:55:15		⚙
> 8	VMware	vCenter	vm-vcenter	07.12.2022, 16:09:11	07.12.2022, 16:09:11		⚙
> 9	VMware	Nsx	vm-nsx	07.12.2022, 16:29:09	07.12.2022, 16:29:09		⚙
> 10	Solaris		solaris	07.12.2022, 17:23:47	07.12.2022, 17:23:47		⚙
> 11	FreeBsd		freebsd	07.12.2022, 17:24:54	07.12.2022, 17:24:54		⚙

20 Page 1 of 2 (25 items) < 1 2 > Всего: 25

Добавить учётные данные ...

Шаг 2. Укажите имя и выберите тип учетной записи → заполните необходимые параметры для выбранного типа учетной записи → **Сохранить**.

Значения, находящиеся в неактивных полях, могут быть изменены при выборе соответствующего режима сканирования. Например, активация поля **Указать SSH порт** откроет доступ для изменения порта.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	some
Тип учётной записи	Windows
Имя пользователя	
Пароль	
Подтверждение пароля	
Домен	
	☐ Указать WinRM порт
WinRM порт	5985
	☐ WinRM через HTTPS
	☐ Указать порт RedCheck Agent
Порт RedCheck Agent	8732
	☐ Указать порт RedCheck Update Agent
Порт RedCheck Update Agent	8733

Для того, чтобы быстро создать копию уже существующей учетной записи, в Менеджере учетных записей нажмите  → **Дублировать**;

Редактирование учетной записи

Необходимая роль: RedCheck_Admins / RedCheck_Systems

RedCheck предоставляет возможность изменить имя, параметры доступа и привилегий. Нажмите **Инструменты** → **Менеджер учетных записей** →  → **Редактировать**;

Чтобы быстро сменить имя учетной записи, в Менеджере учетных записей нажмите  → **Переименовать** → введите новое имя → **Переименовать**;

Редактирование учётной записи

Имя профиля:

Переименовать

3.2 Подбор учетных записей для сканирования

При создании задания можно указать несколько учетных записей, которые будут использоваться для сканирования. В процессе выполнения задания служба сканирования будет последовательно пробовать пройти аутентификацию на хосте с помощью каждой учетной записи. Перебор будет происходить до первой удачной аутентификации. Хост считается недоступным, если ни одна из учетных записей не подошла.

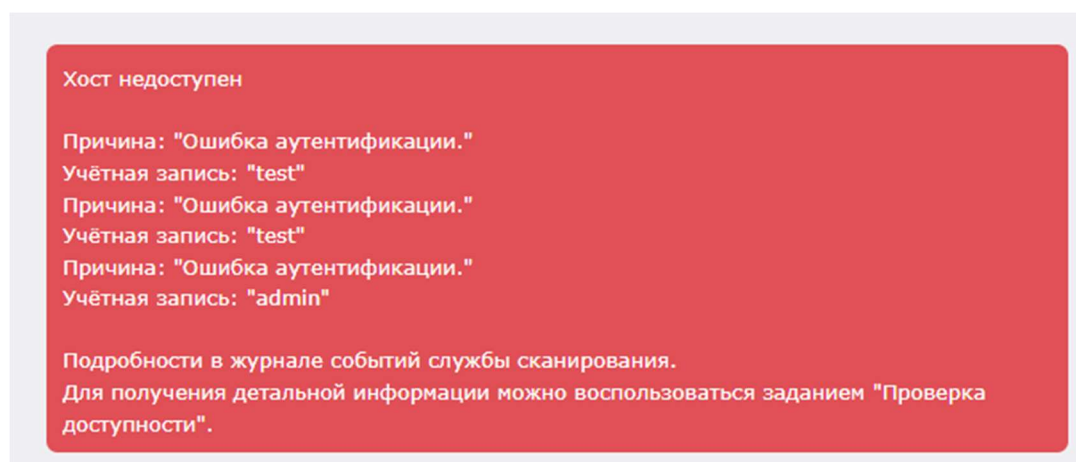
Задания, для которых реализован данный функционал:

- Аудит уязвимостей / обновлений
- Аудит конфигураций
- Инвентаризация
- Аудит СУБД

Порядок проверки учетной записи. При создании и редактировании задания можно задавать порядок учетных записей, согласно которому служба сканирования будет проверять учетные данные во время аутентификации на хосте. Чтобы изменить порядок, перетащите строку на нужное место в таблице, используя  рядом с именем учетной записи.

Удаление из списка. Для удаления учетной записи из списка нажмите  → **Удалить**.

Результаты сканирования. В случае, если служба сканирования не смогла пройти аутентификацию ни одной из указанных учетных записей, будет создан результат сканирования со статусом Хост недоступен, где будут перечислены логины учетных записей, не прошедших аутентификацию.



В результате сканирования со статусом Завершено / Ошибка не отображается учетная запись, прошедшая аутентификацию.

Ограничения

Нельзя указывать две и более учетные записи с одинаковыми логинами и протоколами, используемыми во время сканирования.

Некоторые типы учетных записей используют один и тот же протокол для сканирования. Например, SSH, FreeBSD, Solaris, Cisco и еще несколько типов используют SSH протокол. Такие учетные записи не могут быть добавлены в одно и то же задание в случае, если у них один и тот же логин для аутентификации.

На добавление в задание нескольких учетных записей одного типа и с одинаковыми логинами, но разными паролями, ограничений нет.

Например:

1. Учетные записи с типом Windows, «server 2012» с логином test и «server 2019» с логином test, но с другим паролем, **МОГУТ** быть добавлены в одно задание;
2. SSH учетная запись «astra server» с логином test и FreeBSD учетная запись «freebsd server» с логином test **НЕ МОГУТ** быть добавлены в одно задание.

Особенности

Аудит конфигураций. Список доступных для выбора конфигураций будет составлен согласно выбранным типам учетных записей. Например, если указаны две учетные записи Windows и SSH, то выбрать можно будет как Unix, так и Windows конфигурации.

Инвентаризация. В случае, если для задания указаны учетные записи разных типов, профиль инвентаризации будет установлен как Мультиплатформенный, т.е. для каждого хоста будет применен подходящий профиль с включением всех возможных параметров, но детализировать профиль (добавить или исключить параметры) будет нельзя.

Параметры инвентаризации

Укажите профиль инвентаризации

Профиль Мультиплатформенный

[Выбрать все](#) [Сбросить все](#)

- ☒ Аппаратное обеспечение
- ☒ Программное обеспечение
- ☒ OVAL-Инвентаризация

4 Задания для сканирования

RedCheck предоставляет 10 различных типов задания:

- [4.1 Аудит уязвимостей](#)
- [4.2 Аудит обновлений](#)
- [4.3 Аудит конфигураций](#)
- [4.4 Инвентаризация](#)
- [4.5 Фиксация \(контроль целостности\)](#)
- [4.6 Аудит уязвимостей АСУ ТП](#)
- [4.7 Проверка доступности](#)
- [4.8 Обнаружение хостов](#)
- [4.9 Аудит в режиме "Пентест"](#)
- [4.10 Аудит уязвимостей Docker / Инвентаризация Docker](#)
- [4.11 Сканирование YARA правил](#)
- [4.12 Настройка расписания для задания](#)
- [4.13 Повторный перезапуск недоступных хостов во время сканирования](#)

Запуск задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы просмотреть список заданий, перейдите в **Задания** → нажмите  → **Запустить**;

Для сортировки заданий воспользуйтесь фильтром:

Задания

Создание заданий сканирования и управление ими.

Период создания
Все

Создано с

Создано по
30 января, 2023

Задание

...

Хост

...

Тип сканирования

Тип запуска

Статус

Применить фильтр

Остановка задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для остановки задания нажмите  → **Остановить**;

Остановка задания подразумевает завершение сканирования без возможности запуска с точки остановки.

Приостановка и возобновление задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для приостановки выполнения задания нажмите  → **Приостановить**;

Приостановка задания позволяет:

- Возобновить выполнение задания с точки приостановки (текущие сканирования хостов будут закончены);

- Посмотреть результаты уже отсканированных хостов;
- Создать отчет по уже отсканированным хостам.

Для возобновления задания нажмите  → **Запустить**;

Перезапуск задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для перезапуска задания нажмите  → **Перезапустить** → выберите один из вариантов:

- Все – будет выполнено сканирование всех хостов, указанных в задании на момент перезапуска;
- Кроме успешных (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом, отличным от **Завершено**;
- Только ошибочные (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом **Ошибка**;
- Только недоступные (последний запуск) – будет выполнено сканирование хостов, указанных в задании на момент перезапуска, которые при последнем выполнении задания завершились со статусом **Хост недоступен**;

Редактирование задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Нажмите  → **Свойства**;

- Основные – возможность изменить имя, тип запуска, транспорт и другую информацию;

ОСНОВНЫЕ

УЧЁТНЫЕ ДАННЫЕ

ХОСТЫ И ГРУППЫ

ДОСТАВКА ОТЧЁТА

ИСТОРИЯ ЗАПУСКОВ

Свойства задания и входные данные

ID

104

UID

3d84f2d7-8a83-4e4f-8ac9-01fa0d6c5c4b

Тип

Аудит уязвимостей

Дата создания

23.10.2024 11:31:07

Имя

1_26

Описание

Запуск

По требованию

Служба сканирования

Тип сканирования

Полное

☐ Повторно запускать неуспешные хосты
 ☐ Ограничить максимальное время выполнения задания
 ☐ Оповещать по e-mail
 ☐ Расширенная идентификация хоста
 ☐ Сохранять файл результатов
 ☐ Сохранять файл системных характеристик
 ☐ Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации

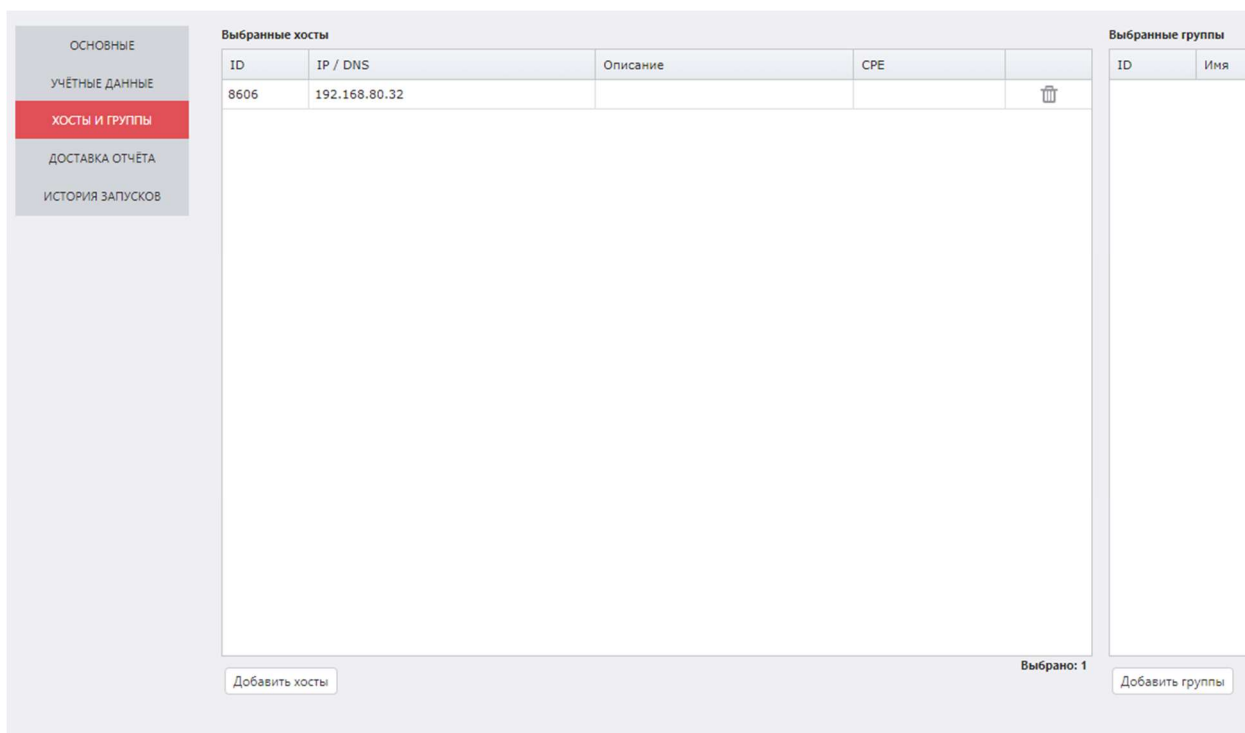
Сохранить

Отмена

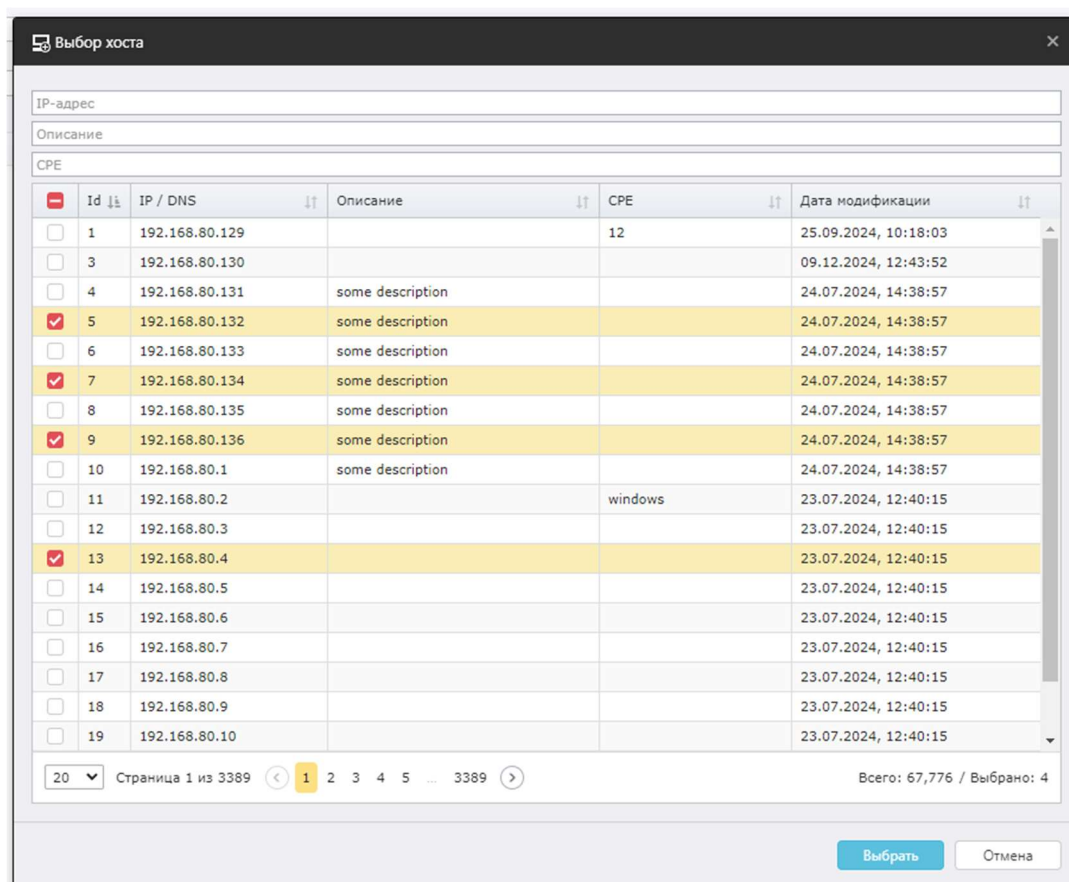
Контент

Авто

- Учетные данные – возможность изменить список учетных записей для сканирования ([3.2 Подбор учетных записей для сканирования](#));
- Хосты и группы – возможность изменить список сканируемых хостов и групп;



Чтобы удалить хост или группу, нажмите . Чтобы добавить хост или группу, нажмите **Добавить хосты / Добавить группы** → отметьте необходимые хосты → **Выбрать**.



Нажмите **Сохранить** для внесения изменений.

- Конфигурации – возможность изменить список конфигураций и профилей для задания. Доступно для Аудита конфигураций.

Конфигурации

Фильтр по платформам... Фильтр по продуктам...

Поиск конфигураций

Имя

- ☐ Ubuntu - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ SUSE Linux Enterprise / openSUSE - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ SAP HANA - Общие настройки безопасности СУБД - АЛТЭК-СОФТ
- ☐ ROSA Linux - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ RED OS - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Red Hat Enterprise Linux / CentOS / Oracle Linux / AlmaLinux - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Red Hat Enterprise Linux / CentOS / Oracle Linux / AlmaLinux - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Red Hat Enterprise Linux / CentOS / Oracle Linux - Оценка соответствия стандарту версии 3.2.1 - PCI DSS
- ☐ PHP - Аудит безопасности - АЛТЭК-СОФТ
- ☐ Photon OS - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ nginx - Аудит безопасности - АЛТЭК-СОФТ
- ☐ Linux - Рекомендации по безопасной настройке - ИД ФСТЭК России от 25.12.2022
- ☐ Kubernetes - Общие настройки безопасности отдельного рабочего узла - CIS
- ☐ Kubernetes - Общие настройки безопасности главного узла - CIS
- ☐ Docker - Аудит безопасности платформы контейнеризации - CIS
- ☐ Debian - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Debian - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Astra Linux SE и CE / ALT / RED OS 7.3 - Оценка соответствия стандарту - ГОСТ Р 57580.1-2017
- ☐ Astra Linux SE и CE / ALT / RED OS 7.3 - Аудит безопасности критической информационной инфраструктуры - ФСТЭК №239
- ☐ Astra Linux SE и CE / ALT / RED OS 7.3 - Аудит безопасности АСУ ТП - ФСТЭК №31
- ☒ Astra Linux SE и CE - Общие настройки безопасности - АЛТЭК-СОФТ
- ☐ Astra Linux SE 1.7 - Настройки по руководству Red Book - РусБИТех
- ☐ Astra Linux SE 1.6 - Настройки по руководству Red Book - РусБИТех

Всего: 27 Выбрано: 1

Astra Linux SE и CE - Общие настройки безопасности - АЛТЭК-СОФТ

- ☒ Профиль по умолчанию
- ☐ Astra Linux SE и CE - Общие настройки безопасности - АЛТЭК-СОФТ

☐ Сканировать все профили

☒ Пропускать непримененные конфигурации

Чтобы добавить или убрать конфигурацию / профиль конфигурации, отметьте или снимите отметку с конфигурации / профиля → **Сохранить**.

- Доставка отчета – возможность назначить шаблоны для отчетов и адреса для их доставки;

ОСНОВНЫЕ

УЧЁТНЫЕ ДАННЫЕ

ХОСТЫ И ГРУППЫ

КОНФИГУРАЦИИ

ДОСТАВКА ОТЧЁТА

ИСТОРИЯ ЗАПУСКОВ

Доставка отчёта

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя
Нет данных для отображе...	

20

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	Путь
Нет данных для отображе...		

20

Добавить адрес доставки...

Чтобы указать шаблон отчета ([7.3 Шаблоны отчетов](#)), нажмите **Добавить шаблон отчета** → выберите шаблон отчета → **Выбрать**.

Чтобы указать адрес доставки, выберите добавленный шаблон отчета и нажмите **Добавить адрес доставки** → выберите адрес доставки → **Выбрать**.

Для внесения изменений нажмите **Сохранить**.

- История запусков – история сканирований и статистика по каждому из них.

ОСНОВНЫЕ	История запусков							
УЧЁТНЫЕ ДАННЫЕ	№	Начало	Завершение	Всего хостов	Успешных	Недоступных	С ошибками	Не обработано
ХОСТЫ И ГРУППЫ	109	14.10.2024, 16:25:04	14.10.2024, 16:25:49	2	2	–	–	–
КОНФИГУРАЦИИ	103	09.10.2024, 11:08:13	09.10.2024, 11:08:22	1	1	–	–	–
ДОСТАВКА ОТЧЁТА								
ИСТОРИЯ ЗАПУСКОВ								

Статистика актуальна для следующих типов заданий:

- Аудит в режиме «Пентест»;
- Обнаружение хостов;
- Проверка доступности

4.1 Аудит уязвимостей

RedCheck выполняет централизованное сетевое или локальное сканирование хостов на наличие уязвимостей ОС, общесистемного и прикладного ПО, а также сетевого оборудования. Во время сканирования сопоставляется состояние параметров системы сигнатурам уязвимостей, содержащихся в открытом Репозитории OVALdb и описанных в формате SCAP.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит уязвимостей**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был

проверен во время сканирования (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);

- Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации – при включенном параметре служба сканирования сохраняет в БД информацию о всех уязвимостях, которые были проверены во время сканирования, даже если они не были обнаружены. При выключенном параметре сохраняются только обнаруженные уязвимости. Выключенный параметр экономит место в БД;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Аудит уязвимостей

Служба сканирования

debian12_local

Запуск

По требованию

Расширенный лог

☒ Запустить сразу после закрытия мастера

☐ Повторно запускать неуспешные хосты

☐ Сохранять файл результатов

☐ Сохранять файл системных характеристик

☐ Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации

Дополнительно

☐ Оповещать по e-mail

☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	☒ Безагент
5	UserGate		http	☒ Безагент
10	Windows		windows	☒ С использованием агента ☐ Безагент WinRM

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

[Подробнее про подбор учетных записей](#)

Шаг 5. Выберите профиль и тип сканирования → **Вперед**:

- Быстрое – не будут применяться рекурсивные сигнатуры. Сканирование выполнится быстрее.
- Полное – при сканировании будут использоваться глубокие (рекурсивные) сигнатуры, являющиеся трудоемкими. Аудит займет больше времени;
- Полное с дополнительным сканированием JAR-файлов – при сканировании будут использоваться дополнительные сигнатуры для проверки jar-файлов. Аудит займет больше времени. Только для сканирования Linux-платформ;

Настройки Группы и хосты Учётные данные **Профили сканирования**

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили

☒ Без профилей
☐ Выбранные вручную

☐ динамик (Ulx)
 Динамический профиль
☒ статик (Ulx)
 Статический профиль

Тип сканирования

☐ Быстрое
☐ Полное
☒ Полное с дополнительным сканированием JAR-файлов

Укажите каталоги поиска jar файлов для следующих учётных записей: [Ssh].
 Задание корневых каталогов может привести к существенному увеличению времени сканирования.

Каталог

Каталог	ИИ	
/var/lib		

Всего: 1

О создании профилей сканирования смотрите в [5.1 Профили сканирования](#).

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки Группы и хосты Учётные данные Профили сканирования **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ИИ	Имя	Тип данных	Команды
Нет данных для отображения				

20 ▾ Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ИИ	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20 ▾ Всего: 0

Добавить адрес доставки...

Назад Вперед Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.2 Аудит обновлений

RedCheck позволяет обнаружить неустановленные обновления безопасности на узлах сети и сформировать необходимые ссылки для загрузки недостающих обновлений. Результат аудита обновлений содержит: наименования обновлений, сведения о рисках, связанных с отсутствием недостающего обновления на узле сети, ссылку на производителя, заявившего о выходе обновления, ссылку на репозиторий (базу), где хранятся доступные для загрузки обновления.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит обновлений**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;

- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации – при включенном параметре служба сканирования сохраняет в БД информацию о всех уязвимостях, которые были проверены во время сканирования, даже если они не были обнаружены. При выключенном параметре сохраняются только обнаруженные уязвимости. Выключенный параметр экономит место в БД;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя	
Описание	
Тип сканирования	Аудит обновлений
Служба сканирования	debian12_local
Запуск	По требованию
	☒ Запустить сразу после закрытия мастера ☐ Повторно запускать неуспешные хосты
Расширенный лог	☐ Сохранять файл результатов ☐ Сохранять файл системных характеристик ☐ Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации
Дополнительно	☐ Оповещать по e-mail ☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки **Группы и хосты**

Группы и хосты
Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE
Нет данных для отображения			

Всего: 0

Добавить хосты

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Всего: 0

Добавить группы

Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройки **Группы и хосты** **Учётные данные**

Учётные данные задания
Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	☒ Безагент
5	UserGate		http	☒ Безагент
10	Windows		windows	☒ С использованием агента ☐ Безагент WinRM

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

[Подробнее про подбор учетных записей](#)

Шаг 5. Выберите профиль и тип сканирования → **Вперед**:

- **Полный** – при сканировании будут использоваться детальные (рекурсивные) сигнатуры, являющиеся трудоемкими. Аудит займет больше времени;
- **Быстрый** – не будут применяться детальные сигнатуры. Сканирование будет выполняться быстрее.

Настройки Группы и хосты Учётные данные **Профили сканирования**

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили

Тип сканирования

☒ Без профилей

☐ Быстрое

☐ Выбранные вручную

☒ Полное

Не создано ни одного профиля

Для создания профилей воспользуйтесь менеджером аудитов

О создании профилей сканирования смотрите в [5.1 Профили сканирования](#).

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки
Группы и хосты
Учётные данные
Профили сканирования
Отчёт

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				
20 Добавить шаблон отчёта...				

Всего: 0

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						
20 Добавить адрес доставки...						

Всего: 0

Назад
Ещё раз
Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.3 Аудит конфигураций

RedCheck позволяет автоматизировать процесс контроля параметров безопасности и осуществлять оценку соответствия информационных систем, ее отдельных компонентов, СУБД или хостов, стандартам, политикам безопасности, рекомендациям вендоров или другим «признанным практикам» (best practices). RedCheck содержит большое количество готовых конфигураций, разработанных на основе требований международных стандартов и рекомендаций. Поддержка стандартизованного формата SCAP позволяет пользователям загружать сторонние конфигурации, или использовать собственные.

При сканировании СУБД RedCheck позволяет проверять параметры конфигураций безопасности, например:

- требование к парольной политике;
- требование к методам аутентификации;
- требование к разграничению доступа БД;
- требование к резервному копированию и восстановлению БД.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admis / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит конфигураций**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;

- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять фактические значения xccdf – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *любой статус проверки*;
- Сохранять только настроенные фактические значения – сохранение фактических значений для проверяемых в процессе сканирования правил, имеющих *статус проверки, отличный от **Соответствие***. Можно активировать только при отмеченном параметре **Сохранять фактические значения xccdf**;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Аудит конфигураций

Служба сканирования

debian12_local

Запуск

По требованию

☒ Запустить сразу после закрытия мастера
 ☐ Повторно запускать неуспешные хосты

Расширенный лог

☐ Сохранять файл результатов
☐ Сохранять файл системных характеристик
☐ Сохранять фактические значения xccdf
☐ Сохранять только ненастроенные фактические значения

Дополнительно

☐ Оповещать по e-mail
☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

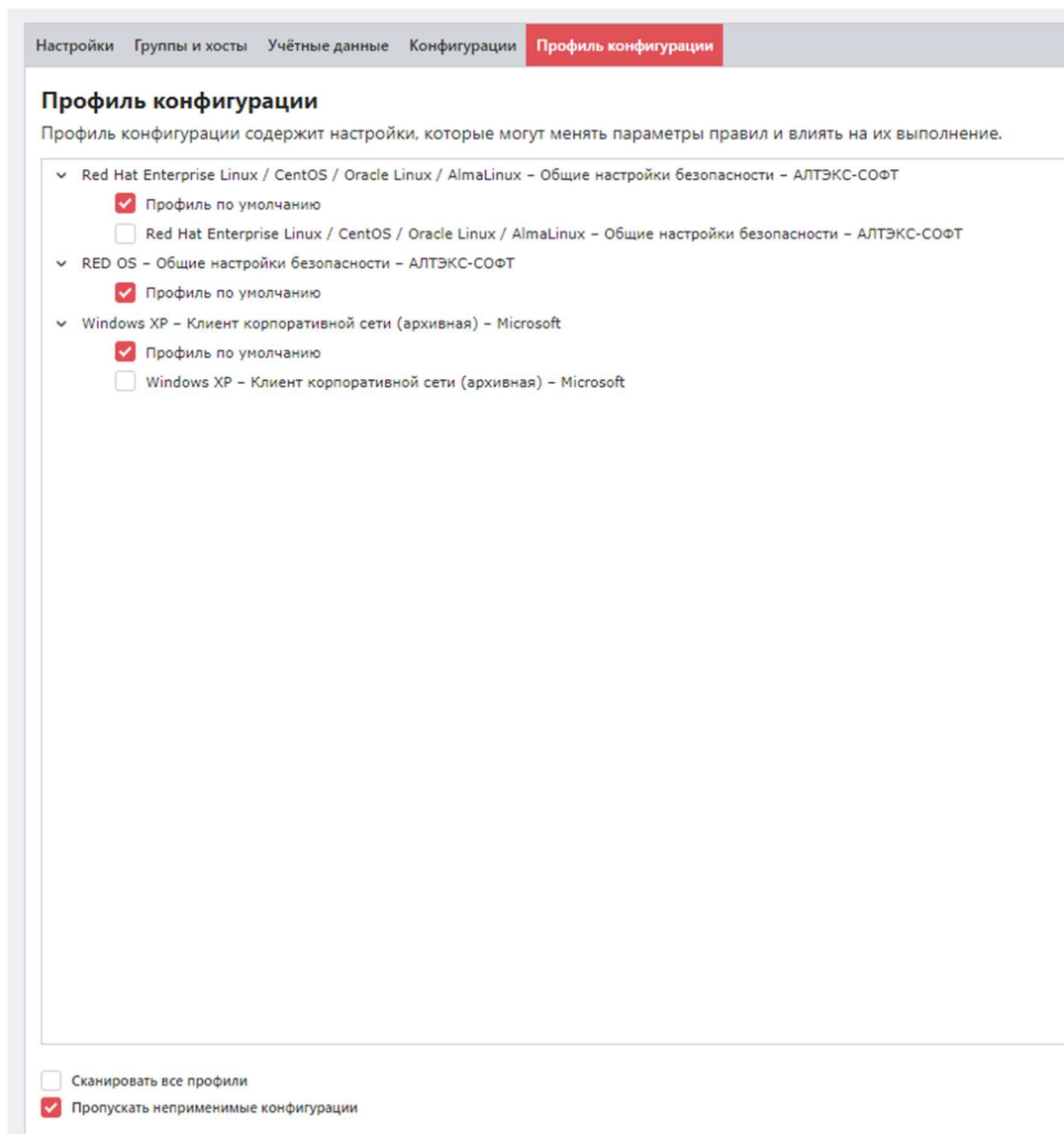
Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

[Подробнее про подбор учетных записей](#)

Шаг 5. Отметьте в списке необходимые конфигурации → **Вперед**;

Шаг 6. Выберите необходимый профиль для каждой из конфигураций → **Вперед;**



Настройки Группы и хосты Учётные данные Конфигурации **Профиль конфигурации**

Профиль конфигурации

Профиль конфигурации содержит настройки, которые могут менять параметры правил и влиять на их выполнение.

- ▼ Red Hat Enterprise Linux / CentOS / Oracle Linux / AlmaLinux – Общие настройки безопасности – АЛТЭК-СОФТ
 - ☒ Профиль по умолчанию
 - ☐ Red Hat Enterprise Linux / CentOS / Oracle Linux / AlmaLinux – Общие настройки безопасности – АЛТЭК-СОФТ
- ▼ RED OS – Общие настройки безопасности – АЛТЭК-СОФТ
 - ☒ Профиль по умолчанию
- ▼ Windows XP – Клиент корпоративной сети (архивная) – Microsoft
 - ☒ Профиль по умолчанию
 - ☐ Windows XP – Клиент корпоративной сети (архивная) – Microsoft

☐ Сканировать все профили
☒ Пропускать неприменимые конфигурации

О добавлении новых конфигураций и редактировании профилей для них смотрите в [5.2 Конфигурации](#).

Шаг 7. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед;**

Настройки
Группы и хосты
Учётные данные
Конфигурация
Профиль конфигурации
Отчёт

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20

Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20

Всего: 0

Добавить адрес доставки...

Назад
Вперед
Отмена

Шаг 8. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.4 Инвентаризация

RedCheck позволяет получать детальную информацию об аппаратных и программных средствах сканируемых хостов, включая: типы и описание оборудования, версии и редакции операционных систем, установленные пакеты обновлений и исправлений, установленное ПО, запущенные службы, пользователей и групп, сведения об общих папках. Глубокая детализация отчетов и использование функции Контроль позволяет отслеживать самые незначительные изменения в составе программного и аппаратного обеспечения сети. Реализована возможность инвентаризации образов Docker.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Инвентаризация**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания ([Настройка расписания](#));
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;

- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Служба сканирования

Запуск

☒ Запустить сразу после закрытия мастера

☐ Повторно запускать неуспешные хосты

Расширенный лог ☐ Сохранять файл результатов

Дополнительно

☐ Оповещать по e-mail

☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройка **Группы и хосты**

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE
Нет данных для отображения			

Всего: 0

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Всего: 0

Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройка **Группы и хосты** **Учётные данные**

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	☒ Безагент
5	UserGate		http	☒ Безагент
10	Windows		windows	☒ С использованием агента ☐ Безагент WinRM

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед;**

[Подробнее про подбор учетных записей](#)

Шаг 5. Выберите параметры инвентаризации → **Вперед;**

Настройки Группы и хосты Учётные данные **Параметры инвентаризации**

Параметры инвентаризации
Укажите профиль инвентаризации

Профиль upix
[Выбрать все](#) [Сбросить все](#)

- > ☒ Аппаратное обеспечение
- ▼ ☒ Программное обеспечение
 - > ☒ Операционная система
 - ▼ ☒ Пакеты
 - ▼ ☒ Пакет
 - ☒ Имя
 - ☒ Расширенное название
 - ☒ Версия
 - ☒ Релиз
 - ☒ Архитектура
 - ☒ Эпоха
 - ☒ Идентификатор ключа
 - ☒ Дата установки
 - ☒ Размер
 - ☒ Группа
 - ☒ Распространение
 - ☒ Копирайт
 - ☒ URL
 - ☒ Дата сборки
 - ☒ Вендор
 - ☒ Сборщик
 - ☒ Узел сборки
 - ☒ Источник
- > ☐ Docker
- ☐ OVAL-Инвентаризация

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед;**

Настройки
Группы и хосты
Учётные данные
Параметры инвентаризации
Отчёты

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20
Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20
Всего: 0

Добавить адрес доставки...

Назад
Вперёд
Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.5 Фиксация (контроль целостности)

RedCheck может обнаружить и оповестить о несанкционированных изменениях целостности в конфигурационных файлах, папках, ветках реестра (автозагрузка, файл hosts, файл конфигурации межсетевого экрана). Включение режима Контроль позволяет с заданной периодичностью осуществлять проверку целостности эталонных файлов.

Контроль целостности папок и файлов осуществляется по выбранной маске наименования методом контрольного суммирования по алгоритмам MD5, SHA1, SHA256, SHA512, ГОСТ 34.11-2012.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Не рекомендуется выполнять фиксацию файлов размером более 500Мб на **Linux-платформах**, т.к. это приводит к максимальной нагрузке ЦП на длительное время, что может привести к сбоям в работе, а также повлечь за собой отказ сканируемого оборудования.

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Фиксация**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания ([Настройка расписания](#));

- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Шаг 4. Выберите учетную запись для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройки Группы и хосты **Учётные данные** Фиксация файловой системы

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	Безагент

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед;**

Шаг 5. Укажите в поле **Каталог** полный путь к директории, которую хотите зафиксировать / исключить → при необходимости введите имя файла или паттерн (или воспользуйтесь кнопкой **...** [импорта каталогов из csv-файла](#)) → нажмите **+** → выберите необходимый метод снятия контрольной суммы из списка, расположенного после таблицы → **Вперед;**

Настройки Группы и хосты Учётные данные **Фиксация файловой системы**

Укажите каталоги, которые должны быть зафиксированы и каталоги, которые должны быть исключены из процесса фиксации.

Каталоги

Каталог	Имя файла	Вкл. подпапки	Исключить	
/var/opt	*	☒	☐	

Метод снятия КС: MD5

Всего: 1

Шаг 5.1. Для фиксации на Windows хостах. Укажите при необходимости ветки реестра и параметры, которые нужно зафиксировать → **Вперед;**

Настройки Группы и хосты Учётные данные Фиксация файловой системы **Фиксация реестра**

Укажите ключи реестра, которые должны быть зафиксированы и ключи реестра, которые должны быть исключены из процесса фиксации.

Ключи реестра: HKEY_LOCAL_MACHINE

Ключ	Вкл. подключки	Исключить	
HKEY_LOCAL_MACHINE\Microsoft	☒	☐	

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед;**

Шаг 7. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

Структура CSV-файла

Формат CSV – это текстовый файл с информацией, представленной в виде таблицы. В первой строке через разделитель «,» указываются названия столбцов. Последующие строки таблицы являются записями с информацией.

Path	FileName	IncludeSubdirectories	IsExclusion
Каталог	Имя файла или паттерн	# – включить подпапки	! – исключить

Пример

Код

```
Path,FileName,IncludeSubdirectories,IsExclusion
C:\ALTEX-SOFT\Red*,,,
C:\ProgramData\Test0,*.exe,#,
C:\ProgramData\Test1,*.dll,!
C:\ProgramData\Test2,*.ocr,#,!
C:\ProgramData\Test3,,,!

```

Не допускается использование спецсимволов в Path

4.6 Аудит уязвимостей АСУ ТП

Аудит уязвимостей АСУ ТП предназначен для проведения проверок на наличие уязвимостей протоколов АСУ ТП. Выявление уязвимостей проводится путем сопоставления сигнатур, хранящихся в БД RedCheck, с идентификационными сведениями о запущенном и опубликованном на сканируемом хосте ПО.

Сканирование выполняется на сетевом уровне, без использования привилегий или учетных записей (Черный ящик).

Создание задания

Необходимая роль: RedCheck_Admis / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит уязвимостей АСУ ТП**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания ([Настройка расписания](#));
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранные данные будут доступны в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Аудит уязвимостей АСУ ТП

Служба сканирования

debian12_local

Запуск

По требованию

☒

Запустить сразу после закрытия мастера

☐

Сохранять файл результатов

☐

Оповещать по e-mail

☐

Расширенная идентификация хоста

Расширенный лог

Дополнительно

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки
Группы и хосты

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

Id

IP / DNS

Описание

CPE

Нет данных для отображения

Всего: 0

20

Добавить хосты

Выбранные группы

Id

Имя

Описание

Нет данных для отображения

Всего: 0

20

Добавить группы

Шаг 4. Отметьте необходимые протоколы АСУ ТП / ПЛК → **Вперед**;



71

Настройки
Группы и хосты
Модули сканирования

Модули сканирования

Укажите требуемые протоколы АСУ ТП/ПЛК

☒ Simatic ALM
☒ Simatic S7
☒ Sicam PAS IPC
☒ Citect SCADA
☒ Modbus TCP/UDP
☒ Profinet IO
☒ ArchestrA Logger
☒ BACnet/IP
☒ Ethernet/IP
☒ GenBroker (GENESIS32/64)
☒ Schneider Electric IGSS
☒ FINS
☒ ProConOS
☒ CoDeSysV2
☒ CoDeSysV3
☒ MZTA
☒ Segnetics
☒ IsaGraF

Выбрать всё
Сбросить всё

Шаг 5. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки
Группы и хосты
Модули сканирования
Отчеты

Отчеты

Вы можете формировать один или несколько отчетов после выполнения задания. Для построения отчета используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

20
Всего: 0

Добавить шаблон отчета...

Адреса доставки для отчета

ID	Тип	Путь	Учетная запись	Формат	Команды
Нет данных для отображения					

20
Всего: 0

Добавить адрес доставки...

Назад
Вперед
Отмена

Шаг 6. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.7 Проверка доступности

RedCheck обладает возможностью проверки доступности добавленных хостов для любых системных режимов сканирования с привилегиями (Белый ящик), учитывая настроенные транспорты/протоколы доступа и учетные записи RedCheck для сканирования.

Результатом выполнения задания является информация о доступности хоста для выполнения сканирования с привилегиями (Белый ящик), либо конкретный отсутствующий параметр настройки.

Сканирование выполняется в комбинированном режиме на сетевом уровне, без использования привилегий (Черный ящик) и с использованием привилегий (Белый ящик).

Создание задания

Необходимая роль: RedCheck_Admis / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Обнаружение хостов**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Проверка доступности

Служба сканирования

debian12_local

Запуск

По требованию

Дополнительно

☒ Запустить сразу после закрытия мастера
 ☐ Оповещать по e-mail

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки
Группы и хосты

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

Ид

ИП / DNS

Описание

CPE

Нет данных для отображения

Всего: 0

Добавить хосты

Выбранные группы

Ид

Имя

Описание

Нет данных для отображения

Всего: 0

Добавить группы

Шаг 4. Укажите тип транспорта, доступность которого необходимо проверить → **Вперед**;

Настройки
Группы и хосты
Транспорт

Транспорт

Выберите, доступность какого транспорта требуется проверить. Для проверки будут ис

☒ **Agent**
Компонент RedCheck Agent. Порт по умолчанию: TCP 8732.
 ☐ **WinRM**
Провайдер Windows Remote Management (WinRM).
 ☐ **SSH**
Доступ по протоколу SSH. Порт по умолчанию TCP 22.
 ☐ **HTTP**
Доступ по протоколу HTTP.
 ☐ **SQL**
Доступность баз данных SQL. Требуется учётная запись типа SQL.

Шаг 5. Выберите учетную запись для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных	Команды
5	Windows		winnm		

Всего: 1

Добавить учётные данные...

Назад

Вперёд

Отмена

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперёд**;

Настройки Группы и хосты Транспорт Учётные данные **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчётов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20 ▾

Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчёта

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20 ▾

Всего: 0

Добавить адрес доставки...

Назад Вперёд Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.8 Обнаружение хостов

RedCheck выполняет поиск активных хостов и контроль целостности сети по заданному пулу сетевых адресов. Для обнаруженных в сети хостов определяется их IP-адрес, DNS, FQDN, NetBIOS, тип операционной системы. Также имеется возможность определить наличие агента RedCheck. По результатам выполнения задания впервые выявленные хосты могут быть импортированы в одну из существующих групп Системы, или экспортированы во внешний файл.

Сканирование выполняется без привилегий в режиме Черного ящика.

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Обнаружение хостов**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Уровень логирования [1-4] – уровень детализации логов AltXmap. Чем больше значение, тем детальнее будет лог;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Обнаружение хостов

Служба сканирования

debian12_local

Запуск

По требованию

☒

Запустить сразу после закрытия мастера

Расширенный лог

☐

Сохранять файл результатов

Уровень логирования [1-4]

Дополнительно

☐

Оповещать по e-mail

Шаг 3. Укажите настройки для задания → **Вперед;**

- Профиль сканирования – указываются TCP порты, которые будут сканироваться для определения доступности хоста;
- Определять ОС – ОС будет отображаться в формате CPE. Время сканирования увеличится;

Настройки

Обнаружение хостов

Диапазон хостов для сканирования

Вы можете использовать IP с диапазонами, DNS имена и их комбинации через пробел, например: 192.168.1.34 target1 192.168.0.1/24 10.6.15.2-46

TCP порты для определения доступности

Выберите профиль сканирования

Профиль по умолчанию

Список портов

22,80,139,443,445,1433,3389,8732

Методы определения доступности

☒

ARP

☒

ICMP

☒

TCP_ACK

☒

TCP_SYN

Дополнительные параметры

☒

Определять ОС

Расширенные настройки:

- Профиль временных настроек – настройка для nmap, которой регулируется количество и частота отправляемых пакетов на хост.

Расширенные настройки (экспертный режим)

Профиль временных настроек

Умеренный

Использовать интерфейс (eth[0-n])

Шаг 4. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Шаг 5. Перед закрытием мастера появится сводка о настройках задания → **Создать**.

4.9 Аудит в режиме "Пентест"

В рамках данного аудита RedCheck позволяет выполнить сетевое сканирование без привилегий в режиме Черного ящика. Аудит в режиме «Пентест» может выполнить следующие типы сканирований в рамках одного задания:

- Сканирование портов — проведение сетевой инвентаризации без привилегий для опубликованных служб каждого хоста, выявление ПО и его версии;
- Поиск уязвимостей — проведение аудита уязвимостей без привилегий с выполнением дополнительных скриптов для выявленного по итогам сетевой инвентаризации ПО.
- Подбор паролей — выполнение подбора паролей на основе указанных словарей для требуемых сетевых служб.

Создание задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит в режиме «Пентест»**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;

- Уровень логирования [1-4] – уровень детализации логов Altxmap. Чем больше значение, тем детальнее будет лог;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед;**

Шаг 4. Укажите настройки для сканирования → **Вперед;**

- Профили сканирования – можно выбрать ранее созданный [профиль сканирования Altxmap](#);
- Подбор паролей – разрешить службе сканирования подбирать пароли к:

- СУБД: Microsoft SQL Server, PostgreSQL, Oracle (+парольные хеши), MySQL;
- SSH, FTP;
- Почтовый сервер POP3;
- Поиск уязвимостей – разрешить обнаружение уязвимостей методом Черного ящика;
- Расширенное определение служб –
- WEB уязвимости – разрешить применение скриптов для Altxmap с тегом intrusive. Такие скрипты требуют значительное количество вычислительных ресурсов, что увеличивает время сканирования;
- Профили сканирования – порты, с которыми служба сканирования будет создавать соединение во время сканирования;
 - [Перечень портов для профиля TCP \[ТОП 50\]](#)
 - [Перечень портов для профиля TCP \[ТОП 1000\]](#)
 - [Перечень портов для профиля TCP-UDP \[ТОП 1000\]](#)

The screenshot shows the 'Types of scanning' (Типы сканирования) tab in the Altxmap configuration window. At the top, there's a 'Scanning profiles' (Профили сканирования) section with a dropdown menu set to 'By default' (По умолчанию) and buttons for 'Delete' (Удалить), 'Save' (Сохранить), and 'Save as' (Сохранить как). Below this is the 'Types of scanning' section with a description: 'Select the types of scanning that need to be performed in the task.' (Выберите типы сканирования, которые требуется выполнить в задании). It contains three checkboxes: 'Port scanning' (Сканирование портов) which is checked, 'Password selection' (Подбор паролей) which is unchecked, and 'Vulnerability search' (Поиск уязвимостей) which is checked. The 'Altxmap scanning settings' (Настройки сканирования Altxmap) section includes 'Detect OS and services' (Определять ОС и службы) checked, 'Extended service detection' (Расширенное определение служб) unchecked, and 'WEB vulnerabilities' (WEB уязвимости) unchecked. There's a field for 'Show vulnerable certificates, validity period of which expires in (days)' (Показывать уязвимыми сертификаты, срок действия которых истекает в течение (дней)) set to 30. A 'Select scan profile' (Выберите профиль сканирования) dropdown is set to 'Most popular, TCP [TOP 50]'. At the bottom, there are input fields for 'Exclude TCP ports' (Исключаемые TCP порты) and 'Exclude UDP ports' (Исключаемые UDP порты).

Расширенные настройки:

- Профиль временных настроек – настройка для сетевого сканера, которой регулируется количество и частота отправляемых пакетов на хост;
- Таймаут для хоста (h,m,s) – параметр --host-timeout. Задайте максимальное время ожидания, например, 30 мин, чтобы Altxmap не тратил более получаса на один хост. В течение этого времени Altxmap может сканировать другие хосты. Хост, чье время истекло, пропускается, и для него не собирается ни таблица портов, ни информация об ОС;

- Максимальное кол-во веб страниц – сколько всего страниц будет просканировано в результате рекурсивного поиска по web-приложениям;
- Максимальная глубина поиска веб страниц – параметр глубины для рекурсивного поиска по web-приложениям;
- Максимальное количество запросов для группы хостов – параметр --max-parallelism. По умолчанию Altxmap определяет степень параллелизма на основе производительности сети, начиная с 1 при плохих условиях и до нескольких сотен при идеальных. Опция иногда устанавливается для предотвращения отправки хостам более одного запроса за раз;
- Максимальное количество повторных передач запроса – если Altxmap не получил ответ на запрос сканирования порта, это может означать, что порт фильтруется или запрос потерялся в сети. Также возможно, что хост ограничивает количество ответов, что привело к временной блокировке запроса. В этом случае Altxmap повторяет передачу запроса. Если сеть кажется ненадежной, Altxmap может предпринять множество попыток передачи запроса перед прекращением сканирования. Это увеличивает время сканирования, но повышает достоверность результатов. Для ускорения сканирования можно ограничить количество повторных передач с помощью --max-retries. Установка --max-retries на 0 предотвратит все повторные попытки, хотя это не рекомендуется;
- Использовать TCP SYN сканирование для ускорения определения открытых портов – позволяет сканировать несколько сот портов в секунду, сохраняя при этом сканирующий хост в тени, поскольку никогда не завершает TCP-соединение (большинство утилит мониторинга не регистрируют данные соединения).

Расширенные настройки (экспертный режим)

Профиль временных настроек	Активный
Таймаут для хоста (h,m,s)	1h
Использовать интерфейс (eth[0-n])	
Максимальное количество веб страниц (по умолчанию: 20, без ограничений: -1)	20
Максимальная глубина поиска веб страниц (по умолчанию: 3, без ограничений: -1)	3
Максимальное количество запросов для группы хостов	900
Максимальное время ожидания ответа на запрос (мс)	1250
Максимальное количество повторных передач запроса	6

☐ Использовать TCP SYN сканирование для ускорения определения открытых портов

Шаг 5. Если параметр Подбор паролей был отмечен, мастер предложит настроить данную функцию → **Вперед**;

Настройки Группы и хосты Типы сканирования **Настройки подбора паролей**

Настройки подбора паролей

Укажите тип подбора, порт и имя экземпляра

Тип	Подбор паролей к MS SQL Server
Имя экземпляра	
	☐ Сканировать все экземпляры
Порт	1433
Таймаут подбора (h,m,s). 0 - без ограничений	3h
Использовать интерфейс (eth[0-n])	
Профиль временных настроек	Активный

Подбор паролей происходит на основе словарей. Чтобы заменить словарь, откройте **Инструменты** → **Настройки** → **Сканирование** → **Компонент ALTXMAP** → укажите путь к новому словарю, находящемуся на хосте с установленной службой сканирования

Компонент ALTXMAP

Путь к словарю логинов

Путь к словарю паролей

☐ Использовать встроенные словари

/var/opt/altxmap/nselib/data/usernames.lst

/var/opt/altxmap/nselib/data/passwords.lst

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки

Группы и хосты

Типы сканирования

Отчет

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

20

Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	Путь	Учётная запись	Формат	Команды
Нет данных для отображения					

20

Всего: 0

Добавить адрес доставки...

Назад

Вперед

Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания
→ **Создать**.

 REDCheck

85

4.10 Аудит уязвимостей Docker / Инвентаризация Docker

RedCheck позволяет проводить комплексный аудит безопасности для образов и контейнеров, реализованных на базе платформы контейнеризации Docker, а также системы оркестрации и масштабирования Kubernetes. В рамках данной функции доступны проверки на уязвимости, критичные неустановленные обновления безопасности, неверные настройки параметров конфигураций, инвентаризация, фиксация и контроль целостности. В рамках штатных функциональных возможностей доступна отдельная задача проверки уязвимостей файлов-образов Docker с учетом архитектуры слоев.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Содержание

- [Docker-аудит уязвимостей](#)
- [Docker-инвентаризация](#)

Создание задания (Аудит уязвимостей)

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Аудит Docker** → **Docker аудит уязвимостей**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав  ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;

- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Сохранять файл системных характеристик – сохранение информации о найденных состояниях на хосте без информации о контенте, который был проверен во время сканирования (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/system-characteristics.xml**);
- Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации – при включенном параметре служба сканирования сохраняет в БД информацию о всех уязвимостях, которые были проверены во время сканирования, даже если они не были обнаружены. При выключенном параметре сохраняются только обнаруженные уязвимости. Выключенный параметр экономит место в БД;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Docker аудит уязвимостей

Служба сканирования

debian12_local

Запуск

По требованию

Расширенный лог

☒ Запустить сразу после закрытия мастера
☐ Повторно запускать неуспешные хосты
☐ Сохранять файл результатов
☐ Сохранять файл системных характеристик
☐ Сохранять результаты со всеми статусами для аудита обновлений/уязвимостей и OVAL-инвентаризации

Дополнительно

☐ Оповещать по e-mail
☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки Группы и хосты

Группы и хосты
Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE
Нет данных для отображения			

Всего: 0

Добавить хосты

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Всего: 0

Добавить группы

Шаг 4. Выберите учетную запись для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройки Группы и хосты **Учётные данные**

Учётные данные задания
Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	Безагент

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

RedCheck поддерживает аудит Docker-контейнеров, развернутых только на Linux-системах.

Шаг 5. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки Группы и хосты Учётные данные **Отчёт**

Отчёты
Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

Всего: 0

Добавить шаблон отчета...

Адреса доставки для отчета

ID	Тип	Путь	Учётная запись	Формат	Команды
Нет данных для отображения					

Всего: 0

Добавить адрес доставки...

Назад Вперед Отмена

Шаг 6. Перед закрытием мастера появится сводка о настройках задания
→ **Создать**.

Создание задания (Docker-инвентаризация)

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Нажмите **Действия** → **Инвентаризация**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполнять согласно указанному расписанию;
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания ([Настройка расписания](#));
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Ограничить максимальное время выполнения задания – функция [Остановки задания по времени выполнения](#);
- Сохранять файл результатов – сохранение расширенного лога в формате .xml (по умолчанию располагается в **/var/opt/scan-service/jobs/executionId/uuid/results.xml**). Расширенный лог включает в себя информацию о найденных состояниях на хосте, а также о контенте, который был проверен во время сканирования;
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранная информация будет доступна в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Инвентаризация

Служба сканирования

debian12_local

Запуск

По требованию

☒ Запустить сразу после закрытия мастера
 ☐ Повторно запускать неуспешные хосты

Расширенный лог

☐ Сохранять файл результатов

Дополнительно

☐ Оповещать по e-mail
 ☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки Группы и хосты

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID	IP / DNS	Описание	CPE	
2	192.168.1.6			
4	192.168.100.2			
5	192.168.99.1			
7	192.168.99.3			

Добавить хосты

Выбрано: 4

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Добавить группы

Выбрано: 0

Назад Вперед Отмена

Шаг 4. Выберите учетные записи для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройки Группы и хосты Учётные данные

Учётные данные задания

Укажите требуемые учётные данные для нового задания. Заметьте, что только выбранные учётные данные будут применены к целевым хостам.

	ID	Тип	Подтип	Имя профиля	Метод получения данных
⌵	1	Ssh		redcheck-admin	Безагент

Укажите нужный метод получения данных, измените порядок сканирования при необходимости → **Вперед**;

RedCheck поддерживает аудит Docker-контейнеров, развернутых только на Linux-системах.

Шаг 5. Выберите параметр **Docker** для инвентаризации → **Вперед**;

Настройки Группы и хосты Учётные данные **Параметры инвентаризации**

Параметры инвентаризации

Укажите профиль инвентаризации

Профиль unix
Выбрать все Сбросить все

- > ☐ Локальные пользователи
- > ☐ Переменные среды
- ▼ ☐ Пакеты
 - > ☐ Пакет
- ▼ ☒ Docker
 - ☒ ID
 - ☒ Имя
 - ☒ Версия
 - ☒ Операционная система
 - ☒ Тип ОС
 - ☒ Версия ядра
 - ☒ Архитектура
 - ☒ Корневая директория
 - ☒ Драйвер хранилища
 - ☒ Драйвер журналирования
 - ☒ Драйвер cgroup
 - ☒ Контейнеров запущено
 - ☒ Контейнеров приостановлено
 - ☒ Контейнеров остановлено
 - ☒ Контейнеров всего
 - ☒ образов всего
 - ☒ InitBinary
 - ☒ ExperimentalBuild
 - ☒ MemoryLimit
 - ☒ SwapLimit
 - ☒ KernelMemory
 - ☒ KernelMemoryTcp
 - ☒ CpuCfsPeriod
 - ☒ CpuCfsQuota
 - ☒ CpuShares
 - ☒ CpuSet

Шаг 6. Укажите шаблон для отчета (**Добавить шаблон отчета**) и адреса для его доставки (**Добавить адрес доставки**) → **Вперед**;

Настройки
Группы и хосты
Учётные данные
Параметры инвентаризации
Отчёт

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	ID	Имя	Тип данных	Команды
Нет данных для отображения				

20
Всего: 0

Добавить шаблон отчёта...

Адреса доставки для отчета

ID	Тип	ID	Путь	Учётная запись	Формат	Команды
Нет данных для отображения						

20
Всего: 0

Добавить адрес доставки...

Назад
Вперёд
Отмена

Шаг 7. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.11 Сканирование YARA правил

RedCheck позволяет автоматизировать обнаружение вредоносных объектов за счет применения сигнатурного анализа на основе набора пользовательских YARA правил.

Сканирование выполняется по безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

На данный момент сканирование YARA правил возможно только после импорта пользовательских сигнатур ([5.7 Импорт YARA-правил](#))

Создание задания

Необходимая роль: RedCheck_Admis / RedCheck_Adminis

Чтобы создать задание, выполните следующие шаги.

Шаг 1. Откройте **Действия** → **Сканирование YARA**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

- Служба сканирования – служба сканирования, которая будет выполнять задание. Если в БД зарегистрировано несколько служб сканирования, то ее необходимо явно выбрать, нажав ([Мониторинг служб сканирования](#));
- Тип запуска:
 - По требованию – запуск задания вручную;
 - По расписанию – задание будет выполняться согласно настроенному расписанию ([Настройка расписания](#));
- Запустить сразу после закрытия мастера – задание начнет выполняться сразу после создания;
- Повторно запускать неуспешные хосты – функция [Повторного перезапуска недоступных хостов](#);
- Оповещать по e-mail – отчет о сканировании будет отправлен на настроенную заранее почту;
- Расширенная идентификация хоста – будут собираться данные о хосте: FQDN, netBIOS-имя, MAC-адрес, IP-адрес. Собранные данные будут доступны в результате сканирования на вкладке Расширенные параметры;

Настройки

Настройки нового задания

Укажите требуемые параметры для нового задания и выберите включаемые в него целевые хосты.

Имя

Описание

Тип сканирования

Сканирование YARA

Служба сканирования

debian12_local

Запуск

По требованию

Дополнительно

☒ Запустить сразу после закрытия мастера
☐ Повторно запускать неуспешные хосты
☐ Оповещать по e-mail
☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые помогут идентифицировать хост, такие как IP, MAC, FQDN и т.д. Просмотр параметров доступен на странице результатов сканирования.

Шаг 3. Выберите хосты (**Добавить хосты**) и/или группы (**Добавить группы**) для сканирования → **Вперед**;

Настройки Группы и хосты

Группы и хосты

Выберите список групп и / или список хостов для нового задания.

Выбранные хосты

ID IP / DNS Описание CPE

Нет данных для отображения

Всего: 0 20

Добавить хосты

Выбранные группы

ID Имя Описание

Нет данных для отображения

Всего: 0 20

Добавить группы

Шаг 4. Выберите учетные записи (тип SSH) для сканирования целевых хостов, нажав **Добавить учетные записи** → **Выбрать**;

Настройки Группы и хосты Учётные данные

Учётные данные задания

Укажите требуемые учетные данные для нового задания. Заметьте, что только выбранные учетные данные будут применены к целевым хостам.

ID	Тип	Подтип	Имя профиля	Метод получения данных
1	Ssh		redcheck-admin	☒ Безагент
5	UserGate		http	☒ Безагент
10	Windows		windows	☒ С использованием агента ☐ Безагент WinRM

[Подробнее про подбор учетных записей](#)

Шаг 5. Укажите каталоги для сканирования с помощью YARA-правил → **Вперед**;

Настройки Группы и хосты Учётные данные **Настройки сканирования YARA**

Каталоги для сканирования YARA-правилами

Укажите каталоги для сканирования с помощью YARA-правил.

Каталоги

Каталог

/opt/		
-------	--	--

Всего: 1

Шаг 6. Перед закрытием мастера появится сводка о настройках задания
→ **Создать.**

4.12 Настройка расписания для задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Расписание можно настроить как в момент создания задания, так и при редактировании ранее созданного.

Форма с параметрами выглядит следующим образом:

- Когда следует запускать задание – периодичность запуска задания;
- Время запуска – дата и время запуска задания;
- Истекает – дата и время окончания работы расписания;
- Повторят каждые – показатель, через сколько задание будет запускаться повторно;
- Ограничить максимальное время выполнения задания – позволяет останавливать задание, которое выполняется больше указанного времени. Не учитывается время приостановки задания по расписанию;
- Приостанавливать задание – дата, время и дни недели, когда расписание не будет выполняться.

Расписание задания

Укажите расписание для нового планового задания.

Когда следует запускать задание

Ежечасно

Время запуска

09.07.2025 11:32

☐ Истекает

09.07.2025 12:34

Повторять каждые 1 (часы)

☒ Ограничить максимальное время выполнения задания

Максимальное время, ч. 1

☒ Приостанавливать задания

Время Длительность

18:30 15:00

☒ Понедельник

☐ Вторник

☐ Среда

☐ Четверг

☐ Пятница

☐ Суббота

☐ Воскресенье

Если указано время приостановки задания. Разница между окончанием приостановки и последующим запуском задания должна составлять не менее 1 минуты. Например, если приостановка заканчивается в 23:00, то запуск должен быть запланирован как минимум на 23:01

Во время приостановки можно запустить задание. Это продолжит выполнение с момента приостановки. Такой запуск никак не повлияет на последующие приостановки и запуски задания, установленные расписанием.

Во время выполнения можно приостановить задание. Это аналогично паузе, т.е. последующий запуск продолжит выполнение задания с момента приостановки. Это также не повлияет на выполнение расписания.

Пример использования

Запуск задания каждую неделю в 12:00 на протяжении месяца.

Расписание

Тип: Еженедельно

Время первого запуска: 06.04.2023 12:00:00

Время истечения: 06.05.2023 12:00:00

Повтор: Повторять каждые 1 (недели)

Расписание задания

Укажите расписание для нового планового задания.

Тип запуска

По расписанию

Когда следует запускать задание

Ежеминутно

Время запуска

01.01.0001

02:30

☐ Истекает

01.01.0001

02:30

Повторять каждые 0 (минуты)

☐ Ограничить максимальное время выполнения задания

Максимальное время, ч. 1

☐ Приостанавливать задания

Время

Длительность

18:30

15:00

☐ Понедельник

☐ Вторник

☐ Среда

☐ Четверг

☐ Пятница

☐ Суббота

☐ Воскресенье

Настройка в момент создания

Выберите на начальной странице мастера тип запуска **По расписанию**. В одном из последующих шагов будет страница с настройками расписания.

Тип запуска

По расписанию

☐ Запустить сразу после закрытия мастера

☐ Оповещать по e-mail

☐ Расширенная идентификация хоста

Перед выполнением задания производится сбор дополнительных данных, которые
Просмотр параметров доступен на странице результатов сканирования.

Настройка при редактировании задания

Зайдите в свойства задания → нажмите  в параметре **Запуск** → измените **Тип запуска** на **По расписанию**.

Запуск

По требованию 

Служба сканирования

a2e2f25a-ad8d-4c8a-b021-71382a8e2af7 

Не изменяйте тип запуска во время приостановки или выполнения задания. Для этого необходимо завершить итерацию выполнения задания, нажав **Остановить**

4.13 Повторный перезапуск недоступных хостов во время сканирования

Необходимая роль: RedCheck_Admis / RedCheck_Adminis

Функции повторного запуска неуспешных хостов и ограничения максимального времени выполнения задания можно настроить как в момент создания задания, так и при редактировании ранее созданного.

Скриншот фрагмента интерфейса настройки сканирования. Вверху есть флажок ☒ с надписью 'Повторно запускать неуспешные хосты'. Ниже расположены два поля: 'Интервал повторного запуска' со значением '1 час' и выпадающим списком, и 'Количество попыток' со значением '3'.

а) Повторный перезапуск касается хостов, которые служба определила как недоступные (например, не смогла подключиться за определенный интервал времени). Под повторный перезапуск не попадают хосты, для которых не подошла ни одна из указанных при создании задания учетных записей (на данный момент для транспорта WinRM не применяется данное условие). Результаты сканирования таких хостов будут сразу записаны в Историю.

б) Хост, который оказался недоступен, будет запущен через указанное в параметре **Интервал повторного запуска** время. Точкой отсчета для интервала является время завершения неудачного сканирования. Если на момент запланированного перезапуска служба не закончила основное сканирование, то приоритетно будут сканироваться основные хосты, а только потом будут перезапущены недоступные. В случае повторной недоступности перезапуск хоста произойдет через указанное в параметре **Интервал повторного запуска** время с момента завершения очередного неудачного сканирования. Количество повторных попыток задается в параметре **Количество попыток**

в) В случае, если время перезапуска недоступного хоста приходится на время приостановки задания по расписанию, то перезапуск будет отложен на момент возобновления сканирования. Если на момент возобновления сканирования служба не завершила сканирование основных хостов, то недоступный хост будет перезапущен после окончания основного сканирования.

5 Расширенные возможности для заданий сканирования

RedCheck предлагает следующие расширенные возможности для заданий:

- Создавать профили сканирования, в которых можно указывать конкретные OVAL-определения для поиска на хосте;
- Добавлять собственную конфигурацию для необходимого продукта, или изменять уже имеющуюся в БД RedCheck;
- Добавлять свои собственные OVAL-определения в Систему.

Содержание

- [5.1 Профили аудитов](#)
- [5.2 Конфигурации](#)
- [5.3 OVAL-определения](#)
- [5.4 Отслеживание изменений результатов сканирования \(Контроль\)](#)
- [5.5 Профили сканирования Altxmap](#)
- [5.6 Импорт скриптов для пентеста](#)
- [5.7 Импорт YARA-правил](#)

5.1 Профили аудитов

RedCheck позволяет выбрать OVAL-определения уязвимостей и обновлений для добавления их в профиль аудитов. Такой профиль позволяет искать на хостах только нужные уязвимости и неустановленные обновления, а также наоборот, исключать из отчетов указанные в профиле OVAL-определения. Создание профилей аудитов происходит в [Менеджере профилей](#).

Типы профилей

Существует два типа профилей:

- Статический – сигнатуры указываются вручную;
- Динамический – сигнатуры находятся автоматически, исходя из указываемых параметров поиска.

Профили сканирования можно применить только для аудитов уязвимостей и обновлений.

Пример использования

Создадим статический профиль для поиска на хостах нескольких интересующих нас уязвимостей.

Раскроем **Инструменты** → **Менеджер профилей** → **Создать статический профиль**;

OVAL-профили

Просмотр и редактирование OVAL-профилей.

Семейство

Unix

Класс

Уязвимость

☒ Статические профили
 ☒ Динамические профили

Создать статический профиль...

Создать динамический профиль...

ID	Имя	Описание
1	статик	
2	динамик	

Укажем имя, платформу и класс OVAL-определений для нашего профиля (подробнее в [5.1.1 Менеджер профилей](#)).

Новый профиль

Статический профиль, содержит вручную сформированный набор аудитов.

Имя

Тестовый профиль

Описание

Семейство

Windows

Класс

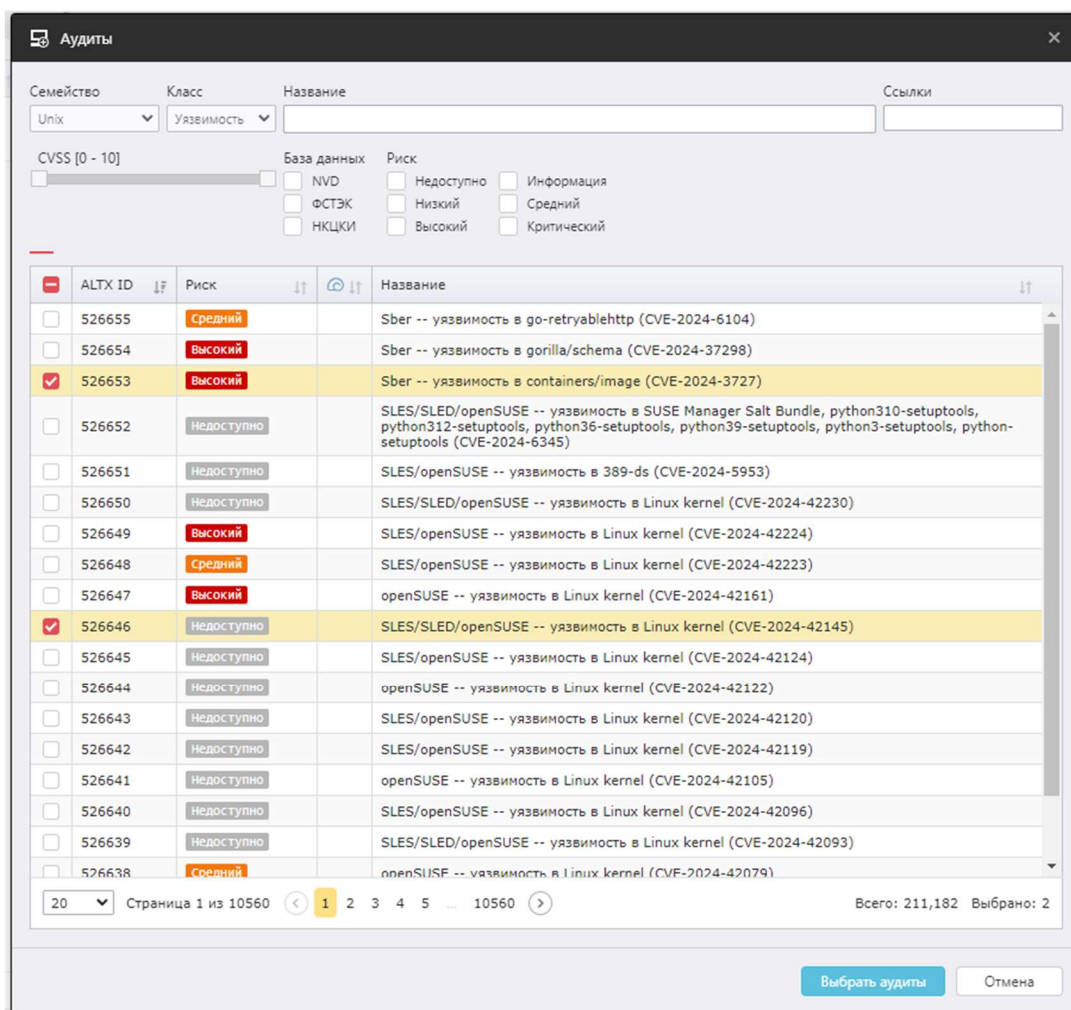
Уязвимость

Добавить аудиты...

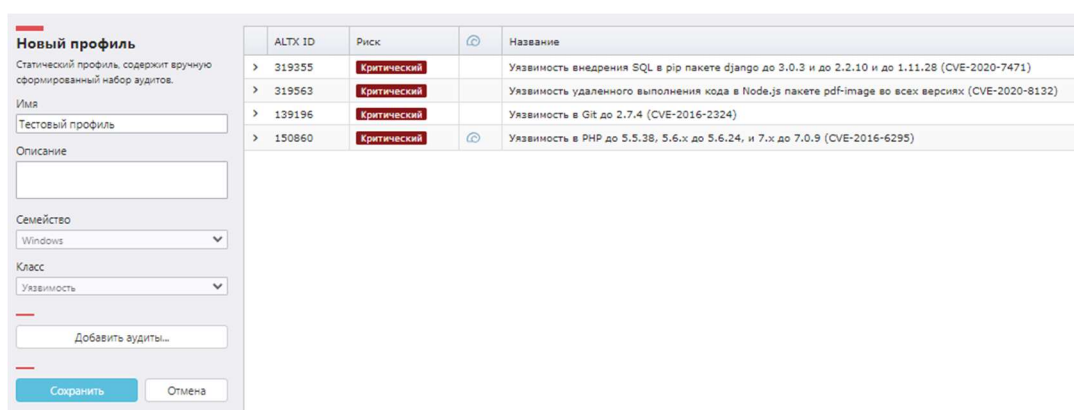
Сохранить

Отмена

Нажав **Добавить аудиты**, выберем необходимые OVAL-определения → **Выбрать аудиты**.



Сохраним созданный профиль, нажав соответствующую кнопку.



Создадим задание Аудит уязвимостей. Дойдем до шага **Профили сканирования** → отметим **Выбранные вручную** и укажем созданный нами профиль.

Настройки
Группы и хосты
Учётные данные
Профили сканирования

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили

☐ Без профилей
☒ Выбранные вручную

☐ динамик (Unix)
Динамический профиль
☐ статик (Unix)
Статический профиль

Перейдем в **История** и посмотрим результаты сканирования;

ИСТОРИЯ КОНТРОЛЬ ОТЧЁТЫ ПОЛЬЗОВАТЕЛИ								
№	Хост	Статус	Риск	К	Задание	А	Профиль	Е
257	10.0.0.183	Завершено			тестовое задание	[-]	Аудит уязвимостей	1
256	10.0.0.182	Завершено			тестовое задание	[-]	Аудит уязвимостей	1

Видим, что на двух просканированных хостах указанных в профиле уязвимостей не найдено.

5.1.1 Менеджер профилей

Создание профиля аудитов

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для того, чтобы создать профиль аудитов, выполните следующие шаги.

Шаг 1. Откройте **Инструменты** → **Менеджер профилей**;

Шаг 2. Выберите необходимый тип профиля, нажав **Создать статический профиль** / **Создать динамический профиль**;

ID	Имя	Описание
1	статик	
2	динамик	

Статический профиль

Шаг 3. Укажите имя, платформу и класс OVAL-определения для создаваемого профиля → **Добавить аудиты**;

Новый профиль

Статический профиль, содержит ручную сформированный набор аудитов.

Имя

Описание

Семейство

Windows

Класс

Уязвимость

Добавить аудиты...

Сохранить

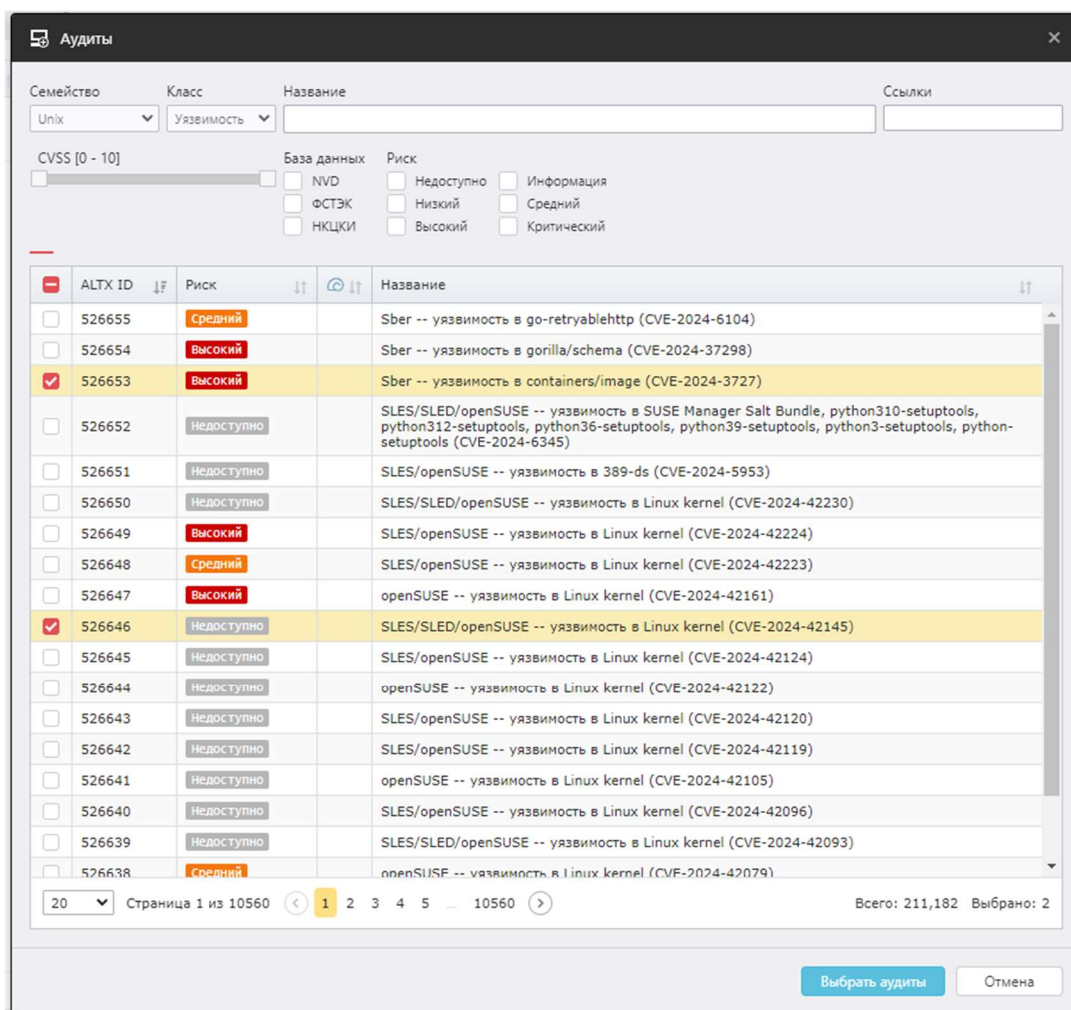
Отмена

ALT X ID	Риск
----------	------

Шаг 4. Отметьте в списке нужные OVAL-определения, воспользовавшись фильтром при необходимости → **Выбрать аудиты;**

 REDCheck

107



Сохраните профиль, нажав соответствующую кнопку.

Динамический профиль

Шаг 3. Укажите параметры для поиска OVAL-определений, воспользовавшись фильтром → **Сохранить**;

При изменении настроек фильтрации в таблице будут отображаться OVAL-определения, которые попадут в профиль.

Новый профиль

Динамический профиль, содержит набор аудитов, удовлетворяющих фильтрам.

Имя

Описание

Семейство

Класс

Фильтр по названию

Фильтр по описанию

☐

NVD

☐

ФСТЭК

☐

НКЦКИ

Дата публикации (начало)

☒ Не учитывать

☐ Начиная с

☐ Начиная с дней назад

Дата публикации (конец)

☒ Не учитывать

☐ Заканчивая

☐ Заканчивая дней назад

Риск

☐ Недоступно ☐ Информация

☐ Низкий ☐ Средний

☐ Высокий ☐ Критический

CVSS [0 - 10]

☐ Наличие эксплоита

CVSS3 векторы атаки

☐ Сетевой ☐ Смежная сеть

☐ Локальный ☐ Физический

CVSS3 параметры

☐ Высокая сложность атаки

☐ Значит. влияние на целостность

☐ Значит. влияние на доступность

☐ Низкий уровень привилегий

☐ Влияние на друг. compon. системы

☐ Взаимодействие с пользователем

Редактирование профиля аудитов

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Для того, чтобы отредактировать созданный ранее профиль аудитов, выполните следующие шаги.

Откройте **Инструменты** → **Менеджер профилей** →  → **Редактировать**;

Редактирование профиля

Статический профиль, содержит вручную сформированный набор аудитов.

Имя
profile

Описание

Семейство
Windows

Класс
Уязвимость

ALTX ID	Риск	Название
> 169224	Критический	Уязвимость в Adobe ColdFusion 2016 Update 4 и ниже, ColdFusion 11 update 12 и ниже (CVE-2017-11283)
> 170747	Критический	Уязвимость в NetIQ Access Manager 4.3 и 4.4 (CVE-2017-14803)
> 171328	Критический	Уязвимость в NetVault Backup 11.3.0.12 (CVE-2018-1161)
> 171330	Критический	Уязвимость в NetVault Backup 11.3.0.12 (CVE-2018-1163)
> 174219	Критический	Уязвимость в NordVPN 6.12.7.0 (CVE-2018-10170)
> 170835	Критический	Уязвимость в SUPERAntiSpyware 6.0.1254 (CVE-2018-6476)
> 170752	Критический	Уязвимость в BMC Track-It! 11.4 до Hotfix 3 (CVE-2016-6598)
> 173767	Критический	Уязвимость в Apache HTTP Server до 1.3.2 (CVE-1999-1199)
> 175138	Критический	Уязвимость в HPE Intelligent Management Center (IMC) PLAT 7.3 E0504P04 (CVE-2017-5816)
> 175154	Критический	Уязвимость в HPE Intelligent Management Center (IMC) PLAT 7.3 E0504P2 и ниже (CVE-2017-12556)
> 169982	Критический	Уязвимость в Advantech WebAccess до 8.3 (CVE-2017-16720)
> 171660	Критический	Уязвимость в HPE Data Protector 8.x до 8.17, и 9.x до 9.09 (CVE-2017-5807)
> 169253	Высокий	Уязвимость чтения за пределами выделенной памяти в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16376)
> 169255	Высокий	Уязвимость обхода безопасности в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16380)
> 169256	Высокий	Уязвимость чтения за пределами выделенной памяти в Adobe Acrobat Reader 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16403)
> 169342	Высокий	Уязвимость доступа к освобожденной памяти в Google Chrome до 63.0.3239.84 (CVE-2017-15412)
> 169343	Высокий	Уязвимость в Google Chrome до 63.0.3239.84 (CVE-2017-15413)
> 169455	Высокий	Уязвимость в Adobe Acrobat и Reader: 2017.012.20098 и ниже, 2017.011.30066 и ниже, 2015.006.30355 и ниже, и 11.0.22 и ниже (CVE-2017-16376)

20 Page 1 of 3 (44 items) < 1 2 3 >

При редактировании профиля аудитов есть возможность изменить имя профиля и добавить / убрать OVAL-определения.

Добавление: Для добавления OVAL-определений в профиль аудитов нажмите **Добавить аудиты** → отметьте в списке нужные определения, воспользовавшись фильтром при необходимости → **Выбрать аудиты**.

Удаление: Для удаления уже добавленных определений нажмите  ;

	ALTX ID	Риск		Название	Дата публикации	
>	169982	Критический		Уязвимость в Adva	05.01.2018, 08:29:00	
>	171660	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	
>	170752	Критический		Уязвимость в BMC	30.01.2018, 20:29:00	
>	175138	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	
>	175154	Критический		Уязвимость в HPE	15.02.2018, 22:29:00	
>	170835	Критический		Уязвимость в SUPE	31.01.2018, 19:29:00	

После внесения изменений нажмите **Сохранить**.

Применение профилей аудитов при создании задания

При создании заданий типа Аудит уязвимостей / обновлений ([4.1 Аудит уязвимостей](#), [4.2 Аудит обновлений](#)) есть возможность указать профиль аудитов.

Для этого на шаге 5 (Профили сканирования) выберите **Выбранные вручную** → отметьте необходимые профили → **Далее**;

Настройки
Группы и хосты
Учётные данные
Профили сканирования

Профили сканирования

Сканирование может осуществляться без профилей, либо с указанными ниже профилями из списка.

Профили

☐ Без профилей
☒ Выбранные вручную

☐ динамик (Unix)
Динамический профиль
☐ статик (Unix)
Статический профиль

Применение статических профилей аудитов к отчетам

При создании отчета ([7.1 Создание простого отчета](#)) типа Уязвимости / Обновления есть возможность указать **только** статические профили аудитов.

RedCheck позволяет включить и исключить профиль из отчета. При включенном профиле в отчет попадут только те OVAL-определения, которые указаны в выбранном профиле. При исключении указанные в профиле определения не попадут в отчет.

Для добавления / удаления профиля в отчет выполните следующие шаги.

Шаг 1. При создании отчета в разделе **Фильтрация результатов сканирования** раскройте список **Включаемые / Исключаемые статические профили аудитов** → **Добавить профиль аудитов**;

Включаемые статические профили аудитов ▼

ID	Название	Семейство	
4	test	windows	

Выбрано: 1

[Добавить профиль аудитов](#)

Исключаемые статические профили аудитов ▶

Шаг 2. Отметьте нужные профили аудитов → **Выбрать**.

Выбор профиля аудитов

Название

☐	ID	Название	Семейство
☐	1	profile	Windows
☐	4	test	Windows

20

Page 1 of 1 (2 items)

< 1 >

Всего: 2 / Выбрано: 0

Выбрать

Отмена

5.2 Конфигурации

RedCheck предоставляет возможность изменять конфигурации, имеющиеся в базе данных, для проведения Аудита конфигураций согласно собственным настройкам правил проверки. Работа с конфигурациями происходит в Менеджере конфигураций.

Пример использования

Отредактируем конфигурацию «Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft».

Необходимая роль: RedCheck_Admis / RedCheck_Adminis / RedCheck_Users

Раскроем **Инструменты** → **Менеджер конфигураций** → выберем в фильтре по платформам **Microsoft Windows Server, version 1809**;

Имя	
Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft	
Windows Server 2019 / Windows Server версия 1809 и выше – Настройки для роли контроллера домена - Microsoft	
Windows – Оценка соответствия стандарту версии 3.2.1 - PCI DSS	

Всего: 3

Импортировать конфигурацию...

Для редактирования конфигурации для сервера общего назначения нажмем ➡

Выберите конфигурацию

К списку конфигураций | Развернуть | Критичность: Все | Профиль: Профиль не выбран | Создать

Конфигурация

Название: Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft

Версия: 7

Файл: Benchmark\WS2019-Member\ALTIX-WS2019-Member-xcdf.xml

Платформа: Microsoft Windows Server 2019 (cpe:/o:microsoft:windows_server_2019) Microsoft Windows Server, version 1809 (cpe:/o:microsoft:windows_server:1809) Microsoft Windows Server, version 1903 (cpe:/o:microsoft:windows_server:1903) Microsoft Windows Server, version 1909 (cpe:/o:microsoft:windows_server:1909) Microsoft Windows Server, version 2004 (cpe:/o:microsoft:windows_server:2004) Microsoft Windows Server, version 20H2 (cpe:/o:microsoft:windows_server:20h2)

Описание

Название: Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft

Описание: Конфигурация предназначена для обеспечения безопасного функционирования ОС Microsoft Windows Server на основе Security Baseline – это группа рекомендуемых корпорацией Майкрософт параметров конфигурации, которая объясняет их влияние на безопасность. Эти параметры основаны на отзывах специалистов по обеспечению безопасности Microsoft, групп развития продуктов, партнеров и клиентов.

Примечание

Создадим собственный профиль для изменения правил в конфигурации. Для этого нажмем **Создать** → введем имя для профиля → **Создать**.

После создания профиля можно изменять нужные нам правила.

Отключим правило Включить наблюдение за поведением. В списке **Статус правила** выберем **Выключено** → **Применить изменения**. Возле правила изменится иконка, уведомляющая, что правило неактивно.

Изменим эталонное значение для правила **Проверять съемные носители**. Отметим **Переопределить эталонное значение** и изменим в списке значение с **Enabled (0)** на **Disabled (1)** → **Применить изменения**. Возле правила изменится иконка, уведомляющая, что эталонное значение правила было переопределено.

- Включить проверку электронной почты
- Запретите пользователям и приложениям получать доступ к опасным веб-сайтам
- Настроить отчеты Microsoft SpyNet
- Настроить правила сокращения возможных направлений атак
- Настроить правила сокращения возможных направлений атак
- Настройка обнаружения потенциально нежелательных приложений
- Отправка образцов
- Проверять съемные носители**
- Настройка функции "Блокировка при первом появлении"
- Выберите уровень защиты в облаке
- Проверять все загруженные файлы и вложения
- Выключить защиту в реальном времени
- Ведение журнала событий
- PNP-действие аудита
- Аудит базовых параметров безопасности

Редактирование правила

Проверять съемные носители

Статус правила: Включено [Применить изменения](#)

Эталонное значение (из конфигурации): 0

Переопределенное значение (профиль): 1

☒ Переопределить значение [Disabled \(1\)](#)

Критичность: Средний

Сохраним созданный нами профиль, нажав **Сохранить профиль**.

Создадим задание Аудит конфигураций → на шаге **Конфигурация** выберем отредактированную конфигурацию → **Далее**.

Настройки Группы и хосты Учётные данные **Конфигурации**

Выберите конфигурацию

Microsoft Windows Server, version 1809 [Фильтр по продуктам...](#)

[Выбрать все](#) [Сбросить все](#)

Поиск конфигураций

#	Имя
☐	Windows Server 2019 / Windows Server версия 1809 и выше – Настройки для роли контроллера домена - Microsoft
☒	Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft
☐	Windows – Оценка соответствия стандарту версии 3.2.1 - PCI DSS

Отметим созданный нами профиль → **Далее**.

Настройки Группы и хосты Учётные данные Конфигурации **Профиль конфигурации**

Профиль конфигурации

Профиль конфигурации содержит настройки, которые могут менять параметры правил и влиять на их выполнение.

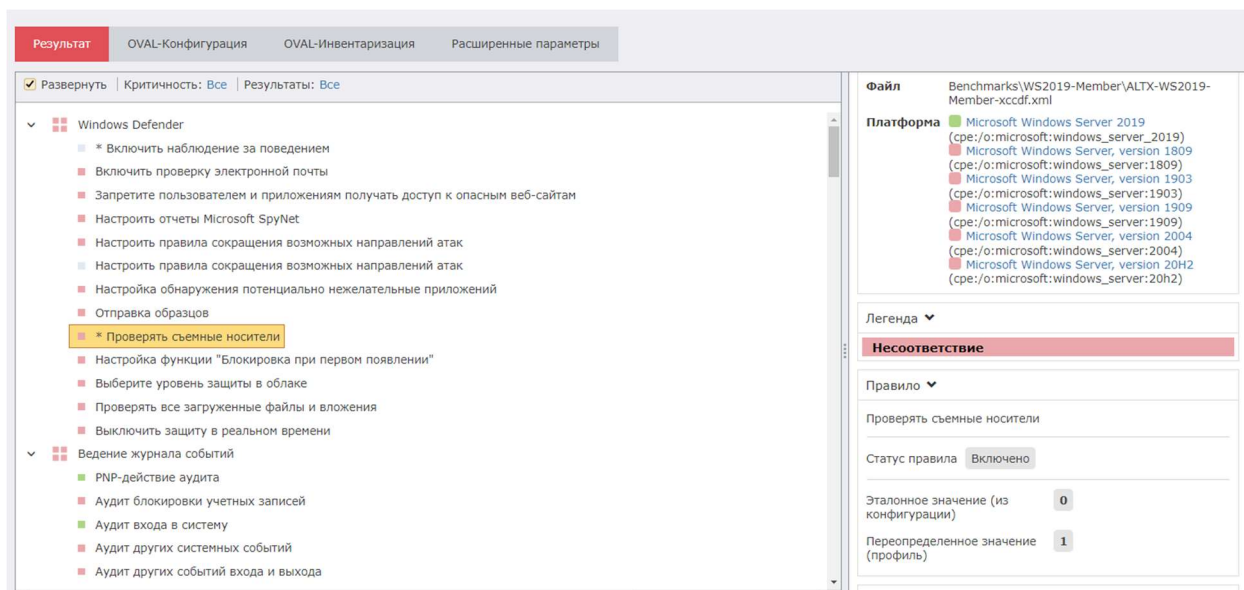
Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft

- ☐ Профиль по умолчанию
- ☐ Windows Server 2019 и Windows Server версия 1809 (Build 17763)
- ☐ Windows Server версия 1903 (Build 18362)
- ☐ Windows Server версия 1909 (Build 18363)
- ☐ Windows Server версия 2004 (Build 19041)
- ☐ Windows Server версия 20H2 (Build 19042)
- ☒ **тестовый профиль**

Перейдем в **История** и посмотрим результат сканирования, нажав **Завершено**.

№	Хост	Статус	Риск	К	Задание
258	10.0.0.182	Завершено	86 25 4		тестовое задание конфигурация

Видим, что измененные правила помечаются перед своим названием знаком *. Для правил, в которых было переопределено эталонное значение, пишется стандартное и переопределенное значение.



В RedCheck есть возможность импортировать собственные конфигурации ([5.2.1 Импорт конфигураций](#)). Конфигурация должна быть написана с использованием открытого стандарта [OVAL](#). ALT-X-SOFT предоставляет услуги написания конфигураций. За подробностями обращайтесь в службу тех. поддержки (контакты указаны на [странице вендора](#)).

5.2.1 Импорт конфигураций

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы импортировать конфигурацию в базу данных, выполните следующие шаги.

Шаг 1. Откройте **Инструменты** → **Менеджер конфигураций**;

Шаг 2. В менеджере можно просматривать имеющиеся в Системе конфигурации. Нажмите **Импортировать конфигурацию** → выберите необходимые файлы;

Конфигурация состоит из 4-х файлов:

- NAME-cpe-dictionary.xml
- NAME-cpe-oval.xml
- NAME-oval.xml
- NAME-xccdf.xml

Выберите конфигурацию

Фильтр по платформам... Фильтр по продуктам...

Поиск конфигураций

Имя	
ALT - Общие настройки безопасности - АЛТЭК-СОФТ	→
Apache HTTP Server - Аудит безопасности - АЛТЭК-СОФТ	→
Apache Tomcat - Аудит безопасности - АЛТЭК-СОФТ	→
Astra Linux SE 1.6 - Настройки по руководству Red Book - РусBITex	→
Astra Linux SE 1.7 - Настройки по руководству Red Book - РусBITex	→
Astra Linux SE и CE - Общие настройки безопасности - АЛТЭК-СОФТ	→
Check Point Firewall - Общие настройки безопасности межсетевого экрана - АЛТЭК-СОФТ	→
Cisco IOS - Оценка уровня безопасности Level-1 (минимальный) Router - CIS	→
Cisco IOS - Оценка уровня безопасности Level-1 (минимальный) Switch - CIS	→
Cisco IOS - Оценка уровня безопасности Level-2 (расширенный) Router - CIS	→
Cisco IOS - Оценка уровня безопасности Level-2 (расширенный) Switch - CIS	→
Cisco NX-OS - Общие настройки безопасности - Cisco	→
Dallas Lock 6.0 - Оценка соответствия классу 1Г - РД АС	→
Debian - Общие настройки безопасности - АЛТЭК-СОФТ	→
Docker - Аудит безопасности платформы контейнеризации - CIS	→
FortiGate - Общие настройки безопасности межсетевого экрана - CIS	→
Huawei VRP - Общие настройки безопасности - АЛТЭК-СОФТ	→
IBM DB2 - Общие настройки безопасности СУБД - CIS	→
IIS и .NET - Аудит безопасности - АЛТЭК-СОФТ	→
Kubernetes - Общие настройки безопасности главного узла - CIS	→
Kubernetes - Общие настройки безопасности отдельного рабочего узла - CIS	→
Microsoft Office 2013 - Настройки уровня пользователя - Microsoft	→

Всего: 116

Импортировать конфигурацию...

Конфигурация

Название ALT - Общие настройки безопасности - АЛТЭК-СОФТ

Версия 6

Файл Benchmarks\ALT\ALT-XCCDF.xml

Платформа ALT 10.x (cpe:/o:alt:alt_10)
ALT 8 SP (cpe:/o:alt:alt_8_sp)
ALT 9.x (cpe:/o:alt:alt_9)

Описание

Название ALT - Общие настройки безопасности - АЛТЭК-СОФТ

Описание Конфигурация предназначена для обеспечения безопасного функционирования ОС ALT

Примечание Не рекомендуется применять настройки данной конфигурации без предварительного тестирования и проверки в непродуктивной среде. В случае возникновения вопросов Вы можете обратиться в службу технической поддержки компании АЛТЭК-СОФТ: support@alt-soft.ru

5.3 OVAL-определения

RedCheck предоставляет возможность добавлять собственные OVAL-определения для проведения Аудита уязвимостей, обновлений, конфигураций и Инвентаризации.

Классы OVAL-определений

Все OVAL-определения делятся на 4 класса:

- Соответствие (compliance) – правило для конфигураций;
- Инвентарь – определения для Инвентаризации;
- Уязвимость;
- Обновление;

Уровни критичности

OVAL-определения имеют разный уровень критичности:

Недоступно – вендор не предоставил значение уровня критичности;

Информация – OVAL-определение для инвентаря (ПО).

Низкий, **Средний**, **Высокий** и **Критический** – стандартные определения уровня критичности.

Просмотр OVAL-определений

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Раскройте **Инструменты** → **Менеджер аудитов**;

В менеджере можно посмотреть OVAL-определения, находящиеся в используемой базе данных.

Аудиты

Просмотр аудитов.

Класс

Уязвимость

Семейство

Windows

Название

Описание

Ссылки

ALTX ID	Риск	Ссылки
> 169106	Средний	EXPLOIT-DB,CVE
> 169224	Высокий	CVE
> 169226	Средний	CVE
> 169238	Средний	Oracle,CVE
> 169253	Высокий	CVE,Adobe
> 169255	Высокий	CVE,Adobe
> 169256	Высокий	CVE,Adobe
> 169283	Средний	FSPEC,CVE,Mozilla
> 169342	Высокий	CVE,Google
> 169343	Высокий	CVE,Google
> 169439	Средний	CVE,Adobe
> 169455	Высокий	CVE,Adobe
> 169458	Высокий	CVE,Adobe
> 169495	Высокий	Microsoft,CVE
> 169496	Низкий	EXPLOIT-DB,Microsoft,CVE
> 169571	Средний	CVE
> 169573	Высокий	FSPEC,Securityfocus,CVE
> 168545	Высокий	FSPEC,CVE,Oracle
> 169675	Средний	CVE,Foxitsoftware
> 169706	Средний	FSPEC,CVE

Информация об уязвимости состоит из:

- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности. Расчет критичности производится с учетом базовых и временных метрик CVSS на основании данных вендора сканера, вендора ПО, экспертных организаций;
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Исправление – информация по устранению уязвимости;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;

84757	Средний	CVE,Wireshark	Уязвимость в pcapng парсере в Wireshark 1.12.x до 1.12.8 (CVE-2015-7830)
ALTX ID	84757		
Риск	Средний		
OVAL	oval:ru.altx-soft.win:def:42416 (Версия 4)		
Название	Уязвимость в pcapng парсере в Wireshark 1.12.x до 1.12.8 (CVE-2015-7830)		
Описание	Функция pcapng_read_if_descr_block в wiretap/pcapng.c в pcapng парсере в Wireshark 1.12.x до 1.12.8 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.		
Исправление	Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта http://www.wireshark.org/download.html .		
Ссылки	CVE	CVE-2015-7830	
	Wireshark	wnpa-sec-2015-30	

Импортирование OVAL-определения

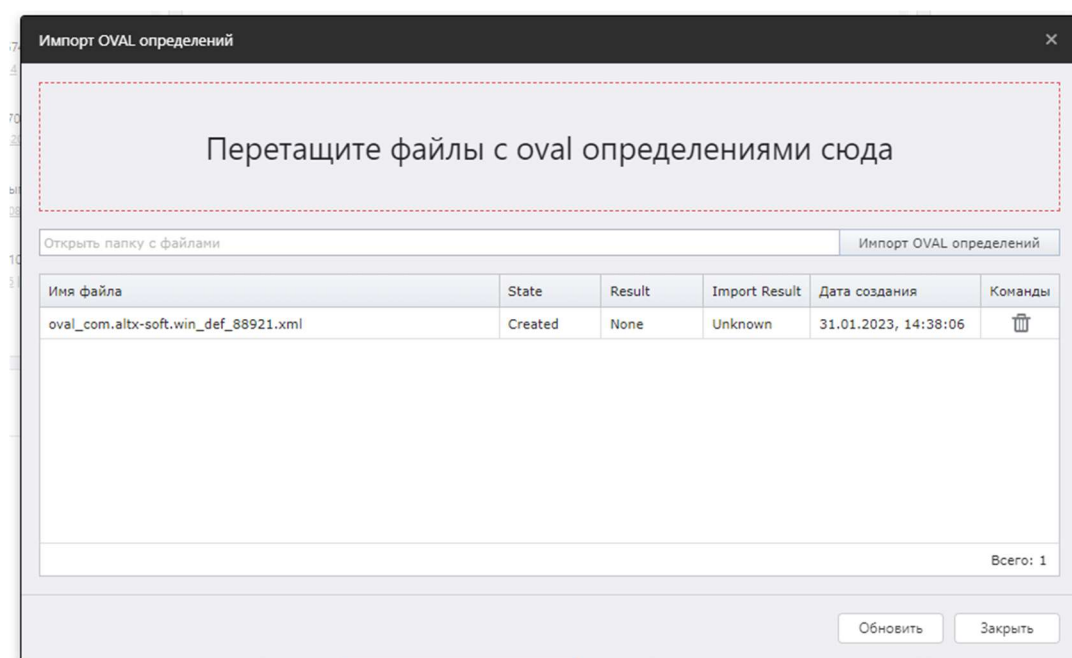
Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Размер файла OVAL-определения не должен превышать 10 МБ.

Чтобы импортировать свое собственное OVAL-определение, выполните следующие шаги.

Шаг 1. Раскройте **Инструменты** → **Импорт OVAL определений**;

Шаг 2. Перетащите / выберите в проводнике XML-файл, нажав **Импорт OVAL определений**;



Шаг 3. Через некоторое время нажмите **Обновить**. При успешном добавлении столбец **State** поменяет значение на **Finished**, а столбцы **Result** и **Import Result** на **Success**.

Имя файла	State	Result	Import Result	Дата создания	Команды
oval_com.altx-soft.win_def_88921.xml	Finished	Success	Success	31.01.2023, 14:38:06	

Добавленное определение будет доступно для просмотра в Менеджере аудитов.

5.4 Отслеживание изменений результатов сканирования

(Контроль)

Для того, чтобы следить за изменениями на хосте, в RedCheck существует функция Контроль. Данная функция позволяет назначить один из результатов сканирования выбранного задания эталоном для сравнения. При дальнейших выполнениях задания результат будет автоматически сравниваться с эталоном и уведомлять о несоответствиях.

Доступные типы заданий

Функция контроль доступна только для следующих типов заданий:

- Аудит уязвимостей;
- Аудит конфигураций;
- Инвентаризация;
- Фиксация.

Результат контроля

Статус контроля может иметь следующие значения:

Соответствие – вся информация текущего результата сканирования совпадает с эталоном;

Несоответствие – текущий результат сканирования не совпадает с эталоном;

Не проведен – после назначения эталона сканирований не проводилось.

Типы статуса

Добавлен – в результате сканирования появилось новое OVAL-определение, отсутствующее в эталоне;

Удален – OVAL-определение, имеющееся в эталоне, не было обнаружено в результате сканирования;

Изменен – какой-либо параметр был изменен.

Пример использования

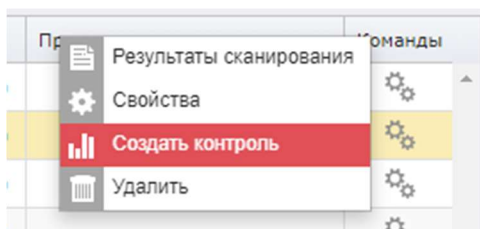
Необходимая роль: любая

Воспользуемся функцией Контроль, чтобы следить за тем, какие изменения вносятся на хосте для устранения уязвимостей.

У нас есть результат сканирования хоста заданием Аудит конфигураций.

№	Хост	Статус	Риск	К	Примечание	Команды
258	10.0.0.182	Завершено	86 25 4		Benchmarks\WS2019-Member\ALT-X-WS2019-Member-xccdf.xml f40d217c-af77-4055-b8d8-32d4d6d1daac	⚙
252	10.0.0.182	Завершено	83 24 4		Benchmarks\WS2019-Member\ALT-X-WS2019-Member-xccdf.xml WS2019_WS1809	⚙

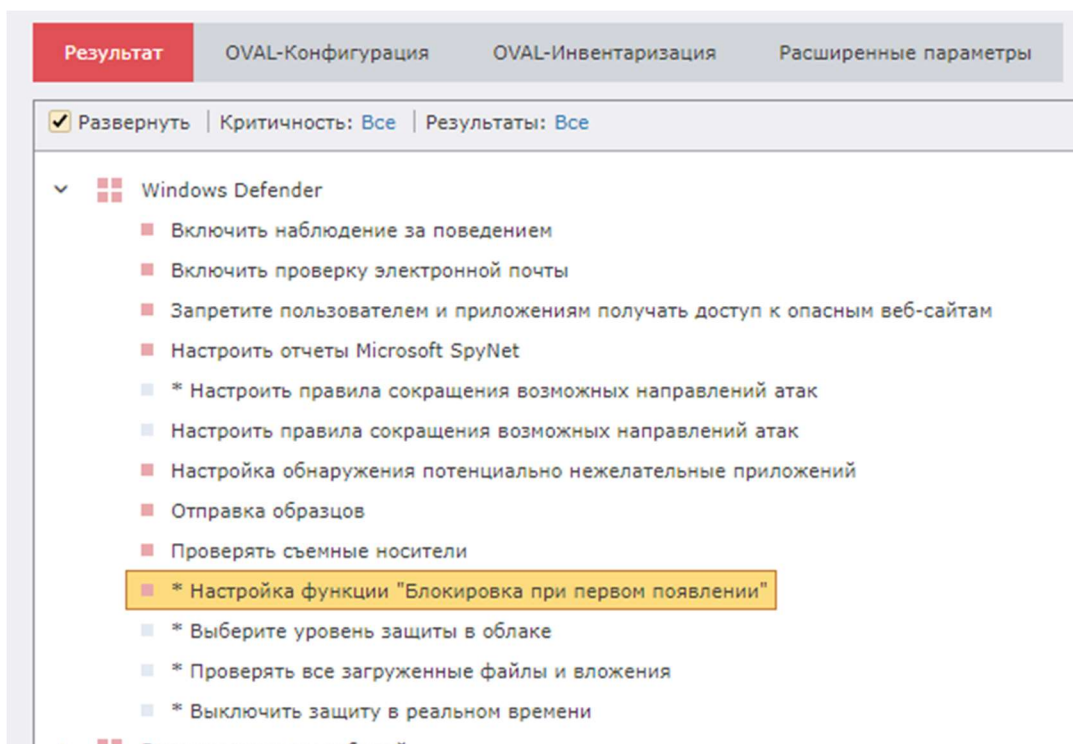
Нажмем ⚙ → **Создать контроль**;



После этого данный результат сканирования будет помечен как **Эталон** (📊)

252	10.0.0.182	Завершено	83 24 4	📊	test-conf_2
-----	------------	-----------	---------	---	-------------

Исправим несоответствие некоторых правил конфигурации на хосте.



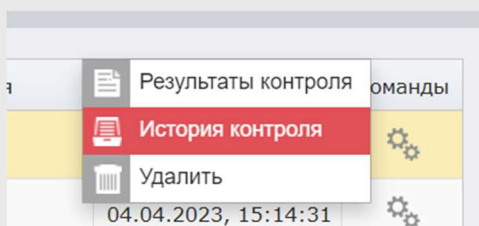
Проведем повторное сканирование. Видим, что в столбце К (Статус или результат Контроля) появился знак несоответствия с эталоном.

№	Хост	Статус	Риск	К	Задание
259	10.0.0.182	Завершено	79 22 4	✗	test-conf_2

Перейдем в **Контроль** → откроем результат, нажав **Несоответствие** в столбце **Статус**.

ИСТОРИЯ КОНТРОЛЬ ОТЧЁТЫ ПОЛЬЗОВАТЕЛИ					
№	Хост	Статус	Задание	№ сканирования	Команды
23	10.0.0.182	Несоответствие	test-conf_2	252	⚙️

Чтобы посмотреть историю контроля, нажмите ⚙️ → **История контроля**.



Видим, что было изменено 6 правил.

Эталонное значение – значение, которое было в эталонном результате сканирования.

Категория	Подкатегория	Имя	Статус	Эталонное значение	Текущее значение
	Windows Defender	Включить наблюдение за поведением	Изменён	Несоответствие	Соответствие
	Windows Defender	Запретите пользователям и приложениям получать доступ к опасным веб-сайтам	Изменён	Несоответствие	Соответствие
	Windows Defender	Настройка обнаружения потенциально нежелательных приложений	Изменён	Несоответствие	Соответствие
	Windows Defender	Настройка функции "Блокировка при первом появлении"	Изменён	Несоответствие	Соответствие
	Windows Defender	Отправка образцов	Изменён	Несоответствие	Соответствие
	Windows Defender	Проверять съемные носители	Изменён	Несоответствие	Соответствие
Page 1 of 1 (6 items) Группировать по статусу Группировать по категории Группировать по подкатегории Всего: 6 Эталон Результат Открыть отчёт					

Чтобы посмотреть эталонный результат сканирования или текущий, нажмите **Эталон** или **Результат** соответственно.

5.5 Профили сканирования Altxmar

RedCheck позволяет сохранять настройки для Altxmar и затем использовать их в других заданиях типа Аудит в режиме «Пентест».

Создать профиль сканирования можно на вкладке **Типы сканирования** при создании задания **Аудит в режиме «Пентест»**.

Шаг 1. Укажите новые значения для нужных параметров;

Шаг 2. Нажмите **Сохранить как** → укажите имя → **Сохранить**;

Профиль будет создан.

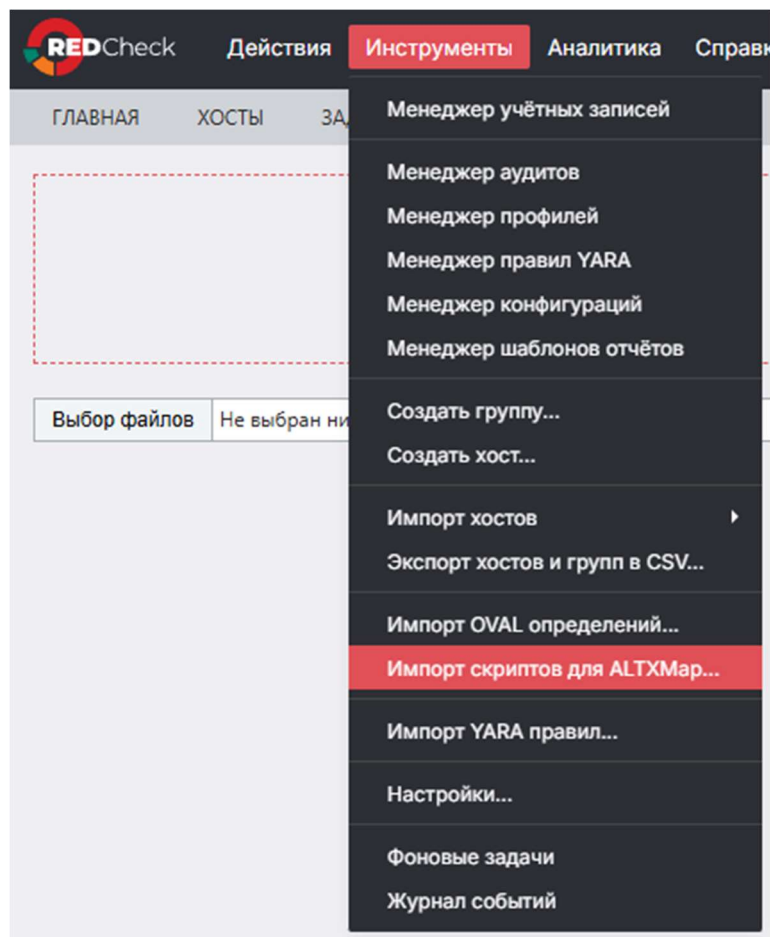
Чтобы внести изменения в профиль, нажмите на **Сохранить**;

Для удаления профиля нажмите **Удалить**;

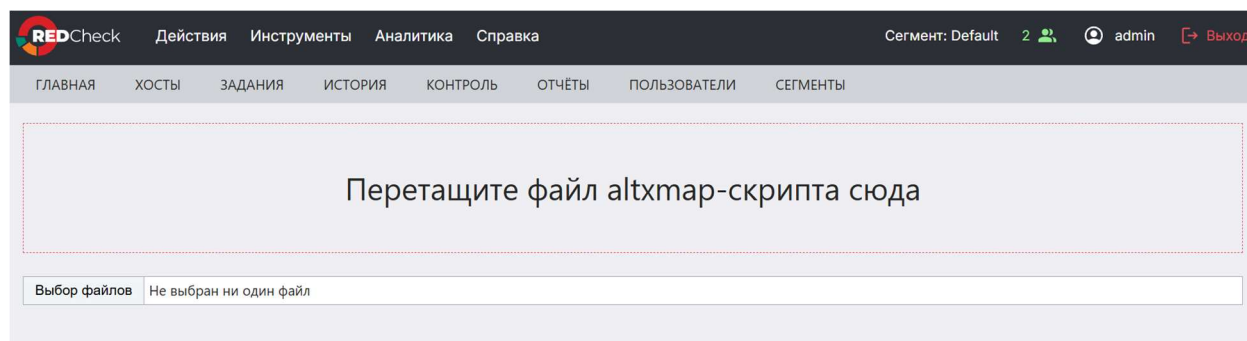
5.6 Импорт скриптов для пентеста

RedCheck позволяет импортировать NSE и Lua-скрипты для использования их в задании **Аудит в режиме «Пентест»**.

Нажмите **Инструменты** → **Импорт скриптов для ALTXMap**;



Перетащите файл скрипта в поле или выберите файлы, нажав **Выбор файлов**.



Требования к скрипту:

- Скрипт должен быть написан на языке Lua и иметь расширение .lua или .nse
- Скрипт должен иметь два блока: метаданные и тело скрипта

Требования к метаданным:

- Метаданные должны быть закомментированы («--»)
- В качестве уникального идентификатора уязвимости может быть указан либо общеизвестный идентификатор CVE, либо собственный
 - Существующий CVE указывается в следующем формате: CVE-XXXX-X..X, где второй блок состоит из 4 цифр, а третий блок – от 1 до 11 цифр. Общая длина поля 20 символов
 - Общая длина уникального пользовательского идентификатора не должна превышать 12 символов

Метаданные содержат следующие поля:

Параметр	Принимаемые значения	Обязательный	Описание параметра
is_tcp	true / false	Да	Запускать или нет скрипт на TCP портах
is_udp	true / false	Да	Запускать или нет скрипт на UDP портах
port_conditions	Цифры (номера портов, разделенные запятой)	Нет*	Номера портов, на которых будет запускаться скрипт
service_conditions	Название служб (как они отображаются в результатах сканирования на вкладке «Инвентаризация»), через запятую	Нет*	Список служб, для которых будет запускаться скрипт

is_web	true / false	Нет	Параметр, указывающий, что скрипт будет запущен только при установке флага «WEB уязвимости». Значение по умолчанию: false
vuln_id	Цифры, буквы, символ «-»	Да	Уникальный идентификатор уязвимости: либо CVE, либо собственный
description	Текстовое поле	Да, если vuln_id пользовательский	Описание уязвимости
cvss_score	Десятичное число от 0 до 10 с одним знаком после запятой. В качестве разделителя целой и дробной части может быть точка или запятая	Да, если vuln_id пользовательский	Числовая оценка критичности уязвимости
cvss_vector	Строка, максимальная длина 128 символов	Нет	Вектор CVSS, выводится в описании уязвимости
cwe	Строка, максимальная длина 20 символов	Нет	Идентификатор CWE, выводится в описании уязвимости

* – должен быть заполнен хотя бы один из параметров: *port_conditions* или *service_conditions*

Требования к телу скрипта:

В скрипте обязательно должна быть функция action, которая будет являться точкой входа

В результате скрипт должен возвращать таблицу следующего вида:

local result = {vuln = {title = 'Details', state = 'NOT VULNERABLE'}}, где

- title – детальная информация о найденной уязвимости. Выводится в результатах сканирования в поле «Детализация»
- state – результат сканирования. Может принимать следующие значения:
 - NOT VULNERABLE – уязвимость не найдена
 - VULNERABLE – уязвимость найдена (точность высокая**)
 - LIKELY VULNERABLE – уязвимость возможна (точность средняя**)
 - VULNERABLE (Exploitable) – уязвимость найдена и эксплуатируется (точность высокая**)

*** точность – уровень достоверности определения уязвимости*

Пример скрипта:

Lua

```
-- Метаданные скрипта для интеграции в RedCheck
-- is_web = 'true', --скрипты категории WEB запускаются, если в
интерфейсе установлен флаг "WEB уязвимости"
-- is_tcp = 'true', --запускать ли скрипт на TCP портах
-- is_udp = 'false', --запускать ли скрипт на UDP портах
-- port_conditions = '80, 443, 8080, 8443 ,9000', --номера портов,
на которых будет запускаться скрипт
-- service_conditions = 'http,https', --список служб, для которых
будет запускаться скрипт
-- vuln_id = 'lua-12345'
-- description = '43353636', --описание уязвимости
-- cvss_score = '3.2', --cvss score
-- cvss_vector = 'CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H', --
вектор CVSS
-- cwe = 'CWE-787', -- идентификатор CWE
-----
-- Исполняемое тело скрипта
action = function ()

    local result = {vuln = {title = 'Details', state = 'NOT
VULNERABLE'}} --таблица с информацией об уязвимости

    -- основной код, включающий критерии детекта уязвимости.
    if (true) then
        result.vuln.state = 'VULNERABLE'
    end

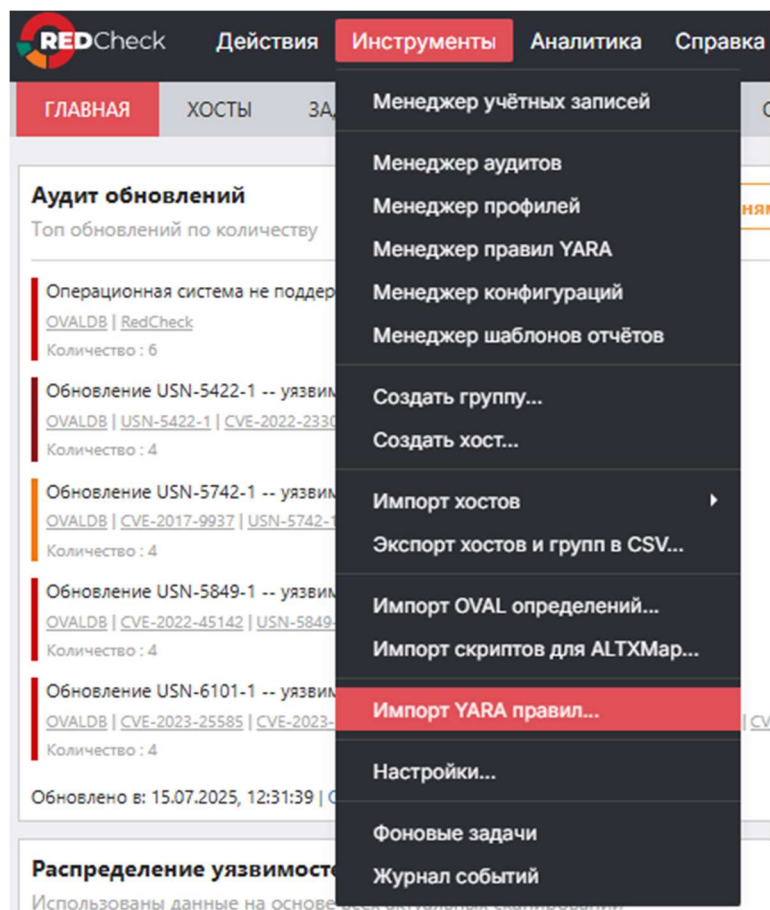
    -- возвращаем таблицу
```

```
    return result  
end
```

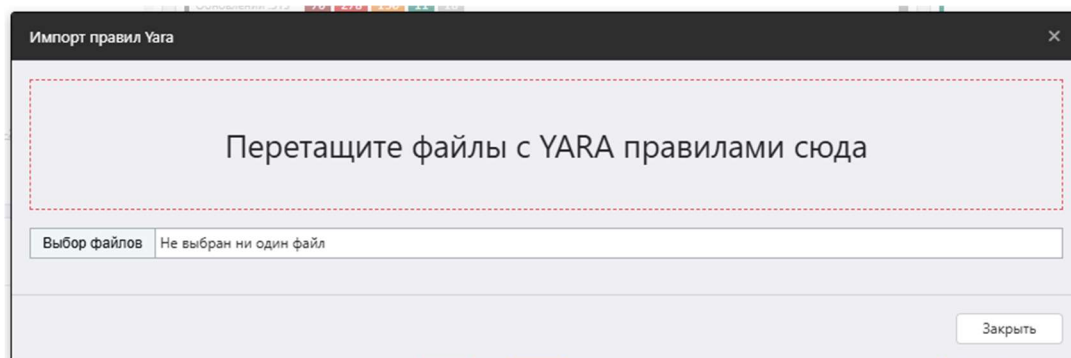
5.7 Импорт YARA-правил

RedCheck позволяет импортировать пользовательские сигнатуры для сканирования YARA правил.

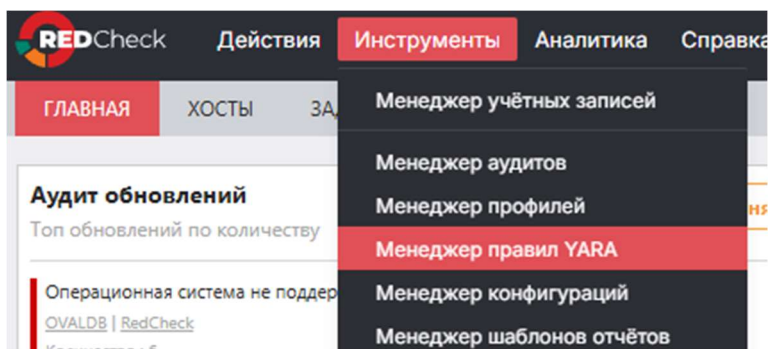
Шаг 1. Нажмите **Инструменты** → **Импорт YARA правил**



Шаг 2. Перенесите файл с YARA правилами в поле или нажмите **Выбор файлов**;



Для просмотра импортированных YARA правил нажмите **Инструменты** → **Менеджер правил YARA**;



В таблице отображается информация об имеющихся в БД правилах.

Правила YARA				
Просмотр правил YARA				
Тип				
Backdoor				
Идентификатор				
Описание				
☐ Тип авторства: ALTX				
☐ Тип авторства: USER				
Идентификатор	Описание	Тип авторства	Тип	
> Ext_Linux_Exaramel_Struct	Beginning of type _type struct for some of the most important structs	USER	Backdoor	
> Ext_Linux_Exaramel_TaskNames	Name of the tasks received by the CC	USER	Backdoor	
> Ext_Linux_Exaramel_SocketPath	Path of the unix socket created to prevent concurrent executions	USER	Backdoor	
> Ext_Linux_Exaramel_ConfigurationFileCiphertext	Content of the configuration file (encrypted with key odhyrfcnfkdbalt, sample e1ff72[...])	USER	Backdoor	
> Ext_Linux_Exaramel_ConfigurationFilePlaintext	Detects contents of the configuration file used by Exaramel (plaintext)	USER	Backdoor	
> Ext_Linux_Exaramel_ConfigurationNameEncrypted	Detects the specific name of the configuration file in Exaramel malware as seen in sample e1ff72[...]	USER	Backdoor	

6 Результаты сканирований

Результат сканирования каждого хоста является отдельной записью в базе данных RedCheck. Каждая запись может состоять из списка OVAL-определений (уязвимостей, найденных на хосте; установленного ПО и ОС), отображать соответствие конфигурации, предоставлять информацию о зафиксированных файлах и ключах реестра и другой информации.

Уровни критичности

OVAL-определения подразделяются по уровню критичности:

Недоступно – вендор не предоставил значение уровня критичности;

Информация – OVAL-определение для инвентаря (ПО).

Низкий, **Средний**, **Высокий**, **Критический** – стандартные определения уровня критичности.

Расчет критичности производится с учетом базовых и временных метрик CVSS на основании данных вендора сканера, вендора ПО, экспертных организаций;

Статус сканирования

Сканирование хоста может завершиться с одним из трех статусов:

Завершено – выполнение аудита для указанного хоста завершено успешно;

Ошибка – при сканировании произошла ошибка;

Хост недоступен – служба сканирования не смогла подключиться указанным транспортом к хосту;

Просмотр результатов сканирований

Необходимая роль: любая

Чтобы посмотреть результаты сканирований, перейдите в **История**.

ГЛАВНАЯ

ХОСТЫ

ЗАДАНИЯ

ИСТОРИЯ

КОНТРОЛЬ

ОТЧЕТЫ

ПОЛЬЗОВАТЕЛИ

Сканирования

Интервал

Все

Начало

Завершение

07 апреля, 2023

Быстрый фильтр

Хост

Группа

Задание

Тип сканирования

Ссылки (CVE, экспл.)

Статус

Сканирования

Все

Актуальные

Применить фильтр

№	ID	Хост	Статус	Риск	К	Задание	А	Профиль	Е	Начало	Завершение	Время	Примечание	Команды
259		10.0.0.182	Завершено	70 20 10	⊖	test-conf_2	[-]	Аудит конфигураций	171	06.04.2023, 16:29:58	06.04.2023, 16:30:03	00:00:05	Benchmarks\WS2019-Member-vccdf.xml WS2019_WS1809	ⓘ
258		10.0.0.182	Завершено	40 20 10		тестовое задание конфигурация	[-]	Аудит конфигураций	170	06.04.2023, 12:18:29	06.04.2023, 12:18:34	00:00:04	Benchmarks\WS2019-Member-vccdf.xml F40d217c-a777-4035-8688-32466d1dae	ⓘ
257		10.0.0.183	Завершено			тестовое задание	[-]	Аудит уязвимостей	169	06.04.2023, 10:18:37	06.04.2023, 10:19:08	00:00:30		ⓘ
256		10.0.0.182	Завершено			тестовое задание	[-]	Аудит уязвимостей	169	06.04.2023, 10:18:37	06.04.2023, 10:19:01	00:00:24		ⓘ
255		10.0.0.182	Ошибки			test_1	[-]	Аудит конфигураций	168	05.04.2023, 12:28:25	05.04.2023, 12:28:25	00:00:00	Benchmarks\ALTIX Win8\ALTIX-Win8-vccdf.xml	ⓘ
254		10.0.0.182	Ошибки			test-fix	[-]	Фиксация	160	05.04.2023, 10:59:27	05.04.2023, 10:59:30	00:00:02		ⓘ
253		10.0.0.183	Ошибки			test-fix	[-]	Фиксация	160	05.04.2023, 10:59:27	05.04.2023, 10:59:28	00:00:01		ⓘ
252		10.0.0.182	Завершено	70 20 10	⊖	test-conf_2	[-]	Аудит конфигураций	158	05.04.2023, 10:45:52	05.04.2023, 10:45:58	00:00:05	Benchmarks\WS2019-Member-vccdf.xml WS2019_WS1809	ⓘ
251		10.0.0.183	Завершено	70 20 10 10		test-vulns	[-]	Аудит уязвимостей	154	05.04.2023, 10:20:49	05.04.2023, 10:29:17	00:08:27		ⓘ
250		10.0.0.183	Завершено			test-invent	[-]	Инвентаризация	155	05.04.2023, 10:24:52	05.04.2023, 10:28:24	00:03:31		ⓘ
249		10.0.0.183	Завершено	70		test-upd	[-]	Аудит обновлений	153	05.04.2023, 10:19:08	05.04.2023, 10:22:31	00:03:22		ⓘ
248		10.0.0.182	Завершено	20 10 10		test-upd	[-]	Аудит обновлений	152	05.04.2023, 10:12:56	05.04.2023, 10:16:16	00:03:19		ⓘ
247		10.0.0.183	Хост недоступен			test-upd	[-]	Аудит обновлений	152	05.04.2023, 10:12:56	05.04.2023, 10:12:58	00:00:02		ⓘ
246		10.0.0.182	Завершено	70 20 10 10		test-vulns	[-]	Аудит уязвимостей	151	05.04.2023, 09:51:46	05.04.2023, 10:00:14	00:08:27		ⓘ
245		10.0.0.173	Завершено	70		astra-postgre	[-]	Аудит PostgreSQL	150	04.04.2023, 16:56:47	04.04.2023, 16:58:20	00:01:33		ⓘ
244		10.0.0.182	Завершено	70 20 10		microsoft-conf	[-]	Аудит конфигураций	149	04.04.2023, 15:14:28	04.04.2023, 15:14:30	00:00:01	Benchmarks\WS2019-Domain\ALTIX-WS2019-Domain-vccdf.xml WS2019_WS1809	ⓘ
243		10.0.0.182	Завершено	70 20 10	⊕	microsoft-conf	[-]	Аудит конфигураций	149	04.04.2023, 15:14:25	04.04.2023, 15:14:28	00:00:02	Benchmarks\WS2019-Member-vccdf.xml WS2019_WS1809	ⓘ

20

Page 1 of 7 (131 items)

1234567

Всего: 131

В таблице будет содержаться следующая информация:

- ID задания;
- Хост – IP-адрес или имя хоста;
- Статус – показатель, уведомляющий о результате, с которым завершилось сканирование;
- Риск – количество уязвимостей, найденных на хосте;
- К – статус или результат контроля;
- Задание – название задания;
- А – использовался или нет Agent RedCheck для сканирования хоста;
- Профиль – тип задания;
- Е – идентификатор выполненного задания;
- Время начала и окончания сканирования, общее время выполнения задания.
- Приложение – название конфигурации, которая использовалась при сканировании (Аудит конфигураций, Аудит СУБД).

Для просмотра информации о результате сканирования хоста нажмите на значение в столбце **Статус**, или  → **Результат сканирования**.

Каждый тип задания предоставляет отличную от других информацию о выполненном сканировании.

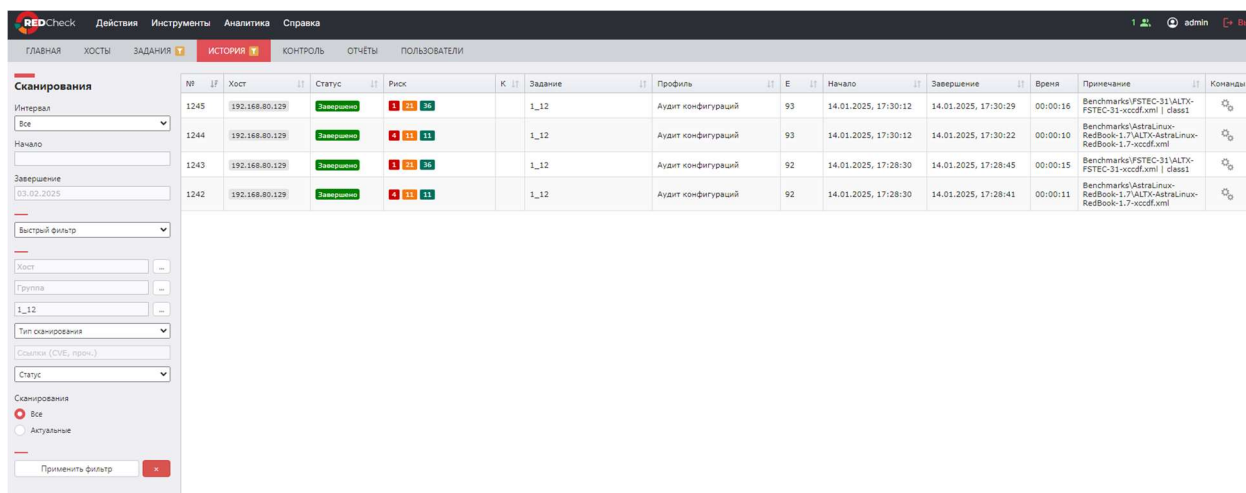
- [6.1 Аудит уязвимостей](#)
- [6.2 Аудит обновлений](#)
- [6.3 Аудит конфигураций](#)

- [6.4 Инвентаризация](#)
- [6.5 Фиксация \(контроль целостности\)](#)
- [6.6 Аудит уязвимостей АСУ ТП](#)
- [6.7 Аудит СУБД](#)
- [6.8 Проверка доступности](#)
- [6.9 Обнаружение хостов](#)
- [6.10 Аудит в режиме "Пентест"](#)
- [6.11 Аудит уязвимостей Docker / Инвентаризация Docker](#)
- [6.12 Статистика выполненных заданий](#)

Просмотр истории сканирования определенного задания

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Шаг 1. Перейдите в **Задания** →  → **История**;



ИД	Хост	Статус	Риск	К	Задание	Профили	Е	Начало	Завершение	Время	Примечание	Команды
1245	192.168.80.129	Завершено	4 11 11	1	1_12	Аудит конфигураций	93	14.01.2025, 17:30:12	14.01.2025, 17:30:29	00:00:16	Benchmarks/PSTEC-31/ALT-X-FSTEC-31-ccodf.xml class1	
1244	192.168.80.129	Завершено	4 11 11	1	1_12	Аудит конфигураций	93	14.01.2025, 17:30:12	14.01.2025, 17:30:22	00:00:10	Benchmarks/AstraLinux-RedBook-1.7/ALT-X-AstraLinux-RedBook-1.7-ccodf.xml	
1243	192.168.80.129	Завершено	4 11 11	1	1_12	Аудит конфигураций	92	14.01.2025, 17:28:30	14.01.2025, 17:28:45	00:00:15	Benchmarks/PSTEC-31/ALT-X-FSTEC-31-ccodf.xml class1	
1242	192.168.80.129	Завершено	4 11 11	1	1_12	Аудит конфигураций	92	14.01.2025, 17:28:30	14.01.2025, 17:28:41	00:00:11	Benchmarks/AstraLinux-RedBook-1.7/ALT-X-AstraLinux-RedBook-1.7-ccodf.xml	

Шаг 2. Нажмите  → **Результаты сканирования**;

6.1 Аудит уязвимостей

Описание результатов сканирования задания Аудит уязвимостей.

Результат

Вкладка отображает список найденных на хосте уязвимостей. Каждую уязвимость можно раскрыть и просмотреть дополнительную информацию.

ГЛАВНАЯ ХОСТЫ ЗАДАНИЯ ИСТОРИЯ КОНТРОЛЬ ОТЧЁТЫ ПОЛЬЗОВАТЕЛИ					
Аудит уязвимостей					
№ сканирования 1238		Поиск по ссылкам...		☒ Критичность	
Хост 192.168.80.129				☒ Критический	☒ Высокий
Задание vuln				☒ Низкий	☒ Средний
Профиль Аудит уязвимостей				☒ Информация	☒ Недоступно
Запуск 09.12.2024 17:33:52					
Завершение сканирования 09.12.2024 17:35:03					
ID выполнения задания 87					
Создать быстрый отчёт					
ALTIX ID	Риск	IF	Название		
> 425334	Критический		Доступ за пределами памяти в WebHID в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)		
> 429555	Критический		Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.137 (CVE-2023-2136)		
> 469988	Критический		Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 119.0.6045.199 (CVE-2023-6345)		
> 476873	Критический		Потеря значимости целочисленных значений в WebUI в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0808)		
> 476877	Критический		Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0806)		
> 476878	Критический		Ошибка реализации в Downloads в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0805)		
> 480024	Критический		Уязвимость, связанная с подменой типа в V8 в Google Chrome, Chromium и Chromium-gost для Linux до 122.0.6261.94 (CVE-2024-1938)		
> 486944	Критический		Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2883)		
> 486947	Критический		Уязвимость, связанная с подменой типа в WebAssembly в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2887)		
> 410680	Критический		Astra Linux -- уязвимость в python2.7 (CVE-2015-20107)		
> 413840	Критический		Astra Linux -- уязвимость в linux, linux-5.10 (CVE-2022-20368)		
> 413887	Критический		Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-2602)		
> 414003	Критический		Astra Linux -- уязвимость в linux-5.10, linux-5.15, linux (CVE-2022-39842)		
> 429217	Критический		Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)		
> 435717	Критический		Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2023-26545)		
> 435719	Критический		Astra Linux -- уязвимость в linux-5.15, linux, linux-5.10 (CVE-2023-26607)		
> 443348	Критический		Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)		
> 443421	Критический		Astra Linux -- уязвимость в chromium (CVE-2023-1528)		
> 443422	Критический		Astra Linux -- уязвимость в chromium (CVE-2023-1529)		
> 443443	Критический		Astra Linux -- уязвимость в chromium (CVE-2023-2033)		

Дополнительная информация состоит из:

- ALTIX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Детализация – файлы, подверженные уязвимости;

6.2 Аудит обновлений

Описание результатов сканирования задания Аудит обновлений.

Результат

Вкладка отображает список неустановленных на хосте обновлений. Каждую уязвимость можно раскрыть и просмотреть дополнительную информацию.

ГЛАВНАЯХОСТЫЗАДАНИЯИСТОРИЯКОНТРОЛЬОТЧЁТЫПОЛЬЗОВАТЕЛИ									
Аудит уязвимостей									
№ сканирования 1238		Результат		Расширенные параметры					
Хост 192.168.80.129		Поиск по ссылкам...		Критичность					
Задание vuln				КритическийВысокийСреднийНедоступно					
Профиль Аудит уязвимостей				Критический					
Запуск 09.12.2024 17:33:52				Критический					
Завершение сканирования 09.12.2024 17:35:03				Критический					
ID выполнения задания 87				Критический					
Создать быстрый отчёт									
		ALTIX ID	Риск	ИФ	ИТ	Название			
		> 425334	Критический			Доступ за пределами памяти в WebUI в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)			
		> 429555	Критический			Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.137 (CVE-2023-2136)			
		> 469988	Критический			Целочисленное переполнение в Skia в Google Chrome, Chromium и Chromium-gost для Linux до 119.0.6045.199 (CVE-2023-6345)			
		> 476873	Критический			Потеря значимости целочисленных значений в WebUI в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0808)			
		> 476877	Критический			Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0806)			
		> 476878	Критический			Ошибка реализации в Downloads в Google Chrome, Chromium и Chromium-gost для Linux до 121.0.6167.85 (CVE-2024-0805)			
		> 480024	Критический			Уязвимость, связанная с подменой типа в VB в Google Chrome, Chromium и Chromium-gost для Linux до 122.0.6261.94 (CVE-2024-1938)			
		> 486944	Критический			Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2883)			
		> 486947	Критический			Уязвимость, связанная с подменой типа в WebAssembly в Google Chrome, Chromium и Chromium-gost для Linux до 123.0.6312.86 (CVE-2024-2887)			
		> 410680	Критический			Astra Linux -- уязвимость в python2.7 (CVE-2015-20107)			
		> 413840	Критический			Astra Linux -- уязвимость в linux, linux-5.10 (CVE-2022-20368)			
		> 413887	Критический			Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-2602)			
		> 414003	Критический			Astra Linux -- уязвимость в linux-5.10, linux-5.15, linux (CVE-2022-39842)			
		> 429217	Критический			Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)			
		> 435717	Критический			Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2023-26545)			
		> 435719	Критический			Astra Linux -- уязвимость в linux-5.15, linux, linux-5.10 (CVE-2023-26607)			
		> 443348	Критический			Astra Linux -- уязвимость в thunderbird, firefox (CVE-2019-25136)			
		> 443421	Критический			Astra Linux -- уязвимость в chromium (CVE-2023-1528)			
		> 443422	Критический			Astra Linux -- уязвимость в chromium (CVE-2023-1529)			
		> 443443	Критический			Astra Linux -- уязвимость в chromium (CVE-2023-2033)			

Дополнительная информация состоит из:

- ALTIX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Продукты – название продукта;

▼330431

Критический

2020-07 Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64)

ALTIX ID

330431

Риск

Критический

OVAL

oval:ru.altix-soft.win:def:70334 (Версия 1)

Название

2020-07 Накопительный пакет для .NET Framework 3.5 и 4.8 для Windows Server 2019, Windows 10 для систем на базе 64-разрядных (x64) процессоров (KB4565632)

Описание

В программном продукте Microsoft обнаружена проблема безопасности, которая может повлиять на вашу систему.

Ссылки

VENDOR

windows10.0-kb4565632-x64-ndp48_dbab0773d0b336c20b095d9144120d487992066c.msu

MSWSUSID

acead73c-d39e-44a9-9adc-fb033898ee1b

MSWSUSID

45df7d20-5fd9-4aa0-8c1f-4010e30f3662

Microsoft

CVE-2020-1147

Microsoft

KB4565632

Продукты

Microsoft .NET Framework 3.5

Microsoft .NET Framework 4.8

Детализация

Показать собранные OVAL-элементы

(AV:N/AC:M/Au:N/C:P/I:P/A:P)

(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

NVD-CWE-Other

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.3 Аудит конфигураций

Описание результатов сканирования задания Аудит конфигураций.

Статус проверки правила

Соответствие – значение параметра на хосте соответствует эталонному значению в конфигурации;

Несоответствие – значение параметра на хосте не соответствует эталонному значению в конфигурации;

Ошибка – критическая ошибка при выполнении проверки. При возникновении обратитесь в службу тех. поддержки;

Не проверено – в конфигурации нет информации для правила (эталонного значения, исправления и т.д.);

Не выбрано – правило отключено в профиле конфигурации;

Неизвестно – ошибка при проверке правила. Убедитесь, что используемая для сканирования учетная запись обладает нужными правами, а примененные на хосте групповые политики позволяют проводить необходимые проверки;

Неприменимо – данное правило неприменимо для проверяемой платформы;

Результат

Вкладка содержит список проверенных правил конфигурации.

Аудит конфигураций

№ сканирования: 258

Хост: 10.0.0.182

Задание: тестовое задание конфигурации

Профиль: Аудит конфигураций

Запуск: 06.04.2023 12:18:29

Завершение сканирования: 06.04.2023 12:18:34

ID выполнения задания: 170

Создать быстрый отчет

Результат | OVAL-Конфигурация | Расширенные параметры

✓ Развернуть | Критичность: Все | Результаты: Все

- Windows Defender
 - * Включить наблюдение за поведением
 - Включить проверку электронной почты
 - Запретите пользователям и приложениям получать доступ к опасным веб-сайтам
 - Настроить отчеты Microsoft SpyNet
 - Настроить правила сокращения возможных направлений атак
 - Настроить правила сокращения возможных направлений атак
 - Настройка обнаружения потенциально нежелательных приложений
 - Отправка образцов
 - * Проверять съемные носители
 - Настройка функции "Блокировка при первом появлении"
 - Выберите уровень защиты в облаке
 - Проверять все загруженные файлы и вложения
 - Выключить защиту в реальном времени
- Ведение журнала событий
 - PNP-действие аудита
 - Аудит блокировки учетных записей
 - Аудит входа в систему
 - Аудит других системных событий
 - Аудит других событий входа и выхода

Всего уникальных правил: 162 | 44 Соответствие | 115 Несоответствие | 1 Ошибка | 2 Не выбрано

Конфигурация

Название: Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения – Microsoft

Версия: 7

Файл: Benchmarks\WS2019-Member\ALT-X-WS2019-Member-xccdf.xml

Платформа: Microsoft Windows Server 2019 (cpe:/o:microsoft:windows_server:2019)

Описание: Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения – Microsoft

Описание: Конфигурация предназначена для обеспечения безопасного функционирования ОС Microsoft Windows Server на основе Security Baseline – это группа рекомендуемых корпоративной Майкрософт параметров конфигурации, которая объясняет их влияние на безопасность. Эти параметры основаны на отзывах специалистов по обеспечению безопасности.

Правила входят в группы, которые обозначаются иконкой

Информация о группе

- Конфигурация – информация о конфигурации:
 - Версия конфигурации;
 - Путь к файлу конфигурации;
 - Платформы, для которых применима конфигурация. Платформа, установленная на хосте, отображается иконкой 
- Легенда – итоговый статус проверки и количественная статистика. Итоговый статус определяется следующим образом: если в группе есть хоть одно правило со статусом **Несоответствие**, то группа будет иметь такой же статус.
- Критичность – информация о уровнях критичности правил группы; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- Дополнительно – дополнительная информация о группе.

Конфигурация ▾

Название

Windows Server 2019 / Windows Server версия 1809 и выше – Настройки безопасности сервера общего назначения - Microsoft

Версия

7

Файл

Benchmarks\WS2019-Member\ALTX-WS2019-Member-xccdf.xml

Платформа

 Microsoft Windows Server 2019
(cpe:/o:microsoft:windows_server_2019)

 Microsoft Windows Server, version 1809
(cpe:/o:microsoft:windows_server:1809)

 Microsoft Windows Server, version 1903
(cpe:/o:microsoft:windows_server:1903)

 Microsoft Windows Server, version 1909
(cpe:/o:microsoft:windows_server:1909)

 Microsoft Windows Server, version 2004
(cpe:/o:microsoft:windows_server:2004)

 Microsoft Windows Server, version 20H2
(cpe:/o:microsoft:windows_server:20h2)

Легенда ▾

 **Несоответствие**

0

Соответствие

0

Не проверено

0

Информация

11

Несоответствие

2

Не выбрано

0

Исправлено

0

Ошибка

0

Неизвестно

0

Неприменимо

Критичность ▾

10

Высокий

3

Средний

0

Информация

0

Недоступно

0

Низкий

Дополнительно ▾

ID

Windows_Defender

Информация о правиле

 REDCheck

142

- Легенда – статус проверки;
- Правило – название правила;
- Статус правила – включено или нет правило в используемом профиле конфигурации;
 - Эталонное значение – значение из конфигурации, с которым происходит сравнение.
- Критичность – информация о уровне критичности правила; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- Ссылки – расположение параметра безопасности;
- Описание – описание правила;
- Фактическое значение – значение параметра, которое было обнаружено на хосте;
- Дополнительно – дополнительная информация о правиле.

Легенда ▼	
Несоответствие	
Правило ▼	
Включить проверку электронной почты	
Статус правила	Включено
Эталонное значение (из конфигурации)	0
Критичность ▼	
Средний	
Ссылки ▼	
Тип	GPO
Источник	Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Защитник Windows (Endpoint Protection)\Проверка
Описание ▼	
Эталонное значение: Включено Этот параметр политики позволяет настроить проверку электронной почты. Когда проверка электронной почты включена, модуль защиты анализирует почтовый ящик и файлы почты (тексты сообщений и вложения) в соответствии с их форматом. На данный момент поддерживается несколько форматов электронной почты, например pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac). Если вы включаете этот параметр политики, проверка электронной почты включена. Если вы отключаете или не настраиваете этот параметр политики, проверка электронной почты отключена.	
Дополнительно ▼	
ID	Turn_on_e-mail_scanning
OVAL ID	oval:ru.altx-soft.win:def:28384
OVAL URL	ALTX-WS2019-Member-oval.xml

OVAL-Конфигурация

Вкладка содержит детализацию проверок правил конфигурации.

Результат	ОVAL-Конфигурация	ОVAL-Инвентаризация	Расширенные параметры
Поиск по ссылкам...			
ALTIX ID	Название		
> 295427	PNP-действие аудита		
> 65433	Автоматически выполнить вход последнего текущего пользователя после инициированной системой перезагрузки		
> 46721	Аудит входа в систему		
> 46782	Блокировка страниц в памяти - Никто		
> 295443	Включение защиты от перезаписи обработчика структурных исключений (SEHOP)		
> 46842	Выполнение задач по обслуживанию томов - Администраторы		
> 46856	Доступ к диспетчеру учетных данных от имени доверенного вызывающего - Никто		
> 46860	Доступ к сети: разрешить трансляцию анонимного SID в имя		
> 46868	Загрузка и выгрузка драйверов устройств - Администраторы		
> 46884	Изменение параметров среды изготовителя - Администраторы		
> 46909	Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам		
> 46917	Контроль учетных записей: Все администраторы работают в режиме одобрения администратором		
> 46918	Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав		
> 46922	Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах		
> 46924	Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя		
> 46933	Максимальный срок действия пароля		
> 295429	Отключение протокола Windows SMB 1.0		
> 295428	Отключение протокола Windows SMB 1.0		
> 46981	Отладка программ - Администраторы		
> 46987	Пароль должен отвечать требованиям сложности		

ОVAL-определение состоит из:

- ALTIX ID – внутренний идентификатор уязвимости;
- OVAL – ссылка на страницу уязвимости в OVALdb;

▼ 295427	PNP-действие аудита
ALTIX ID	295427
OVAL	oval:ru:altix-soft.win:def:29893 (Версия 1)
Название	PNP-действие аудита
Описание	Этот параметр политики позволяет выполнять аудит, когда самонастраивающееся устройство обнаруживает внешнее устройство.
Детализация	
Показать собранные OVAL-элементы	

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.4 Инвентаризация

Описание результата сканирования задания Инвентаризация.

Инвентаризация

Вкладка содержит информацию о аппаратном и программном обеспечении, обнаруженном на хосте.

Инвентаризация	
Расширенные параметры	
- Аппаратное обеспечение - Список CPU - CPU - Материнская плата - BIOS - Слоты памяти - Видеоконтроллеры - Сетевые адаптеры - Физические диски - Оптические приводы - Логические диски - Программное обеспечение - Операционная система - Установленное ПО - Дополнительные компоненты - Компоненты сервера	Имя
	Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz
	Описание
	Intel64 Family 6 Model 165 Stepping 5
	Производитель
	GenuineIntel
	Максимальная частота
	2904
	ID устройства
	CPU0

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.5 Фиксация (контроль целостности)

Описание результата сканирования задания Фиксация.

Файловая система

Вкладка отображает список зафиксированных файлов на хосте.

Файловая система		
Результат сканирования		
Путь к файлу	Контрольная сумма	
> D:\Temp\some\packedges.txt	9131096C	
> D:\Temp\some\server.py	FB00170B	

Каждая запись содержит следующую информацию о файле:

- Путь к файлу;
- Контрольная сумма.

Путь к файлу	Контрольная сумма
▼ D:\Temp\some\packedges.txt	9131096C
Путь к файлу D:\Temp\some\packedges.txt Контрольная сумма 9131096CB5910A88240477BAF0EA3899	

Реестр

Вкладка отображает зафиксированные ключи и параметры реестра.

Реестр		
Результат сканирования		
Ключ	Параметр	Значение
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ASP.NET Core\Shared Framework	InstallDir	C:\Program Files\dotnet\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX		1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MinFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MaxFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	D3D12MinFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	D3D12MaxFeatureLevel	49408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	MaxDedicatedVideoMemory	134217728
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastSeen	133198781070805030
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	InstalledVersion	00-00-00-09-00-00-00-00
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	Version	4.09.00.0904
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastUpdaterStartTimestamp	UTC.2022-09-21.13:39:04
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectX	LastUpdaterStartHresult	0

6.6 Аудит уязвимостей АСУ ТП

Описание результатов сканирования задания Аудит уязвимостей АСУ ТП.

Результат

Вкладка отображает список найденных на хосте уязвимостей. Каждую уязвимость можно раскрыть и просмотреть дополнительную информацию.

Результат

Инвентаризация

Расширенные параметры

Поиск по ссылкам...

Критичность

Критический

Высокий

Средний

Низкий

Информация

Недоступн

ALTX ID	Риск	И	Название
> 308542	Высокий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8565)
> 308543	Высокий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2018-11455)
> 308536	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4530)
> 308537	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4531)
> 308538	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4532)
> 308540	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8563)
> 308541	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2016-8564)
> 308544	Средний		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2018-11456)
> 281419	Средний		Уязвимость средств разработки Siemens Simatic STEP7 и пакета программ Simatic PCS7 (CVE-2012-3015)
> 281496	Средний		Уязвимость программного обеспечения Siemens SIMATIC STEP 7 (CVE-2015-1594)
> 308539	Низкий		Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2012-4691)

20

Page 1 of 1 (12 items)

1

Группировать по риску

Информация об уязвимости состоит из:

- ALTx ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Исправление – способ устранения уязвимости;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Детализация – файлы, подверженные уязвимости;
- Продукты – название ПО.

▼	281418	Высокий	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4529)
ALTx ID	281418		
Риск	Высокий		
OVAL	oval:ru.altx-soft.scada:def:1 (Версия 5)		
Название	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) (CVE-2011-4529)		
Описание	Уязвимость менеджера лицензий Siemens Automation License Manager (ALM) связана с некорректной проверкой входных данных при Siemens ALM до версии 5.1 sp1 upd1 включительно		
Исправление	Обновление ПО Siemens ALM до версии 5.1 sp1 upd2.		
Ссылки	CVE	CVE-2011-4529	{AV:N/AC:L/Au:N/C:P/I:P/A:P} CWE-119
Продукты	Siemens ALM		
Показать собранные OVAL-элементы			

Инвентаризация

Вкладка содержит информацию о контроллерах, протоколах или ПО, обнаруженном на сканируемом хосте.

Информация о найденном ПО включает в себя:

- Риск – уровень критичности;
- Продукты – CPE найденного модуля;
- Порт – порт и протокол определения;
- Модуль – название найденного продукта.

Результат							Инвентаризация	Расширенные параметры	
	Порт	Протокол	Риск	SCADA CPE	Модуль	Дополнительно			
▼	4410	tcp	Высокий	cpe:2.3:a:siemens:automation_license_manager:5.1:::~::~	Simatic ALM				
Риск Высокий Продукты cpe:2.3:a:siemens:automation_license_manager:5.1:::~::~ Порт 4410 (tcp) Модуль Simatic ALM									
►	4410	tcp	Информация	cpe:2.3:a:siemens:simatic_step_7:5.5::~::~	Simatic ALM				

Page 1 of 1 (2 items) < 1 >

Всего: 2

Справа отображается список с информацией о найденном ПО (раскрывающийся список с необнаруженных ПО будет пустой).

Simatic ALM ▼	
Инфо	4410 tcp - сервис Simatic Automation License Management, версия 5.1. Установленное ПО (лицензии): STEP 7, версия 5.5 STEP 7 Professional Edition 2010, версия 5.5
ПО	Siemens ALM 5.1 Simatic STEP 7 5.5
Simatic S7 ▼	
Sicam PAS IPC ▼	
Citect SCADA ▼	
Modbus TCP/UDP ▼	
Profinet IO ▼	
ArchestrA Logger ▼	
BACnet/IP ▼	
Ethernet/IP ▼	
GenBroker (GENESIS32/64) ▼	
Schneider Electric IGSS ▼	
FINS ▼	
ProConOS ▼	

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.7 Проверка доступности

Описание результата сканирования задания Проверка доступности. Данный тип задания также предоставляет [дополнительную статистику](#).

Результат

Вкладка содержит список хостов, проверенных на доступность.

Запись о хосте содержит следующую информацию:

- Транспорт (Тип пинга) – способ подключения к хосту, который был выбран для проверки;
- Доступность – статус проверки:

Доступен – выполнение проверки для указанного хоста завершено успешно;

Ошибка – при проверке произошла ошибка;

Хост недоступен – служба сканирования не смогла подключиться указанным транспортом к хосту;

- Учетная запись для сканирования, с помощью которой выполнялось задание;
- Сообщение об ошибке;
- Версия агента RedCheck, если он установлен на хосте.

Результат				
	Транспорт	Доступность	Учётная запись	Сообщение
▼ Wmi		Доступен	windows	
Тип пинга WMI				
Учётная запись windows (Windows)				

6.8 Обнаружение хостов

Описание результата сканирования задания Обнаружение хостов. Данный тип задания также предоставляет [дополнительную статистику](#), по результатам которой можно [добавить обнаруженные хосты](#) в базу данных.

Обнаружение хостов

Вкладка содержит записи хостов, обнаруженных во время выполнения задания.

Обнаружение хостов							
Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Порты	Агент
ARP	10.0.0.3	dc3.altx-soft.ru			cpe:/o:microsoft:windows	139,445,3389,8732	Да
ARP	10.0.0.5				cpe:/o:microsoft:windows	3389	Нет
ARP	10.0.0.4	dc2.altx-soft.ru			cpe:/o:microsoft:windows	139,445,3389,8732	Да
ARP	10.0.0.14						Нет
ARP	10.0.0.120				cpe:/h:hp:integrated_lights-out cpe:/h:hp:integrated_lights-out:1.30	22,80,443	Нет
ARP	10.0.0.121				cpe:/o:vmware:esxi_server	22,80,443	Нет
ARP	10.0.0.124						Нет
ARP	10.0.0.12						Нет
ARP	10.0.0.133				cpe:/o:microsoft:windows	445,3389,8732	Да
ARP	10.0.0.135				cpe:/o:microsoft:windows	80,3389	Нет
ARP	10.0.0.137				cpe:/o:qnap:qts	22,80,443	Нет
ARP	10.0.0.141					80	Нет
ARP	10.0.0.150						Нет
ARP	10.0.0.151	ASSRVTS.altx-soft.ru		ASSRVTS	cpe:/o:microsoft:windows_10:1809 cpe:/o:microsoft:windows_server_2019	80,139,445,3389	Нет
ARP	10.0.0.161	DPBOOKPRO					Нет
ARP	10.0.0.167	zvs-pc.altx-soft.ru		ZVS-PC	cpe:/o:microsoft:windows_7:sp1 cpe:/o:microsoft:windows_server_2008:r2:sp1	139,443,445,3389	Нет
ARP	10.0.0.178				cpe:/o:canonical:ubuntu_linux	22	Нет
ARP	10.0.0.130				cpe:/o:unix:unix	22,80,443	Нет
ARP	10.0.0.136	PC-18.altx-soft.ru			cpe:/o:microsoft:windows	139,443,445,3389,8732	Да

20

Page 1 of 3 (44 items)

1

2

3

Всего: 44

Информация о хосте состоит из:

- Способа обнаружения (ARP, TCP, UDP и т.д.);
- IP-адреса, DNS-имени, FQDN, NetBIOS;
- Тип ОС – CPE операционной системы;
- Порты – открытые порты на хосте;
- Агент – статус наличия агента RedCheck на хосте.

6.9 Аудит в режиме "Пентест"

Описание результата сканирования задания Аудит в режиме «Пентест».

Поиск уязвимостей

Вкладка отображает список найденных методом черного ящика уязвимостей на хосте.

Аудит в режиме "Пентест"

№ сканирования
149

Хост
10.0.0.150

Задание
п

Профиль
Аудит в режиме "Пентест"

Запуск
07.02.2023 14:13:25

Завершение сканирования
07.02.2023 14:19:22

ID выполнения задания
82

Создать быстрый отчет

Поиск уязвимостей	Инвентаризация	Информация о хосте	Расширенные параметры		
CVE	Порт	IF	Риск	Точность	Описание
> ALTIXID-416982	8080		Высокий	Высокая	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. отвечает на HTTP-запросы с произвольным значением заголовка Host.
> ALTIXID-404180	8080		Высокий	Средняя	Обнаружена DDoS уязвимость (Slowloris) веб-серверов, атака осуществляется на основании большого количества открытых соединений путем непрерывной отправки незавершенных HTTP-запросов
> CVE-2010-0097	53		Низкий	Высокая	ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta не проверяет должным образом DNSSEC (1) NSEC и (2) NSEC3 записи, которые позволяют удаленным злоумышленникам добавить флаг аутентифицированных данных (AD) к поддельному ответу NXDOMAIN для существующего домена.
> CVE-2010-0290	53		Низкий	Средняя	Неизвестная уязвимость в ISC BIND от 9.0.x до 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta, с включенной проверкой DNSSEC и отключенной проверкой (CD), позволяет удаленным злоумышленникам проводить атаки с отравлением кеша DNS, получая рекурсивный клиентский запрос и отправляя ответ, содержащий (1) записи CNAME или (2) DNAME, которые не имеют предполагаемой проверки перед кэшированием, также известная как ошибка 20737.
> CVE-2010-0382	53		Низкий	Средняя	ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P5, 9.5 до 9.5.2-P2, 9.6 до 9.6.1-P3 и 9.7.0 beta обрабатывает out-of-bailiwick данные, сопровождающие безопасный ответ без повторной выборки из исходного источника, что позволяет удаленным злоумышленникам оказывать неопределенное воздействие с помощью созданного ответа, также известная как ошибка 20819.
> CVE-2009-4022	53		Низкий	Средняя	Неуказанная уязвимость в ISC BIND с 9.0.x по 9.3.x, 9.4 до 9.4.3-P4, 9.5 до 9.5.2-P1, 9.6 до 9.6.1-P2 и 9.7 beta до 9.7.0b3, с включенной проверкой DNSSEC и отключенной проверкой (CD), позволяет удаленным злоумышленникам проводить атаки с отравлением DNS-кеша, получая рекурсивный клиентский запрос и отправляя ответ, содержащий дополнительный раздел с созданными данными, которые не обрабатываются должным образом при обработке ответа "однозначно с запросом записей DNSSEC (DO)".
> CVE-2012-5166	53		Средний	Высокая	ISC BIND 9.x до 9.7.6-P4, 9.8.x до 9.8.3-P4, 9.9.x до 9.9.1-P4 и 9.4-ESV до 9.6-ESV- R7-P4 позволяет удаленным злоумышленникам вызвать отказ в обслуживании (с именем daemon Hang) с помощью неопределенных комбинаций записей ресурсов.
> CVE-2015-5477	53		Средний	Высокая	named в ISC BIND 9.x до 9.9.7-P2 и 9.10.x до 9.10.2-P3, позволяет удаленным злоумышленникам вызывать отказ в обслуживании через запросы TKEY.
> CVE-2016-1285	53		Средний	Высокая	Уязвимость компонента named сервера DNS BIND существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании (появление окна с ошибкой "Assertion failure", завершение работы демона) при помощи специально сформированного пакета в mdc.
20 Page 1 of 3 (56 items) 1 2 3 Группировать по точности Группировать по риску Группировать по продуктам Группировать по порту Всего: 56					

Информация об уязвимости состоит из:

- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- CVE – ссылка-идентификатор CVE;
- Продукты – CPE продукта;
- CWE – ссылка-идентификатор CWE;
- CVSSv2 – показатели метрики в CVSS v2;
- Порт – на котором работает продукт;
- Точность – достоверность определенной уязвимости;
- Детализация – версия продукта.

▼	ALTIXID-416982	8080	Высокий	Высокая	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. значением заголовка Host.
Описание	Веб сервер подвержен семейству атак Anti DNS pinning (DNS rebinding), т.к. отвечает на HTTP-запросы с произвольным значением заголовка Host.				
Риск	Высокий				
CVE	ALTIXID-416982				
Продукты	cpe:/a::zyxel_zywall_usg210_http_config:				
Порт	8080 (tcp)				
Точность	Высокая				
Детализация	domain rebinding iatptfyn.com (http-dns-rebinding)				

Инвентаризация

Вкладка отображает список служб, которые работают на открытых портах.

Поиск уязвимостей Инвентаризация Информация о хосте Расширенные параметры							
	Порт	↓↑	Протокол	Риск	Продукт	Служба	Дополн
>	21		tcp	Высокий		ftp	
>	53		tcp	Высокий	cpe:/a:isc:bind:9.6-ESV-R11	domain	
>	8080		tcp	Высокий	cpe:/a::zyxel_zywall_usg210_http_config:	http	

Информация о службе включает в себя:

- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- Продукты – CPE продукта;
- Порт – порт, на котором работает служба;
- Служба – название службы;

▼	53	tcp	Высокий	cpe:/a:isc:bind:9.6-ESV-R11
Риск Высокий				
Продукты cpe:/a:isc:bind:9.6-ESV-R11				
Порт 53 tcp				
Метод определения Probed				
Служба domain				
Дополнительно				

Количество информации может изменяться в зависимости от службы.

Информация о хосте

Вкладка содержит информацию о хосте, которую определил RedCheck методом черного ящика.

Поиск уязвимостей Инвентаризация Информация о хосте Расширенные параметры			
Общая информация			
		DNS-имя	ydv-pc.altx-soft.ru
		Домен	altx-soft.ru
		NetBIOS-имя	YDV-PC
		Домен NetBIOS	ALT-X-SOFT
		ipv4Address	
OS Windows build 10.0.20348			
		Имя	Windows build 10.0.20348
		cpe	cpe:/o:microsoft:windows

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.10 Аудит уязвимостей Docker / Инвентаризация Docker

Docker-аудит уязвимостей

Описание результата сканирования задания Аудит Docker.

Информация по образам

Вкладка содержит информацию о найденных образах на сканируемом хосте:

- Название репозитория;
- Количество уязвимостей;
- Количество контейнеров;
- Тег образа;
- Размер образа;
- ОС и архитектура;
- Дата создания образа;
- Имя образа (хеш).

829

Хост

proxy

Задание

proxy

Профиль

Docker аудит уязвимостей

Запуск

10.02.2023 15:00:29

Завершение сканирования

10.02.2023 15:02:27

ID выполнения задания

429

Создать быстрый отчет

Информация по образам

Результат

Расширенные параметры

2

КОЛИЧЕСТВО ОБРАЗОВ

2

КОЛИЧЕСТВО УЯЗВИМЫХ ОБРАЗОВ

2

КОЛИЧЕСТВО ОБРАЗОВ С УЯЗВИМОСТЯМИ ВЫСОКОГО РИСКА

☐ Только образы с высоким или критичным риском

Поиск по репозиториям...

Поиск по тегам...

ID	И	Репозиторий	Уязвимости	Количество контейнеров	Теги	Размер	Операционная система	Архитектура	Дата создания	Имя обр
1		postgres	1 10 5	0		latest	374MB	Debian GNU/Linux 11 (bullseye)	amd64	18.11.2021, 00:55:48 sha256:1
2		nginx	1 25 47 7 1	1		latest	141MB	Debian GNU/Linux 11 (bullseye)	amd64	17.11.2021, 13:38:14 sha256:1

Результат

Вкладка содержит информацию об уязвимостях, найденных в образах, состоит из:

- ALTX ID – внутренний идентификатор уязвимости;
- Риск – уровень критичности; ([Сведения об интегральной оценке по базовым метрикам CVSS](#))
- OVAL – ссылка на страницу уязвимости в OVALdb;
- Ссылки – страницы уязвимости в различных базах данных уязвимостей;
- Продукты – ПО, подверженное уязвимости;
- Детализация – файлы, подверженные уязвимости;

Содержит информацию о найденном ПО в сканируемом Docker-образе.

Инвентаризация Docker

Подробные параметры сканирования.

Хост
192.168.10.203

Задание
Job_4025

Профиль
Инвентаризация Docker

Запуск
28.07.2021 15:17:09

Завершение
28.07.2021 15:18:22

Учётная запись
root (Ssh)

№ сканирования
6047

№ выполнения задания
2104

GUID
5cf75a37-6d2b-40af-9a83-c69d23dc3dde

Инвентаризация

Программное обеспечение

Docker

Плагины тома

Сетевые плагины

Плагины журнала

Опции безопасности

Репозитории

alpine

Образы

sha256:cc0abc535e36a7ede7

Слои

2

1

bkimminich/juice-shop

browserless/chrome

centos

docker-chrome

goharbor/clair-adapter-photon

goharbor/clair-photon

goharbor/harbor-core

goharbor/harbor-db

goharbor/harbor-jobservice

goharbor/harbor-log

goharbor/harbor-portal

goharbor/harbor-registryctl

goharbor/nginx-photon

goharbor/prepare

goharbor/redis-photon

Имя
1

ID
<missing>

Размер
5.59MB

Дата создания
12/24/2019 22:20:12

Команда
/bin/sh -c #(nop) ADD file:36fdc8cb08228a87093fb227736f4ce1d4d6c15366326dea541fbbd863976ee5 in /

Статистика

[Просмотр статистики по результату сканирования](#)

Статистика содержит итоговую информацию о количестве образов, а также контейнеров и уязвимостей, найденных в образах.

Статистика

Статистические данные по выбранному выполнению задания.

Задание
проху

Профиль
Docker аудит уязвимостей

Запуск
10.02.2023 15:00:29

Завершение
10.02.2023 15:02:27

№ выполнения задания
429

Экспорт в CSV

1
ХОСТЫ

1
ДОСТУПНО

1
КОЛИЧЕСТВО ХОСТОВ С
ОБРАЗАМИ

1
КОЛИЧЕСТВО ХОСТОВ С
УЯЗВИМЫМИ ОБРАЗАМИ

2
КОЛИЧЕСТВО ОБРАЗОВ

2
КОЛИЧЕСТВО ОБРАЗОВ С
УЯЗВИМОСТЯМИ ВЫСОКОГО
РИСКА

1
КОНТЕЙНЕРЫ

Группы: Все хосты

Статус: Все статусы

Хост	Результат	Уязвимостей всего	Количество образов	Количество образов с уязвимостями высокого риска	Количество контейнеров
проху	Завершено	21 35 155 7 1	2	2	1

6.11 Сканирование YARA правил

Описание результатов сканирования задания Сканирование YARA правил.

Результат

Вкладка отображает список правил с положительным срабатыванием на хосте.

Сканирование YARA

№ сканирования
4559

Хост
debkvm-astra176

Задание
9830_1

Профиль
Сканирование YARA

Запуск
06.06.2025 13:27:59

Завершение сканирования
06.06.2025 13:28:43

ID выполнения задания
920

Создать быстрый отчёт

Результат

Расширенные параметры

Поиск по правилу...

Тип

Все типы

Правило	Тип	Количество срабатываний
> eicar_substring_test_3	Unknown	1
> eicar_substring_test_2	Unknown	1
> eicar_substring_test	Unknown	1

Каждое правило можно раскрыть и просмотреть дополнительную информацию, которая состоит из:

- Yara Rule Id – идентификатор сигнатуры;
- Описание – описание сигнатуры;
- Тип – тип сигнатуры;
- Количество срабатываний – в скольких файлах сигнатура отработала положительно;
- Детализация – файлы, в которых сигнатура отработала положительно;

Правило	
▼	eicar_substring_test_3
Yara Rule Id	eicar_substring_test_3 [REDACTED]
Описание	Standard AV test, checking for an EICAR substring
Тип	Unknown
Количество срабатываний	1
Детализация	Цель /home/test/yara_eicar_test.txt

Расширенные параметры

Вкладка содержит дополнительную информацию о задании и хосте:

Хост
Задание
Профиль
Запуск
Завершение сканирования
Длительность
ID сканирования
ID выполнения задания
DNS-имя
FQDN
NetBIOS-имя
IPv4 1
MAC 1

6.12 Статистика выполненных заданий

Необходимая роль: RedCheck_Admins / RedCheck_Adminis

Некоторые типы заданий имеют дополнительную информацию (статистику), которую можно экспортировать в CSV-файл. Такая возможность есть для:

- Обнаружение хостов;
- Проверка доступности;

Перейдите в **Задания** → нажмите  → **Свойства** → **Дополнительно** → **Статистика**;

Статистика «Обнаружение хостов»

Запись об обнаруженном хосте содержит следующую информацию:

- Способ обнаружения – протокол, которым удалось обнаружить хост;
- IP-адрес;
- DNS-имя;
- FQDN-имя;
- NetBIOS-имя;
- Операционная система – CPE хоста;
- Агент – установлен Агент сканирования на хосте или нет;

Статистика Статистические данные по выбранному выполнению задания. Задание 80-я Профиль Обнаружение хостов Запуск 17.09.2024 11:42:23 Завершение 17.09.2024 11:42:54 № выполнения задания 3 Экспорт в CSV	4 ВСЕГО ХОСТОВ ОБНАРУЖЕНО	2 ИЗ НИХ НЕТ СООТВЕТСТВИЯ В СИСТЕМЕ	Соответствие в БД: ☒ Есть ☐ Нет Операционная система: ☐ Windows ☐ Linux ☐ ОС не определена ☐ Другое Поиск по IP хоста: Поиск по имени хоста, DNS, FQDN, NetBIOS:				
	Способ обнаружения	IP	DNS	FQDN	NetBIOS	Операционная система	Агент
	ARP	192.168.80.129					Нет
	ARP	192.168.80.254					Нет
	ARP	192.168.80.1					Нет
	LOCALHOST	192.168.80.8					Нет

Статистика «Проверки доступности»

Запись о доступном хосте содержит следующую информацию:

- IP-адрес (имя) хоста;
- Проверяемый транспорт;

- Статус проверки;
- Учетная запись для сканирования, которая использовалась при сканировании;
- Сообщение об ошибке;
- Версия агента RedCheck, если он установлен на хосте.

Статистика Статистические данные по выбранному выполнению задания. Задание: проверка доступности linux Профиль: Проверка доступности Запуск: 13.02.2023 14:52:54 Завершение: 13.02.2023 14:53:16 № выполнения задания: 93 Экспорт в CSV	1 доступно		1 недоступно			
	☒ Доступен		☒ Недоступен			
	Все хосты		Все учетные записи		Все версии агентов	
	Поиск					
	Хост	Транспорт	Доступность	Учетная запись	Сообщение	Версия агента
	10.0.0.173	Ssh	Доступен	linux		
	192.168.1.4	Ssh	Недоступен	linux	Ошибка установления соединения.	

Статистика «Аудит в режиме Пентест»

Запись об уязвимостях, найденных на хосте, содержит следующую информацию:

- IP-адрес (имя) хоста;
- Статус аудита;
- Количество найденных уязвимостей;
- Количество и значения открытых портов на хосте;

Статистика

Статистические данные по выбранному выполнению задания.

Задание 1_18

Профиль Аудит в режиме "Пентест"

Запуск 27.01.2025 11:53:29

Завершение 27.01.2025 11:54:36

№ выполнения задания 100

Экспорт в CSV

1	1	4	1	1
хосты	количество доступных хостов	количество открытых портов	количество уязвимых хостов	количество хостов с уязвимостями с высоким и критичным риском
Группы: Все хосты Статус: Все статусы Критичность: Все Порты: Поиск по портам				
Хост	Статус	Риск	Количество открытых портов	Открытые порты
192.168.80.129	Завершено	5 45 59 3	4	TCP: 22, 139, 445, 5432

Экспорт в CSV

В окне статистики нажмите **Экспорт в CSV**;

Статистика

Статистические данные по выбранному выполнению задания.

Задание
проверка доступности_2

Профиль
Проверка доступности

Запуск
30.01.2023 11:30:49

Завершение
30.01.2023 11:30:50

№ выполнения задания
44

Экспорт в CSV

0

доступно

1

недоступно

☐ До

Все хос

	Хост	Транспорт
>	192.168.80.129	Winrm

1. Обнаружение хостов. Файл будет иметь название **HostDiscovery-N-statistics.csv**, где N – ID итерации запуска.

Структура CSV файла

Ip	IP-адрес хоста
Reason	Протокол, которым удалось обнаружить хост
Dns	DNS-имя хоста
Fqdn	FQDN-имя хоста
NetBIOS	NetBIOS-имя хоста
Os	CPE
OpenPorts	Открытые порты, по которым удалось обнаружить хост
IsAgent	Установлен агент на хосте или нет
IdExistingHost	ID хоста, существующего в базе данных RedCheck

Пример:

Код
Ip, Reason, Dns, Fqdn, NetBIOS, Os, OpenPorts, IsAgent, IdExistingHost
192.168.80.129, ARP, , , , , False, 67
192.168.80.8, LOCALHOST, , , , , False, 69

2. Проверка доступности. Файл будет иметь название **Ping-N-statistics.csv**, где N – ID итерации запуска.

Структура CSV файла

ConnectionAddress	IP-адрес или DNS-имя хоста
PingType	Проверяемый протокол
Result	Результат проверки: False или True
Credential	Название учетной записи, используемой для проверки
Message	Сообщение об ошибке. если хост недоступен
AgentVersion	Версия Агента сканирования, если он установлен на хосте

Пример:

Код

```
ConnectionAddress,PingType,Result,Credential,Message,AgentVersion
192.168.80.210,Winrm,False,winrm
test,HTTPConnectionPool(host='192.168.100.210', port=5985): Max
retries exceeded with url: /wsman (Caused by
NewConnectionError('<urllib3.connection.HTTPConnection object at
0x701ef5a13550>: Failed to establish a new connection: [Errno 111]
Connection refused')),
```

7 Отчеты

RedCheck обладает инструментом создания отчетов. Отчет – файл с информацией о проведенном сканировании. В отчет могут входить результаты сканирования множества хостов одновременно. Возможность использовать профили аудитов ([5.1 Профили аудитов](#)) позволяет выбирать / исключать из результатов сканирования конкретные OVAL-определения.

RedCheck предлагает пять форматов отчета: html, pdf, mht, csv, xml.

Если необходимо автоматически доставлять отчеты после завершения сканирований, [настройте сервис доставки отчетов](#).

Типы отчетов

В Системе есть две разновидности отчетов: простой и дифференциальный.

- Простой – это собранные в один документ результаты сканирований по указанным хостам ([7.1 Создание простого отчета](#));
- Дифференциальный – документ, в котором происходит сравнение двух результатов сканирования между собой. Отчет будет состоять из разницы между результатами сканирования ([7.2 Создание дифференциального отчета](#)).

Пример создания простого отчета

Раскроем **Действия** → **Создать отчет**;

Укажем следующие настройки для отчета:

- Тип – Простой;
- Отчет – Обновления, т. е. отчет для задания Аудит обновлений.
- Выбор данных – по заданию, т.е. отчет по результатам сканирования одного задания.

Настройки

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон

Нет

Имя отчёта

отчет обновление

Тип

Простой

Отчёт

Обновления

Выбор данных

По заданию

Описание

Выберем задание → **Вперед;**

Настройки Задания

Задания

№ п/п	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
96	test-upd	05.04.2023, 10:19:08	05.04.2023, 10:22:31	00:00:22	2	2
65	my-comp-update	03.02.2023, 16:53:05	03.02.2023, 16:54:23	00:00:17	2	2

20

Page 1 of 1 (2 items)

1

Всего: 2

Назад Вперед

Выберем результат сканирования → **Вперед;**

Настройки Задания Результаты сканирования

Результаты сканирования

№ п/п	Задание	Начало	Завершение	Всего	Успешно
153	test-upd	05.04.2023, 10:19:08	05.04.2023, 10:22:31	1	1
152	test-upd	05.04.2023, 10:12:56	05.04.2023, 10:16:16	2	1

20

Page 1 of 1 (2 items)

1

Всего: 2

Назад Вперед

Добавим хосты. В данном случае только один хост, так как второй был недоступен в момент выполнения задания → **Вперед;**

Настройки Задания Результаты сканирования **Хосты**

Выбранные хосты

ID	IP / DNS	Описание	CPE
47	10.0.0.182		cpe:/o:microsoft:windows_server_2019

Добавить хосты

Выбрано: 1

Выбранные группы

ID	Имя	Описание
----	-----	----------

Нет данных для отображения

Добавить группы

Выбрано: 0

☐ Выбрать все

Назад Вперед

Укажем следующие настройки фильтрации результатов сканирования: исключим из отчета OVAL-определения с уровнем критичности Недоступно и без CVSS.

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

☒ Критический ☒ Высокий ☒ Средний
☒ Низкий ☒ Недоступно

Cvss: от до

☒ Включать уязвимости без CVSS

Наличие в любой из баз данных

☐ NVD ☐ ФСТЭК ☐ НКЦКИ

Дополнительно

☐ Наличие эксплойта
☐ Эксплуатация по сети (удалённое использование)

Оставим стандартные настройки содержимого отчета → **Создать;**

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Диаграмма распределения уязвимостей по уровням риска
- ☒ Таблица распределения уязвимостей по хостам
- ☒ Таблица распределения уязвимостей по продуктам
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список уязвимостей

Выберите, как следует сгруппировать найденные уязвимости

- ☒ По хостам
- ☐ По продуктам
- ☐ По уровням риска

Дождемся окончания процесса создания отчета.

Создание отчёта

Создание отчёта ...

Операция может занять довольно длительное время.

отчёт создан

Заккрыть

Перейдем в **Отчеты** → выберем html формат.

ГЛАВНАЯ ХОСТЫ ЗАДАНИЯ ИСТОРИЯ КОНТРОЛЬ **ОТЧЕТЫ** ПОЛЬЗОВАТЕЛИ

Отчёты

Интервал
Сегодня

Начиная с

Заканчивая

Имя и описание

Тип отчёта

Тип данных

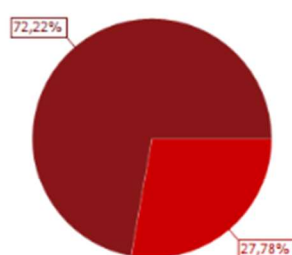
Применить фильтр

№	Тип	Имя	Тип данных	Создан	Статус	Описание	Команды
55	Простой	отчет обновление	Обновления	10.04.2023, 16:00:25	html pdf mht csv xml		

Отчет имеет следующий вид.

	ОТЧЁТ
№ отчёта	4a161f62-cb43-4df7-804c-96adcbd22ac6
Профиль	Обновления
Задание	test-upd
Начало/завершение сканирования	05.04.2023 10:12:56 / 05.04.2023 10:16:16
Формирование отчёта	10.04.2023 16:00:25
Имя	отчет обновление
Хосты [1]	10.0.0.182

Диаграмма распределения обновлений по уровням риска



Риск	Количество
Критический	26
Высокий	10
Средний	0
Низкий	0
Всего	36

Фильтрация результатов сканирования	
Уровни риска	Критический, Высокий, Средний, Низкий
CVSSv3, от	0
CVSSv3, до	10
CVSSv2 (при отсутствии CVSSv3), от	0
CVSSv2 (при отсутствии CVSSv3), до	10
Включать обновления без CVSS	Нет

Таблица распределения обновлений по хостам

Хост / Риск	Критический	Высокий	Средний	Низкий	Всего
10.0.0.182	26	10	0	0	36
Всего	26	10	0	0	36

1

Более подробное описание создания отчета находится в разделе [7.1 Создание простого отчета](#).

7.1 Создание простого отчета

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы создать простой отчет, выполните следующие шаги.

Шаг 1. Раскройте **Действия** → **Создать отчет**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

Настройки

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон: Нет

Имя отчёта:

Тип: Простой

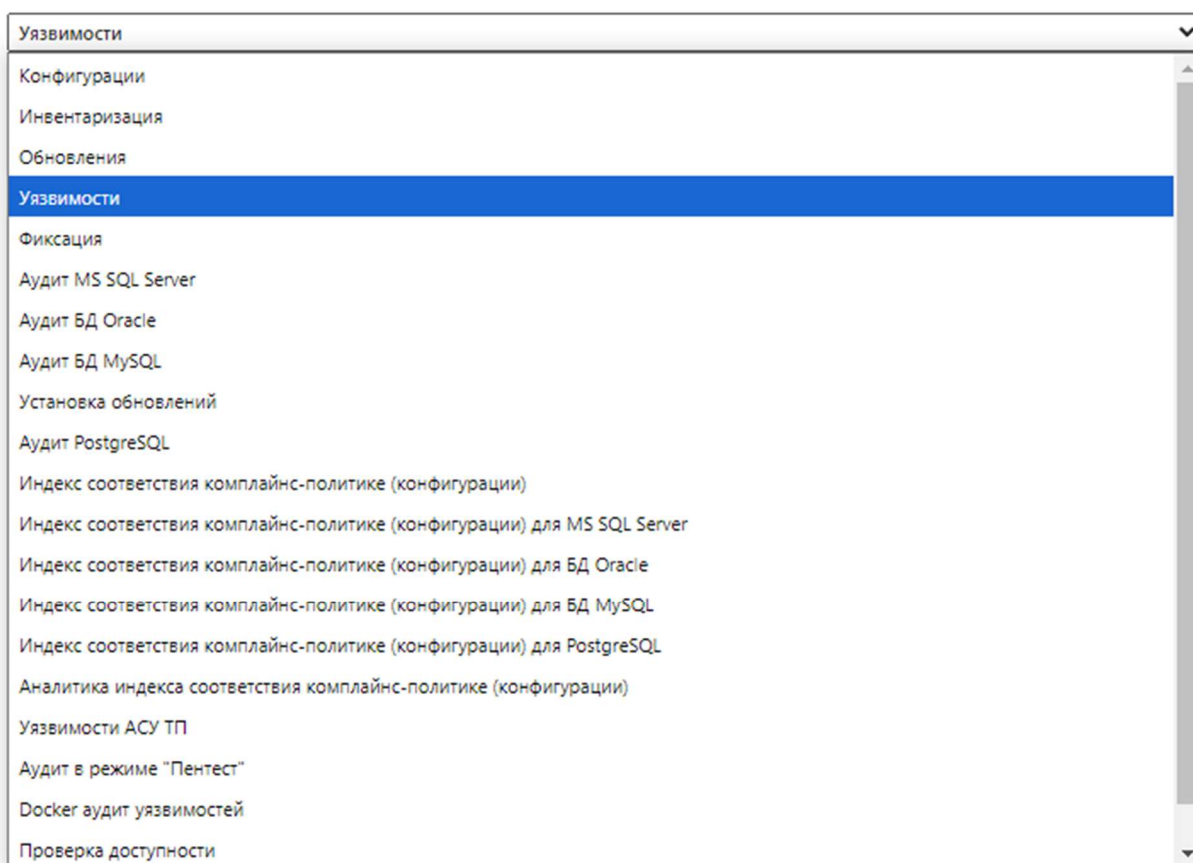
Отчёт: Конфигурации

Выбор данных: По заданию

Описание:

Вперёд

Параметр **Отчет** – тип данных, из которых будет создаваться отчет. В зависимости от выбранного значения последовательность создания отчета может измениться из-за дополнительных параметров;



Параметр **Выбор данных:**

[По заданию](#): отчет по одному результату сканирования выбранного задания для нескольких хостов;

[По хостам \(актуальные сканирования\)](#): отчет по актуальным результатам сканирования выбранных заданий для указанных хостов;

[По единичному хосту \(с выбором сканирования\)](#): отчет по одному результату сканирования для одного хоста;

Выбор данных: По заданию

Шаг 3. Выберите задание, по результатам которого будет строиться отчет
→ **Вперед:**

Настройки Задания						
Задания						
№	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
78	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	00:00:03	2	2
69	уязвимости	27.01.2023, 10:37:32	27.01.2023, 10:41:23	00:00:50	1	1

20 Page 1 of 1 (2 items) 1 Всего: 2

Назад Вперед

Шаг 4. Выберите результат сканирования, по которому будет строиться отчет
→ **Вперед:**

Настройки Задания Результаты сканирования					
Результаты сканирования					
№	Имя	Начало	Завершение	Всего	Успешно
27	уязвимости	27.01.2023, 10:37:32	27.01.2023, 10:41:23	1	1

20 Page 1 of 1 (1 items) 1 Всего: 1

Назад Вперед

Шаг 5. Добавьте hosts (**Добавить hosts**) / группы (**Добавить группы**) из результата сканирования, которые хотите видеть в отчете → **Вперед:**

Настройки Задания Результаты сканирования Хосты				
Выбранные хосты				
ID	IP / DNS	Описание	CPE	
17	ydv-pc.altx-soft.ru		cpe:/o:microsoft:windows_server_2022	

Добавить hosts Выбрано: 1

Выбранные группы		
ID	Имя	Описание
Нет данных для отображения		

Добавить группы Выбрано: 0 ☐ Выбрать все

Назад Вперед

Шаг 6. Укажите дополнительные настройки для отчета ([7.1.1 Настройки для разных типов заданий](#))

Выбор данных: По хостам

Шаг 3. Добавьте хосты (**Добавить хосты**) / группы (**Добавить группы**), которые хотите видеть в отчете → **Вперед:**

Настройки **Хосты**

Выбранные хосты

ID	IP / DNS	Описание	CPE
Нет данных для отображения			

Добавить хосты

Выбрано: 0

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Добавить группы

Выбрано: 0

☐ Выбрать все

Назад Вперед

Шаг 4. Выберите задания, которые хотите видеть в отчете, или воспользуйтесь фильтром по дате запуска → **Вперед:**

Настройки **Хосты** **Задания**

Задания

Дата запуска, от

01 февраля, 2023

☒ Использовать все задания, выполнявшиеся в течение выбранного периода

№	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
78	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	00:00:03	2	2

Шаг 5. Укажите дополнительные настройки для отчета ([7.1.1 Настройки для разных типов заданий](#))

Выбор данных: По единичному хосту

Шаг 3. Добавьте хост (**Добавить хосты**), который хотите видеть в отчете → **Вперед:**

Настройки Задания Результаты сканирования **Хосты**

Выбранные хосты

ID	IP / DNS	Описание	CPE
Нет данных для отображения			

Добавить хосты

Выбрано: 0

Выбранные группы

ID	Имя	Описание
Нет данных для отображения		

Добавить группы

Выбрано: 0

☐ Выбрать все

Назад Вперед

Шаг 4. Выберите результат сканирования → **Вперед:**

Настройки	Хосты	Результаты сканирования
Результаты сканирования		
№	Задание	Начало
93	уязвимости_1	01.02.2023, 10:23:00
92	уязвимости_1	30.01.2023, 17:09:46
28	уязвимости	27.01.2023, 10:37:32

Шаг 5. Укажите дополнительные настройки для отчета ([7.1.1 Настройки для разных типов заданий](#))

7.1.1 Настройки для разных типов задания

Содержание

- [Конфигурации](#)
- [Инвентаризация](#)
- [Уязвимости / Уязвимости Docker](#)
- [Обновления](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Индекс соответствия комплайнс-политике \(конфигурации\)](#)
- [Аналитика индекса соответствия комплайнс-политике \(конфигурации\)](#)
- [Аудит в режиме «Пентест»](#)
- [Проверка доступности](#)
- [Обнаружение хостов](#)
- [Уязвимости АСУ ТП](#)

Конфигурации

Выберите конфигурации, сведения о которых хотите включить в отчет → **Вперед**:

Настройки Задания Результаты сканирования Хосты **Выполненные конфигурации**

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

- ▼ Astra Linux SE 1.7 – Настройки по руководству Red Book - РусБИТех
 - ☒ Профиль по умолчанию
- ▼ Astra Linux SE и CE / ALT / RED OS 7.3 – Аудит безопасности АСУ ТП - ФСТЭК №31
 - ☒ 1 класс защищенности

Укажите настройки содержимого отчета и фильтрации результатов → **Создать**:

Настройки Задания Результаты сканирования Хосты Выполненные конфигурации **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Сводная таблица результатов сканирования
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Фактические значения параметров
- ☒ Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

☒ Соответствие	☒ Несоответствие	☒ Ошибка
☒ Неизвестно	☒ Неприменимо	☒ Не проверено
☒ Не выбрано	☒ Информация	☒ Исправлено

Критичность правил

☒ Недоступно	☒ Информация	☒ Низкий
☒ Средний	☒ Высокий	

Дополнительно

☐ Отображать пустые группы в отчёте

Инвентаризация

Укажите настройки содержимого отчета → **Создать**:

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Профиль
- ☒ Результаты сканирования
- ☐ Описание хостов

Уязвимости / Уязвимости Docker

Укажите настройки для фильтрации результата сканирования → **Вперед**:

- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязвимости, CVSS для которых не было определено;
- Дополнительно:
 - Наличие эксплойта – OVAL-определение имеет эксплойт;
 - Эксплуатация по сети – эксплойт можно воспроизвести удаленно;

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

☒ Критический ☒ Высокий ☒ Средний

☒ Низкий ☒ Недоступно

Cvss: от до

☒ Включать уязвимости без CVSS

Наличие в любой из баз данных

☐ NVD ☐ ФСТЭК ☐ НКЦКИ

Дополнительно

☐ Наличие эксплойта

☐ Эксплуатация по сети (удалённое использование)

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

Укажите, что будет содержаться в отчете и варианты группировки уязвимостей
→ **Создать:**

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

☒ Заголовок отчёта

☒ Диаграмма распределения уязвимостей по уровням риска

☒ Таблица распределения уязвимостей по хостам

☒ Таблица распределения уязвимостей по продуктам

☒ Результаты сканирования

☐ Описание хостов

☒ Список уязвимостей

Выберите, как следует сгруппировать найденные уязвимости

☒ По хостам

☐ По продуктам

☐ По уровням риска

Обновления

Укажите настройки для фильтрации результата сканирования → **Вперед:**

- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязвимости, CVSS для которых не было определено;
- Дополнительно:
 - Наличие эксплойта – OVAL-определение имеет эксплойт;

- Эксплуатация по сети – эксплойт можно воспроизвести удаленно;

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

☒ Критический ☒ Высокий ☒ Средний

☒ Низкий ☒ Недоступно

Cvss: от до

☒ Включать обновления без CVSS

Наличие в любой из баз данных

☐ NVD ☐ ФСТЭК ☐ НКЦКИ

Дополнительно

☐ Наличие эксплойта

☐ Эксплуатация по сети (удалённое использование)

☐ Скрыть заменённые

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

Укажите, что будет содержаться в отчете и вариант группировки найденных обновлений → **Создать**:

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

☒ Заголовок отчёта

☒ Диаграмма распределения обновлений по уровням риска

☒ Таблица распределения обновлений по хостам

☒ Таблица распределения обновлений по продуктам

☒ Результаты сканирования

☐ Описание хостов

☒ Список обновлений

Выберите, как следует сгруппировать найденные обновления

☒ По хостам

☐ По продуктам

☐ По уровням риска

Фиксация

Укажите, что будет содержаться в отчете → **Создать**:

Настройки
Задания
Результаты сканирования
Хосты
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Настройки задания
- ☒ Результаты сканирования
- ☐ Описание хостов

Аудит СУБД

Выберите профиль конфигурации, проверку с которым хотите увидеть в отчете
→ **Вперед:**

Настройки
Задания
Результаты сканирования
Хосты
Выполненные конфигурации

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

PostgreSQL - Общие настройки безопасности СУБД - CIS

☒ Профиль по умолчанию

Укажите настройки содержимого отчета и фильтрации результатов → **Создать:**

Настройки
Задания
Результаты сканирования
Хосты
Выполненные конфигурации
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Сводная таблица результатов сканирования
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Фактические значения параметров
- ☒ Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

☒ Соответствие	☒ Несоответствие	☒ Ошибка
☒ Неизвестно	☒ Неприменимо	☒ Не проверено
☒ Не выбрано	☒ Информация	☒ Исправлено

Критичность правил

☒ Недоступно	☒ Информация	☒ Низкий
☒ Средний	☒ Высокий	

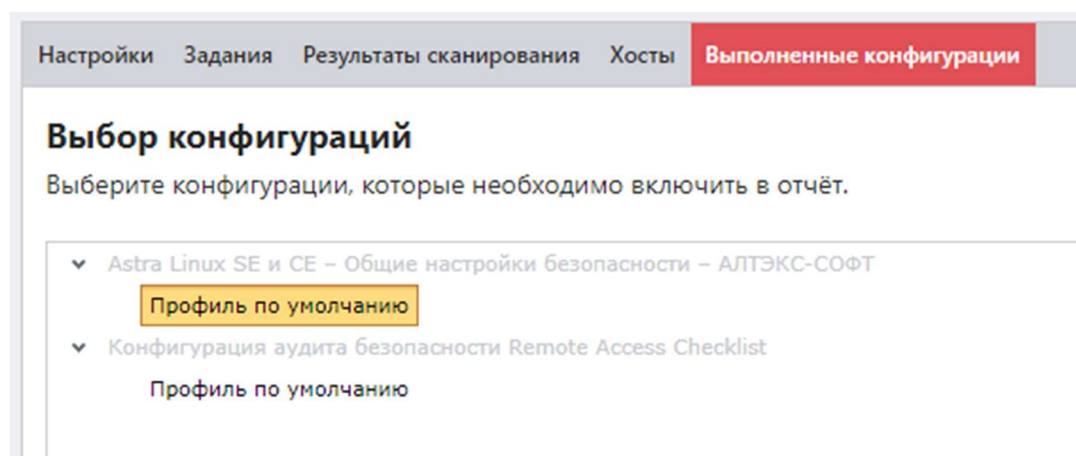
Дополнительно

☐ Отображать пустые группы в отчёте

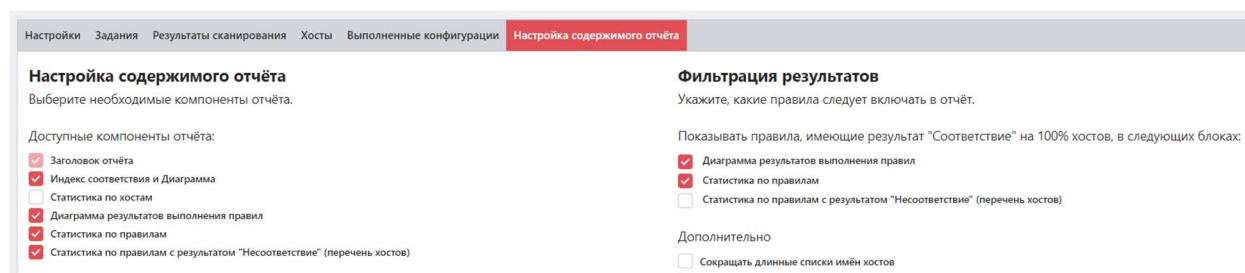
Индекс соответствия комплайнс-политике (конфигурации)

Отчет показывает, насколько хосты соответствуют выбранной конфигурации, детально информируя о каждом правиле.

Выберите конфигурацию, соответствие с которой хотите увидеть в отчете
→ **Вперед:**



Укажите настройки содержимого отчета и фильтрации результатов → **Создать:**



Аналитика индекса соответствия комплайнс-политике (конфигурации)

Отчет будет содержать данные о количестве успешно просканированных хостах и их соответствии выбранной конфигурации. Отчет не показывает соответствие с каждым правилом конфигурации.

Укажите результаты сканирования или воспользуйтесь фильтром по дате запуска и завершения

Настройки
Задания
Результаты сканирования

Результаты сканирования

Дата запуска, от

Дата завершения, до

☒ Использовать все результаты за выбранный период

№ ↓↑	Задание	Начало
93	1_12	14.01.2025, 17:30:
92	1_12	14.01.2025, 17:28:

Выберите конфигурацию, аналитику которой хотите включить в отчет → **Вперед:**

Настройки
Задания
Результаты сканирования
Выполненные конфигурации

Выбор конфигураций

Выберите конфигурации, которые необходимо включить в отчёт.

ВНИМАНИЕ: в отчёт будут включены только результаты сканирований по конфигурации/профилю, выбранному на данном шаге.

- Astra Linux SE и CE – Общие настройки безопасности – АЛТЭКС-СОФТ

Профиль по умолчанию
- Конфигурация аудита безопасности Remote Access Checklist

Профиль по умолчанию

Укажите, что будет содержаться в отчете → **Создать:**

Настройки
Задания
Результаты сканирования
Выполненные конфигурации
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Таблица индекса соответствия комплайнс-политике
- ☒ График индекса соответствия комплайнс-политике
- ☒ График количества хостов на 100% соответствующих комплайнс-политике

Аудит в режиме «Пентест»

Укажите, что будет содержаться в отчете → **Создать:**

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Сканирование портов
- ☒ Подбор паролей
- ☒ Поиск уязвимостей
- ☒ Информация о хосте на основе данных ALTХmap
- ☐ Описание хостов
- ☒ Список уязвимостей

Выберите степень точности отображения уязвимостей

Точность: Средняя и высокая

Проверка доступности

Укажите, что будет содержаться в отчете → **Создать:**

Настройки Задания Результаты сканирования Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты проверки доступности

- ☒ Успешно
- ☒ Не успешно

Сортировка результатов

- ☐ По хостам
- ☒ По результату - сначала недоступные
- ☐ По результату - сначала доступные

Обнаружение хостов

Укажите, что будет содержаться в отчете → **Создать:**

Настройки Задания Результаты сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования

Уязвимости АСУ ТП

Укажите, что будет содержаться в отчете → **Создать:**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Диаграмма распределения уязвимостей по уровням риска
- ☒ Таблица распределения уязвимостей по хостам
- ☒ Таблица распределения уязвимостей по продуктам
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список уязвимостей

7.2 Создание дифференциального отчета

Необходимая роль: RedCheck_Admins / RedCheck_Adminis / RedCheck_Users

Чтобы создать дифференциальный отчет, выполните следующие шаги.

Шаг 1. Раскройте **Действия** → **Создать отчет**;

Шаг 2. Заполните начальную страницу мастера → **Вперед**:

Настройки

Настройки нового отчёта

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Использовать шаблон: Нет

Имя отчёта:

Тип: Дифференциальный

Отчёт: Конфигурации

Выбор данных: По заданию

Описание:

Вперёд

Отчет – тип данных, из которых будет создаваться отчет. В зависимости от выбранного значения последовательность создания отчета может измениться из-за дополнительных параметров;

Отчёт

Выбор данных

Описание

Конфигурации

Конфигурации

Инвентаризация

Обновления

Уязвимости

Фиксация

Аудит MS SQL Server

Аудит БД Oracle

Аудит БД MySQL

Аудит PostgreSQL

Уязвимости АСУ ТП

Аудит в режиме "Пентест"

Шаг 3. Выберите задание → **Вперед:**

Настройки Задания						
Задания						
№	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
78	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	00:00:03	2	2
Page 1 of 1 (1 items) 1						
Всего: 1						
Назад Вперед						

Шаг 4. Выберите в верхней таблице более ранний результат сканирования, после чего выберите в нижней таблице один из появившихся более поздних результатов → **Вперед:**

НастройкиЗаданияРезультаты сканирования

Результаты сканирования

Сканирование 1 (Исходное)

№	Задание	Начало	Завершение	Всего	Успешно
46	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	1	1
45	уязвимости_1	30.01.2023, 17:08:50	30.01.2023, 17:10:24	1	1

20

Page 1 of 1 (2 items)

1

Всего: 2

Сканирование 2 (Текущее)

№	Задание	Начало	Завершение	Всего	Успешно
46	уязвимости_1	01.02.2023, 10:21:59	01.02.2023, 10:26:03	1	1

20

Page 1 of 1 (1 items)

1

Всего: 1

Назад

Вперёд

Шаг 5. Добавьте хосты (**Добавить хосты**) / группы (**Добавить группы**) из результата сканирования, которые хотите видеть в отчете → **Вперед:**

Настройки
Задания
Результаты сканирования
Хосты

Выбранные хосты

ID	IP / DNS	Описание	CPE	
Нет данных для отображения				

Добавить хосты

Выбрано: 0

Выбранные группы

ID	Имя	Описание	
Нет данных для отображения			

Добавить группы

Выбрано: 0

☐
Выбрать все

Назад
Вперед

Шаг 6. Укажите дополнительные настройки для отчета ([7.2.1 Настройки для разных типов заданий](#))

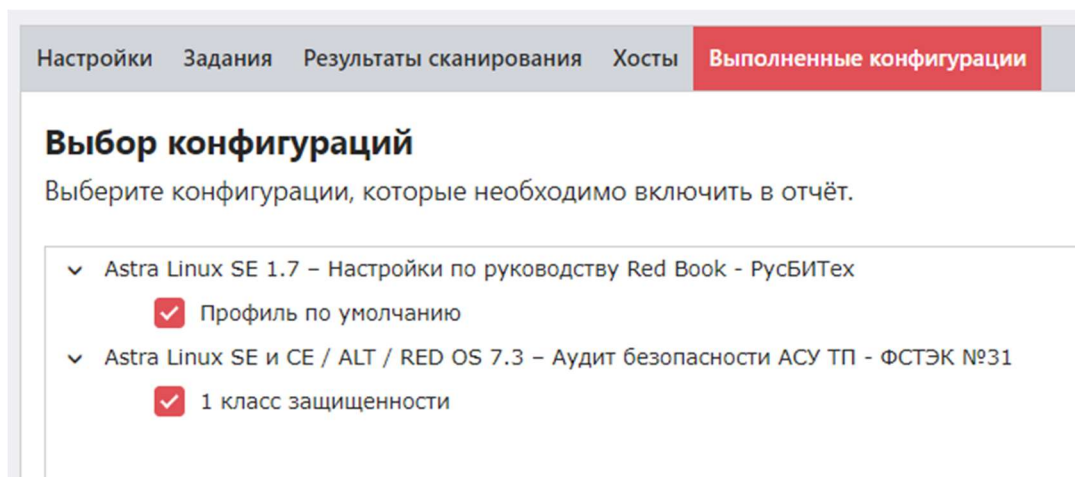
7.2.1 Настройки для разных типов задания

Содержание

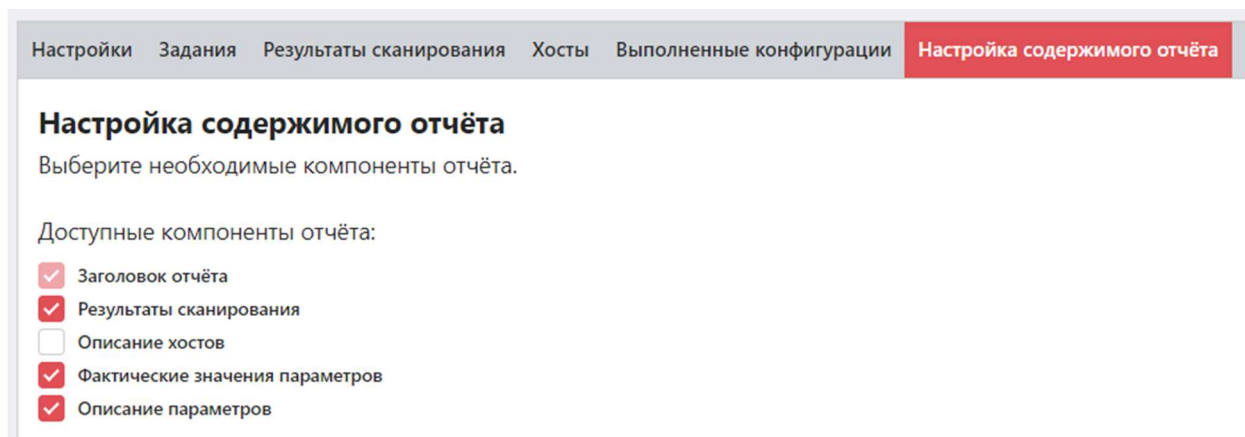
- [Конфигурации](#)
- [Инвентаризация](#)
- [Обновления](#)
- [Уязвимости](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Аудит в режиме «Пентест»](#)

Конфигурации

Выберите конфигурации, сравнение которых будет в отчете → **Вперед;**

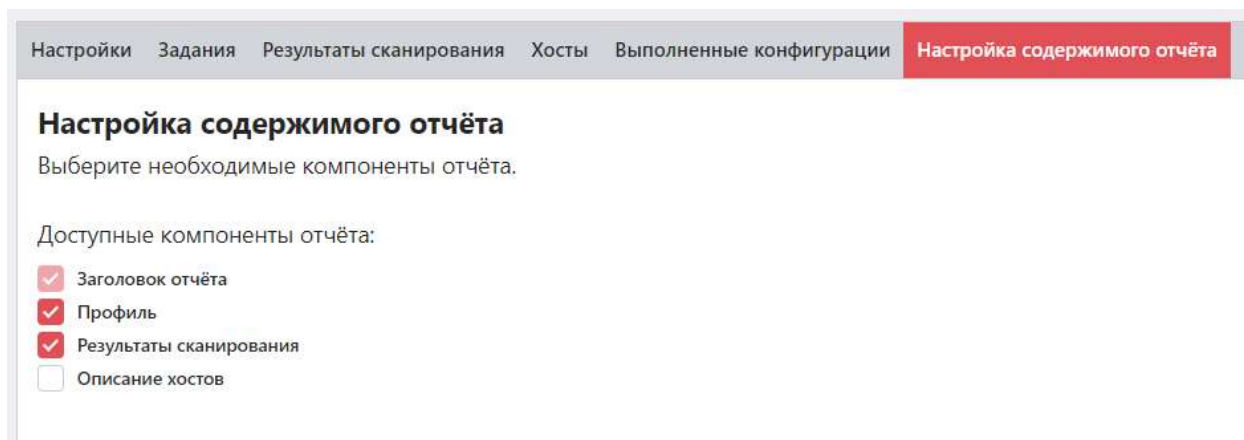


Укажите, что будет содержать отчет → **Создать;**



Инвентаризация

Укажите, что будет содержать отчет → **Создать**;



Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Профиль
- ☒ Результаты сканирования
- ☐ Описание хостов

Обновления

Укажите, что будет содержать отчет → **Создать**;



Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список обновлений

Уязвимости

Укажите, что будет содержать отчет → **Создать**;

НастройкиЗаданияРезультаты сканированияХостыВыполненные конфигурацииНастройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список обновлений

Фиксация

Укажите, что будет содержать отчет → **Создать**;

НастройкиЗаданияРезультаты сканированияХостыНастройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Настройки задания
- ☒ Результаты сканирования
- ☐ Описание хостов

Аудит СУБД

Укажите, что будет содержать отчет → **Создать**;

НастройкиЗаданияРезультаты сканированияХостыВыполненные конфигурацииНастройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Фактические значения параметров
- ☒ Описание параметров

Аудит в режиме «Пентест»

Укажите, что будет содержать отчет → **Создать**;

Настройки

Задания

Результаты сканирования

Хосты

Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

☒

Заголовок отчёта

☒

Сканирование портов

☒

Подбор паролей

☒

Поиск уязвимостей

☒

Информация о хосте на основе данных ALTXmap

☐

Описание хостов

☒

Список уязвимостей

Выберите степень точности отображения уязвимостей

Точность

Средняя и высокая

7.3 Шаблоны отчетов

Шаблоны отчетов позволяют автоматизировать создание отчетов, а также предоставляют гибкую настройку того, что будет включено в отчет.

Шаблон отчетов может быть создан только для простых отчетов.

Пример создания и использования

Раскроем **Инструменты** → **Менеджер шаблонов отчетов** → нажмем **Добавить шаблон отчета**;

Шаблоны отчётов									
№ 	Тип	Имя	Тип данных	Дата создания	Дата модификации	Имя отчёта	Описание	Команды	
1	Простой	тест	Уязвимости	02.12.2022, 14:23:59		какое-то имя			
2	Простой	уязвимости	Аудит в режиме "Пентест"	03.02.2023, 14:36:29		уязвимости			

Заполним начальную форму в мастере → **Вперед;**

Выбор хостов:

- Выбранные хосты и/или группы – в отчет попадут выбранные хосты / группы;
- Все хосты, попавшие в выбранные сканирования – в отчет будут включены хосты в соответствии со значением следующего параметра;

Выбор заданий и сканирований:

- Только результаты из текущего выполнения – в отчете будут результаты выполнения задания, в котором используется шаблон;
- Текущее задание (то, в котором используется шаблон) – в отчет будут добавлены актуальные результаты сканирования задания, в котором используется шаблон, начиная с N (указывается число) дней до текущего времени построения отчета;

- Список выбранных заданий + текущее задание – в отчет будут добавлены актуальные результаты сканирования выбранных заданий, начиная с N (указывается число) дней до текущего времени построения отчета;

Настройки

Настройки нового шаблона отчётов

Укажите требуемые параметры для нового отчёта и заполните описание, если нужно.

Название шаблона

Имя отчёта

Тип

Простой

Отчёт

Конфигурации

Выбор хостов

☒ Выбранные хосты и/или группы
☐ Все хосты, попавшие в выбранные сканирования

Выбор заданий и сканирований

☒ Только результаты из текущего выполнения
☐ Текущее задание (то, в котором используется шаблон)
☐ Список выбранных заданий + текущее задание

Описание

Выберем задания, которые будут попадать в отчет → **Вперед;**

Настройки
Задания

Задания

☐ Использовать все задания, выполнявшиеся в течение выбранного периода

№	Имя	Время запуска	Время завершения	Длительность	Всего	Успешно
106	тестовое задание	06.04.2023, 10:18:35	06.04.2023, 10:19:08	00:00:32	1	1
95	test-vulns	05.04.2023, 10:19:49	05.04.2023, 10:29:17	00:00:28	2	2
83	уязвимости_3	03.02.2023, 17:45:22	03.02.2023, 17:47:36	00:00:13	1	1
78	уязвимости_1	01.02.2023, 13:21:59	01.02.2023, 13:26:03	00:00:03	2	2
69	уязвимости	27.01.2023, 13:37:32	27.01.2023, 13:41:23	00:00:50	1	1

Всего: 5 / Выбрано: 2

Назад
Вперёд

Укажем следующие параметры для фильтрации результатов сканирования.

Настройки
Хосты
Фильтрация результатов сканирования

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

☒ Критический
☒ Высокий
☒ Средний

☒ Низкий
☒ Недоступно

CVSS: от до

☒ Включать уязвимости без CVSS

Наличие в любой из баз данных

☐ NVD
☐ ФСТЭК
☐ НКЦКИ

Дополнительно

☐ Наличие эксплойта
☐ Эксплуатация по сети (удалённое использование)

Укажем профиль аудитов для исключения некоторых уязвимостей из отчета. Раскроем список **Исключаемые статические профили аудитов** → **Добавить профиль аудитов**;

Исключаемые статические профили аудитов ▼

ID	Название	Семейство	
Нет данных для отображения			

Добавить профиль аудитов

Выбрано: 0

Выберем профиль → **Выбрать** → **Вперед**;

Укажем настройки содержимого отчета и группировки → **Создать шаблон**.

Настройки Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Диаграмма распределения уязвимостей по уровням риска
- ☒ Таблица распределения уязвимостей по хостам
- ☒ Таблица распределения уязвимостей по продуктам
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список уязвимостей

Выберите, как следует сгруппировать найденные уязвимости

- ☒ По хостам
- ☐ По продуктам
- ☐ По уровням риска

Настройки шаблона отличаются друг от друга в зависимости от выбранного типа задания ([7.3.1 Настройки для разных типов задания](#)).

Создадим задание Аудит уязвимостей. На шаге Отчет → **Добавить шаблон отчета** → выберем шаблон → **Выбрать** → **Вперед**;

Настройки Группы и хосты Учётные данные Профили сканирования **Отчёт**

Отчёты

Вы можете формировать один или несколько отчётов после выполнения задания. Для построения отчёта используется заранее подготовленный шаблон.

Шаблоны для построения отчетов

Тип	Имя	Тип данных	Команды
Нет данных для отображения			

20 Всего: 0

[Добавить шаблон отчёта...](#)

[Назад](#) [Вперёд](#) [Отмена](#)

После завершения сканирования посмотрим созданный по шаблону отчет. Перейдем в **Отчеты** и скачаем в формате html отчет.

ГЛАВНАЯ

ХОСТЫ

ЗАДАНИЯ

ИСТОРИЯ

КОНТРОЛЬ

ОТЧЁТЫ

ПОЛЬЗОВАТЕЛИ

Отчёты

Интервал

Сегодня

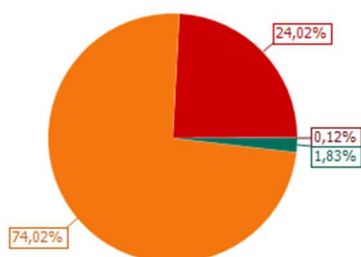
Начиная с

№	Тип	Имя	Тип данных	Создан	Статус	Описание	Команды
56	Простой	уязвимость по профилю_173	Уязвимости	12.04.2023, 17:09:07	html pdf mht csv xml		

Отчет был создан и в него попали все результаты сканирования, полученные в течении прошедших 30 дней для указанных заданий в шаблоне отчета.

№ отчёта	dcd4f077-69c8-4c63-98d9-0248742510d5
Профиль	Уязвимости
Задания	тест шаблона, тестовое задание
Начало/завершение сканирования	06.04.2023 10:16:37 / 12.04.2023 17:06:58
Формирование отчёта	12.04.2023 17:09:07
Имя	уязвимость по профилю_173
Хосты [3]	10.0.0.182, 10.0.0.175, 10.0.0.183

Диаграмма распределения уязвимостей по уровням риска



Риск	Количество
Критический	2
Высокий	393
Средний	1211
Низкий	30
Всего	1636

Фильтрация результатов сканирования

Уровни риска	Критический, Высокий, Средний, Низкий
CVSSv3, от	0
CVSSv3, до	10
CVSSv2 (при отсутствии CVSSv3), от	0
CVSSv2 (при отсутствии CVSSv3), до	10
Включать уязвимости без CVSS	Нет
Исключаемые статические профили аудитов	profile (windows)

Таблица распределения уязвимостей по хостам

Хост / Риск	Критический	Высокий	Средний	Низкий	Всего
-------------	-------------	---------	---------	--------	-------

7.3.1 Настройки для разных типов задания

Содержание

- [Конфигурации](#)
- [Инвентаризация](#)
- [Обновления](#)
- [Уязвимости / Уязвимости Docker](#)
- [Фиксация](#)
- [Аудит СУБД](#)
- [Аудит в режиме «Пентест»](#)
- [Проверка доступности](#)
- [Обнаружение хостов](#)
- [Уязвимости АСУ ТП](#)

Конфигурации

Выберите конфигурации из общего списка, которые попадут в отчет, если будут в результате сканирования → **Вперед**;

Настройки Хосты **Конфигурации**

Выберите конфигурацию

Фильтр по платформам... Фильтр по продуктам...

Выбрать все Сбросить все

Поиск конфигураций

#	Имя
☒	Windows XP - Клиент корпоративной сети (архивная) - Microsoft
☒	Windows XP - Клиент корпоративной сети (архивная) - Microsoft
☒	Windows XP - Безопасная среда (архивная) - Microsoft
☐	Windows XP - Безопасная среда (архивная) - Microsoft
☐	Windows Server 2022 - Настройки для роли контроллера домена - Microsoft
☐	Windows Server 2022 - Настройки безопасности сервера общего назначения - Microsoft
☐	Windows Server 2019 / Windows Server версия 1809 и выше - Настройки для роли контроллера домена - Microsoft
☐	Windows Server 2019 / Windows Server версия 1809 и выше - Настройки безопасности сервера общего назначения - Microsoft
☐	Windows Server 2016 - Настройки для роли контроллера домена - Microsoft
☐	Windows Server 2016 - Настройки безопасности сервера общего назначения - Microsoft
☐	Windows Server 2012 R2 - Расширенная конфигурация безопасности сервера общего назначения - Microsoft

Всего: 101 Выбрано: 3

Конфигурация

Название: Windows XP - Безопасная среда (архивная) - Microsoft

Версия: 42

Файл: Benchmarks\ALTIX-WindowsXP-SSLP\ALTIX-WindowsXP-SSLP-xccdf.xml

Платформа: Microsoft Windows XP (cpe:/o:microsoft:windows_xp)

Описание

Название: Windows XP - Безопасная среда (архивная) - Microsoft

Описание: Конфигурация предназначена для обеспечения безопасного функционирования ОС Microsoft Windows XP на основе Security Baseline - это группа рекомендуемых корпорацией Майкрософт параметров конфигурации, которая объясняет их влияние на безопасность. Эти параметры основаны на отзывах специалистов по обеспечению безопасности Microsoft, групп развития продуктов, партнеров и клиентов.

Примечание

Назад Вперед

Отметьте профили конфигурации для отчетов, использующих шаблон → **Вперед**;

Настройки
Хосты
Конфигурации
Профиль конфигурации

Профиль конфигурации

Профиль конфигурации содержит настройки, которые могут менять параметры правил и влиять на их выполнение.

Windows XP – Безопасная среда (архивная) – Microsoft
☒ Профиль по умолчанию
☐ Windows XP – Безопасная среда (архивная) – Microsoft

Windows XP – Клиент корпоративной сети (архивная) – Microsoft
☒ Профиль по умолчанию
☐ Windows XP – Клиент корпоративной сети (архивная) – Microsoft

Windows XP – Клиент корпоративной сети (архивная) – Microsoft
☒ Профиль по умолчанию
☐ Windows XP – Клиент корпоративной сети (архивная) – Microsoft

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки
Хосты
Конфигурации
Профиль конфигурации
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:
☒ Заголовок отчёта
☒ Сводная таблица результатов сканирования
☒ Результаты сканирования
☐ Описание хостов
☐ Фактические значения параметров
☒ Описание параметров

Фильтрация результатов
Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил
☒ Соответствие
☒ Неизвестно
☒ Не выбрано

☒ Несоответствие
☒ Неприменимо
☒ Информация

☒ Ошибка
☒ Не проверено
☒ Исправлено

Критичность правил
☒ Недоступно
☒ Средний

☒ Информация
☒ Высокий

☒ Низкий

Дополнительно
☐ Отображать пустые группы в отчёте

Назад
Создать шаблон

Инвентаризация

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Профиль
- ☒ Результаты сканирования
- ☐ Описание хостов

Обновления

Укажите настройки для фильтрации результата сканирования → **Вперед**:

- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязвимости, CVSS для которых не было определено;
- Дополнительно:
 - Наличие эксплойта – OVAL-определение имеет эксплойт;
 - Эксплуатация по сети – эксплойт можно воспроизвести удаленно;

Настройки Задания Результаты сканирования Хосты **Фильтрация результатов сканирования**

Фильтрация результатов сканирования

Выберите результаты, которые нужно включить в отчёт.

Риск

☒ Критический ☒ Высокий ☒ Средний
☒ Низкий ☒ Недоступно

Cvss: от до

☒ Включать обновления без CVSS

Наличие в любой из баз данных

☐ NVD ☐ ФСТЭК ☐ НКЦКИ

Дополнительно

☐ Наличие эксплойта
☐ Эксплуатация по сети (удалённое использование)
☐ Скрыть заменённые

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;

Настройки Задания Результаты сканирования Хосты Фильтрация результатов сканирования **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

☒ Заголовок отчёта
☒ Диаграмма распределения обновлений по уровням риска
☒ Таблица распределения обновлений по хостам
☒ Таблица распределения обновлений по продуктам
☒ Результаты сканирования
☐ Описание хостов
☒ Список обновлений

Выберите, как следует сгруппировать найденные обновления

☒ По хостам
☐ По продуктам
☐ По уровням риска

Уязвимости / Уязвимости Docker

Укажите настройки для фильтрации результата сканирования → **Вперед**:

- Риск – фильтрация по категориям риска;
- В отчет попадут только те уязвимости, метрика CVSS которых будет в указанном интервале;
- Включать уязвимости без CVSS – в отчете будут уязвимости, CVSS для которых не было определено;

- Дополнительно:
 - Наличие эксплойта – OVAL-определение имеет эксплойт;
 - Эксплуатация по сети – эксплойт можно воспроизвести удаленно;

К отчету можно применить профиль сканирования ([5.1 Профили сканирования](#)).

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;

Фиксация

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон**;

Настройки
Хосты
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Настройки задания
- ☒ Результаты сканирования
- ☐ Описание хостов

Аудит СУБД

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки
Хосты
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Сводная таблица результатов сканирования
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Фактические значения параметров
- ☒ Описание параметров

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты выполнения правил

☒ Соответствие	☒ Несоответствие	☒ Ошибка
☒ Неизвестно	☒ Неприменимо	☒ Не проверено
☒ Не выбрано	☒ Информация	☒ Исправлено

Критичность правил

☒ Недоступно	☒ Информация	☒ Низкий
☒ Средний	☒ Высокий	

Дополнительно

- ☐ Отображать пустые группы в отчёте

Аудит в режиме «Пентест»

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки
Хосты
Настройка содержимого отчёта

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Сканирование портов
- ☒ Подбор паролей
- ☒ Поиск уязвимостей
- ☒ Информация о хосте на основе данных ALTХmap
- ☐ Описание хостов
- ☒ Список уязвимостей

Выберите степень точности отображения уязвимостей

Точность

Средняя и высокая

Проверка доступности

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования

Фильтрация результатов

Укажите, какие правила следует включать в отчёт.

Результаты проверки доступности

- ☒ Успешно
- ☒ Не успешно

Сортировка результатов

- ☐ По хостам
- ☒ По результату - сначала недоступные
- ☐ По результату - сначала доступные

Обнаружение хостов

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройки Хосты **Настройка содержимого отчёта**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Результаты сканирования

Уязвимости АСУ ТП

Укажите, что будет содержать отчет, использующий шаблон → **Создать шаблон;**

Настройка содержимого отчёта

Выберите необходимые компоненты отчёта.

Доступные компоненты отчёта:

- ☒ Заголовок отчёта
- ☒ Диаграмма распределения уязвимостей по уровням риска
- ☒ Таблица распределения уязвимостей по хостам
- ☒ Таблица распределения уязвимостей по продуктам
- ☒ Результаты сканирования
- ☐ Описание хостов
- ☒ Список уязвимостей

7.4 Просмотр CSV отчетов

В RedCheck отчет в формате csv соответствует стандарту RFC 4180. Это означает, что разделителем между столбцами является запятая.

Разные офисные пакеты открывают отчет в формате csv по-разному. Это приводит к ошибкам отображения. Ниже предлагаются инструкции правильного открытия csv отчетов для следующих офисных пакетов:

- [Microsoft Excel](#);
- [R7 Офис](#);
- [Libre Office / Open Office](#);

Microsoft Excel

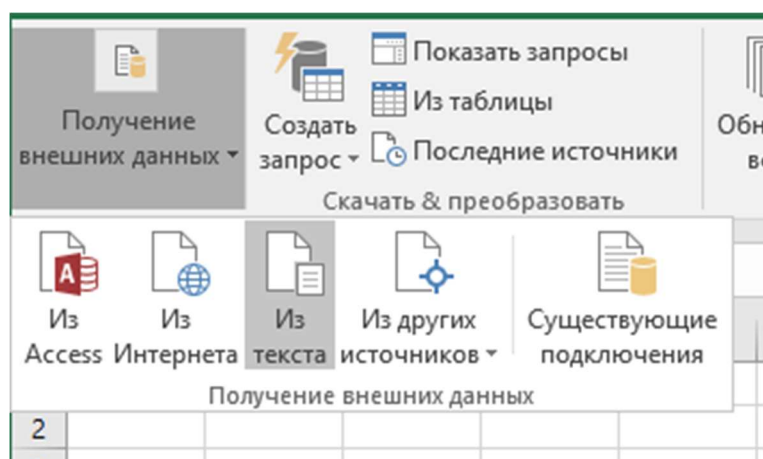
В примере используется Excel 2016. Для других версий шаги идентичны.

1-й способ

Нажмите **Файл** → **Открыть** → выберите отчет в формате csv;

2-й способ

Нажмите **Данные** → **Получение внешних данных** → **Из текста** → выберите отчет в формате csv;



Шаг 1. В появившемся окне укажите формат данных **с разделителями** → **Далее**;

Мастер текстов (импорт) - шаг 1 из 3

Данные восприняты как список значений с разделителями.
Если это верно, нажмите кнопку "Далее >", в противном случае укажите формат данных.

Формат исходных данных

Укажите формат данных:

☒ с разделителями — значения полей отделяются знаками-разделителями

☐ фиксированной ширины — поля имеют заданную ширину

Начать импорт со строки: 1 Формат файла: 65001 : Юникод (UTF-8)

☐ Мои данные содержат заголовки

Предварительный просмотр файла C:\Users\Administrator\Downloads\Отчет-уязвимостями.csv.

1	Кост,AltId,Критичность,Название,Описание,Продукты,Детализация,Cvss2,Cvss2 Вектор,
2	dc-01,330270,Критический,Уязвимость удаленного выполнения кода в Windows DNS Serve
3	dc-01,334369,Критический,Уязвимость несанкционированного получения прав Netlogon (
4	dc-01,423344,Критический,Уязвимость обхода функции защиты Microsoft Defender for E
5	dc-01,37186,Высокий,"Уязвимость WinVerifyTrust, связанная с проверкой подписи (CVE

< >

Отмена < Назад Далее > Готово

Шаг 2. Отметьте **запятая** в списке **Символом-разделителем является** → **Далее**;

Мастер текстов (импорт) - шаг 2 из 3

В этом диалоговом окне можно установить разделители для текстовых данных. Результат выводится в окне образца разбора.

Символом-разделителем является:

☐ знак табуляции

☐ точка с запятой

☒ запятая

☐ пробел

☐ другой:

☐ Считать последовательные разделители одним

Ограничитель строк: *

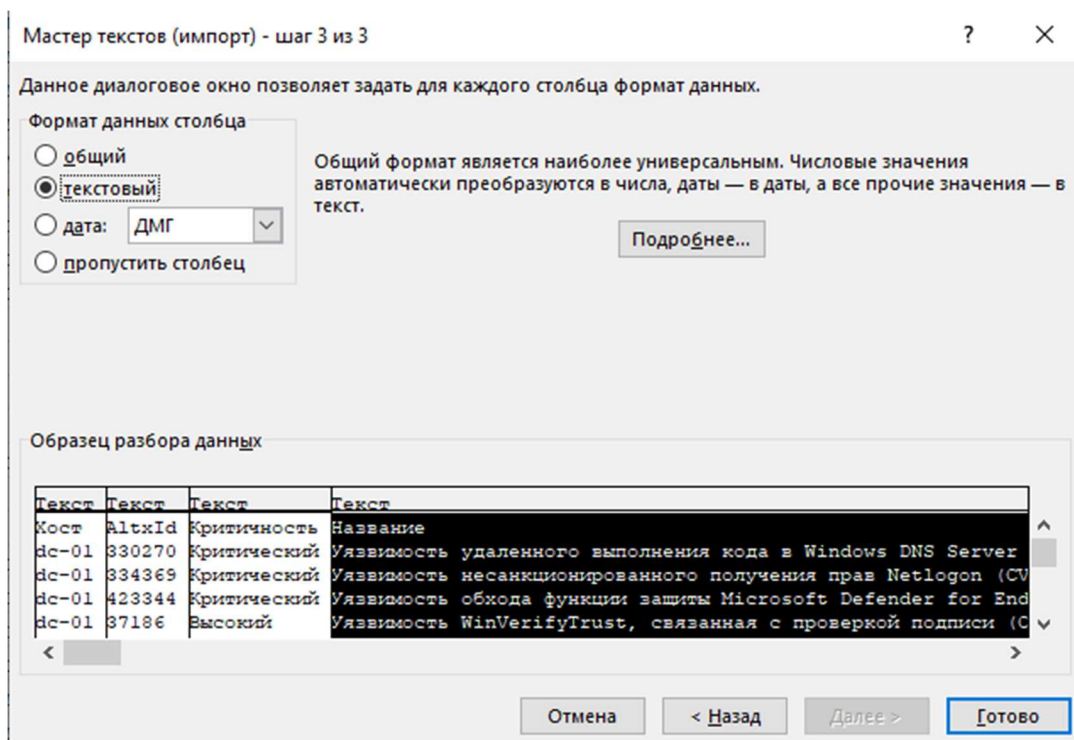
Образец разбора данных

Кост	AltId	Критичность	Название
dc-01	330270	Критический	Уязвимость удаленного выполнения кода в Windows DNS Server
dc-01	334369	Критический	Уязвимость несанкционированного получения прав Netlogon (CV
dc-01	423344	Критический	Уязвимость обхода функции защиты Microsoft Defender for End
dc-01	37186	Высокий	Уязвимость WinVerifyTrust, связанная с проверкой подписи (C

< >

Отмена < Назад Далее > Готово

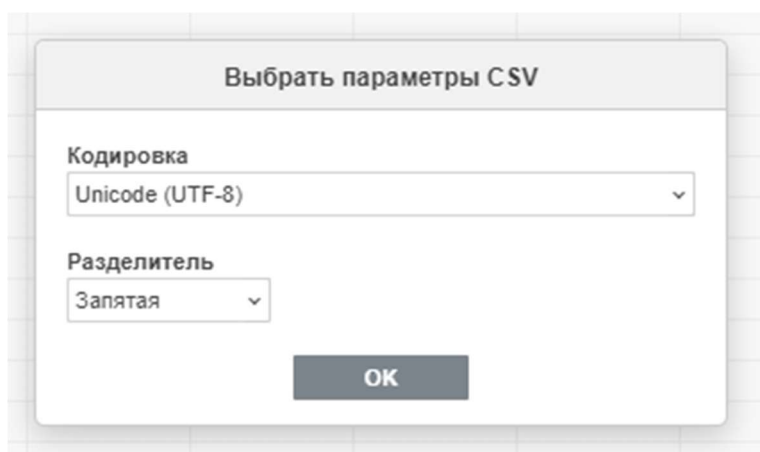
Шаг 3. Для каждого столбца укажите **текстовый** формат данных → **Готово**;



Это необходимо для корректного отображения вещественных чисел, которые Microsoft Excel по умолчанию пытается представить в виде даты.

R7 Офис

Откройте csv отчет с помощью R7 Офиса → в появившемся окне выберите **Запятая** из списка **Разделитель** → **ОК**;



Libre Office / Open Office

Откройте csv отчет с помощью Libre Office → в появившемся окне выберите **Разделитель** в **Параметры разделителя** → отметьте **Запятая** → **ОК**;

Импорт текста - [Отчет-уязвимостями.csv]

Импорт

Кодировка: Юникод (UTF-8)

Локаль: Стандарт - Русский

Со строки: 1

Параметры разделителя

☐ Фиксированная ширина ☒ Разделитель

☐ Табуляция ☒ Запятая ☐ Точка с запятой ☐ Пробел ☐ Другой

☐ Объединять разделители ☐ Обрезать пробелы

Разделитель строк: "

Другие параметры

☐ Поля в кавычках как текст ☐ Распознавать особые числа

☐ Вычислять формулы

Поля

Тип столбца:

	С
1	

Справка

OK

Отменить

8 Аналитика

Модуль Аналитики необходим для контроля сканирования инфраструктуры, анализа и устранения уязвимостей и соответствия конфигурациям безопасности. Инструмент позволяет точно определить как проблемы доступа к хостам, так и анализ их сканирования в регламент.

Анализ уязвимостей позволяет определить появление новых угроз, количество не устраненных, а также отдельный список по закрытым проблемам безопасности, в указанный пользователем регламент (срок анализа в днях).

Данный функционал приближает классический сканер безопасности RedCheck к возможностям мощных VM-решений без необходимости проводить интеграции и управлять уязвимостями по результатам сканирования в едином интерфейсе.

Доступно только для редакций Expert и Enterprise

Содержание

- [8.1 Актуальность сканирования](#)
- [8.2 Недоступность хостов](#)
- [8.3 Анализ уязвимостей](#)
- [8.4 Контроль устранения уязвимостей](#)
- [8.5 Анализ конфигураций](#)

8.1 Актуальность сканирования

Данная форма аналитики позволяет определить, какие хосты и по какой причине не были успешно просканированы за указанный период.

Для перехода на форму нажмите **Аналитика → Актуальность сканирования**

Поддерживается 4 типа сканирования:

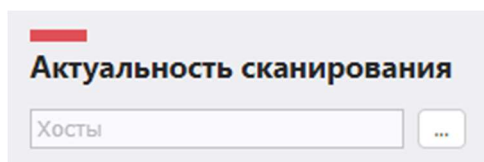
- Аудит уязвимостей;
- Аудит обновлений;
- Аудит конфигураций;
- Аудит в режиме «Пентест».

Информация об актуальности сканирования включает в себя:

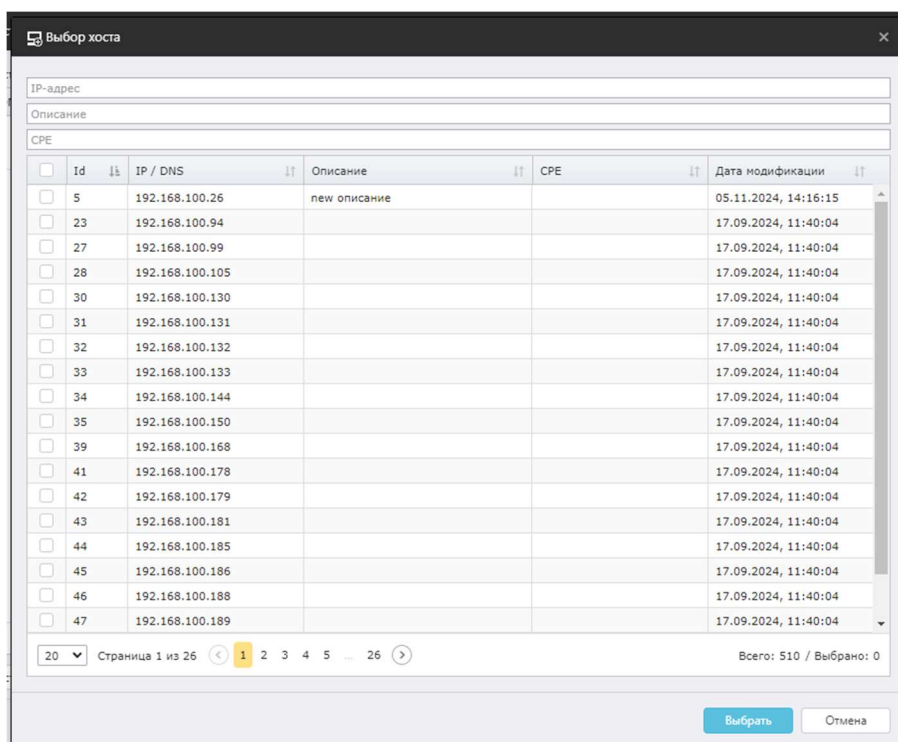
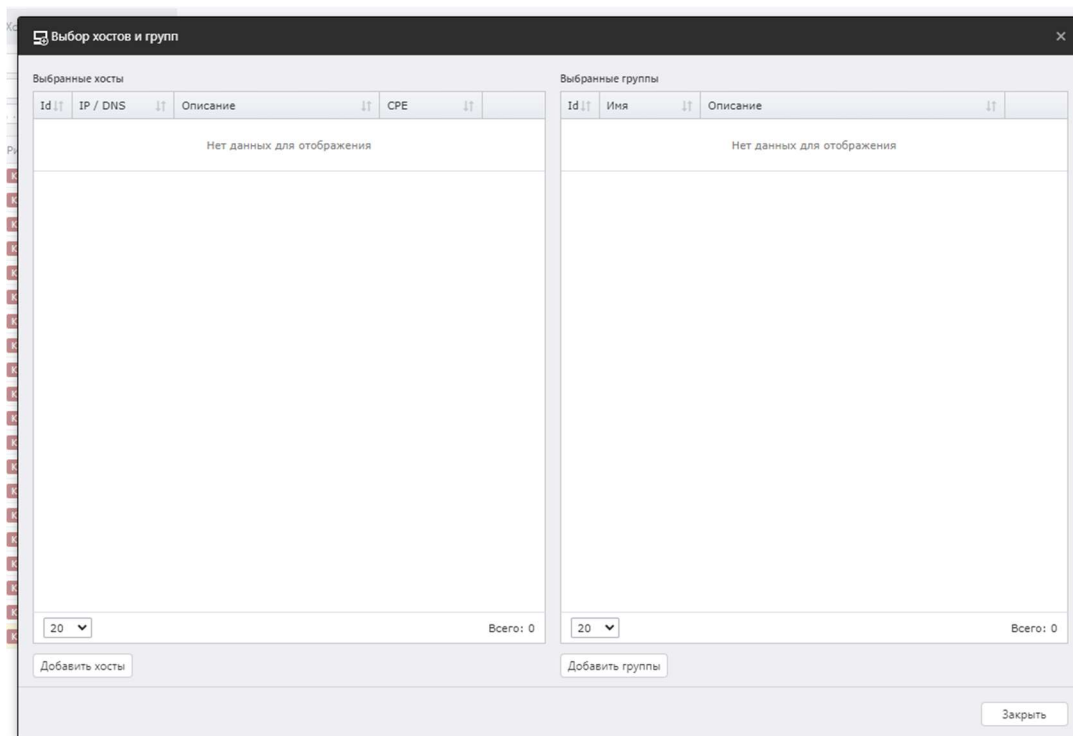
- Хост – IP-адрес или DNS-имя хоста;
- Проблема – отображает информацию о том, почему нет результата сканирования. Может принимать 3 значения:
 - Ошибка или недоступность – сканирование хоста завершилось с ошибкой, или хост оказался недоступен;
 - Нет запуска задания – хост входит в список целей какого-либо задания, но задание ни разу не было запущено;
 - Нет задания – хост не входит в список целей ни для одного задания;
- Наличие в группе – находится ли хост в какой-либо группе.

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.



- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов:



- Тип сканирования – для какого типа сканирования проверять результаты сканирования хостов;
 - Для аудита уязвимостей / обновлений – учитывать или нет задания с профилями сканирования ([5.1 Профили аудитов](#));
- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска проблем;

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Почему нет результатов сканирования – отображать только те хосты, у которых Проблема совпадает с отмеченными. Также показывает количество хостов для каждого типа Проблемы. Можно фильтровать по трем значениям:
 - Ошибка или недоступность – сканирование хоста завершилось с ошибкой, или хост оказался недоступен;
 - Нет запуска задания – хост входит в список целей (в том числе в составе группы) какого-либо задания, но задание ни разу не было запущено;
 - Нет задания – хост не входит в список целей (в том числе в составе группы) ни для одного задания;
- Хост состоит в группе – отображать хосты согласно тому, состоят они в какой-либо группе или нет.

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая находится в таблице после применения фильтров. Для

этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ScanningRelevance-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Наличие в группе	Состоит хост в какой-либо группе или нет. Принимает 2 значения: True и False
Проблема	Почему нет результатов сканирования. Принимает 3 значения: Нет задания, Нет запуска задания, Ошибка или недоступность
Id заданий	ID заданий, которые не были запущены. Указываются через точку с запятой
"Id заданий, в которых сканируется группа, включающая данный хост"	Указываются через точку с запятой
ID сканирований	ID результата сканирования, который завершился ошибкой или недоступностью хоста

Пример:

Bash (оболочка Unix)

Id хоста,Имя хоста,Наличие в группе,Проблема,Id заданий,"Id заданий, в которых сканируется группа, включающая данный хост",ID сканирований
5,192.168.80.26,True,Нет запуска задания,111;112;113,4,

8.2 Недоступность хостов

Данная форма аналитики позволяет определить, сколько хостов оказываются недоступными при сканировании, а также причины недоступности или завершения сканирования ошибкой.

Для перехода на форму нажмите **Аналитика → Недоступность хостов**

Недоступность хостов							Экспорт в CSV
Хосты Выбрать / Снять всё ☒ Проверка доступности ☒ Аудит уязвимостей ☒ Аудит обновлений ☒ Аудит конфигураций ☒ Инвентаризация ☒ Фиксация ☒ Аудит Docker ☒ Аудит уязвимостей ACU TPI ☒ Аудит в режиме "Пентест" ☒ Аудит MS SQL Server ☒ Аудит БД Oracle ☒ Аудит БД MySQL ☒ Аудит PostgreSQL Все задания Все запуски Дата завершения сканирования (с) Дата завершения сканирования (по) Применить фильтр							
Хост	Тип сканирования	Задание	Результат	Причина недоступности	Время завершения		
> 192.168.80.130	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:44:53		
> 192.168.80.129	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:44:25		
> 192.168.80.130	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:34:38		
> 192.168.80.129	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:34:11		
> 192.168.80.130	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:08:09		
> 192.168.80.129	Аудит уязвимостей ACU TPI	1_24	Ошибка	Отсутствуют значимые данные от ACU TPI-модулей. Возможно, хост недоступен.	05.02.2025, 10:07:42		
> 192.168.80.129	Аудит PostgreSQL	postgresql	Хост недоступен	Хост недоступен Причина: "база данных "RedCheck" не существует" Подробности в журнале событий службы сканирования. Для получения детальной информации можно воспользоваться заданием "Проверка доступности".	09.12.2024, 14:29:48		
> 192.168.80.58	Проверка доступности	проверка доступности	Хост недоступен	Ошибка установления соединения.	09.12.2024, 14:28:30		
> 192.168.80.58	Проверка доступности	проверка доступности_1	Хост недоступен	Ошибка установления соединения.	09.12.2024, 14:28:13		
> 9.9.9.9	Проверка доступности	winrm	Хост недоступен	HTTPConnectionPool(host='9.9.9.9', port=5985): Max retries exceeded with url: /wsman (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7f1ed5fee760>: Failed to establish a new connection: [Errno 111] Connection refused'))	06.12.2024, 10:38:05		
> 9.9.9.10	Проверка доступности	winrm	Хост недоступен	HTTPConnectionPool(host='9.9.9.10', port=5985): Max retries exceeded with url: /wsman (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7f1ebeb8d770>: Failed to establish a new connection: [Errno 111] Connection refused'))	06.12.2024, 10:37:44		
HTTPConnectionPool(host='192.168.80.4', port=5985): Max retries exceeded with url: /wsman (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7f1ebeb8d770>: Failed to establish a new connection: [Errno 111] Connection refused'))							
Всего: 34							

Информация о недоступности хоста включает в себя:

- Сканирование – ID результата сканирования;
- Хост – IP-адрес или DNS-имя хоста (ID хоста);
- Тип сканирования задания;
- Задание – название задания;
- Результат сканирования – результат актуального (последнего) сканирования указанного задания для хоста;
- Время завершения сканирования;
- Причина неуспешного результата – описание причины недоступности или ошибки;

Хост	Тип сканирования	Задание	Результат	Причина
192.168.80.25	Аудит уязвимостей	2008 r2 vulns	Ошибка	.NET
Сканирование 1861 Хост 192.168.80.25 (Id = 8545) Тип сканирования Аудит уязвимостей Задание 2008 r2 vulns Результаты сканирования Ошибка Завершение сканирования 09.10.2024, 12:55:39 Причина неуспешного результата .NET 4.0 or later is not installed on "192.168.80.25".				

Общий фильтр

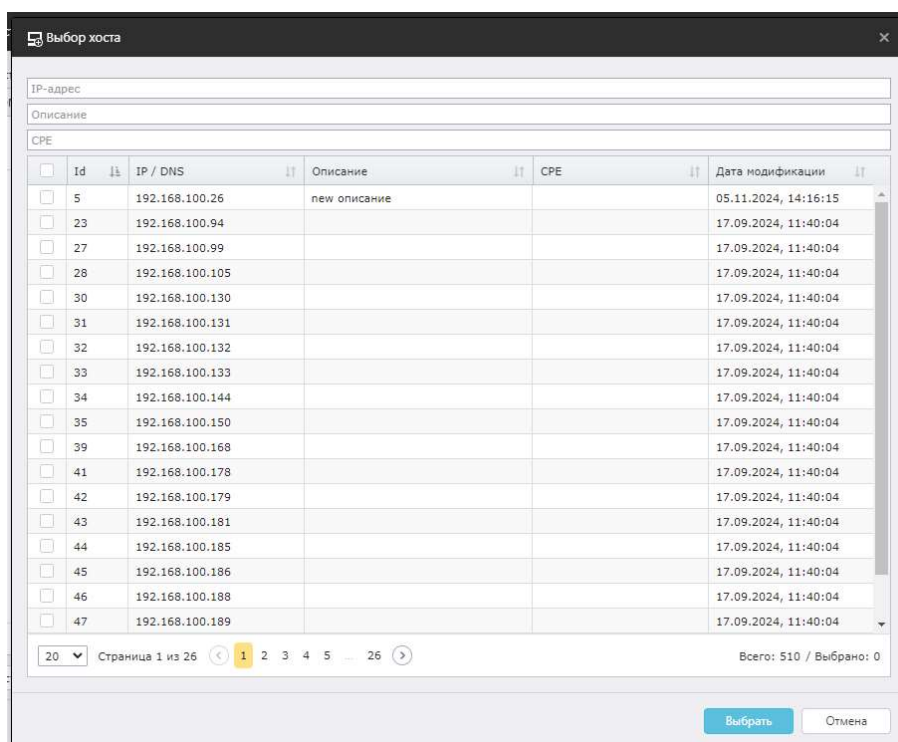
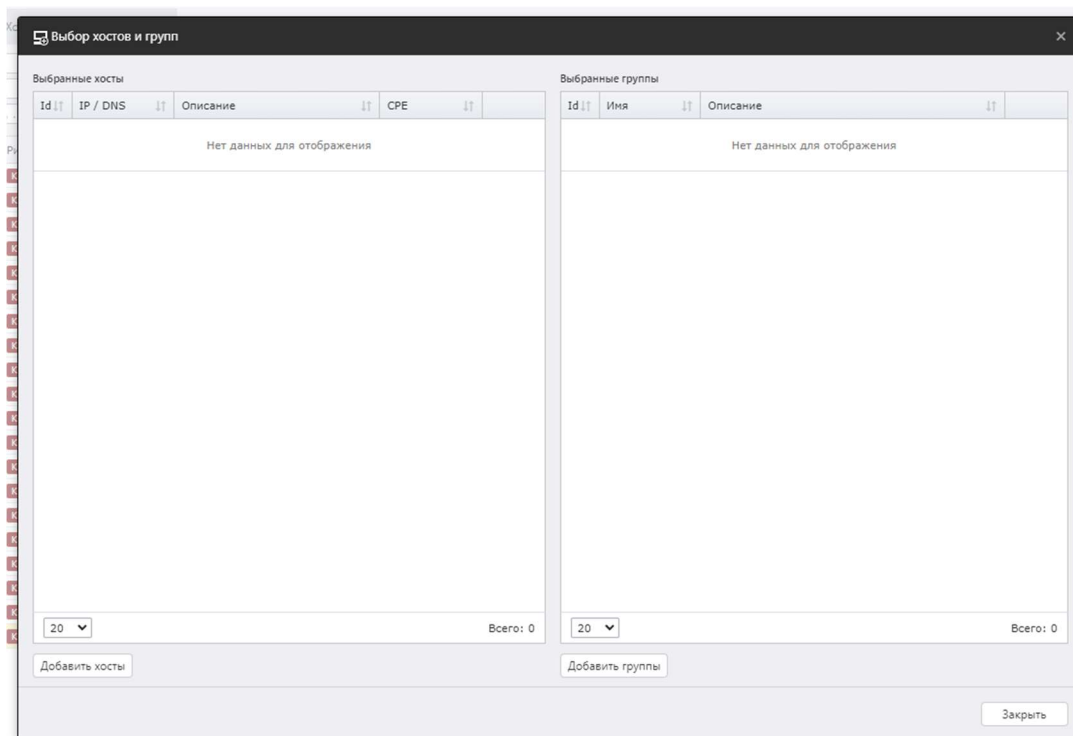
Общий фильтр располагается слева от результирующей таблицы.

Недоступность хостов

Хосты

...

- Хосты** – можно выбрать хосты, которые будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов:



- Типы сканирований, по которым будет производиться поиск причины недоступности хостов;

Выбрать / Снять всё

- ☒ Проверка доступности
- ☒ Аудит уязвимостей
- ☒ Аудит обновлений
- ☒ Аудит конфигураций
- ☒ Инвентаризация
- ☒ Фиксация
- ☒ Аудит Docker
- ☒ Аудит уязвимостей АСУ ТП
- ☒ Аудит в режиме "Пентест"
- ☒ Аудит MS SQL Server
- ☒ Аудит БД Oracle
- ☒ Аудит БД MySQL
- ☒ Аудит PostgreSQL

- Задания – можно выбрать задания, из результатов сканирования которых будет производиться поиск причин недоступности хостов. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Выбрать задания ▼

Задания

Нажмите на , после чего откроется окно выбора заданий;

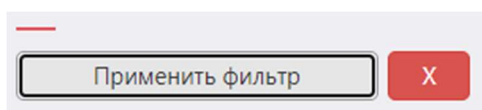
- Запуски задания – из выпадающего списка можно выбрать какие результаты сканирования попадут в результирующую таблицу: Все запуски или Последний (актуальный) запуск:
- Дата завершения сканирования (с / по) – учитывать результаты сканирования, которые завершились в указанный период.

Последний запуск ▼

Дата завершения сканирования (с)

Дата завершения сканирования (по)

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Тип результатов сканирования – Ошибка или Хост недоступен;
- Хост – IP-адрес или DNS-имя хоста;
- Причина недоступности – описание причины недоступности или ошибки. Можно указывать часть причины доступности или ошибки.

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая находится в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **UnavailabilityReasons-dd-mm-yyyy.csv**.

Структура CSV файла

ID сканирования	ID результата сканирования
Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Тип сканирования	Тип сканирования задания
Задание	Название задания
Результаты сканирования	Статус, которым завершилось сканирование: Ошибка или Хост недоступен

Причина недоступности	Описание ошибки или недоступности хоста
Время завершения	Время завершения сканирования
Детализация	Описание для некоторых ошибок в формате xml (для заданий типа Проверка доступности): "<exception name=""TypeException""><prop name=""Message""></prop></exception>"

Пример:

Bash (оболочка Unix)

```
ID сканирования, Id хоста, Имя хоста, Тип
сканирования, Задание, Результаты сканирования, Причина
недоступности, Время завершения, Детализация
1638, 5, 192.168.1.26, Проверка доступности, w, Хост недоступен, Failed to
authenticate the user name_user with negotiate, 17.09.2024
13:11:00, "<exception name=""PythonException""> <prop
name=""Message"">Failed to authenticate the user name_user with
negotiate</prop></exception>"
```

8.3 Анализ уязвимостей

Данная форма аналитики позволяет проводить анализ инфраструктуры на предмет наличия любых или конкретных уязвимостей на хостах за последние N дней.

Для перехода на форму нажмите **Аналитика** → **Анализ уязвимостей**

Содержание

- [8.3.1 Вкладка Уязвимости](#)
- [8.3.2 Вкладка Хосты](#)
- [8.3.3 Вкладка Хост – Уязвимость](#)

8.3.1 Вкладка Уязвимости

В данной вкладке отображается информация об уязвимостях, обнаруженных во время сканирования инфраструктуры, согласно общему фильтру.

По умолчанию уязвимости отсортированы по количеству хостов, на которых они обнаружены, от большего к меньшему.

Информация об уязвимости включает в себя:

- Уникальный идентификатор ALTIX ID;
- Ссылка на страницу уязвимостей в OVALdb;
- Риск и CVSS – [Сведения об интегральной оценке по базовым метрикам CVSS;](#)
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Количество хостов, на которых была обнаружена данная уязвимость;

ALTIX ID	Риск	CVSS	Название	Дата публикации	Количество хостов	Дополнительно
405114	Критический	10	Astra Linux -- уязвимость в chromium (CVE-2022-0289)	12.02.2022	1	Список хостов
ALTIX ID	405114					
OVAL	oval:ru.altx-soft.nix:def:188293					
Риск	Критический					
Оценка CVSS	10,0 (BDU)					
Название	Astra Linux -- уязвимость в chromium (CVE-2022-0289)					
Описание	В продукте chromium обнаружена уязвимость CVE-2022-0289.					
Дата публикации	12.02.2022					
Ссылки	NKCKI FSTEC VENDOR packetstormsecurity NKCKI VENDOR CVE		VULN-20220124.25 BDU:2022-00867 20220829SE16 Chrome-safe_browsing-ThreatDetails-OnReceivedThreatDOMDetails-Use-After-Free VULN-20220124.26 2022-0819SE17 CVE-2022-0289			

Нажав **Список хостов**, вы перейдете на вкладку «Хост – Уязвимость», где в фильтре для результирующей таблицы уже будет указан ALTX ID выбранной уязвимости.

Уязвимости

Хосты

Хост — Уязвимость

Хост

Найдено хостов: 1

Название

405238

Ссылка (CVE, BDU, ...)

Найдено уникальных уязвимостей: 1

✓

Критический (0)

✓

Высокий (0)

✓

Средний (1)

✓

Низкий (0)

✓

Не определено (0)

Экспорт в CSV

	Хост	ALT X ID	Риск	CVSS	Название	Дата публикации
>	192.168.80.129	405238	Средний		Astra Linux -- уязвимость в linux, intel-microcode, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-21125)	15.06.2022

Общий фильтр

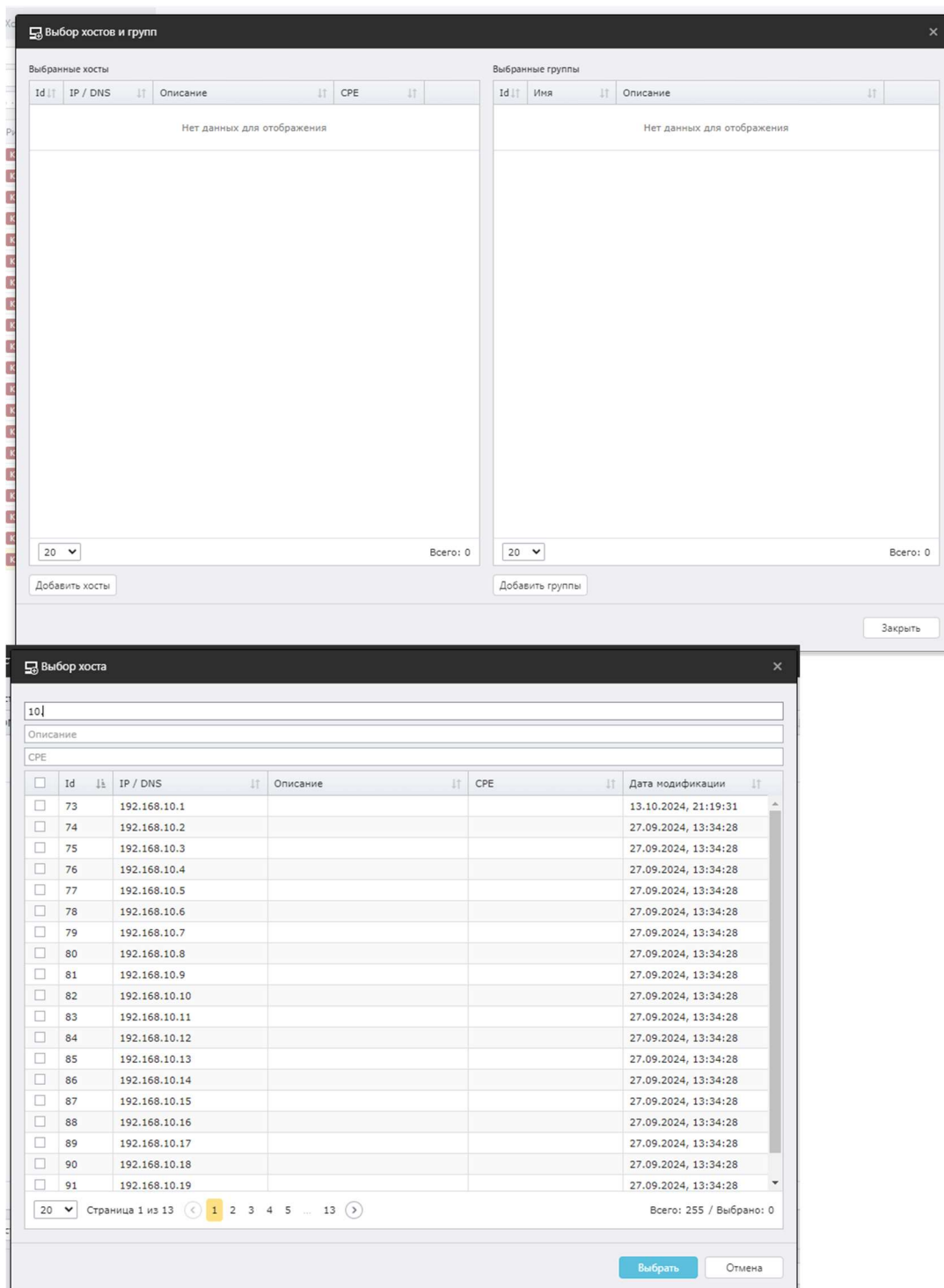
Общий фильтр располагается слева от результирующей таблицы.

Анализ уязвимостей

Хосты

...

- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов:



- **Задания** – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;

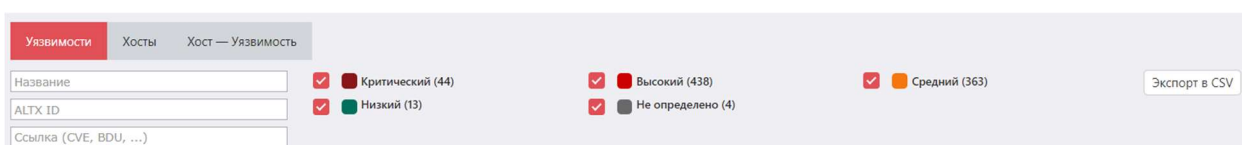
- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Название – название уязвимости;
- ALT X ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Риск – в таблице будут отображаться уязвимости с отмеченными вариантами риска.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-Vulnerabilities-dd-mm-yyyy.csv**.

Структура CSV файла

ALT X ID	Уникальный идентификатор уязвимости
Количество хостов	Количество хостов, на которых обнаружена уязвимость
Хосты	Список ID хостов, на которых обнаружена уязвимость. Если значений больше одного, то они указываются в двойных кавычках через запятую. Например, "67,69"
OVAL определение	Ссылка на страницу уязвимости в OVALdb
Риск	Принимает значения: Критический, Высокий, Средний, Низкий

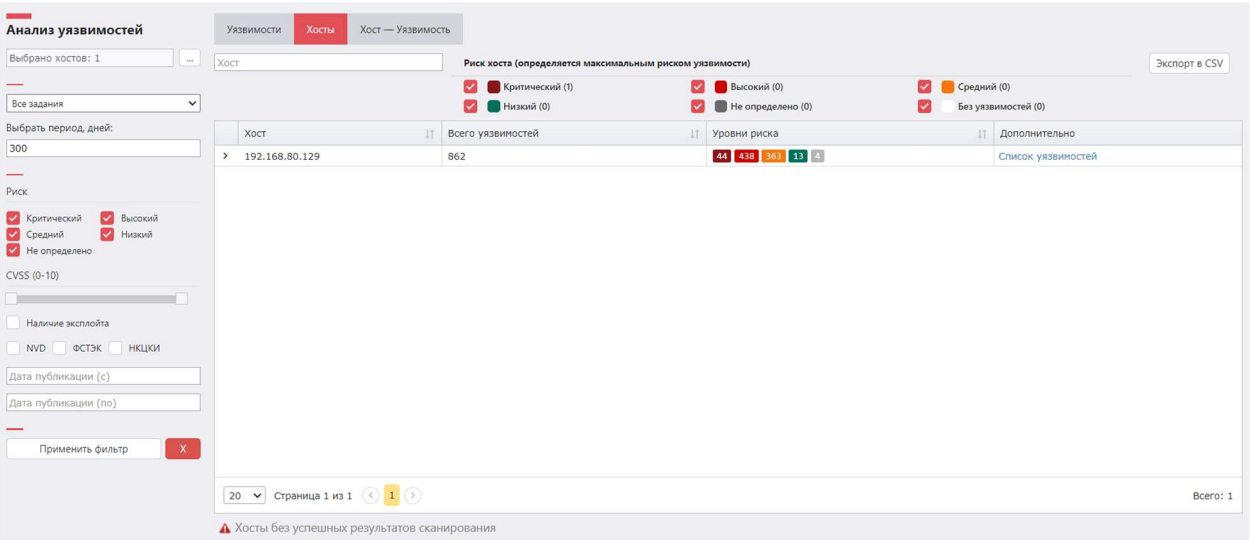
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором

Пример:

Код
ALTX ID, Количество хостов, Хосты, OVAL определение, Уровень критичности, Оценка CVSS, Источник CVSS, Уязвимость, Описание, Дата публикации 362408,1,69,oval:ru.altx-soft.nix:def:156895,Высокий,"8,8",BDU,Astra Linux -- уязвимость в openjpeg2 (CVE-2020-27814),В продукте openjpeg2 обнаружена уязвимость CVE-2020-27814.,26.01.2021

8.3.2 Вкладка Хосты

В данной вкладке отображается информация об уязвимостях на конкретных хостах, которые были обнаружены во время сканирований инфраструктуры, согласно общему фильтру.



В данной вкладке отображается информация о хостах:

- ID хоста;
- IP-адрес или DNS имя хоста;
- Описание хоста;
- ID актуального (последнего) сканирования со статусом **Завершено**;
- Дата актуального сканирования;
- Общее количество уязвимостей на хосте;
- Количество найденных уязвимостей, сгруппированных по уровню риска;

Хост	Всего уязвимостей	Уровни риска	Дополнительно
192.168.80.32	729	23 261 418 17 18	Список уязвимостей
Id хоста Имя хоста ID сканирования Дата сканирования 8606 192.168.80.32 1871 23.10.2024 08:33:51			

Нажав **Список уязвимостей** возле хоста, вы перейдете на вкладку «Хост – Уязвимость», где в фильтре для результирующей таблицы уже будет указан выбранный хост.

Анализ уязвимостей

Выбрано хостов: 1

192.168.80.129

Найдено хостов: 1

Критический (44)

Высокий (438)

Средний (363)

Низкий (13)

Не определено (4)

Экспорт в CSV

Название

ALTIX ID

Ссылка (CVE, BDU, ...)

Найдено уникальных уязвимостей: 862

Все задания

Выбрать период, дней:

300

Риск

Критический

Высокий

Средний

Низкий

Не определено

CVSS (0-10)

Наличие эксплойта

NVD

ЕСТЭК

НКЦКИ

Дата публикации (с)

Дата публикации (по)

Применить фильтр

X

Хост	ALTIX ID	Риск	CVSS	Название	Дата публикации
192.168.80.129	425333	Высокий		Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1528)	21.03.2023
192.168.80.129	425334	Критический		Доступ за пределами памяти в WebHID в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)	21.03.2023
192.168.80.129	425335	Высокий		Уязвимость доступа к освобожденной памяти в PDF в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1530)	21.03.2023
192.168.80.129	425336	Высокий		Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1531)	21.03.2023
192.168.80.129	425337	Высокий		Чтение за пределами выделенной памяти в GPU Video в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1532)	21.03.2023
192.168.80.129	425338	Высокий		Уязвимость доступа к освобожденной памяти в WebProtect в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1533)	21.03.2023
192.168.80.129	425339	Высокий		Чтение за пределами выделенной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1534)	21.03.2023
192.168.80.129	427753	Высокий		Переполнение кучи в Visuals в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1810)	04.04.2023
192.168.80.129	427754	Высокий		Уязвимость доступа к освобожденной памяти в Frames в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1811)	04.04.2023
192.168.80.129	427755	Высокий		Доступ за пределами памяти в DOM Bindings в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1812)	04.04.2023
192.168.80.129	427756	Средний		Ошибка реализации в Extensions в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1813)	04.04.2023

20

Страница 1 из 44

1 2 3 4 5 ... 44

Всего: 862

Под таблицей располагается кнопка **Хосты без успешных результатов сканирования** со списком хостов, для которых в рамках выбранных заданий все сканирования завершились со статусом **Ошибка** или **Хост недоступен**. Данное окно является информационным.

Хосты без данных о проведённых сканированиях

Id хоста	Хост
221	192.168.10.149
222	192.168.10.150
223	192.168.10.151
224	192.168.10.152
225	192.168.10.153
226	192.168.10.154
227	192.168.10.155
228	192.168.10.156
229	192.168.10.157
230	192.168.10.158
231	192.168.10.159
232	192.168.10.160
233	192.168.10.161
234	192.168.10.162
235	192.168.10.163
236	192.168.10.164
237	192.168.10.165
238	192.168.10.166
239	192.168.10.167

50

Страница 5 из 10

1 ... 4 5 6 ... 10

Всего: 497

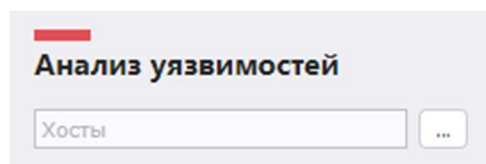
Заккрыть

Общий фильтр

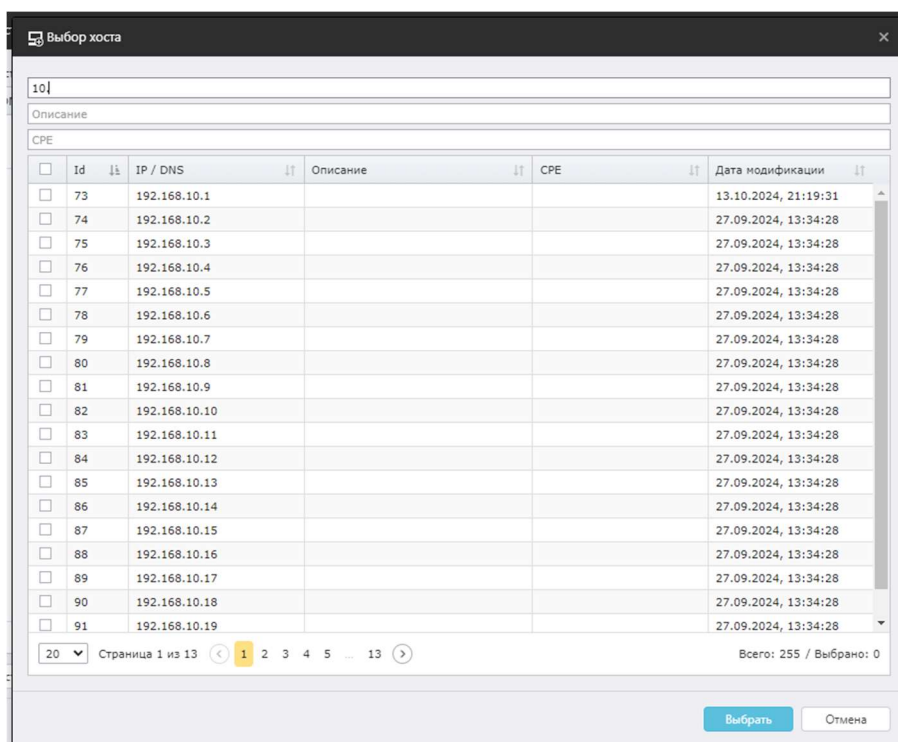
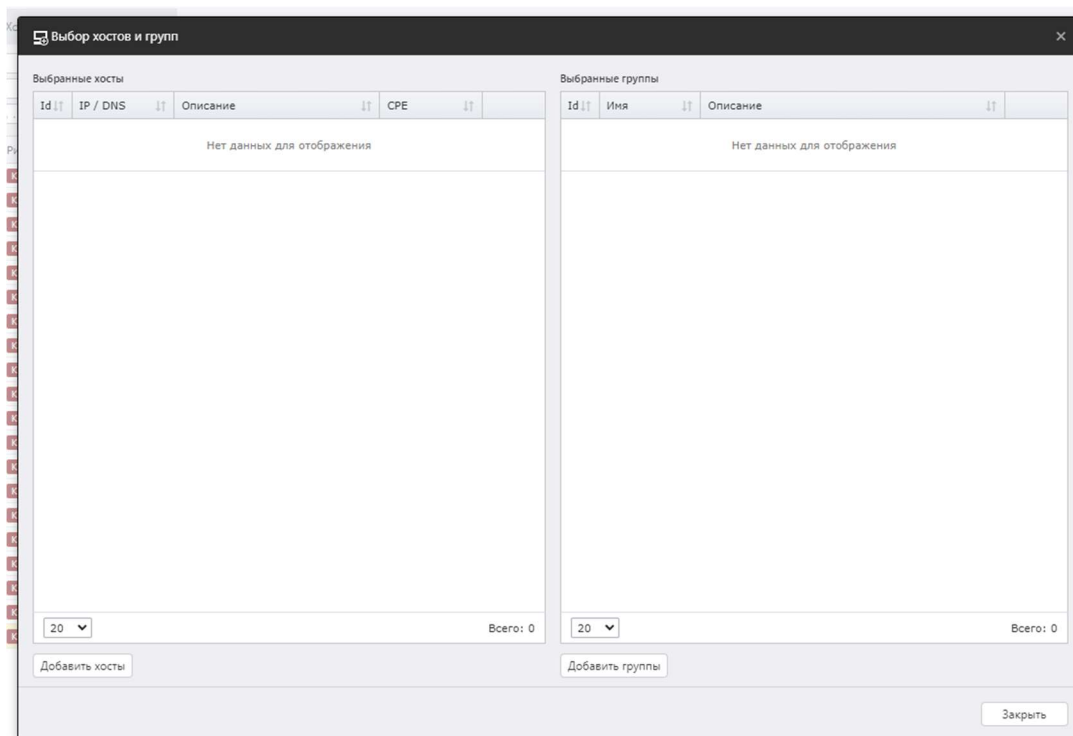
Общий фильтр располагается слева от результирующей таблицы.

REDCheck

231



- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов;



- **Задания** – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;
- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Риск хоста (определяется максимальным риском уязвимости) – будут отображаться хосты, на которых есть хоть одна уязвимость выбранного риска и этот риск является максимальным для хоста.

Например, при фильтрации только по Высокому риску в результирующую таблицу не попадут хосты, у которых обнаружены уязвимости критического уровня.

Хост	Всего уязвимостей	Уровни риска	Дополнительно
> 192.168.80.129	862	44 Критический, 438 Высокий, 363 Средний, 13 Низкий, 4 Не определено	Список уязвимостей
> 192.168.80.5	219	2 Критический, 74 Высокий, 81 Средний, 18 Низкий, 52 Не определено	Список уязвимостей

Хост	Всего уязвимостей	Уровни риска	Дополнительно
Нет данных для отображения			

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-Hosts-dd-mm-yy.csv**.

Структура CSV файла

Id хоста	ID хоста, на котором найдены уязвимости
Имя хоста	IP-адрес или DNS-имя хоста
Описание хоста	Описание хоста
CPE	CPE хоста

Всего уязвимостей	Количество всех уязвимостей, найденных на хосте
Уязвимостей с критичным риском	Количество уязвимостей на хосте с Критическим риском
Уязвимостей с высоким риском	Количество уязвимостей на хосте с Высоким риском
Уязвимостей с средним риском	Количество уязвимостей на хосте со Средним риском
Уязвимостей с низким риском	Количество уязвимостей на хосте с Низким риском
Уязвимостей с неопределенным риском	Количество уязвимостей на хосте с Неопределенным риском
ID сканирования	ID актуального (последнего) результата сканирования со статусом Завершено
Время завершения	Время завершения актуального результата сканирования

Пример:

Код
Id хоста,Имя хоста,Описание хоста,СРЕ,Всего уязвимостей,Уязвимостей с критичным риском,Уязвимостей с высоким риском,Уязвимостей с средним риском,Уязвимостей с низким риском,Уязвимостей с неопределенным риском, ID сканирования,Время завершения 67,192.168.80.129,123,,1430,71,652,549,26,132,1862,14.10.2024 12:45:37

8.3.3 Вкладка Хост – Уязвимость

В данной вкладке отображается информация об уязвимостях с указанием к какому хосту они относятся.

Анализ уязвимостей

Выбрано групп: 9

Выбор задания: Все задания

Выбрать период, дней: 300

Риск: Критический, Средний, Не определено, Высокий, Низкий

CVSS (0-10):

Наличие эксплойта: NVD, ФСТЭК, НКЦКИ

Дата публикации (с):

Дата публикации (по):

Применить фильтр

Уязвимости Хосты Хост — Уязвимость

192.168.80.129 Найдено хостов: 1

Название: ALTIX ID

Ссылка (CVE, BDU, ...): Найдено уникальных уязвимостей: 862

Хост	ALTIX ID	Риск	CVSS	Название	Дата публикации
192.168.80.129	425333	Высокий		Уязвимость доступа к освобожденной памяти в Passwords в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1528)	21.03.2023
192.168.80.129	425334	Критический		Доступ за пределами памяти в WebHID в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1529)	21.03.2023
192.168.80.129	425335	Высокий		Уязвимость доступа к освобожденной памяти в PDF в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1530)	21.03.2023
192.168.80.129	425336	Высокий		Уязвимость доступа к освобожденной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1531)	21.03.2023
192.168.80.129	425337	Высокий		Чтение за пределами выделенной памяти в GPU Video в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1532)	21.03.2023
192.168.80.129	425338	Высокий		Уязвимость доступа к освобожденной памяти в WebProtect в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1533)	21.03.2023
192.168.80.129	425339	Высокий		Чтение за пределами выделенной памяти в ANGLE в Google Chrome, Chromium и Chromium-gost для Linux до 111.0.5563.110 (CVE-2023-1534)	21.03.2023
192.168.80.129	427753	Высокий		Переполнение кучи в Visuals в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1810)	04.04.2023
192.168.80.129	427754	Высокий		Уязвимость доступа к освобожденной памяти в Frames в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1811)	04.04.2023
192.168.80.129	427755	Высокий		Доступ за пределами памяти в DOM Bindings в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1812)	04.04.2023
192.168.80.129	427756	Средний		Ошибка реализации в Extensions в Google Chrome, Chromium и Chromium-gost для Linux до 112.0.5615.49 (CVE-2023-1813)	04.04.2023

Страница 1 из 44

Всего: 862

Информация об уязвимости включает в себя:

- ID последнего сканирования со статусом Завершено, в котором была обнаружена данная уязвимость;
- IP-адрес или DNS имя хоста и ID хоста, на котором обнаружена уязвимость;
- Уникальный идентификатор ALTIX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – Сведения об интегральной оценке по базовым метрикам CVSS;
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Детализация – какие пакеты или файлы уязвимы;

Хост ALTIX ID Риск CVSS Название Дата публикации

192.168.80.129 429217 Критический 10 Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643) 07.12.2022

ID сканирования 1862

Хост 192.168.80.129 (Id = 67)

ALTIX ID 429217

OVAL oval:ru.altix-soft.nix:def:207605

Риск Критический

Оценка CVSS 10 (BDU)

Название Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)

Описание В продуктах linux, linux-5.10, linux-5.15 обнаружена уязвимость CVE-2022-3643.

Дата публикации 07.12.2022

Ссылки CVE CVE-2023-3643

VENDOR 2023-03035E17MD

VENDOR 2.12.46

FSTEC BDU:2023-00265

VENDOR 2023-10235E17

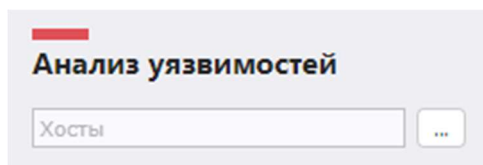
Детализация linux-image-5.4-generic (0:5.4.0-54astra7+cl57)

linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+cl194)

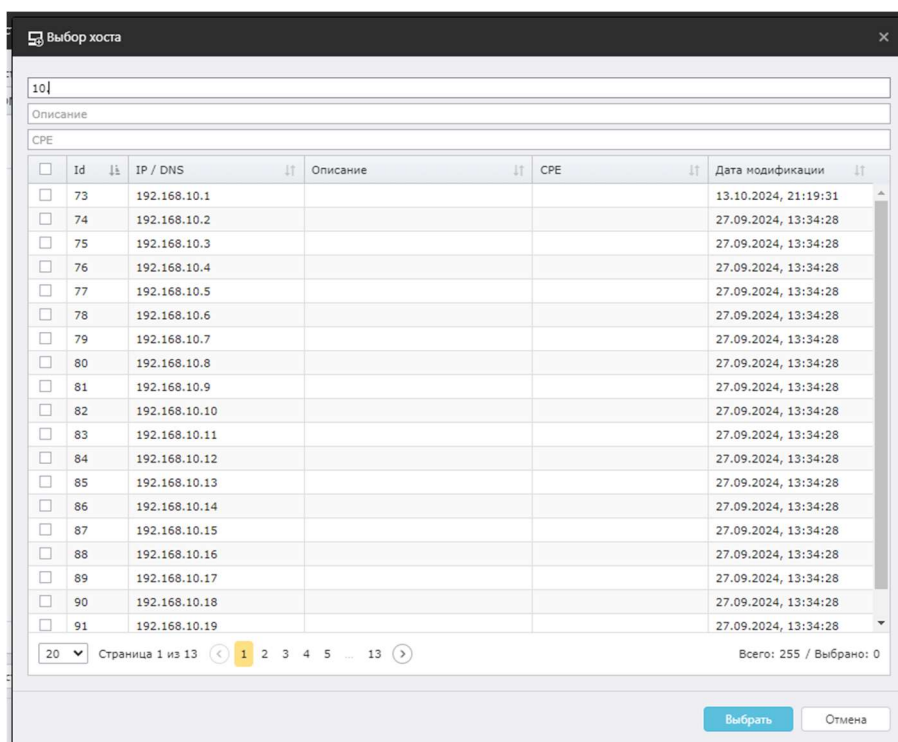
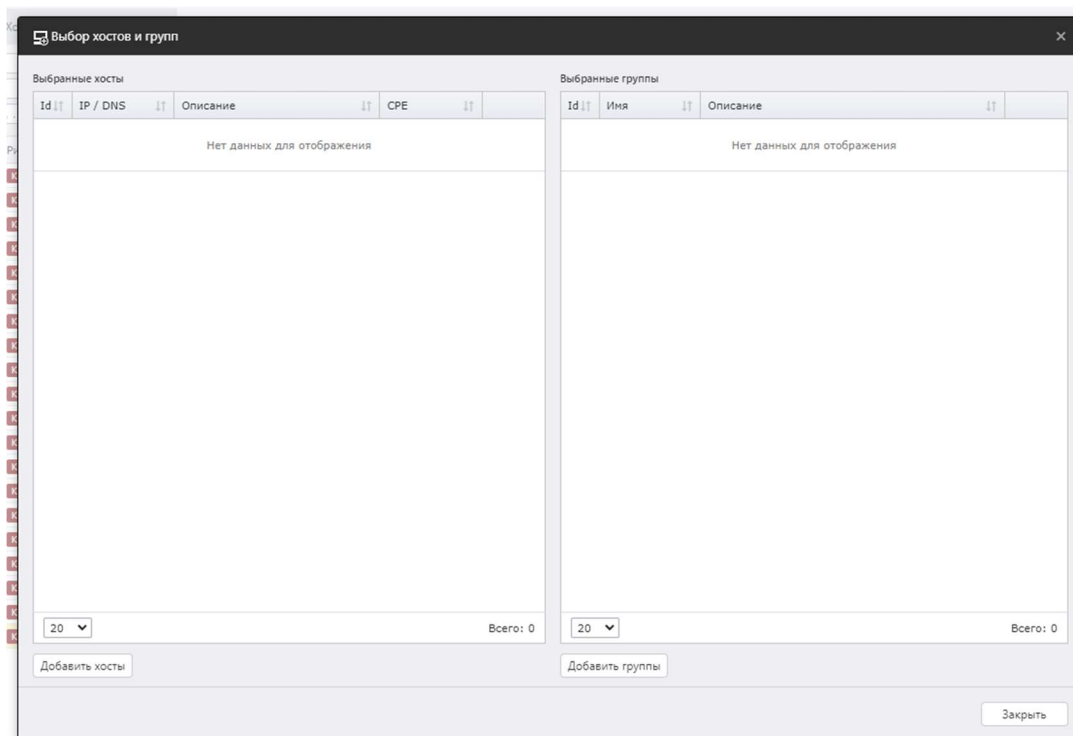
linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+cl49)

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.



- Хосты – можно выбрать хосты, уязвимости для которых будут отображаться. Нажмите на , после чего откроется окно выбора групп и хостов;



- Задания** – можно выбрать задания, из результатов сканирования которых будет производиться поиск уязвимостей. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для поиска уязвимостей;
- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;
- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Название – имя уязвимости;
- ALTX ID – уникальный идентификатор уязвимости;
- Ссылка (CVE, BDU, ...) – идентификатор бюллетеня по данной уязвимости;
- Найдено хостов – количество хостов, отображаемых в таблице согласно данному фильтру;
- Найдено уникальных уязвимостей – количество уязвимостей без дублирования согласно данному фильтру. Уязвимости с одним и тем же ALTX ID могут встречаться несколько раз, если уязвимыми оказались несколько пакетов или файлов (строка Детализация из подробной информации о найденной уязвимости);
- Риск – в таблице будут отображаться уязвимости с отмеченными уровнями риска.

The screenshot shows a filter interface with three tabs: 'Уязвимости', 'Хосты', and 'Хост — Уязвимость'. The 'Хост — Уязвимость' tab is active. It contains three input fields: '192.168.80.129' (with 'Найдено хостов: 1' below it), 'Название' (with 'ALTX ID' below it), and 'Ссылка (CVE, BDU, ...)' (with 'Найдено уникальных уязвимостей: 862' below it). To the right, there are risk level statistics: 'Критический (44)', 'Высокий (438)', 'Средний (363)', 'Низкий (13)', and 'Не определено (4)'. Each has a corresponding colored square and a checkmark. An 'Экспорт в CSV' button is on the far right.

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityAnalysis-VulnerabilitiesForHosts-dd-mm-yyyy.csv**.

Структура CSV файла

ID сканирования	ID актуального (последнего) результата сканирования со статусом Завершено
Id хоста	ID хоста, на котором найдены уязвимости
Имя хоста	IP-адрес или DNS-имя хоста
ALTX ID	Уникальный идентификатор уязвимости
OVAL	Ссылка на страницу уязвимости в OVALdb

определение	
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости. Указывается в двойных кавычках
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетени вендором
Детализация	Уязвимые пакеты или файлы. Если значений несколько, разделяется точкой с запятой

Пример:

Код
ID сканирования, Id хоста, Имя хоста, ALTX ID, OVAL определение, Риск, Оценка CVSS, Источник CVSS, Уязвимость, Описание, Дата публикации, Детализация 1866,69,192.168.80.8,343423,oval:ru.altx- soft.nix:def:144841,Высокий,"8,8",BDU,"Уязвимость доступа к освобожденной памяти в clipboard в Google Chrome, Chromium и Chromium-gost для Linux до 87.0.4280.88 (CVE-2020-16037)",Уязвимость доступа к освобожденной памяти в clipboard в Google Chrome.,08.01.2021,chromium (0:87.0.4280.66-0astragost1)

8.4 Контроль устранения уязвимостей

Данная форма аналитики позволяет проводить сравнение состояния инфраструктуры на предмет наличия уязвимостей в двух временных отметках.

Для перехода на форму нажмите **Аналитика → Контроль устранения уязвимостей**

Содержание

- [8.4.1 Вкладка Уязвимости](#)
- [8.4.2 Вкладка Хосты](#)
- [8.4.3 Вкладка Хост – Уязвимость](#)

8.4.1 Вкладка Уязвимости

В данной вкладке отображается информация о наличии уязвимостей и их устранении на хостах, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.

Контроль устранения уязвимостей

Уязвимости

Хосты

Хост — Уязвимость

Название

1_21 - Duplicate2

ALTIX ID

10.09.2024, 14:14:51 - 10.09.2024

Ссылка (CVE, BDU, ...)

✓ Новые (0)

✓ Неустраненные (847)

✓ Устраненные (0)

Экспорт в CSV

Сравнить с предыдущими результатами

Выбор сканирование

Выбор периода, дней:

30

Хосты

Риск

✓ Критический

✓ Средний

✓ Не определено

✓ Высокий

✓ Низкий

CVSS (0-10)

Наличие эксплойта

NVD

ОСТЭК

НКЦКИ

Дата публикации (с)

Дата публикации (по)

Применить фильтр

ALTIX ID

Риск

CVSS

Название

Дата публикации

Новая для хостов

Неустраненная для хостов

Устраненная для хостов

Дополнительно

➤ 404975

Средний

Astra Linux -- уязвимость в python2.7 (CVE-2021-3733)

10.03.2022

0

1

0

Список хостов

➤ 404976

Высокий

Astra Linux -- уязвимость в python2.7 (CVE-2021-3737)

04.03.2022

0

1

0

Список хостов

➤ 405050

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2021-4197)

23.03.2022

0

1

0

Список хостов

➤ 405151

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-0494)

25.03.2022

0

1

0

Список хостов

➤ 405191

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1011)

18.03.2022

0

1

0

Список хостов

➤ 405192

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1012)

05.08.2022

0

1

0

Список хостов

➤ 405193

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1048)

29.04.2022

0

1

0

Список хостов

➤ 405206

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1184)

29.08.2022

0

1

0

Список хостов

➤ 405208

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1198)

29.08.2022

0

1

0

Список хостов

➤ 405209

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1199)

29.08.2022

0

1

0

Список хостов

➤ 405210

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1204)

29.08.2022

0

1

0

Список хостов

➤ 405222

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.4 (CVE-2022-1353)

29.04.2022

0

1

0

Список хостов

➤ 405231

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1652)

02.06.2022

0

1

0

Список хостов

➤ 405232

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1729)

01.09.2022

0

1

0

Список хостов

➤ 405233

Высокий

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1734)

18.05.2022

0

1

0

Список хостов

➤ 405234

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1974)

31.08.2022

0

1

0

Список хостов

➤ 405235

Средний

Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15, linux-5.4 (CVE-2022-1975)

31.08.2022

0

1

0

Список хостов

20

Страница 1 из 43

12345

43

Всего: 847

Уязвимости в таблице сгруппированы по ALTIX ID. Если уязвимость была обнаружена на одном хосте / нескольких хостах в разных файлах / пакетах, то на этой вкладке сведения по ней будут показаны в рамках одной строки.

Информация об уязвимости включает в себя:

- Уникальный идентификатор ALTIX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Информация о появлении и устранении данной уязвимости на хостах;

ALTIX ID	Риск	CVSS	Название	Дата публикации	Новая для хостов	Неустраненная для хостов	Устраненная для хостов	Дополнительно
429217	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022	0	1	0	Список хостов
ALTIX ID	429217							
OVAL								
Риск	Критический							
Оценка CVSS	10,0 (BDU)							
Название	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)							
Описание	В продуктах linux, linux-5.10, linux-5.15 обнаружена уязвимость CVE-2022-3643.							
Дата публикации	07.12.2022							
Ссылки								
VENDOR	2023-10235E17							
VENDOR	2.12.46							
FSTEC	BDU:2023-00265							
CVE	CVE-2022-3643							
VENDOR	2023-03035E17MD							

Нажав **Список хостов**, вы перейдете на вкладку **«Хост – Уязвимость»**, где в фильтре для результирующей таблицы уже будет указан ALTIX ID выбранной уязвимости. В случае, если одна и та же уязвимость была найдена в разных файлах / пакетах, то для каждого случая в таблице будет собственная строка с информацией.

Если анализируется одна уникальная уязвимость, то под чекбоксами фильтра «по Статусу уязвимости» будет указано количество хостов для каждого статуса.

The screenshot shows the 'Control of vulnerability removal' interface. On the left is a sidebar with filters for task, scan date, risk, CVSS, and exploit status. The main area displays a table of vulnerabilities for host 192.168.80.129. The table has columns for Host, ALTIX ID, Status, Risk, CVSS, Name, and Publication Date. One vulnerability is listed: Astra Linux -- уязвимость в python2.7 (CVE-2021-3733) with a status of 'Not removed' and a risk of 'Critical'.

Хост	ALTIX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.80.129	404975	Неустранен	Средний		Astra Linux -- уязвимость в python2.7 (CVE-2021-3733)	10.03.2022

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

The close-up shows the sidebar with the title 'Control of vulnerability removal'. It has two input fields: 'Задание' (Task) and 'Актуальное сканирование' (Current scan), each with a dropdown arrow.

- Задание – необходимо выбрать задание типа Аудит уязвимостей.

Нажмите на , после чего откроется окно выбора:

- Всего – сколько было запусков задания;
- Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);

Выбор задания

×

Имя

№	Имя	Тип сканирования	Р	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

20

Страница 1 из 1

<

1

>

Всего: 2

Выбрать

Отмена

- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;

Выберите сканирование

×

ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1

20

Страница 1 из 1

<

1

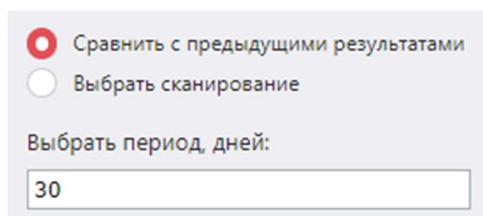
>

Всего: 3

Выбрать

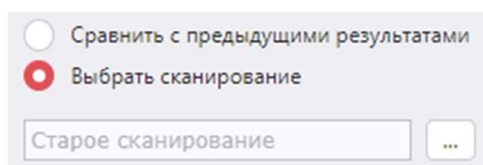
Отмена

- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;



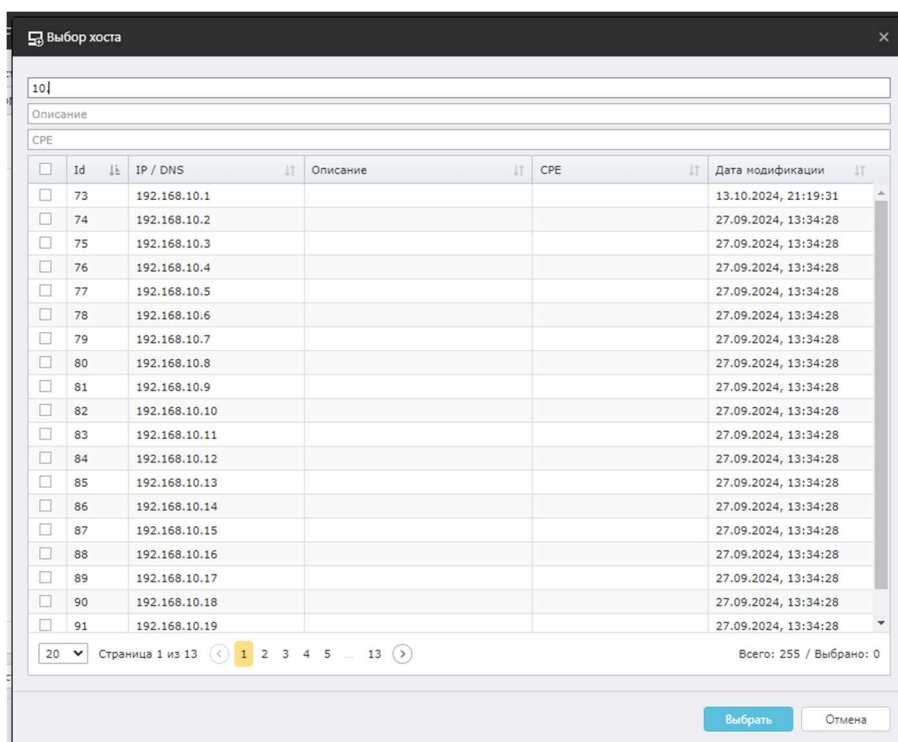
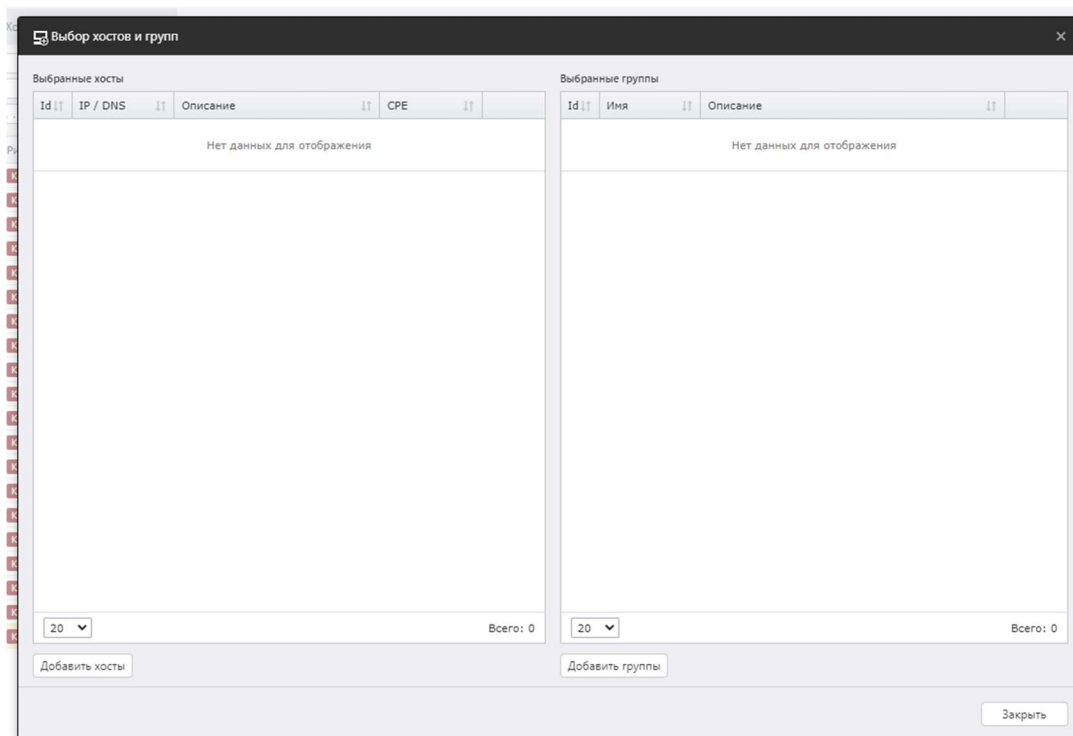
☒ Сравнить с предыдущими результатами
☐ Выбрать сканирование
 Выбрать период, дней:

- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;



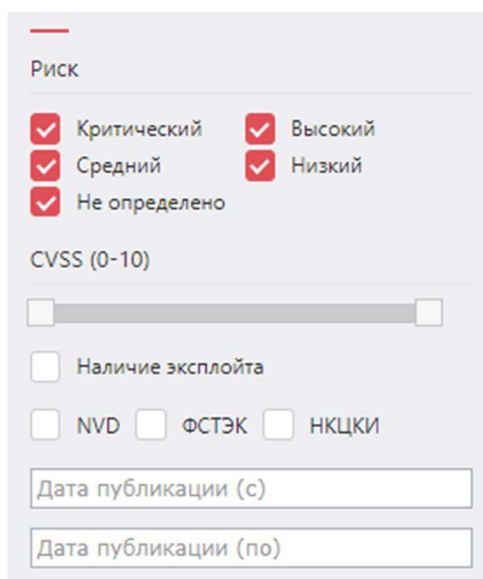
☐ Сравнить с предыдущими результатами
☒ Выбрать сканирование

- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на , после чего откроется окно выбора групп и хостов:

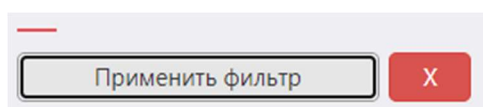


- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;

- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.



Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Название – название уязвимости;
- ALTX ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Статус уязвимости – в таблице будут отображаться уязвимости с отмеченными статусами. Если хотя бы на одном хосте уязвимость имеет выбранный статус, она попадёт в данную таблицу.
 - Новые – уязвимости, появившиеся в актуальном сканировании (итерации запуска);
 - Неустраненные – уязвимости, которые были найдены в предыдущих сканированиях и остались неустраненными в актуальном сканировании;

- Устраненные – уязвимости, которые были найдены в предыдущих сканированиях и устранены в актуальном сканировании;

Уязвимости

Хосты

Хост — Уязвимость

Название

ALTIX ID

Ссылка (CVE, BDU, ...)

✓ Новые (0)

✓ Неустраненные (847)

44

434

352

13

4

✓ Устраненные (0)

Экспорт в CSV

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityRemediationControl-Vulnerabilities-dd-mm-yyyy.csv**.

Структура CSV файла

ALTIX ID	Уникальный идентификатор уязвимости
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости
Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором
Новая для хостов	Количество хостов, для которых данная уязвимость новая, т.е. появилась в актуальном сканировании (итерации запуска)
Неустраненная для хостов	Количество хостов, для которых данная уязвимость была найдены в предыдущих сканированиях и осталась неустраненной в актуальном сканировании
Устраненная для	Количество хостов, для которых данная уязвимость была

 REDCheck

250

ХОСТОВ

найжены в предыдущих сканированиях и устранена в актуальном сканировании

Пример:

Bash (оболочка Unix)

ALTХ ID, Риск, Оценка CVSS, Источник CVSS, Уязвимость, Описание, Дата публикации, Новая для хостов, Неустраненная для хостов, Устраненная для хостов
404856, Средний, "6, 5", BDU, "Astra Linux -- уязвимость в thunderbird, icu (CVE-2020-21913)", "В продуктах thunderbird, icu обнаружена уязвимость CVE-2020-21913.", 20.09.2021, 0, 1, 0

8.4.2 Вкладка Хосты

В данной вкладке отображается информация о наличии или устранении уязвимостей на хостах, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.

Контроль устранения уязвимостей

1234 - put

10.09.2024, 14:11:50 - 10.09.2024

Сравнить с предыдущими результатами

Выбор периода, дней: 30

Хосты

Риск

☒ Критический ☒ Высокий

☒ Средний ☒ Низкий

☒ Не определено

CVSS (0-10)

☐ Наличие эксплойта

☐ NVD ☐ CPE ☐ NCCE

Дата публикации (с)

Дата публикации (по)

Применить фильтр

Уязвимости Хосты Хост — Уязвимость

Хост

Нет устранения уязвимостей (1) Нет новых уязвимостей (1)

Устраненные уязвимости (0) Новые уязвимости (0)

Экспорт в CSV

Хост	Новые уязвимости	Среди них критических и высоких	Неустраненные уязвимости	Среди них критических и высоких	Устраненные уязвимости	Среди них критических и высоких	Дополнительно
192.168.80.5	0		219	2 74	0		Список уязвимостей

Страница 1 из 1

Всего: 1

Информация об уязвимостях на хосте включает в себя:

- Хост – IP-адрес или DNS-имя хоста;
- Новые уязвимости (среди них критических и высоких) – количество новых уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;
- Неустраненные уязвимости (среди них критических и высоких) – количество неустраненных уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;
- Устраненные уязвимости (среди них критических и высоких) – количество устраненных уязвимостей для хоста и сколько среди них с риском Критическая и Высокая;

Нажав **Список уязвимостей**, вы перейдете на вкладку «**Хост – Уязвимость**», где в фильтре для результирующей таблицы уже будет указано имя выбранного хоста. Под каждым чекбоксом фильтра по Статусу уязвимости будет отображаться количество уязвимостей с группировкой по риску.

Контроль устранения уязвимостей

1234 - put

10.09.2024, 14:11:50 - 10.09.2024

Сравнить с предыдущими результатами

Выбрать сканирование

Выбрать период, дней:

30

Хосты

Риск

Критический

Средний

Не определено

Высокий

Низкий

CVSS (0-10)

Наличие эксплойта

NVD

ОСТЭК

НКСКИ

Дата публикации (с)

Дата публикации (по)

Применить фильтр

X

Уязвимости

Хосты

Хост — Уязвимость

192.168.80.5

Найдено хостов: 1

ALTIX ID

Ссылка (CVE, BDU, ...)

Найдено уникальных уязвимостей: 219

Новые уязвимости

Неустраненные уязвимости

Устраненные уязвимости

Экспорт в CSV

Хост	ALTIX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.80.5	516497	Неустраненная	Критический		RED OS -- уязвимость в ghostscript (CVE-2021-3781)	16.02.2022
192.168.80.5	516546	Неустраненная	Критический		RED OS -- уязвимость в httpd (CVE-2024-40898)	18.07.2024
192.168.80.5	514911	Неустраненная	Высокий		RED OS -- уязвимость в gnutls (CVE-2022-2509)	01.08.2022
192.168.80.5	515109	Неустраненная	Высокий		Уязвимость в Oracle Java и OpenJDK (CVE-2024-21147)	16.07.2024
192.168.80.5	515471	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6988)	06.08.2024
192.168.80.5	515472	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6989)	06.08.2024
192.168.80.5	515473	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6991)	06.08.2024
192.168.80.5	515476	Неустраненная	Высокий		Переполнение кучи в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6994)	06.08.2024
192.168.80.5	515479	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6997)	06.08.2024
192.168.80.5	515480	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6998)	06.08.2024
192.168.80.5	515482	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-7000)	06.08.2024
192.168.80.5	516104	Неустраненная	Высокий		Использование неинициализированной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-6990)	01.08.2024
192.168.80.5	516105	Неустраненная	Высокий		Чтение за пределами выделенной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-7255)	01.08.2024
192.168.80.5	516106	Неустраненная	Высокий		Недостаточная проверка данных в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-7256)	01.08.2024
192.168.80.5	516498	Неустраненная	Высокий		RED OS -- уязвимость в automake, cpio (CVE-2021-38185)	08.08.2021
192.168.80.5	516959	Неустраненная	Высокий		Доступ за пределами памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.99 (CVE-2024-7532)	06.08.2024

20

Страница 1 из 11

1 2 3 4 5 11

Всего: 219

Если в актуальном сканировании не найдены хосты, которые были в прошлых итерациях запуска, то появится баннер с указанием количества недоступных хостов.

Уязвимости

Хосты

Хост — Уязвимость

Хост

Нет устранения уязвимостей (2)

Нет новых уязвимостей (5)

Устраненные уязвимости (4)

Новые уязвимости (1)

1

Недоступный хост

Экспорт в CSV

Хост	Новые уязвимости	Среди них критических и высоких	Неустраненные уязвимости	Среди них критических и высоких	Устраненные уязвимости	Среди них критических и высоких	Дополнительно
192.168.10.99	0		2359	102 1032	0		Список уязвимостей
192.168.10.80	32	2 15	619	17 473	0		Список уязвимостей
192.168.10.78	0		124	110	511	8 368	Список уязвимостей
192.168.10.42	0		3277	68 2809	4	1 9	Список уязвимостей
192.168.10.36	0		568	81 129	1	1	Список уязвимостей
192.168.10.250	0		846	87 136	1	1	Список уязвимостей

При нажатии на **Недоступный хост** будет открыта форма «Недоступность хостов» с перечнем хостов и причин их недоступности.

Все результаты

Хост

Причина недоступности

Экспорт в CSV

Хост	Тип сканирования	Задание	Результат	Причина недоступности	Время завершения
192.168.10.99	Аудит уязвимостей	уязвимости windows агент новая задача	Хост недоступен	Агент не найден или не запущен.	16.10.2024, 13:39:56

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

Контроль устранения уязвимостей

Задание

Актуальное сканирование

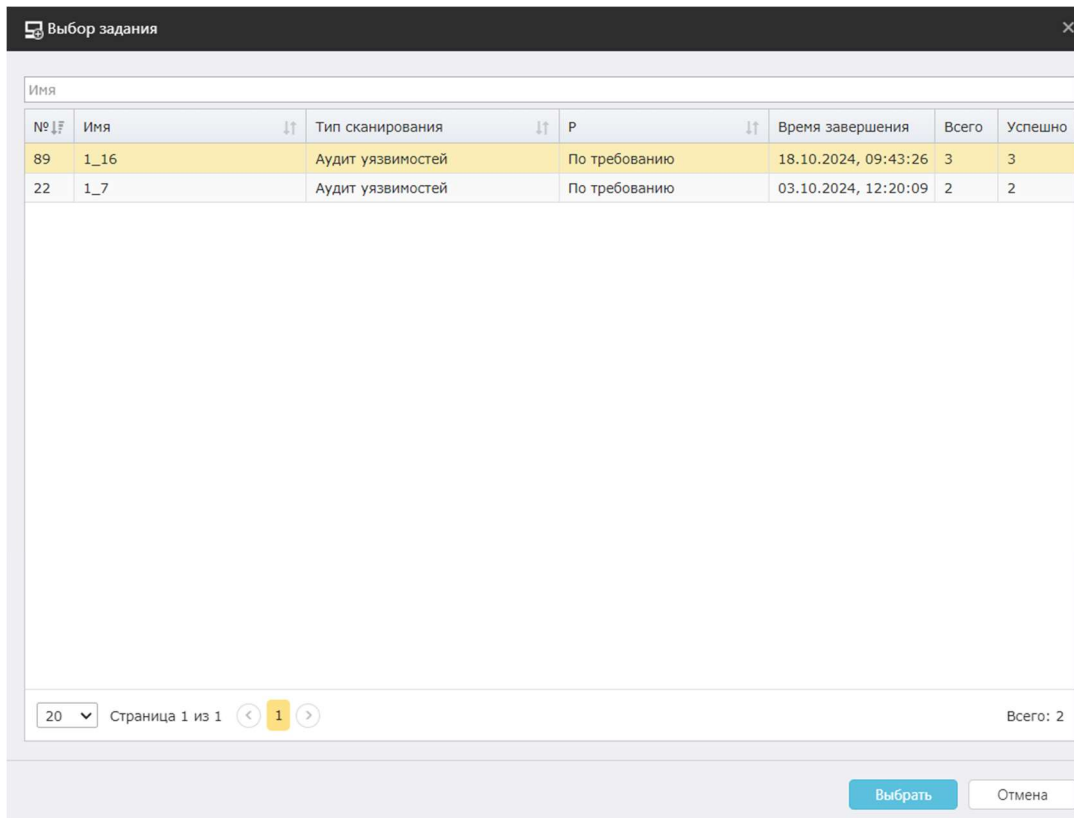
REDCheck

253

- Задание – необходимо выбрать задание типа Аудит уязвимостей.

Нажмите на , после чего откроется окно выбора:

- Всего – сколько было запусков задания;
- Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);



№	Имя	Тип сканирования	Р	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

Страница 1 из 1 1 Всего: 2

Выбрать Отмена

- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;

Выберите сканирование					
ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1

20 Страница 1 из 1 1 Всего: 3

Выбрать Отмена

- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;;

☒ Сравнить с предыдущими результатами
☐ Выбрать сканирование

Выбрать период, дней:

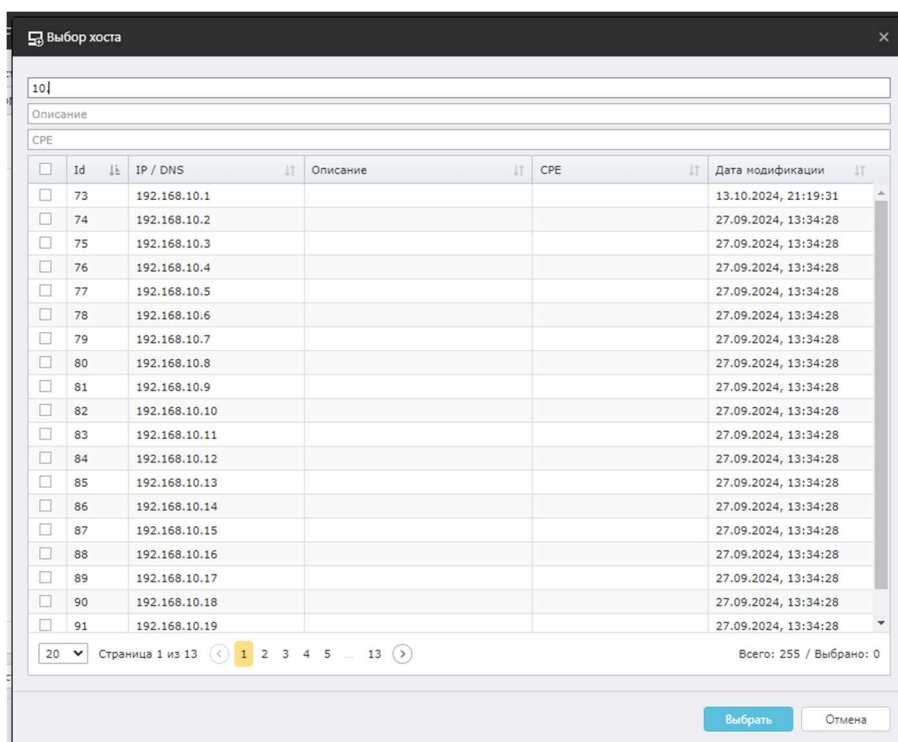
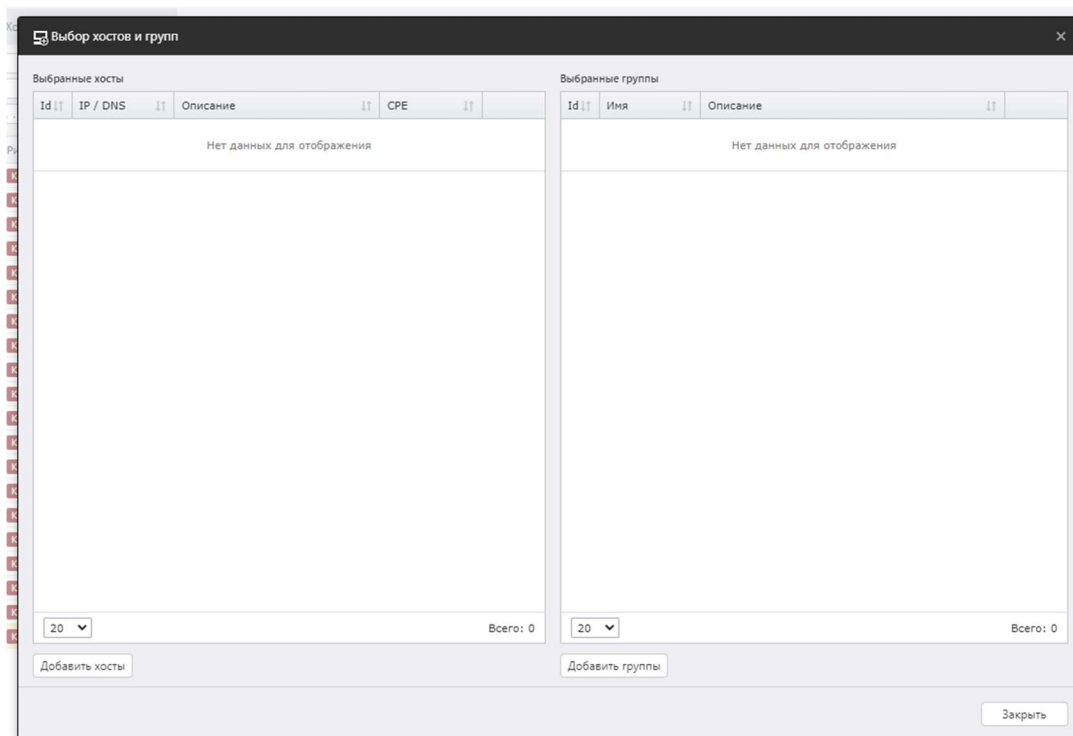
30

- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

☐ Сравнить с предыдущими результатами
☒ Выбрать сканирование

Старое сканирование ...

- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на , после чего откроется окно выбора групп и хостов:



- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;

- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Статус уязвимости – будет отображаться:
 - Нет устранения уязвимостей – хосты, у которых значение столбца **Устраненные уязвимости** равно 0;
 - Нет новых уязвимостей – хосты, у которых значение столбца **Новые уязвимости** равно 0;
 - Устраненные уязвимости – хосты, у которых значение столбца **Устраненные уязвимости** НЕ равно 0;
 - Новые уязвимости – хосты, у которых значение столбца **Новые уязвимости** НЕ равно 0;

Уязвимости
Хосты
Хост — Уязвимость

☒ Нет устранения уязвимостей (1)
☒ Устраненные уязвимости (0)

☒ Нет новых уязвимостей (1)
☒ Новые уязвимости (0)

Экспорт в CSV

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityRemediationControl-Hosts-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Новые уязвимости	Количество новых уязвимостей
Новые критические уязвимости	Количество новых уязвимостей с критическим риском Сведения об интегральной оценке по базовым метрикам CVSS
Новые уязвимости с высокой критичностью	Количество новых уязвимостей с высоким риском
Неустранимые уязвимости	Количество неустранимых уязвимостей
Неустранимые критические уязвимости	Количество неустранимых уязвимостей с критическим риском
Неустранимые уязвимости с высоким уровнем критичности	Количество неустранимых уязвимостей с высоким риском
Устраненные	Количество устраненных уязвимостей

уязвимости	
Устранённые критичные уязвимости	Количество устраненных уязвимостей с критическим риском
Устранённые уязвимости с высокой критичностью	Количество устраненных уязвимостей с высоким риском

Пример:

Bash (оболочка Unix)
Id хоста,Имя хоста,Новые уязвимости,Новые критичные уязвимости,Новые уязвимости с высокой критичностью,Неустраненные уязвимости,Неустраненные критические уязвимости,Неустраненные уязвимости с высоким уровнем критичности,Устраненные уязвимости,Устранённые критичные уязвимости,Устранённые уязвимости с высокой критичностью 67,192.168.80.129,0,0,0,1430,71,652,0,0,0

8.4.3 Вкладка Хост – Уязвимость

В данной вкладке отображается информация о наличии уязвимостей и их устранении с указанием к какому хосту они относятся, согласно выбранному заданию и итерации запуска в сравнении с предыдущими итерациями.

Контроль устранения уязвимостей

1234 - put

10.09.2024, 14:11:50 - 10.09.2024

Сравнить с предыдущими результатами

Выбор сканирования

Выбор периода, дней: 30

Хосты

Риск

☒ Критический

☒ Средний

☒ Не определено

☒ Высокий

☒ Низкий

CVSS (0-10)

☐ Наличие эксплойта

☐ NVD

☐ ФСТЕК

☐ ИКЦИИ

Дата публикации (с)

Дата публикации (по)

Применить фильтр

Уязвимости

Хосты

Хост -- Уязвимость

192.168.80.5

Найдено хостов: 1

Название

ALTIX ID

Ссылка (CVE, BDU, ...)

Найдено уникальных уязвимостей: 219

☒ Новые уязвимости

☒ Неустраненные уязвимости

☒ Устраненные уязвимости

Экспорт в CSV

Хост	ALTIX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.80.5	516497	Неустраненная	Критический		RED OS -- уязвимость в ghostscript (CVE-2021-3781)	16.02.2022
192.168.80.5	516546	Неустраненная	Критический		RED OS -- уязвимость в httpd (CVE-2024-40898)	18.07.2024
192.168.80.5	514911	Неустраненная	Высокий		RED OS -- уязвимость в gnutls (CVE-2022-2509)	01.08.2022
192.168.80.5	515109	Неустраненная	Высокий		Уязвимость в Oracle Java и OpenJDK (CVE-2024-21147)	16.07.2024
192.168.80.5	515471	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6988)	06.08.2024
192.168.80.5	515472	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6989)	06.08.2024
192.168.80.5	515473	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6991)	06.08.2024
192.168.80.5	515476	Неустраненная	Высокий		Переполнение кучи в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6994)	06.08.2024
192.168.80.5	515479	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6997)	06.08.2024
192.168.80.5	515480	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-6998)	06.08.2024
192.168.80.5	515482	Неустраненная	Высокий		Уязвимость доступа к освобожденной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.72 (CVE-2024-7000)	06.08.2024
192.168.80.5	516104	Неустраненная	Высокий		Использование неинициализированной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-6990)	01.08.2024
192.168.80.5	516105	Неустраненная	Высокий		Чтение за пределами выделенной памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-7255)	01.08.2024
192.168.80.5	516106	Неустраненная	Высокий		Недостаточная проверка данных в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.88 (CVE-2024-7256)	01.08.2024
192.168.80.5	516498	Неустраненная	Высокий		RED OS -- уязвимость в automake, cpio (CVE-2021-38185)	08.08.2021
192.168.80.5	516959	Неустраненная	Высокий		Доступ за пределами памяти в Google Chrome, Chromium и Chromium-gost для Linux до 127.0.6533.99 (CVE-2024-7532)	06.08.2024

Страница 1 из 11

Информация об уязвимости включает в себя:

- Хост – IP-адрес или DNS-имя (ID хоста);
- Уникальный идентификатор ALTIX ID;
- Ссылка на страницу уязвимости в OVALdb;
- Риск и CVSS – [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Имя уязвимости, описание, дата публикации вендором;
- Ссылки на бюллетени по данной уязвимости;
- Детализация – какие пакеты или файлы уязвимы;

Хост	ALTIX ID	Статус уязвимости	Риск	CVSS	Название	Дата публикации
192.168.80.129	429217	Неустраненная	Критический	10	Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643)	07.12.2022
Хост ALTIX ID OVAL Риск Оценка CVSS Название Описание Дата публикации Ссылки 192.168.80.129 (Id = 67) 429217 oval:ru.altix-soft.nix:def:207605 Критический 10,0 (BDU) Astra Linux -- уязвимость в linux, linux-5.10, linux-5.15 (CVE-2022-3643) В продуктах linux, linux-5.10, linux-5.15 обнаружена уязвимость CVE-2022-3643. 07.12.2022 VENDOR 2023-1023SE17 VENDOR 2.12.46 FSTEC BDU:2023-00265 CVE CVE-2022-3643 VENDOR 2023-0303SE17MD						
Детализация linux-image-5.4-generic (0:5.4.0-54astra7+c157) linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+c149) linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+c1194)						

Детализация

linux-image-5.4-generic (0:5.4.0-54astra7+ci57)
linux-image-5.4.0-54-generic (0:5.4.0-54.astra31+ci49)
linux-image-5.4.0-110-generic (0:5.4.0-110.astra35+ci194)

Общий фильтр

Общий фильтр располагается слева от результирующей таблицы.

Контроль устранения уязвимостей

Задание

...

Актуальное сканирование

...

- Задание – необходимо выбрать задание типа Аудит уязвимостей.

Нажмите на

...

, после чего откроется окно выбора:

- Всего – сколько было запусков задания;
- Успешно – сколько из них выполнились успешно (хотя бы одно сканирование имеет статус **Завершено**);

Выбор задания

Имя

№	Имя	Тип сканирования	Р	Время завершения	Всего	Успешно
89	1_16	Аудит уязвимостей	По требованию	18.10.2024, 09:43:26	3	3
22	1_7	Аудит уязвимостей	По требованию	03.10.2024, 12:20:09	2	2

20

Страница 1 из 1

< 1 >

Всего: 2

ВыбратьОтмена

- Актуальное сканирование – необходимо выбрать итерацию запуска, с которой будут сравниваться предыдущие запуски. В такой итерации запуска должно быть хотя бы одно успешное сканирование;

Выберите сканирование						
ID	Задание	Начало	Завершение	Всего хостов	Успешно просканировано	
111	1_16	18.10.2024, 12:41:54	18.10.2024, 12:43:26	1	1	
108	1_16	14.10.2024, 15:44:09	14.10.2024, 15:45:40	1	1	
104	1_16	09.10.2024, 11:09:23	09.10.2024, 11:10:37	1	1	

20

Страница 1 из 1

<

1

>

Всего: 3

Выбрать

Отмена

- Сравнивать с предыдущими результатами – сравнить с предыдущим успешным сканированием. Для каждого хоста предыдущее успешное сканирование подбирается индивидуально и может быть взято из разных итерацией запуска. Фильтр по времени позволяет ограничить период, за который подбирается предыдущее успешное сканирование;;

☒ Сравнить с предыдущими результатами
 ☐ Выбрать сканирование

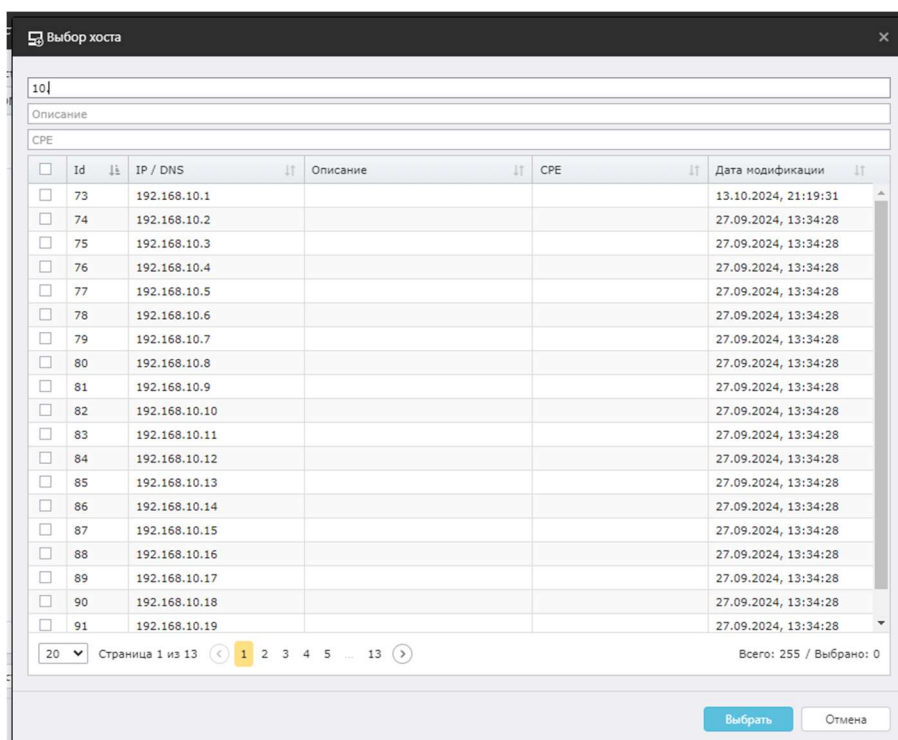
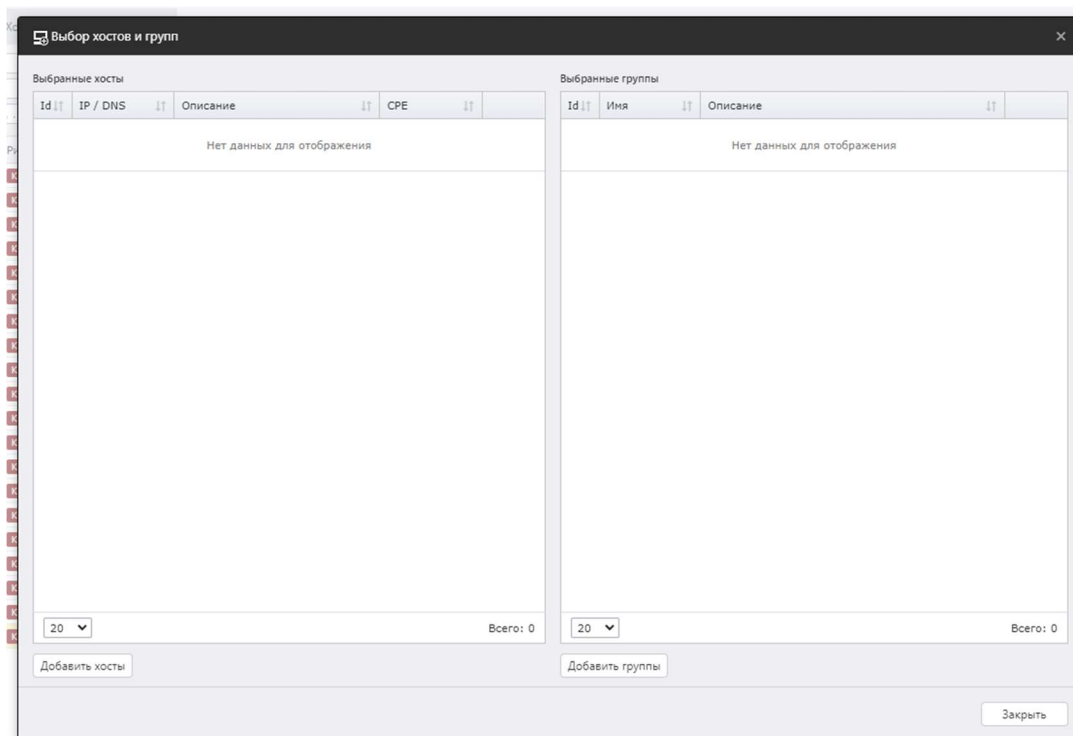
Выбрать период, дней:

- Выбрать сканирование – сравнение выбранной выше итерации будет проходить с одной конкретной итерацией запуска для выбранного задания;

☐ Сравнить с предыдущими результатами
 ☒ Выбрать сканирование

Старое сканирование

- Хосты – можно выбрать хосты, для которых будет проведен контроль устранения уязвимостей. Нажмите на , после чего откроется окно выбора групп и хостов:



- Риск и CVSS – отображать уязвимости с указанным риском и CVSS; [Сведения об интегральной оценке по базовым метрикам CVSS](#);
- Наличие эксплойта – отображать уязвимости, которые имеют эксплойт;
- Базы данных уязвимостей – отображать уязвимости, которые есть в отмеченных базах уязвимостей;

- Дата публикации (с / по) – отображать уязвимости, которые были опубликованы вендором в указанный период.

Риск

☒ Критический ☒ Высокий

☒ Средний ☒ Низкий

☒ Не определено

CVSS (0-10)

☐ Наличие эксплойта

☐ NVD ☐ ФСТЭК ☐ НКЦКИ

Дата публикации (с)

Дата публикации (по)

Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.

Применить фильтр

X

Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста. Можно указывать как полное значение, так и часть;
- Название – название уязвимости;
- ALTX ID – уникальный идентификатор уязвимости, состоящий из цифр;
- Ссылка – идентификатор бюллетеня по данной уязвимости;
- Статус уязвимости – в таблице будут отображаться уязвимости с отмеченными вариантами риска.
 - Новые уязвимости – уязвимости, появившиеся в актуальном сканировании (итерации запуска);
 - Неустраненные уязвимости – уязвимости, которые были найдены в предыдущих сканированиях и остались неустраненными в актуальном сканировании;

- Устраненные уязвимости – уязвимости, которые были найдены в предыдущих сканированиях и устранены в актуальном сканировании;
- Найдено хостов – количество хостов;
- Найдено уникальных уязвимостей – количество уникальных уязвимостей, обнаруженных на всех найденных хостах;

Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **VulnerabilityRemediationControl-HostVulnerability-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
ALTIX ID	Уникальный идентификатор уязвимости
OVAL определение	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Статус уязвимости	Принимает значения: Устраненная, Неустраненная, Новая
Риск	Принимает значения: Критический, Высокий, Средний, Низкий
Оценка CVSS	Значение указывается в двойных кавычках. Сведения об интегральной оценке по базовым метрикам CVSS
Источник CVSS	Название вендора или базы данных уязвимостей, откуда взято значение для оценки CVSS
Уязвимость	Имя уязвимости. Указывается в двойных кавычках

Описание	Описание уязвимости
Дата публикации	Дата публикации бюллетеня вендором
Детализация	Уязвимые пакеты или файлы. Если значений несколько, разделяется точкой с запятой

Пример:

Bash (оболочка Unix)
Id хоста,Имя хоста,ALTX ID,OVAL определение,Статус уязвимости,Риск,Оценка CVSS,Источник CVSS,Уязвимость,Описание,Дата публикации,Детализация <pre>67,192.168.80.129,404856,oval:ru.altx-soft.nix:def:188035,Неустранимая,Средний,"6,5",BDU,"Astra Linux -- уязвимость в thunderbird, icu (CVE-2020-21913)","В продуктах thunderbird, icu обнаружена уязвимость CVE-2020-21913.",20.09.2021,thunderbird (1:102.9.1+build1-0ubuntu1+ci202304061128+astral);thunderbird-locale-ru (1:102.9.1+build1-0ubuntu1+ci202304061128+astral)</pre>

Дополнительная информация на форме

1 Случай. В фильтре для результирующей таблицы указан ALTX ID. В случае, если одна и та же уязвимость будет найдена в разных файлах / пакетах, то для каждого случая в таблице отобразится собственная строка с информацией.

Если анализируется одна уникальная уязвимость, то под чекбоксами фильтра «по Статусу уязвимости» будет указано количество хостов для каждого статуса.

8.5 Анализ конфигураций

Данная форма аналитики позволяет оценить соответствие инфраструктуры правилам выбранной конфигурации.

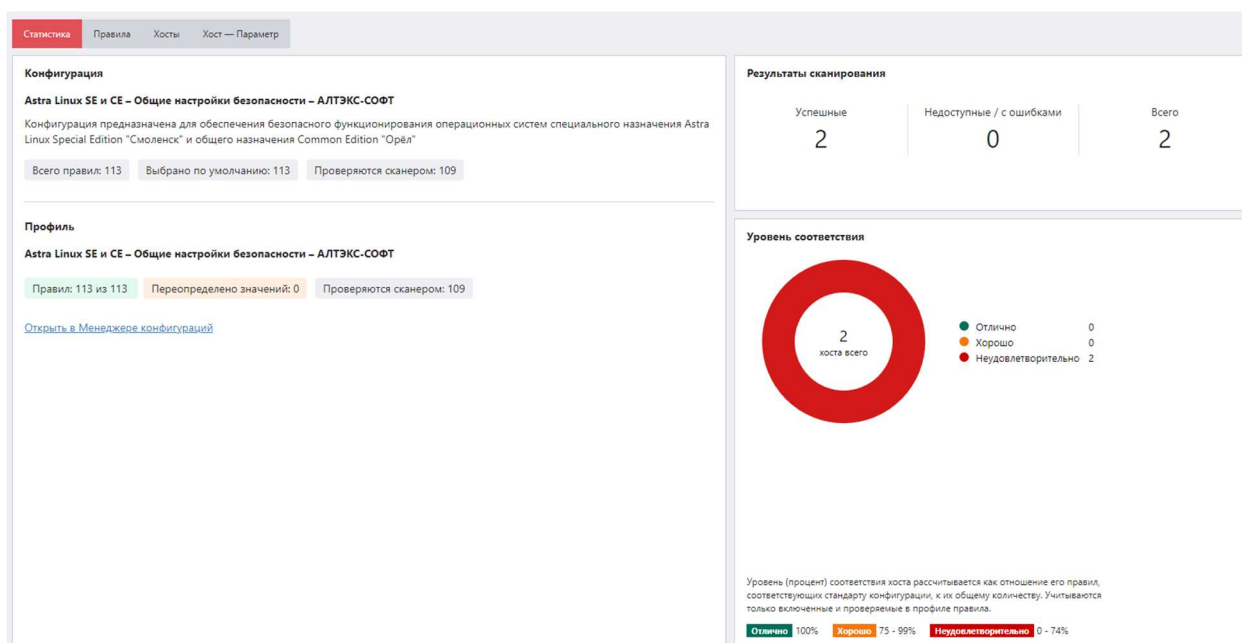
Для перехода на форму нажмите **Аналитика** → **Анализ конфигураций**

Содержание

- [8.5.1 Вкладка Статистика](#)
- [8.5.2 Вкладка Правила](#)
- [8.5.3 Вкладка Хосты](#)
- [8.5.4 Вкладка Хост – Параметр](#)

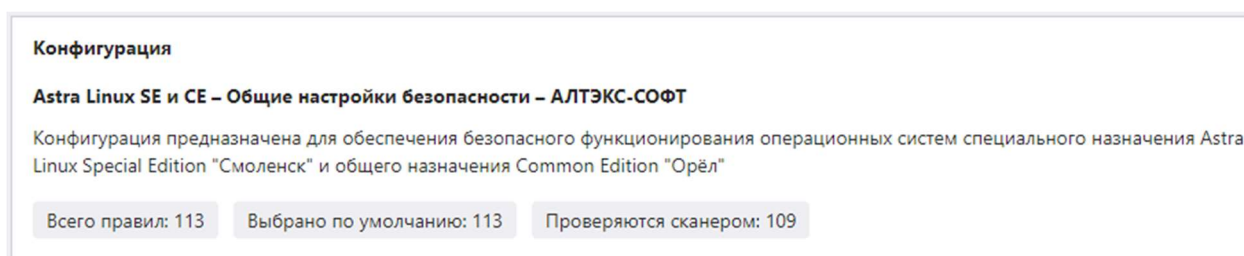
8.5.1 Вкладка Статистика

В данной вкладке отображается базовая информация о выбранной конфигурации, профиле, результатах сканирования и уровне соответствия хостов правилам конфигурации.

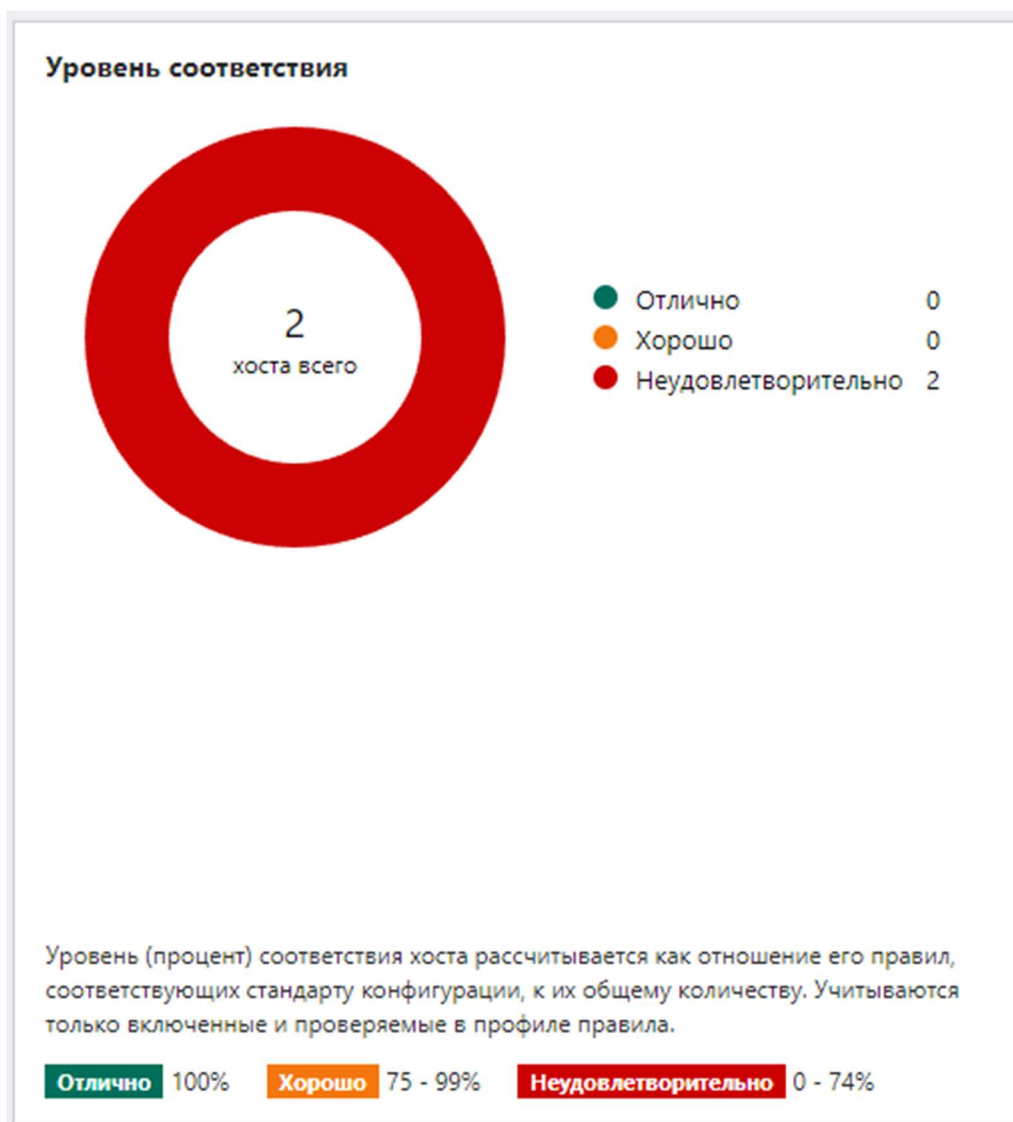


- **Конфигурация** – название и описание конфигурации, сколько всего правил в конфигурации, сколько правил включено для проверки, сколько правил проверяются сканером;

Проверяются сканером – некоторые правила не могут быть проверены сканером. Это касается правил, например, связанных с процессами документирования. Фактически у сканера нет возможности узнать, документирует ли ваша команда какой-либо процесс, однако это является рекомендацией.



- **Профиль** – название профиля, количество включенных правил, количество переопределенных в правилах значений, количество проверяемых сканером правил;

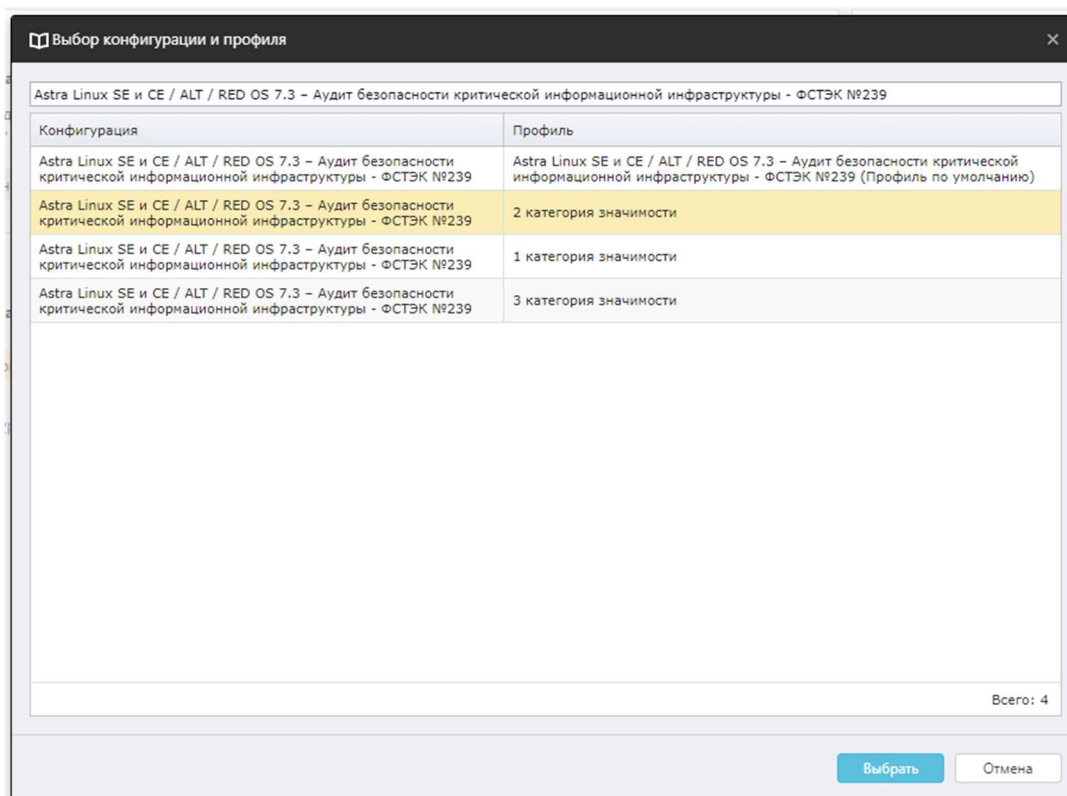


Общий фильтр

Анализ конфигураций

Конфигурация

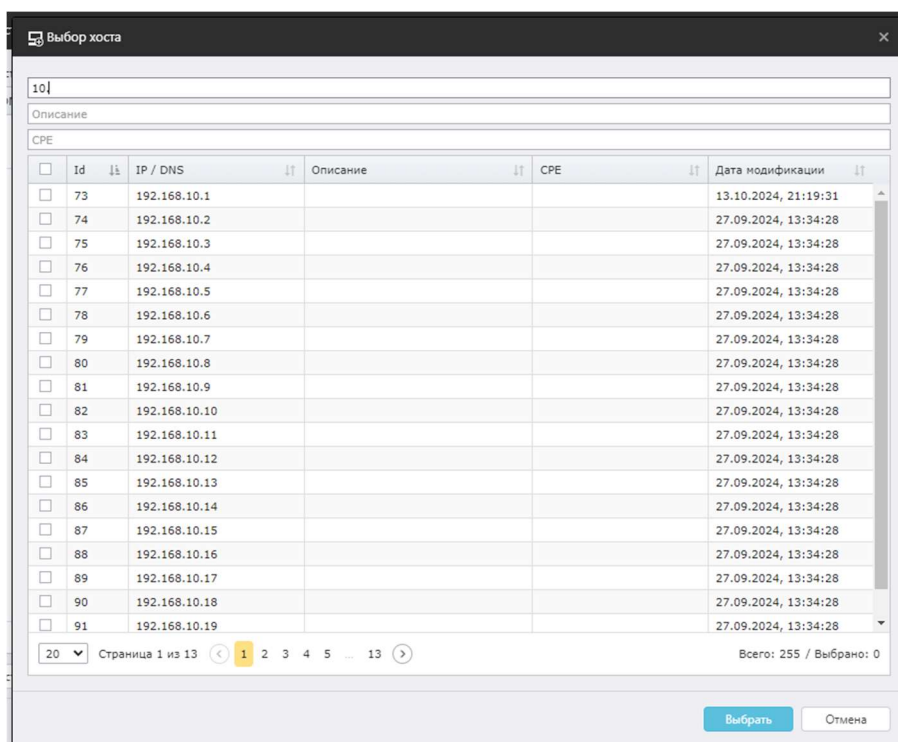
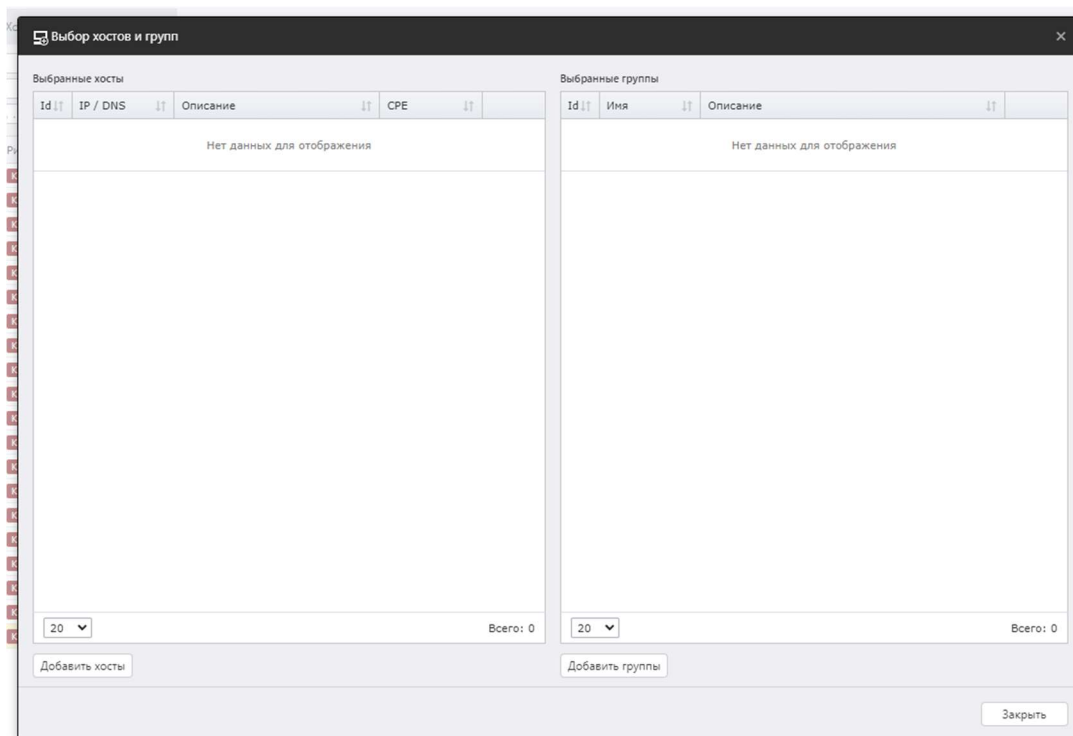
- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на и выберите нужную конфигурацию;



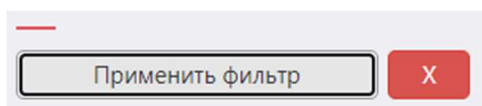
- **Задания** – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- **Выбрать период, дней** – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- **Хосты** – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на , после чего откроется окно выбора групп и хостов:



Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



8.5.2 Вкладка Правила

В данной вкладке отображается информация по каждому проверяемому правилу конфигурации.

Анализ конфигураций

Статистика

Правила

Хосты

Хост — Параметр

Аstra Linux SE 1.7 – Настройки

Правило

✓ Критический

✓ Низкий

✓ Высокий

✓ Не определено

✓ Средний

Экспорт в CSV

Все задачи

Выбрать период, дней:

30

Хосты

Применить фильтр

X

№ п/п	Правило	Риск	Хостов "Соответствие"	Хостов "Несоответствие"	Хостов "Ошибки" или "Неизвестно"	Хостов "Непринимено"	Дополнительно
> 1	Раздел /boot	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 2	Раздел /home	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 3	Раздел /tmp	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 4	Раздел /var/tmp	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 5	Раздел /var	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 6	Ядро hardened	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 7	Запрет трассировки pttrace	Средний	1 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 8	Запрет установки бита исполнения	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 9	Запрет исполнения скриптов пользователя	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 10	Запрет исполнения макросов пользователя	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 11	Запрет консоли	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 12	Системные ограничения ulimits	Высокий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 13	Минимальная длина пароля	Средний	1 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 14	Минимальное количество строчных букв в новом пароле	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 15	Минимальное количество заглавных букв в новом пароле	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 16	Минимальное количество цифр в новом пароле	Низкий	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 17	Минимальное количество дней между сменами пароля	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
> 18	Максимальное количество дней между сменами пароля	Средний	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах

Страница 1 из 1

<

1

>

Всего: 30

Выбранные, но не проверяемые сканером правила

Информация о правиле включает в себя:

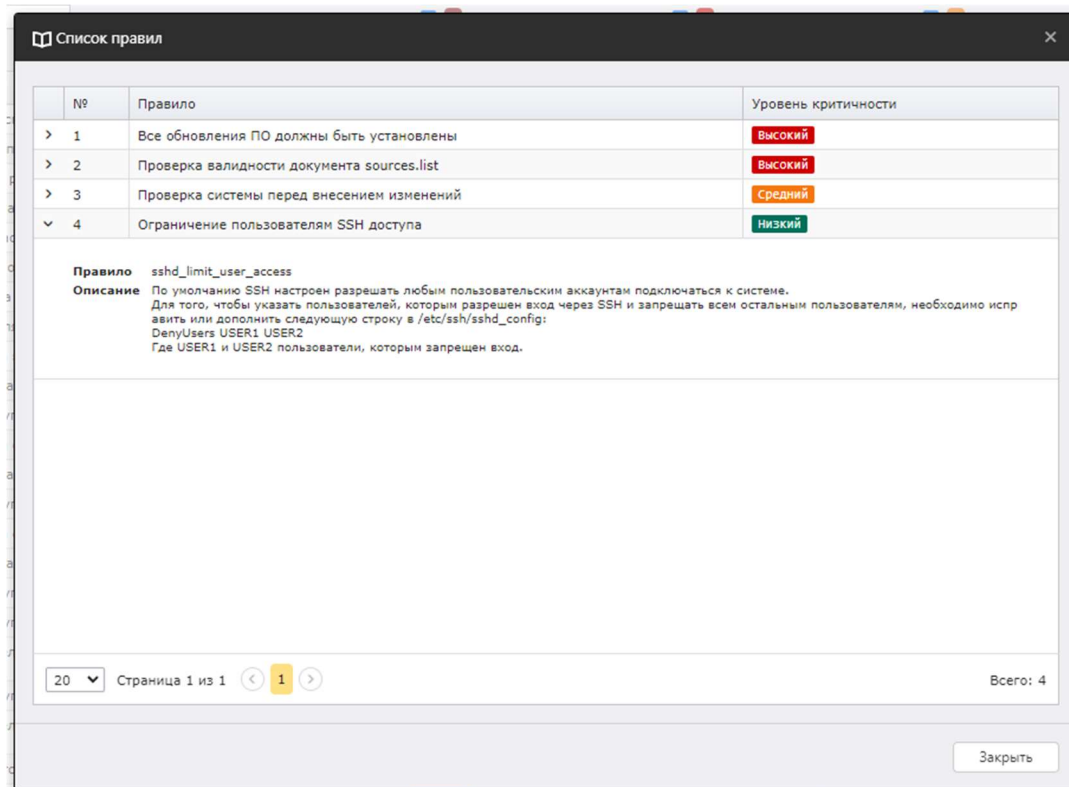
- Порядковый номер правила в конфигурации
- Правило – название и ID правила;
- OVAL – ссылка на страницу правила в OVALdb;
- Описание – описание правила;
- Уровень риска правила;
- Хостов "Соответствие" – количество хостов, которые соответствуют правилу;
- Хостов "Несоответствие" – количество хостов, которые не соответствуют правилу;
- Хостов "Ошибка" или "Неизвестно" – количество хостов, проверка правила на которых завершилась с результатом "Ошибка" или "Неизвестно";
- Хостов "Неприменимо" – количество хостов, для которых правило неприменимо;

№ п/п	Правило	Риск	Хостов "Соответствие"	Хостов "Несоответствие"	Хостов "Ошибка" или "Неизвестно"	Хостов "Неприменимо"	Дополнительно
1	Директория /tmp располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах
2	Директория /var располагается на отдельном разделе	Низкий	0 (0 %)	2 (100 %)	0 (0 %)	0 (0 %)	Значения на хостах

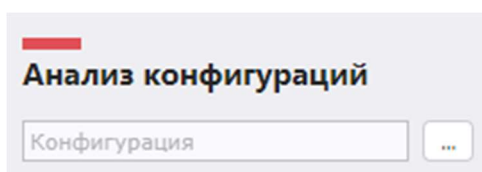
Правило partition_for_var
OVAL oval:linux-aws-soft:unixdef:26021
Описание: Директория /var используется служебной и другими системными сервисами для хранения часто изменяющихся данных. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её подднее, используя LVM.

Нажав **Значения на хостах**, вы перейдете на вкладку «Хост – Параметр», где уже будет выбрано соответствующее правило.

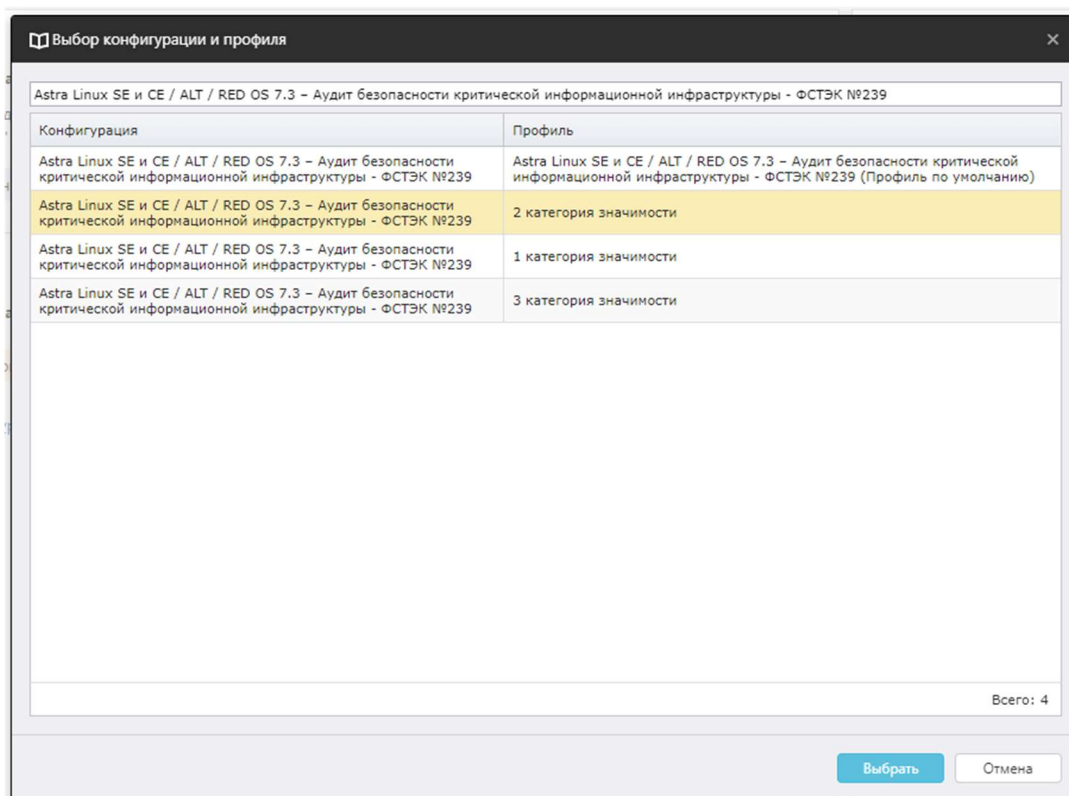
Под таблицей находится кликабельная ссылка **Выбранные, но не проверяемые сканером правила**. При нажатии открывается окно со списком правил, которые не проверяются сканером.



Общий фильтр



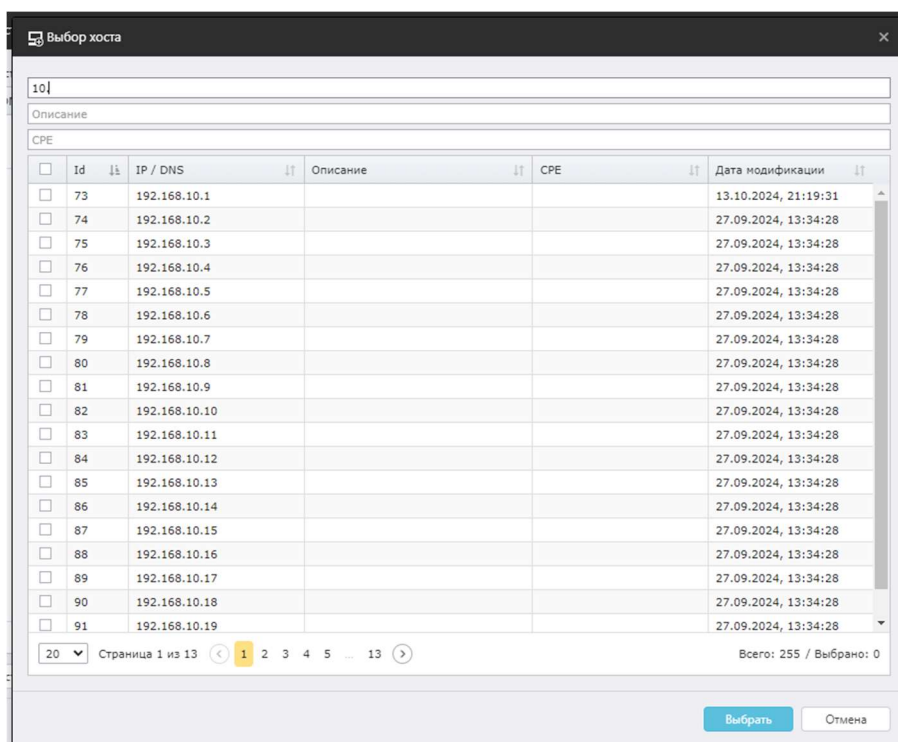
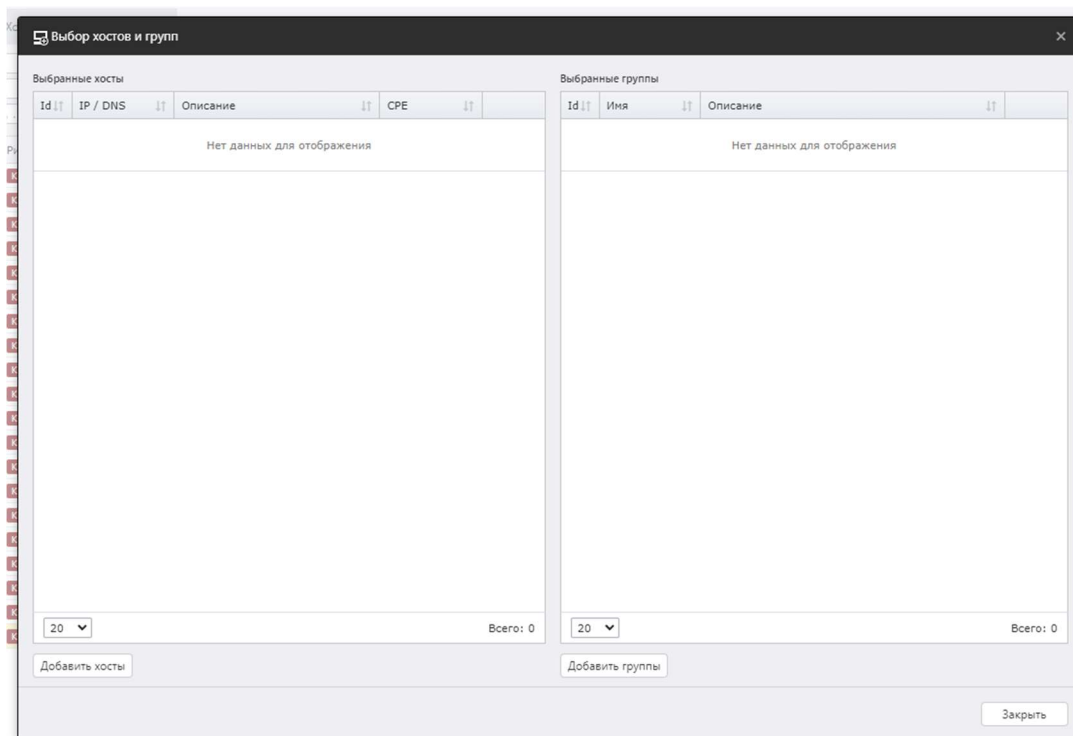
- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на  и выберите нужную конфигурацию;



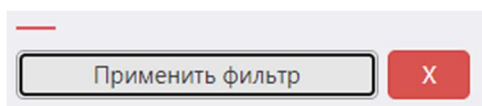
- **Задания** – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- **Выбрать период, дней** – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- **Хосты** – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на , после чего откроется окно выбора групп и хостов:



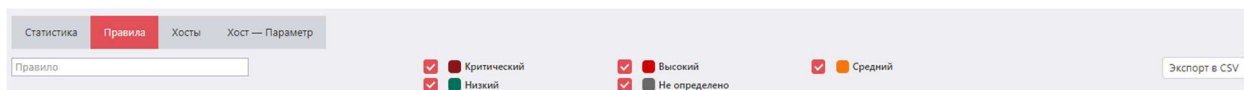
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Правило – название правила;
- Риск – в таблице будут отображаться правила с отмеченными вариантами риска.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-RulesStatistics-dd-mm-yyyy.csv**.

Структура CSV файла

Номер правила	Порядковый номер правила в конфигурации
Правило	Название правила
Уровень критичности	Принимает значения: Критический, Высокий, Средний, Низкий
Количество хостов с результатом проверки правила Соответствие	Хостов "Соответствие"
Количество хостов с результатом проверки правила Несоответствие	Хостов "Несоответствие"

Количество хостов с результатом проверки правила Ошибка или Неизвестно	Хостов "Ошибка" или "Неизвестно"
Количество хостов с результатом проверки правила Неприменимо	Хостов "Неприменимо"
Id правила	ID правила, например partition_for_tmp
OVAL определение	Ссылка на OVAL-определение правила
Описание	Описание правила

Пример:

Код
Номер правила, Правило, Уровень критичности, Количество хостов с результатом проверки правила Соответствие, Количество хостов с результатом проверки правила Несоответствие, Количество хостов с результатом проверки правила Ошибка или Неизвестно, Количество хостов с результатом проверки правила Неприменимо, Id правила, OVAL определение, Описание 1, Директория /tmp располагается на отдельном разделе, Низкий, 0, 2, 0, 0, partition_for_tmp, oval:ru.altx-soft.nix:def:26020, "Директория /tmp доступна для всех на запись и используется для хранения временных файлов. Необходимо убедиться во время установки, что она располагается на отдельном разделе или логическом томе, либо перенести её позднее, используя LVM."

8.5.3 Вкладка Хосты

В данной вкладке отображается информация о соответствии каждого хоста выбранной конфигурации.

Хост	Процент соответствия	Уровень соответствия	Соответствие	Несоответствие	Риск несоответствующих правил	Неизвестно	Ошибка	Неприменимо	Дополнительно
192.168.80.129	33 %	Неудовлетворительно	4	26	4 11 11	0	0	0	Результаты сканирования

Информация о правиле включает в себя:

- Хост – IP-адрес или DNS-имя хоста;
- Процент соответствия – Уровень (процент) соответствия хоста рассчитывается как отношение его правил, соответствующих стандарту конфигурации, к их общему количеству. Учитываются только включенные и проверяемые в профиле правила.;
- Уровень соответствия – оценка соответствия:
 - 100% – Отлично;
 - 75-99% – Хорошо;
 - 0-74% – Неудовлетворительно;
- Соответствие – количество правил со статусом "Соответствие";
- Несоответствие – количество правил со статусом "Несоответствие";
- Риск несоответствующих правил – группировка несоответствующих правил по риску;
- Неизвестно – количество правил со статусом "Неизвестно";
- Ошибка – количество правил со статусом "Ошибка";
- Неприменимо – количество правил со статусом "Неприменимо";

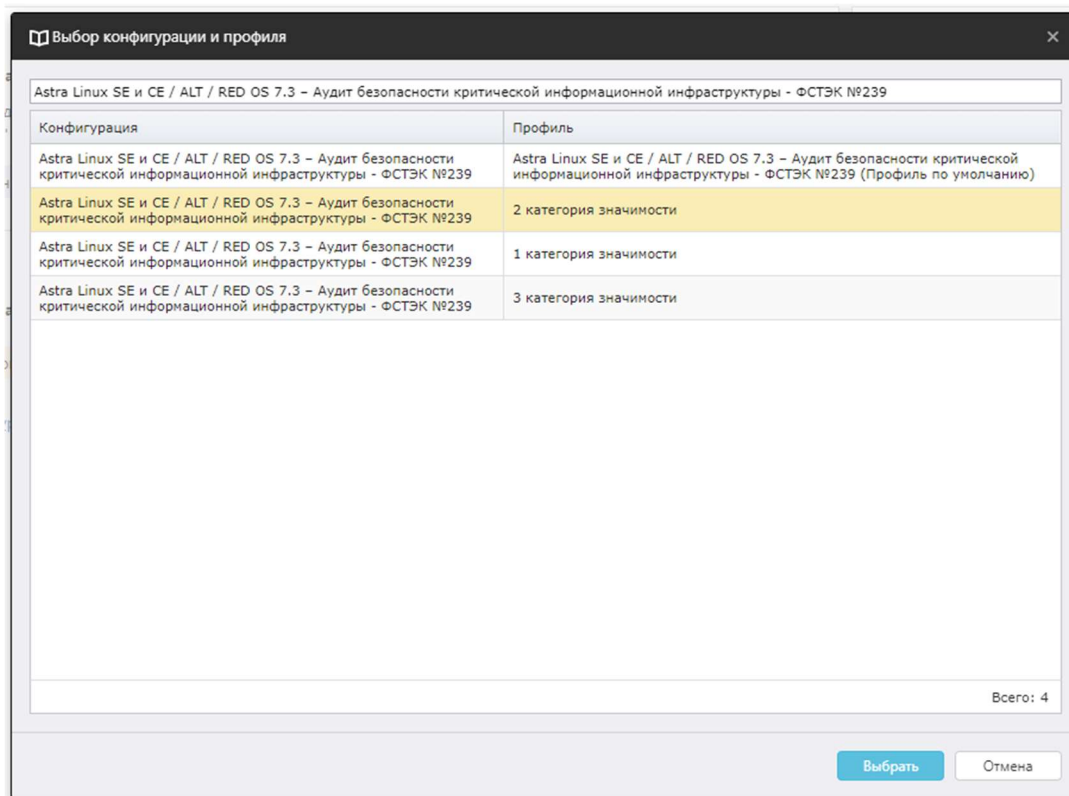
Нажав **Результаты сканирования**, вы перейдете на страницу с актуальным результатом сканирования для данного хоста и выбранной конфигурации.

Общий фильтр

Анализ конфигураций

Конфигурация

- Конфигурация – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на  и выберите нужную конфигурацию;

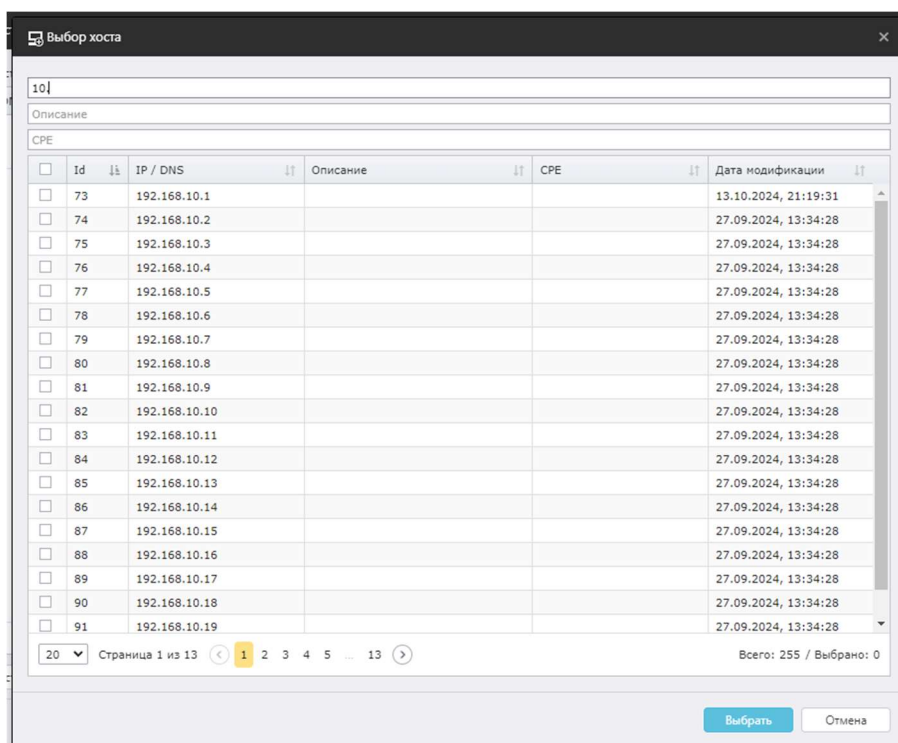
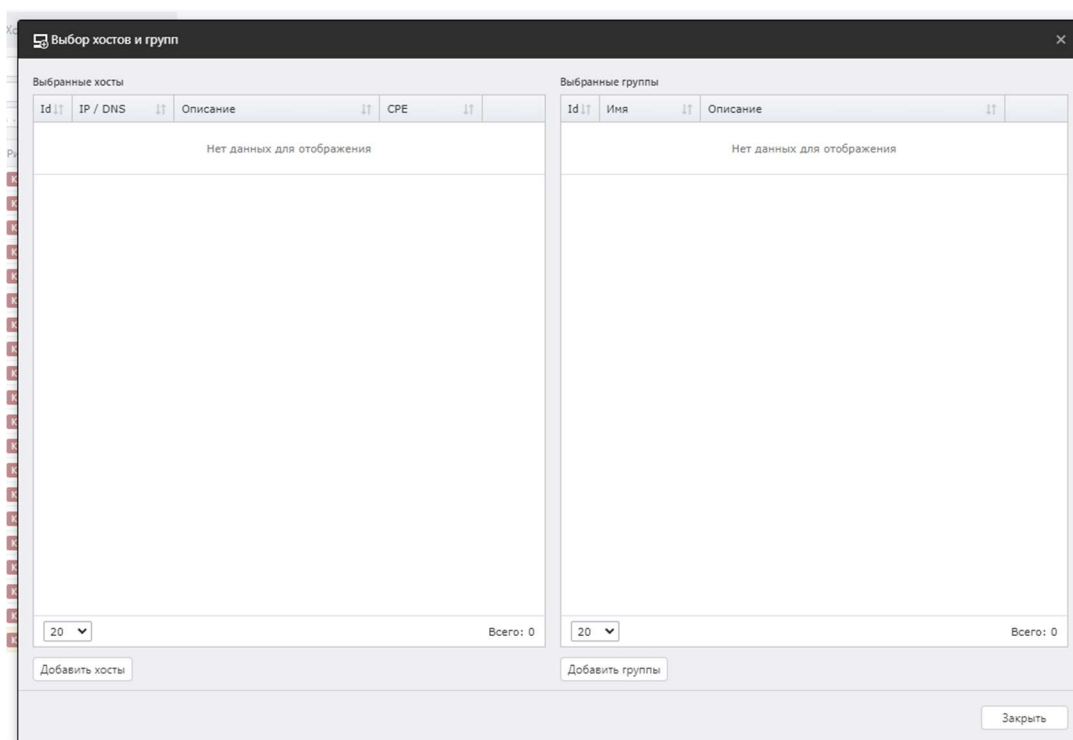


- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

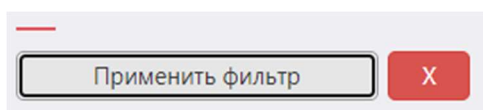
Нажмите на , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;

- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на , после чего откроется окно выбора групп и хостов:



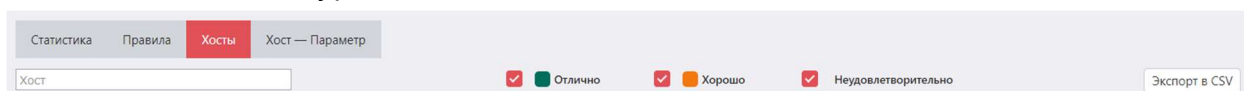
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Уровень соответствия – в таблице будут отображаться хосты с отмеченными уровнями соответствия.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-HostsStatistics-dd-mm-yyyy.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Процент соответствия	Соответствие хоста выбранной конфигурации в процентном соотношении
Состояние конфигурации	Оценка соответствия: 100% – Отлично; 75-99% – Хорошо; 0-74% – Неудовлетворительно
Количество правил со значением Соответствие	Количество проверенных правил со статусом Соответствие

Количество правил со значением Несоответствие	Количество проверенных правил со статусом Несоответствие
Количество критичных правил со значением Несоответствие	Количество правил со статусом Несоответствие и риском Критический
Количество правил высокой критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Высокий
Количество правил средней критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Средний
Количество правил низкой критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Низкий
Количество правил информационной критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Информация
Количество правил без известной критичности со значением Несоответствие	Количество правил со статусом Несоответствие и риском Не определено

Количество правил со значением Неизвестно	Количество правил со статусом Неизвестно
Количество правил со значением Ошибка	Количество правил со статусом Ошибка
Количество правил со значением Неприменимо	Количество правил со статусом Неприменимо

Пример:

Код
Id хоста,Имя хоста,Процент соответствия,Состояние конфигурации,Количество правил со значением Соответствие,Количество правил со значением Несоответствие,Количество критичных правил со значением Несоответствие,Количество правил высокой критичности со значением Несоответствие,Количество правил средней критичности со значением Несоответствие,Количество правил низкой критичности со значением Несоответствие,Количество правил информационной критичности со значением Несоответствие,Количество правил без известной критичности со значением Несоответствие,Количество правил со значением Неизвестно,Количество правил со значением Ошибка,Количество правил со значением Неприменимо 69,192.168.80.8,35,Неудовлетворительно,38,66,0,1,24,41,0,0,3,0,2

8.5.4 Вкладка Хост – Параметр

Статус проверки правила

Соответствие – значение параметра на хосте соответствует эталонному значению в конфигурации;

Несоответствие – значение параметра на хосте не соответствует эталонному значению в конфигурации;

Ошибка – критическая ошибка при выполнении проверки. При возникновении обратитесь в службу тех. поддержки;

Неизвестно – ошибка при проверке правила. Убедитесь, что используемая для сканирования учетная запись обладает нужными правами, а примененные на хосте групповые политики позволяют проводить необходимые проверки;

Неприменимо – данное правило неприменимо для проверяемой платформы;

В данной вкладке отображается информация по выбранному проверяемому правилу конфигурации относительно хоста.

The screenshot shows the 'Host - Parameter' tab in the 'Анализ конфигураций' (Configuration Analysis) tool. The main table displays the following data:

Хост	Результат	Фактический параметр
192.168.80.129	Несоответствие	

The right sidebar provides details for the selected rule:

- Критичность:** Низкий
- Описание:** Раздел /var/tmp рекомендуется монтировать с опциями noexec,nodev,nosuid.
- Дополнительно:**
 - ID: var_tmp
 - OVAL ID: oval:ru.altrix-soft:nix:def:33355
 - OVAL URL: ALTIX-AstraLinux-RedBook-1.7-oval.xml

Сперва необходимо выбрать правило. Нажмите на  и выберите нужное правило.

Информация о правиле включает в себя:

- Хост – IP-адрес или DNS-имя хоста;
- Результат – статус проверки правила;
- Фактический параметр – значения ключей реестра или подстрок конфигурационных файлов, проверяемых во время сканирования. Собирается только при включенной опции **Сохранять фактические значения xccdf** ([4.3 Аудит конфигураций](#));

Если ключа / подстроки нет в реестре / конфигурационном файле, или правило не подразумевает проверку ключа / подстроки, то фактическое значение будет пустым

Справа отображается информация о профиле и правиле.

Профиль ▾

Название

Astra Linux SE и CE – Общие настройки безопасности – АЛТЭКС-СОФТ

Отключено

0 правил

Изменено

0 правил

Правило ▾

Ограничить права на crontab файл

Статус правила

Включено

Критичность ▾

Средний

Описание ▾

Системные файлы crontab доступны только демону cron (с привилегиями суперпользователя) и команде crontab (запускаемая от root). Если непривилегированным пользователям дать права на чтение или (что ещё хуже) модификацию системных crontab файлы, то это может привести к повышению привилегий локального пользователя. Для правильного задания прав и группы, необходимо выполнить команды:

```
# chmod 400 /etc/crontab
# chmod -R 770 /var/spool/cron/
# chown -R 0 /var/spool/cron/
```

Дополнительно ▾

ID

restrict_permissions_on_files

OVAL ID

oval:ru.altx-soft.nix:def:26069

OVAL URL

ALT-X-AstraLinux-oval.xml

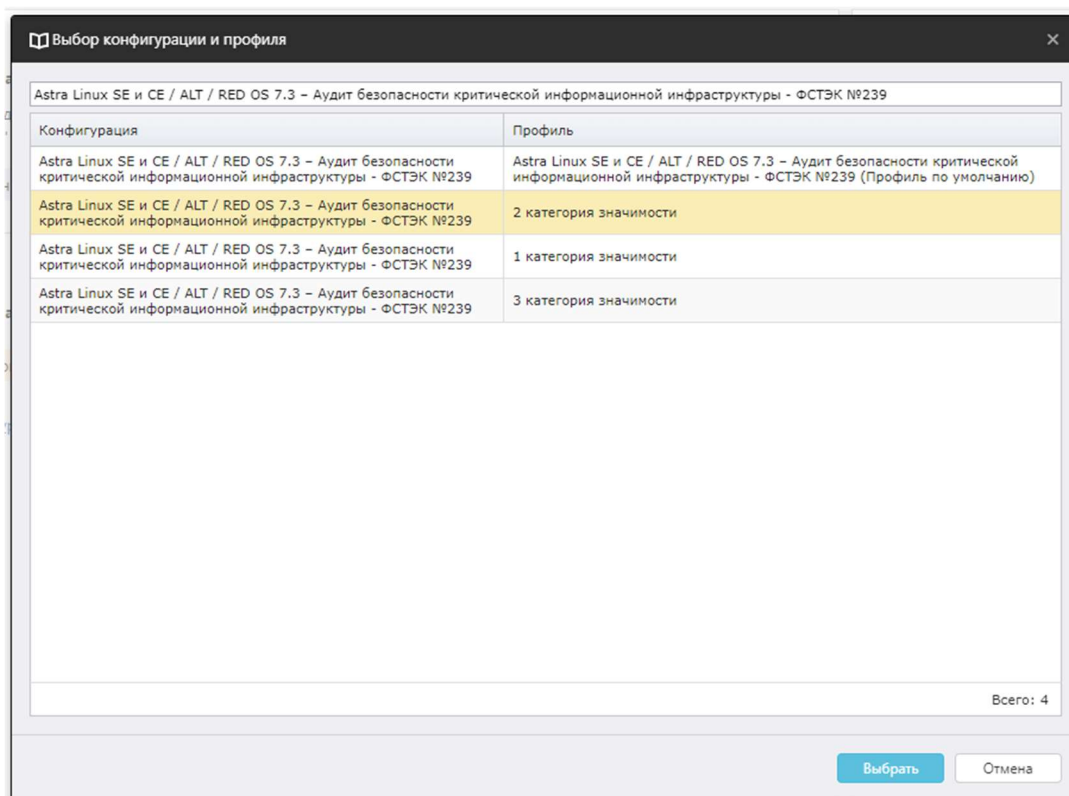
Общий фильтр

Анализ конфигураций

Конфигурация

...

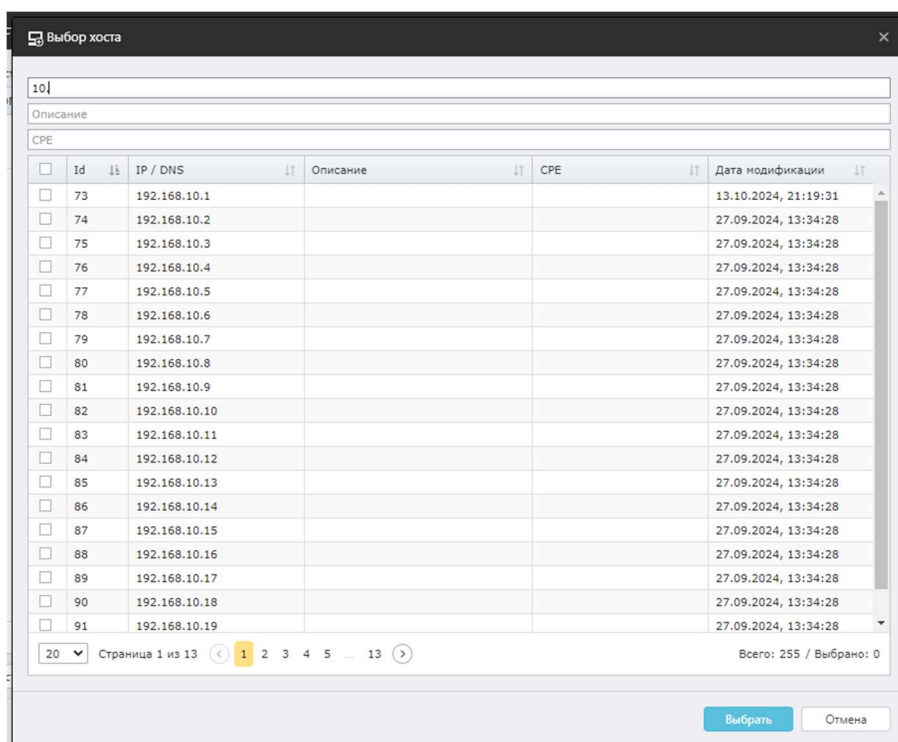
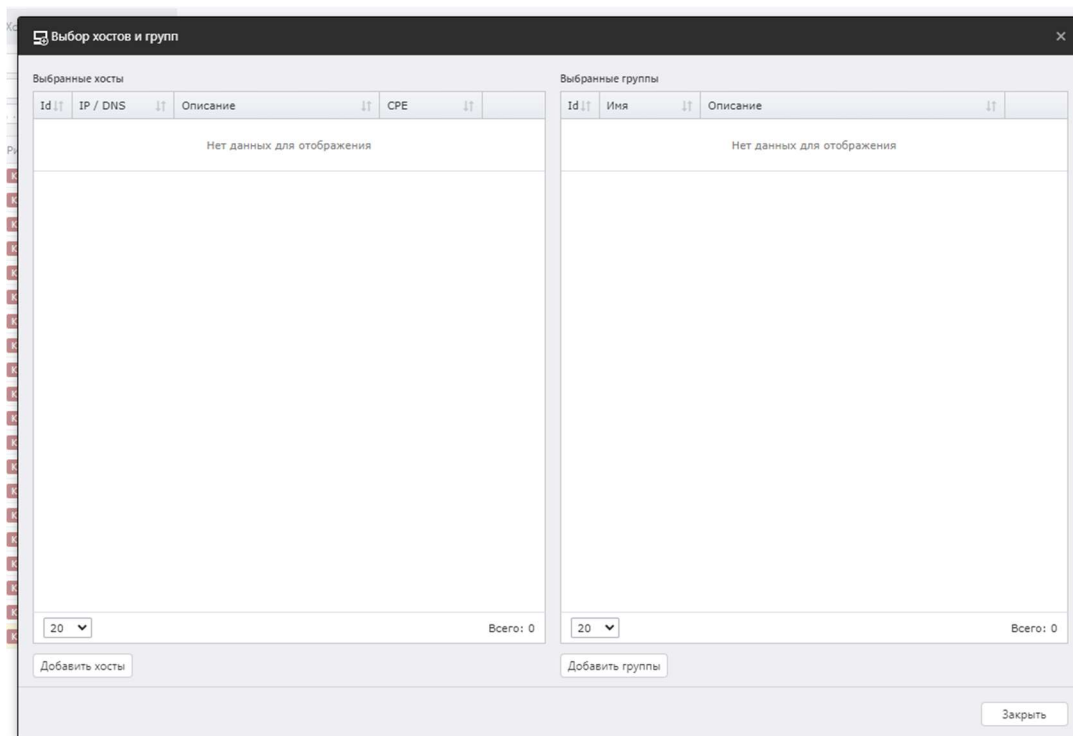
- Конфигурация** – необходимо выбрать конфигурацию, соответствие которой будет определяться. Если у конфигурации есть несколько профилей, то в окне выбора будут отображаться несколько строк одной и той же конфигурации, но с разными профилями. Нажмите на  и выберите нужную конфигурацию;



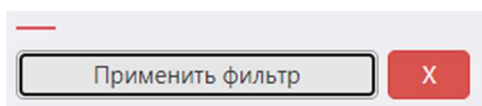
- Задания – можно выбрать задания, из результатов сканирования которых будет производиться анализ конфигураций. Учитываются результаты сканирования со статусом Завершено. Из выпадающего списка можно выбрать два варианта: **Все задания** и **Выбрать задания**. Если указать **Выбрать задания**, появится дополнительное поле:

Нажмите на , после чего откроется окно выбора заданий;

- Выбрать период, дней – максимальное количество дней, за которое учитывать результаты сканирований для анализа конфигураций;
- Хосты – можно выбрать хосты, для которых будет проведен анализ конфигураций. Нажмите на , после чего откроется окно выбора групп и хостов:



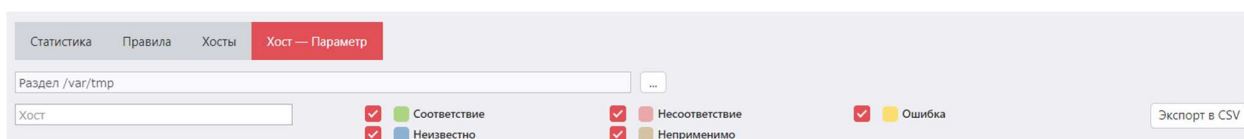
Для применения фильтра нажмите **Применить фильтр**. Для отмены фильтра нажмите красную кнопку с крестиком, что вернет для всех полей значения по умолчанию.



Фильтр для результирующей таблицы

Данный фильтр работает с результатом, уже полученным после применения общего фильтра. В полях можно указывать как полное значение, так и его часть.

- Хост – IP-адрес или DNS-имя хоста;
- Статус проверки правила – в таблице будет отображаться информация только для тех хостов и правил, статусы проверки которых совпадают с отмеченными.



Экспорт в CSV

Результирующую таблицу можно экспортировать в CSV. Экспортироваться будет та информация, которая отображается в таблице после применения фильтров. Для этого нажмите **Экспорт в CSV** справа от фильтра результирующей таблицы. Полученный файл будет называться **ComplianceAnalysis-RuleResults-dd-mm-yyuu.csv**.

Структура CSV файла

Id хоста	ID хоста
Имя хоста	IP-адрес или DNS-имя хоста
Результаты сканирования	Статус проверки правила
Фактическое значение	Значение, обнаруженное на хосте во время проверки правила

Пример:

Код

```
Id хоста,Имя хоста,Результаты сканирования,Фактическое значение
69,192.168.80.8,Несоответствие,Значение параметра <b>uread</b> для
файла <b>/etc/crontab</b> = <b>True</b><br>Значение параметра
<b>uwrite</b> для файла <b>/etc/crontab</b> = <b>True</b><br>Значение
параметра <b>uexec</b> для файла <b>/etc/crontab</b> =
<b>False</b><br>Значение параметра <b>gread</b> для файла
```

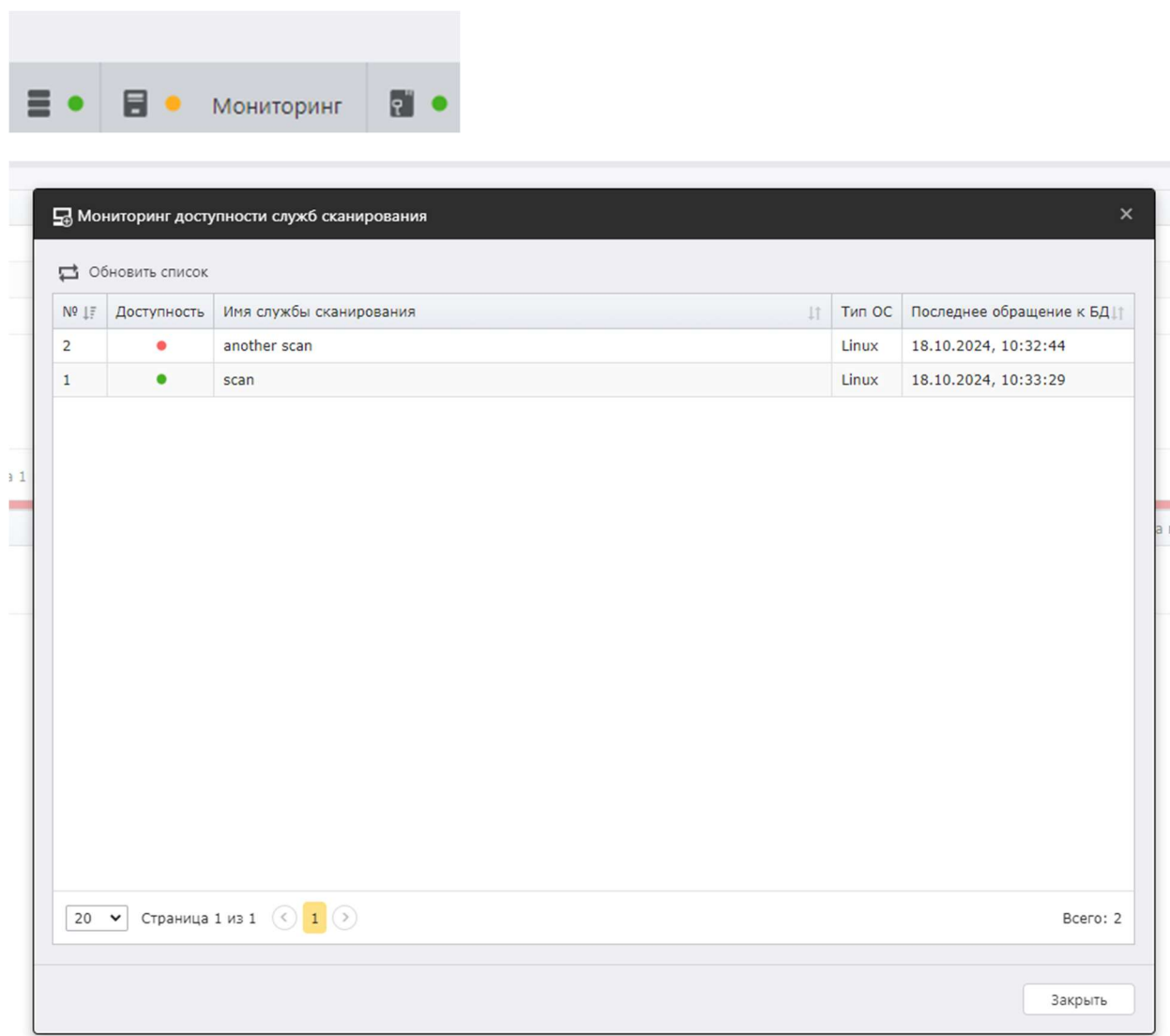

Дополнительные возможности

Содержание

- Мониторинг служб сканирования

Мониторинг служб сканирования

Если в БД установлено две и более служб сканирования, появляется возможность отслеживать состояние каждой из них. Для того, чтобы открыть окно мониторинга, нажмите в статус-баре **Мониторинг**:



Значение столбца **Последнее обращение к БД** в норме обновляется каждые 5 секунд. Если разница между обращением к БД и текущим временем (согласно часовому поясу хоста, на котором установлен компонент redcheck-client) не более 10 секунд, то служба сканирования будет считаться доступной.

Причин недоступности службы сканирования может быть несколько:

- Если значение последнего обращения к БД обновляется, но служба недоступна, возможно на хосте службы сканирования установлено неактуальное время;

- Если значение последнего обращения к БД не обновляется, возможно хост службы сканирования выключен или вне сетевой доступности;
- Если значение последнего обращения к БД не обновляется, возможно компонент redcheck-scan-service был удален с хоста.

Нажав **Обновить список**, данные в таблице обновятся.

Детальную информацию о службах сканирования можно посмотреть в **Справка** → **О программе**.

Подключённые службы сканирования

Имя	ID	UID	По умолчанию	Дата создания	Дата последнего запуска	Имя хоста	ОС	Версия ОС	Разрядность	Последнее обращение к БД	Версия SCAP процессора
another scan		a268e675-8442-4db3-940f-0005097cc829	Нет	07.10.2024, 09:41:15	18.10.2024, 06:34:01	redos	reeds.7.3_x86-64-x64	5.4.0.54	64	18.10.2024, 10:46:50	8.0.0-scap-nlx.425
scan		a268e675-8442-4db3-940f-0005097cc829	Да	07.10.2024, 09:41:15	18.10.2024, 06:34:01	astra	astra.1.7_x86-64-x64	5.4.0.54	64	18.10.2024, 10:35:49	8.0.0-scap-nlx.425

Страница 1 из 1 1 Всего: 2