



MaxPatrol VM

Не даст хакерам шанса использовать
уязвимости для взлома

Познакомимся



Олег Кочетов

Лидер продуктовой практики
MaxPatrol VM, MaxPatrol HCC

✉ okochetov@ptsecurity.com

☎ +7 905 783 90 46

📍 @Bednight

Эксперт по построению результативного процесса
управления уязвимостями

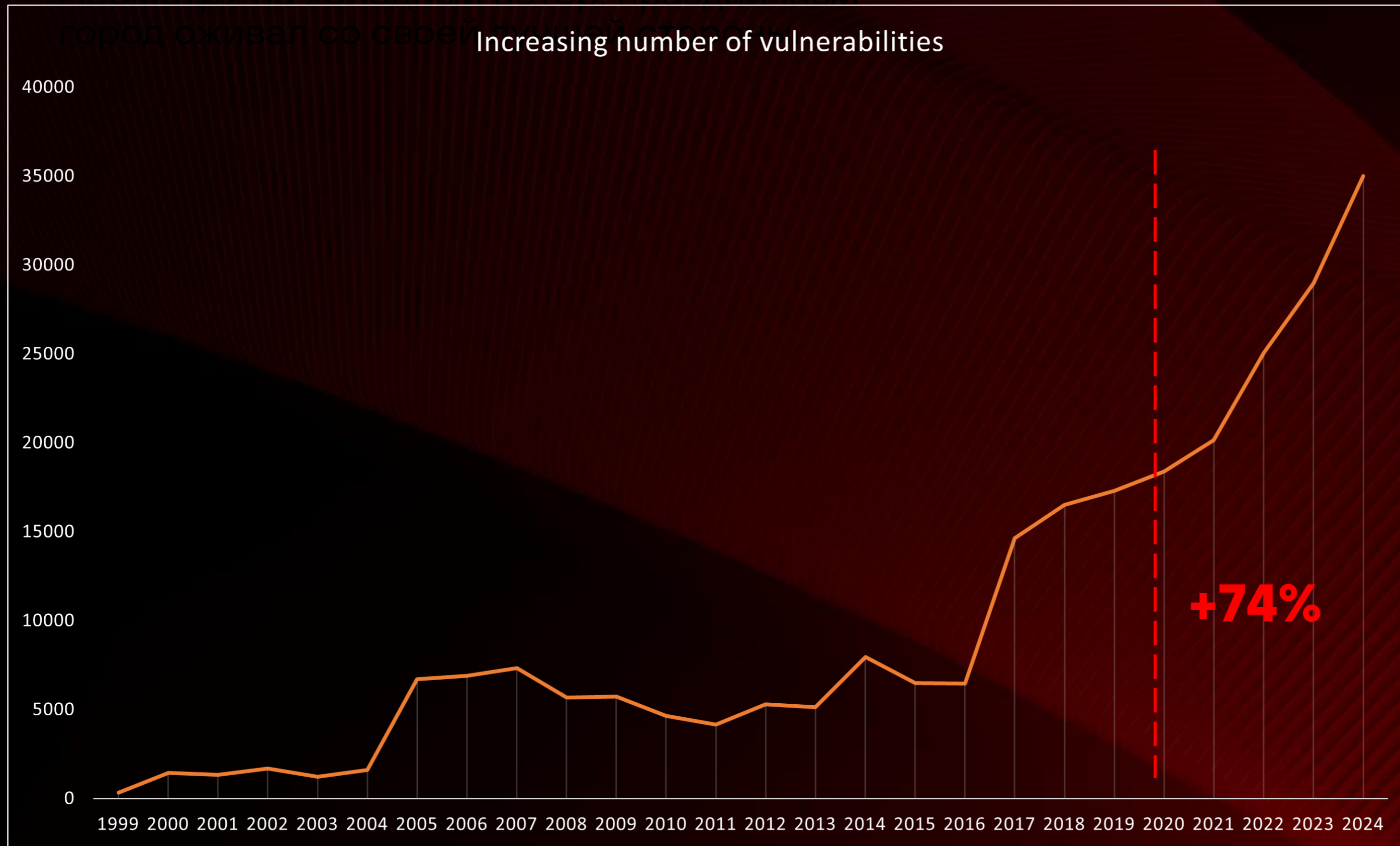
Более 6 лет занимался построением и развитием
процесса безопасной разработки в ведущей российской
компании

Масштаб проблемы

Несмотря на холодный ветер, праздничный

город оживал со своей традицией

Increasing number of vulnerabilities



- 40 077 CVE
опубликовано в 2024-м
- 28 961 CVE
опубликована в 2023-м
- 25 059 CVE
опубликовано в 2022-м
- 20 161 CVE
опубликована в 2021-м
- 18 375 CVE
опубликовано в 2020-м

Три поколения сканеров



Сетевые сканеры уязвимостей

Сканирование в режиме черного ящика, определение открытых портов

1

XSpider

2002



Системы анализа защищенности

Централизованное сканирование узлов и сетевого оборудования в режиме черного и белого ящика, сравнение результатов

2

MaxPatrol 8

2009



Системы управления уязвимостями нового поколения

Управление активами, построение процесса приоритизации, контроля за устранением уязвимостей

3

MaxPatrol VM

2021

Что мешает работать с уязвимостями



1 Нет полноты охвата IT-инфраструктуры

- Присутствуют задержки в получении актуальных данных о сети
- Нет возможности часто сканировать инфраструктуру
- Ибэшник проверяет только те узлы, о которых знает

2 Уязвимостей слишком много

- Все уязвимости закрыть невозможно
- Нет понимания, какие уязвимости наиболее опасны для конкретной инфраструктуры
- Имеются сложности с приоритизацией задач на устранение уязвимостей

3 Нужно договариваться с IT-отделом

- В компании отсутствует плановый патч-менеджмент
- Необходимо каждый раз объяснять IT-специалистам, зачем нужно устранять конкретную уязвимость
- Нет возможности контролировать статус и сроки устранения уязвимостей

Что предлагает MaxPatrol VM



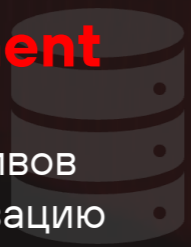
1 Нет полноты охвата
IT-инфраструктуры

2 Уязвимостей
слишком много

3 Нужно договариваться
с IT-отделом

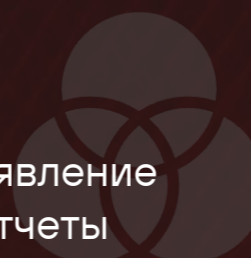
Технология Asset Management

собирает более 3000 параметров IT-активов и позволяет провести полную инвентаризацию инфраструктуры



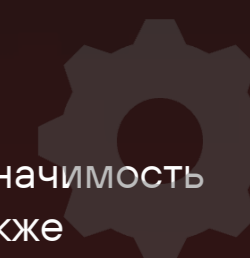
Контроль уязвимостей

с учетом отечественного ПО и ОС, выявление уязвимостей в Docker-контейнерах. Отчеты экспертов Positive Technologies известны за пределами России



Процесс управления

уязвимостями позволяет учитывать значимость активов, опасность уязвимостей, а также обрабатывать их в соответствии с регламентом



MaxPatrol VM



**Архитектура
MaxPatrol VM**

Как MaxPatrol VM собирает данные



MaxPatrol VM

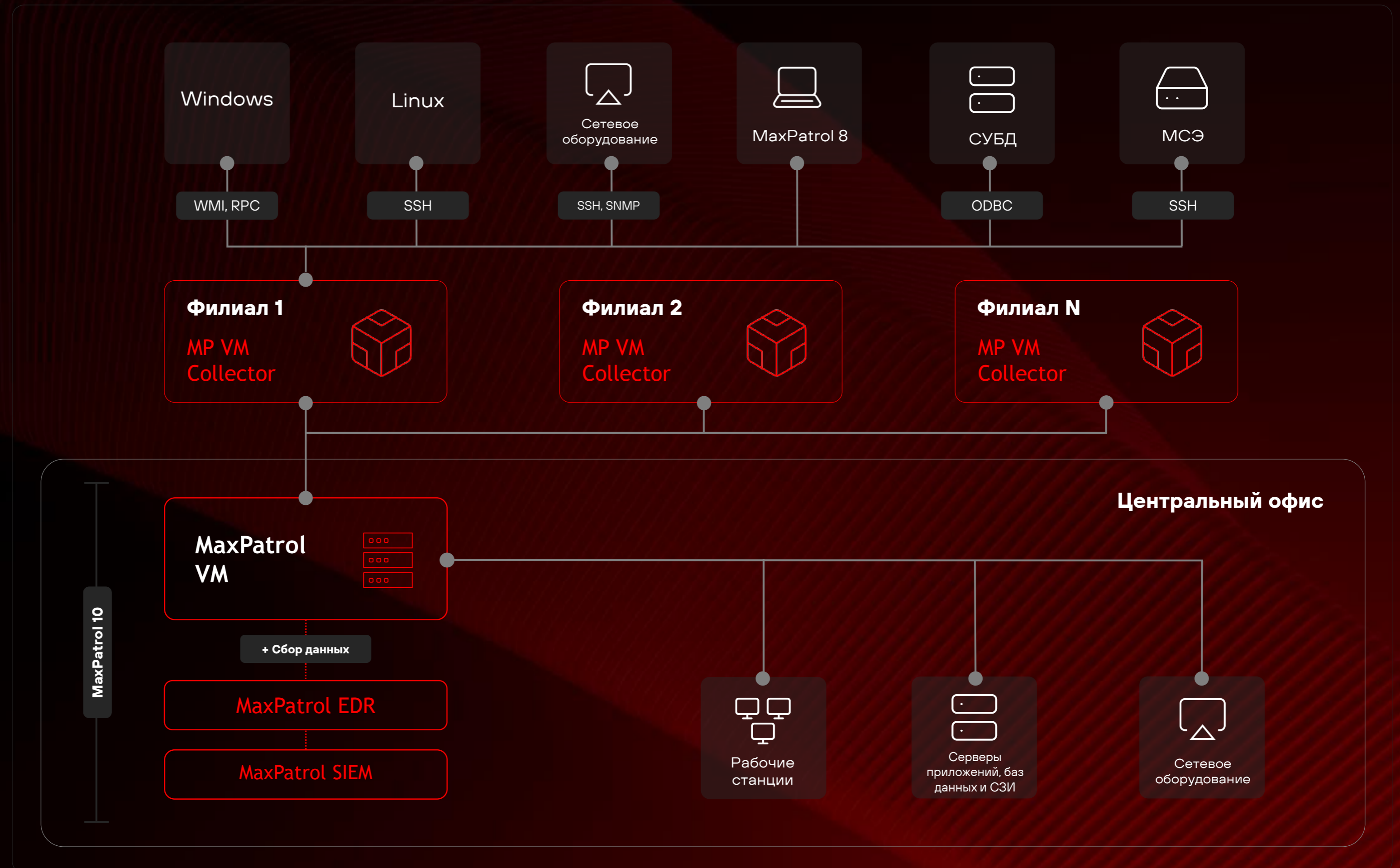
Позволяет сканировать узлы, расположенные в отдельных сетевых сегментах

Коллектор

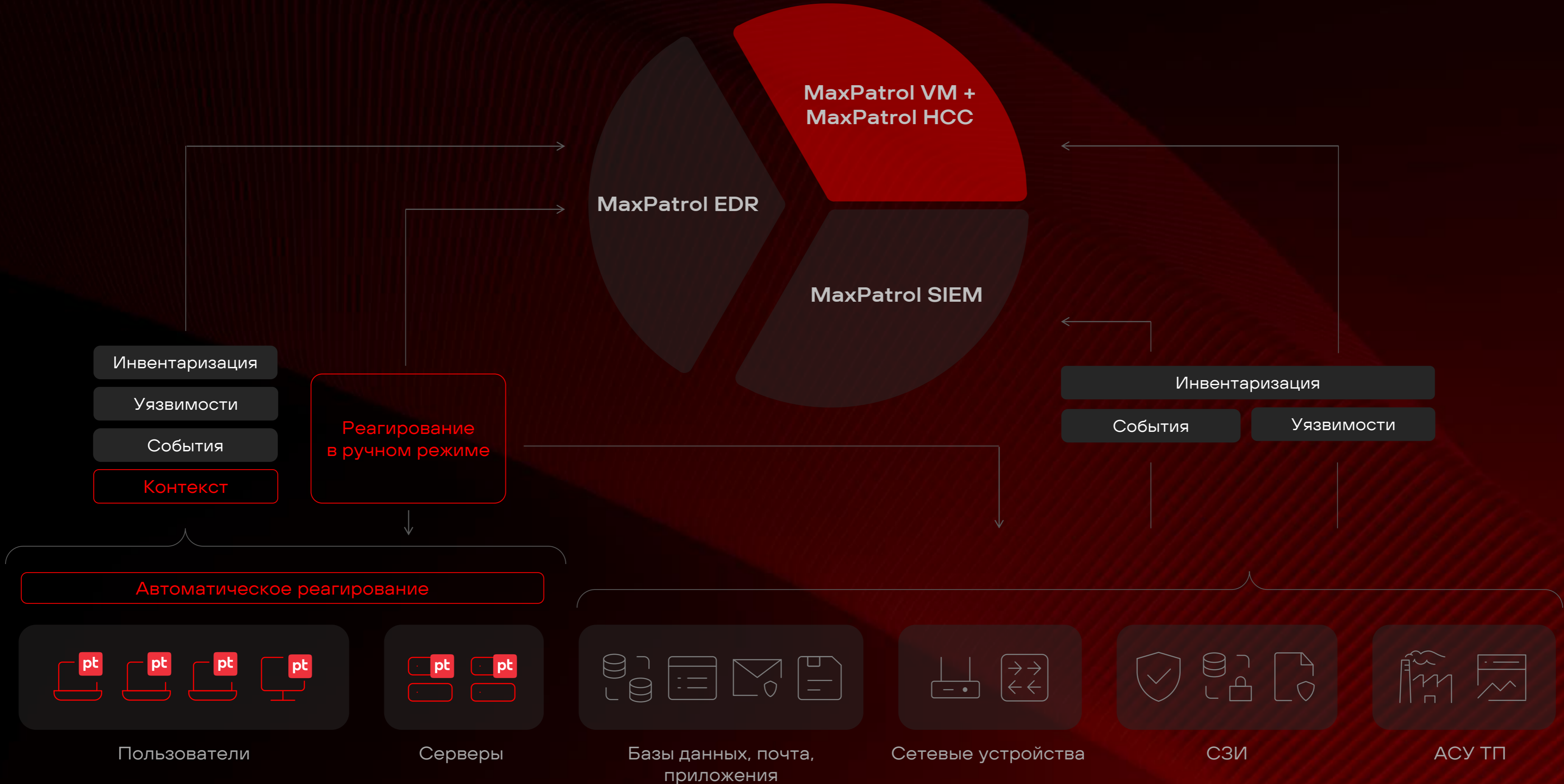
- Собирает и хранит более 3000 параметров активов
- Использует безагентский режим сканирования

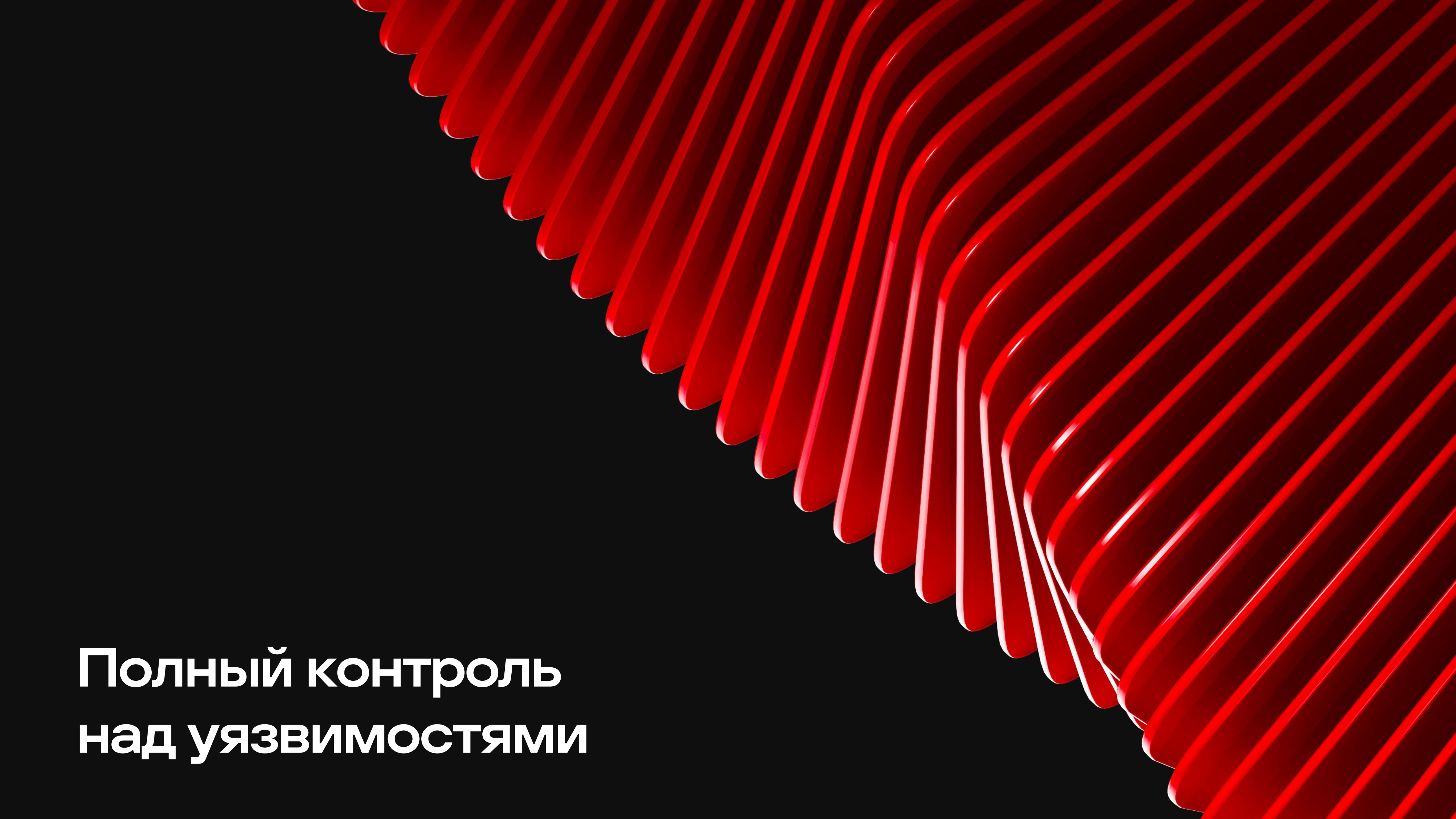
Агентский сбор

Позволяет использовать MaxPatrol EDR для задач сканирования, а также удаленного управления



MaxPatrol SIEM + MaxPatrol EDR + MaxPatrol VM





**Полный контроль
над уязвимостями**

Обнаружение активов



Классификация и оценка активов

Распределение активов по группам

- По принадлежности к структурным подразделениям
- По принадлежности к АС
- По принадлежности к IP-сетям
- По наличию определенных ОС и ПО

Классификация активов

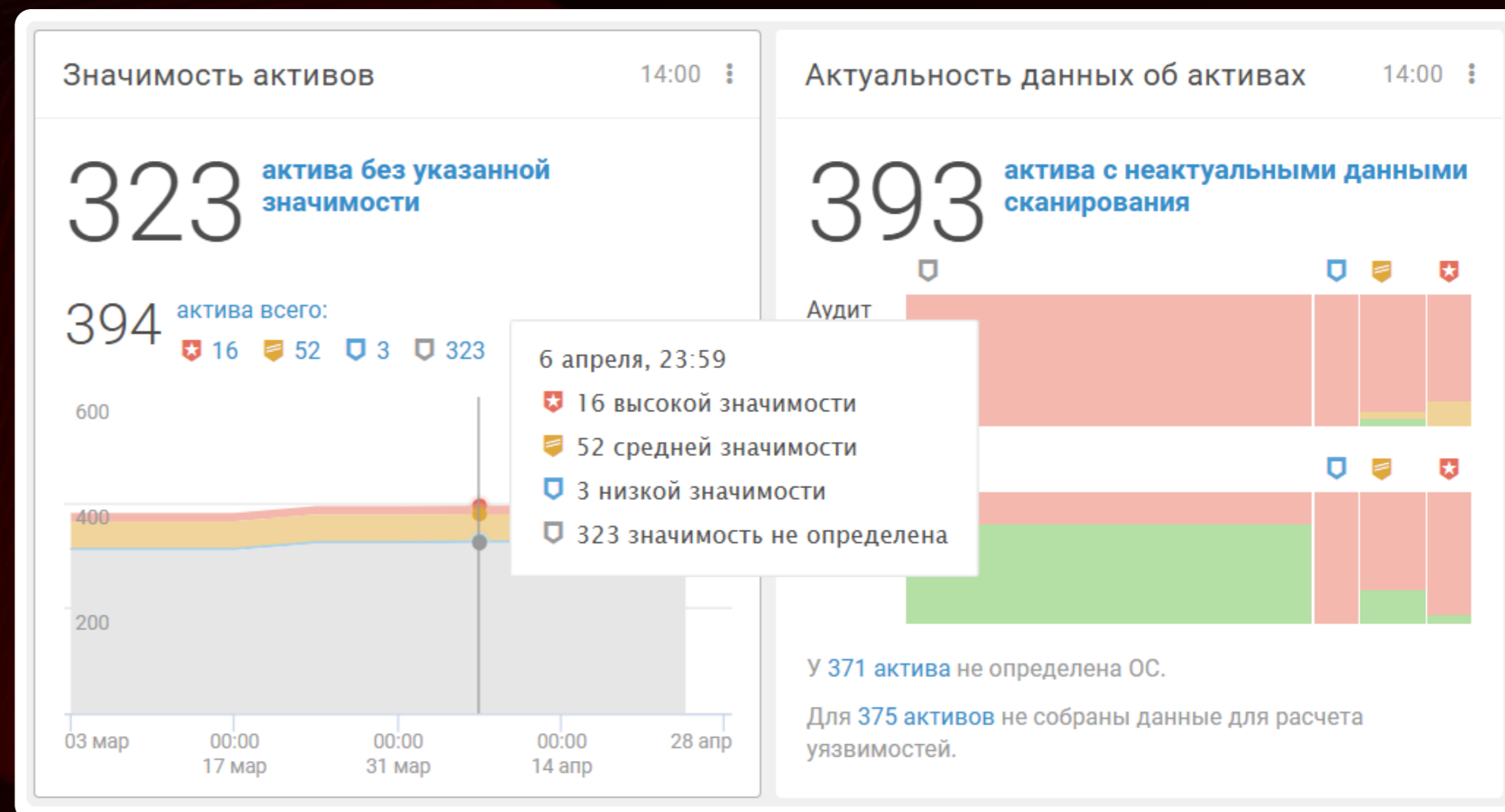
- Динамические группы
- Статические группы
- Триггеры для контроля изменений состава групп

Контроль активов

- Классификация, оценка, регулярное сканирование
- Проверка устаревания

Оценка активов

- Задание степени значимости



Результат применения правила

Группы активов

Значимость актива

Высокая

Трендовые уязвимости



Критерии трендовости

Наличие эксплойта для уязвимости

Популярное ПО для России

CVSS 3.1 выше 7 баллов (высокая опасность)



Информация о трендовых уязвимостях поступает в MaxPatrol VM в течение 12 часов



Исследовательский центр
Positive Technologies

Трендовые уязвимости

19:00

12 февраля

■ **Уязвимость CVE-2025-21391** CVE-2025-21391 66 0 0

Уязвимость повышения привилегий в Windows Storage. Эксплуатация уязвимости позволяет злоумышленнику повысить привилегии до уровня SYSTEM, а также удалить целевые файлы, что может привести к недоступности сервиса....

Поставщик: Microsoft

Уязвимые компоненты: Windows

■ **Уязвимость CVE-2025-21418** CVE-2025-21418 71 0 0

Уязвимость повышения привилегий в драйвере вспомогательных функций Windows для WinSock (AFD.sys). Эксплуатация уязвимости позволяет злоумышленнику повысить привилегии до уровня SYSTEM. Зафиксированы факты эксплуатации...

Поставщик: Microsoft

Уязвимые компоненты: Windows

27 января

■ **Уязвимость CVE-2025-0411** CVE-2025-0411 77 0 0

Уязвимость выполнения произвольного кода в 7-Zip в процессе извлечения файлов из специально подготовленного архива. Успешная эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в контексте...

Поставщик: Igor Pavlov

Уязвимые компоненты: 7-Zip

■ **Уязвимость в 7-zip 7-zip** CVE-2025-0411 Уязвимости не обнаружены

Уязвимость выполнения произвольного кода в 7-Zip в процессе извлечения файлов из специально подготовленного архива. Успешная эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в контексте...

Уязвимости в веб-приложениях



Готовые запросы для поиска веб-уязвимостей

Список уязвимостей с описанием и способом устранения

Приоритизация веб-уязвимостей на ресурсе

Сайт	Уязвимость	Описание уязвимости	Способ устранения уязвимости
@WebSite	Vulner	Description	HowToFix
vulnbank.af.ptsecurity.com	Отсутствует заголовок Content-Security-Policy	Приложение не возвращает заголово...	Определите политику защиты контента вашего приложения и на...
vulnbank.af.ptsecurity.com	Отсутствует заголовок Feature-Policy	Приложение не возвращает заголово...	Для всех страниц вашего приложения укажите заголовок HTTP Fe...
vulnbank.af.ptsecurity.com	Отсутствует заголовок Permissions-Policy	Приложение не возвращает заголово...	Установите заголовок Permissions-Policy в вашем приложении. Ес...
vulnbank.af.ptsecurity.com	Отсутствует заголовок Referrer-Policy	Приложение не возвращает заголово...	Установите значение strict-origin-when-cross-origin в заголовке Ref...
vulnbank.af.ptsecurity.com	Отсутствует заголовок Strict-Transport-Security	Приложение не возвращает заголово...	> **Внимание!** Перед использованием заголовка Strict-Transp...
vulnbank.af.ptsecurity.com	Отсутствует заголовок X-Content-Type-Options	В приложении не используется загол...	Укажите значение nosniff в заголовке X-Content-Type-Options для в...
vulnbank.af.ptsecurity.com	Отсутствует заголовок X-Frame-Options	Приложение не возвращает заголово...	Не настраивайте X-Frame-Options в метатеге, например вот так: &l...
vulnbank.af.ptsecurity.com	Отсутствует заголовок X-XSS-Protection	Приложение не возвращает заголово...	Заголовок X-XSS-Protection поддерживается только в некоторых у...
vulnbank.af.ptsecurity.com	Слабый набор шифров TLS	Приложение допускает использовани...	Измените параметры шифров TLS в конфигурации вашего сервера

ERP- и CRM-системы

Средства разработки
и деплоя

Веб-инструменты для
совместной работы

Корпоративные
веб-порталы

Онлайн-магазины

Одностраничные сайты

Уязвимости в Docker-контейнерах



The screenshot displays the MaxPatrol 10 interface, which is used for monitoring and managing system vulnerabilities. The main view shows a list of vulnerabilities found in Docker images. The interface is divided into several sections:

- Header:** MaxPatrol 10 logo and navigation menu (Активы, События, Инциденты, Стандарты, Сбор данных, EDR, Система).
- Left Sidebar:** Groups of assets (Группы) including AM+VM, imageset, PT Demo, and Unmanaged hosts. A search bar for container vulnerabilities is also present.
- Main Content Area:** A table of vulnerabilities with columns for Image, Package, Vulnerability, and Status. The table lists various packages like curl, dirmngr, dpkg, and git, each with associated CVE identifiers and a 'Новая' (New) status.
- Right Panel:** Details for a specific vulnerability, including a timeline graph showing the history of scans and a list of installed packages with their versions. The 'curl (7.74.0-1.3+deb11u1)' package is highlighted.

Образы Image	Список пакетов Package	Уязвимость Vulnerer	Статус уязвим... Status
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2022-43...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2023-23...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2023-38...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2023-38...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2023-46...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2023-46...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	curl (7.74.0-1.3+deb11u1)	Уязвимость CVE-2024-80...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	dirmngr (2.2.27-2)	Уязвимость CVE-2022-34...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	dpkg (1.20.9)	Уязвимость CVE-2022-16...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	dpkg-dev (1.20.9)	Уязвимость CVE-2022-16...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	e2fsprogs (1.46.2-2)	Уязвимость CVE-2022-13...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	file (1.5.39-3)	Уязвимость CVE-2022-48...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	gir1.2-gdkpixbuf-2.0 (2.42.2+dfsg-1)	Уязвимость CVE-2021-44...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	gir1.2-gdkpixbuf-2.0 (2.42.2+dfsg-1)	Уязвимость CVE-2021-46...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	gir1.2-rsvg-2.0 (2.50.3+dfsg-1)	Уязвимость CVE-2023-38...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	git (1:2.30.2-1)	Уязвимость CVE-2019-13...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	git (1:2.30.2-1)	Уязвимость CVE-2020-52...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	git (1:2.30.2-1)	Уязвимость CVE-2022-23...	Новая
.local:5000... sha256:e1bd01da1b2ee042613fb30009e3b54d2fc20a8793d345313c7ab39344cbe5d0	git (1:2.30.2-1)	Уязвимость CVE-2022-24...	Новая

Ссылки на патчи безопасности



MaxPatrol 10 | Активы | Стандарты | Сбор данных | Система

Активы | Из группы PT Cloud

Группы: Все активы, PT Cloud, File Service, No Domain, Инфраструктурная роль, Контейнеры, ОС, Сетевое оборудование, Check Point, Cisco, Прочее, Инфраструктура

Запросы: Все активы, Стандартные запросы, По времени, Недостаточно данных, Инвентаризация, Роли узла

Запрос: `select(@Host, Host.OsName as OsName, Host.@Vulners.Status as Status, Host.@Vulners.Patch.DisplayName as Patch, Host.@Vulners.Patch.PatchType as PatchType, Host.@Vulners.Patch.PatchDate as PatchDate, Host.@Vulners.Patch.PatchLink as PatchLink) | filter(Patch and PatchType != "EndOfSupport" and Status != "Fixed") | select(@Host, OsName, Patch, PatchType, PatchDate, PatchLink) | unique() | sort(Patch ASC) | sort(@Host ASC)`

Узел	Операционная система	Название патча	Тип патча	Дата выхода патча	Ссылка на патч
@Host	OsName	Patch	PatchType	PatchDate	PatchLink
192.168.0.74	Debian	Обновление пакета linux-image-3.2.0-4-amd...	Обновление версии ПО	01 июня 2018, 15:08	Обновление пакета linux-image...
1c-db.ptrevenge.stf (10.144.1.230)	Windows 2019	Накопительное обновление KB5060531	Пакет обновления	10 июня, 03:00	Накопительное обновление KB...
1c-db.ptrevenge.stf (10.144.1.230)	Windows 2019	Накопительное обновление KB5061978	Пакет обновления	27 мая, 03:00	Накопительное обновление KB...
1c-srv.ptrevenge.stf (10.144.1.231)	Windows 2019	Накопительное обновление KB5061978	Пакет обновления	27 мая, 03:00	Накопительное обновление KB...
1c-srv.ptrevenge.stf (10.144.1.231)	Windows 2019	Накопительное обновление KB5060531	Пакет обновления	10 июня, 03:00	Накопительное обновление KB...
adcs2.ptrevenge.stf (10.144.0.104)	Windows 2016	Накопительное обновление KB5061010	Пакет обновления	10 июня, 03:00	Накопительное обновление KB...
amarshall.ptrevenge.stf (10.144.0.73)	Windows 10	Накопительное обновление KB5063159	Пакет обновления	16 июня, 03:00	Накопительное обновление KB...
amcknight.ptrevenge.stf (10.144.2.73)	Windows 10	Накопительное обновление KB5063159	Пакет обновления	16 июня, 03:00	Накопительное обновление KB...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета perl до версии 0:5.28.1-...	Обновление версии ПО	29 апреля 2023, 03:15	Обновление пакета perl до верс...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета openssh-server до верс...	Обновление версии ПО	18 декабря 2023, 22:15	Обновление пакета openssh-ser...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета mc-data до версии 3:4.8...	Обновление версии ПО	30 августа 2021, 22:15	Обновление пакета mc-data до ...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libksba8 до версии 0:1.1...	Обновление версии ПО	21 декабря 2022, 02:15	Обновление пакета libksba8 до ...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libprocps7 до версии 2:...	Обновление версии ПО	02 августа 2023, 08:15	Обновление пакета libprocps7 д...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libsnmp-base до версии...	Обновление версии ПО	07 ноября 2022, 06:15	Обновление пакета libsnmp-bas...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libunbound8 до версии ...	Обновление версии ПО	06 июня 2024, 20:15	Обновление пакета libunbound8...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета linux-image-5.4.0-54-gen...	Обновление версии ПО	18 февраля, 18:15	Обновление пакета linux-image...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета aspell до версии 0:0.60...	Обновление версии ПО	27 января 2020, 18:15	Обновление пакета aspell до ве...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libssl1.0.2 до версии 0:...	Обновление версии ПО	10 сентября 2019, 20:15	Обновление пакета libssl1.0.2 д...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета cups-bsd до версии 0:2...	Обновление версии ПО	27 сентября 2024, 01:15	Обновление пакета cups-bsd до...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета grub-common до верси...	Обновление версии ПО	10 марта 2022, 20:43	Обновление пакета grub-comm...
astra (192.168.212.124)	Astra Linux SE (Smolensk)	Обновление пакета libxml2 до версии 0:2.9...	Обновление версии ПО	16 ноября 2016, 03:59	Обновление пакета libxml2 до в...

Актив: 192.168.0.74

Обнаружен 07 июня 2024, 15:16 → Последнее обновление 07 июня 2024, 15:19

35,1 Средняя значимость ? Виртуальная машина

История за 15 дней

Интегр. уязвимость

Сканирование

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Информация о системе

- OS: Debian 7.8
- BIOS: Phoenix Technologies LTD 6.00
- CPU: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
- MB: Intel Corporation
- HDD: /dev/sda
- Ethernet: Network Interface Card

Самые опасные уязвимости

- Неподдерживаемая версия
- Уязвимость CVE-2018-8897
- Уязвимость CVE-2018-1093
- Уязвимость CVE-2018-10940
- Уязвимость CVE-2018-1130

Уязвимости ОС и ПО

Debian 7.8 1

Сетевая конфигурация

Инт... По... Сервис ПО

> ip://192.168.0.74

EOL, EOS – конец срока поддержки ПО



The screenshot displays the MaxPatrol 10 interface. The main window shows a search query: "Запрос: Активы с уязвимостями в неподдерживаемом ПО *". The query is: `select(@Host, Host.OsName as OsName, Host.Softs.Name as SoftwareName, Host.Softs.Version as SoftwareVersion, Host.Softs.@Vulners.Status as Status, Host.Softs.@Vulners.Patch as Patch, Host.Softs.@Vulners.Patch.PatchType as PatchType) | filter(PatchType = "EndOfSupport" and Status != "Fixed") | select(@Host, OsName, SoftwareName, SoftwareVersion, Patch, PatchType) | unique() | sort(SoftwareName, SoftwareVersion) | sort(@Host ASC)`. The results table lists several hosts with their OS, software, version, and patch status. The host "conveyorbelts (10.144.1.3)" is highlighted, showing it runs Windows 10 with Microsoft SQL Server 13.0.5026, which is not supported by the manufacturer.

Узел	Операционная система	Название	Версия	Патч	Тип патча
@Host	OsName	SoftwareName	SoftwareVersion	Patch	PatchType
10.144.2.102	null	Microsoft SQL Server	12.0.5000	Неподдерживаемая версия	ПО не поддерживается производит...
192.168.0.77	Windows 2016	Microsoft SQL Server	11.0.5058	Неподдерживаемая версия	ПО не поддерживается производит...
conveyorbelts (10.144.1.3)	Windows 10	Microsoft SQL Server	13.0.5026	Неподдерживаемая версия	ПО не поддерживается производит...
pc11.company.com (192.168.0.97)	Windows 10	Java	8 U281	Неподдерживаемая версия	ПО не поддерживается производит...
pc8.company.com (192.168.0.94)	Windows 7	Java	8 U77	Неподдерживаемая версия	ПО не поддерживается производит...
srv3.company.com (192.168.2.7)	Windows 2012 R2	Microsoft SQL Server	11.0.5058	Неподдерживаемая версия	ПО не поддерживается производит...
srv4.company.com (192.168.1.9)	Windows 2012 R2	Java	8 U261	Неподдерживаемая версия	ПО не поддерживается производит...

The right sidebar shows details for the selected host "conveyorbelts (10.144.1.3)". It indicates that 12,459.6 vulnerabilities were found, with a high significance. The system information section lists hardware and software details, and the "Самые опасные уязвимости" section lists several critical vulnerabilities, including "Неподдерживаемая версия" (Unsupported version) and "Уязвимость CVE-2024-4947".

Host compliance control



MaxPatrol HCC — комплаенс для результативной безопасности

Модуль позволяет:

Проверять инфраструктуру на соответствие стандартам безопасности и отдельным требованиям

Приоритизировать найденные риски

Просматривать актуальные данные о выполнении требований на динамических дашбордах

Устанавливать сроки, в которые несоответствия стандартам должны быть устранены, и контролировать их соблюдение

Требования стандарта PT Essential – Windows Desktop

Тип	Требование
🛡️	🔧 Настроить аудит изменения политики аудита
🛡️	🔧 Настроить аудит использования привилегий, затрагивающих конфиденциальные данные
🛡️	🔧 Настроить аудит проверки учетных данных
🛡️	🔧 Настроить поведение запроса на повышение прав для администраторов в режиме одобрения администратором
🛡️	🔧 Настроить поведение запроса на повышение прав для обычных пользователей
🛡️	🔧 Настроить сложность пароля
🛡️	🔧 Настроить уровень минимальной сеансовой безопасности для клиентов на базе NTLM SSP (включая безопасный RPC)
🛡️	🔧 Настроить уровень минимальной сеансовой безопасности для серверов на базе NTLM SSP (включая безопасный RPC)
🛡️	🔧 Настроить уровень проверки подлинности LAN Manager
🛡️	🔧 Ограничить время хранения паролей в памяти LSASS после окончания пользовательской сессии
🛡️	🔧 Отключить PowerShell v2
🛡️	🔧 Отключить автоматический вход в систему
🛡️	🔧 Отключить драйвер клиента SMBv1
🛡️	🔧 Отключить проверку подлинности WDigest
🛡️	🔧 Отключить протокол LLMNR
🛡️	🔧 Отключить протокол NetBIOS
🛡️	🔧 Отключить протокол SMBv1
🛡️	🔧 Отключить режим гибернации
🛡️	🔧 Принудительно переопределять параметры категории политики аудита параметрами подкатегории политики аудита
🛡️	🔧 Разрешить повышение прав для UIAccess-приложений только при установке в безопасных местах
🛡️	🔧 Установить количество паролей, которое необходимо хранить в журнале паролей
🛡️	🔧 Установить количество предыдущих подключений к кэшу
🛡️	🔧 Установить максимальный срок действия пароля
🛡️	🔧 Установить максимальный срок действия пароля для учетной записи компьютера
🛡️	🔧 Установить минимальную длину пароля
🛡️	🔧 Установить минимальный срок действия пароля

Всего 44 требования

Отключить протокол SMBv1

Описания требования

Краткое описание
Следует отключить обработку протокола SMBv1 на стороне сервера.

Описание
Протокол SMB версии 1 (SMBv1) имеет значительные уязвимости безопасности, поэтому его следует отключить. Отключение SMBv1 может вызвать проблемы совместимости с устаревшими ОС, программным обеспечением или устройствами, которые поддерживают только SMBv1. На сайте корпорации Microsoft опубликован подробный список несовместимостей, связанных с протоколом SMBv1, – этот список постоянно пополняется. Прежде чем применять эту настройку ко всей инфраструктуре, следует провести проверку, чтобы определить последствия ее применения и по возможности устранить выявленные несовместимости совместно с производителем такого приложения или устройства.

Идентификатор требования
Windows.Protocols.SMBv1Server

Ссылки
<https://www.microsoft.com/en-us/download/details.aspx?id=55319>
[https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb1-product-clearinghouse/...](https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb1-product-clearinghouse/)

Параметры требования

exception **BOOL** False

Проверяемый компонент

Проверяемый компонент
OperatingSystem.Windows.WindowsHost

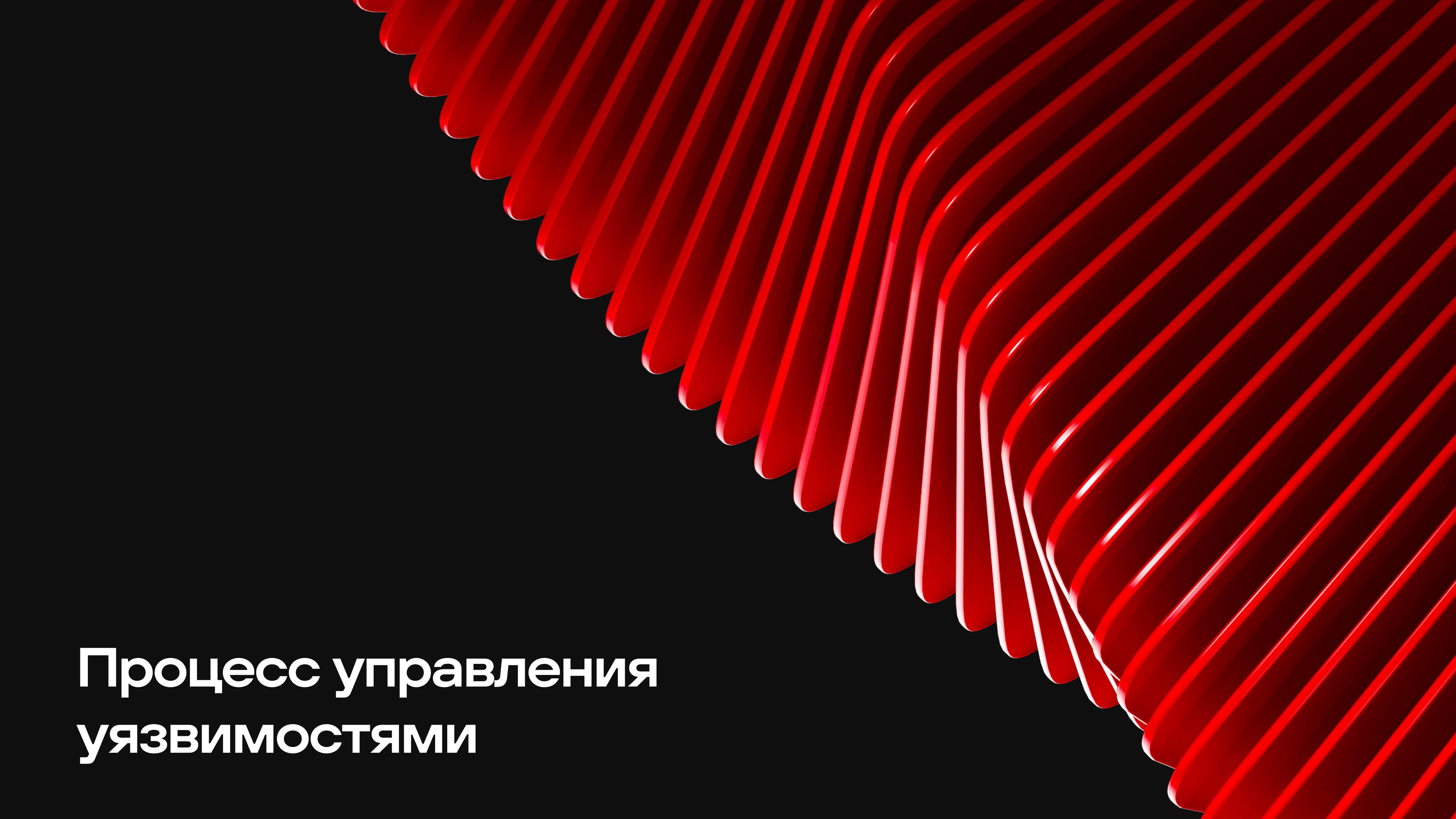
Правило именования проверяемого компонента
@Entity.Fqdn

Предварительные проверки

Условие полноты данных
computability {
 return @Entity.ProtocolsAndCiphers.Protocols.Any();
}

Условие применения требования
applicability {
 return !@exception;
}

Причина неприменимости
Требование исключено из проверки на активе пользовательским переопределением



Процесс управления уязвимостями

Перед тем как начать

Заранее провести предварительные мероприятия

Определить перечень **недопустимых событий**

Распределить **роли** и **функции** среди всех участников процесса

Убедиться, что эти роли есть кому **исполнять**

Согласовать параметры процесса между всеми участниками

Оценить заранее:

- Ресурсы команды
- Технические детали: учетные записи и профили сканирования активов
- SLA и KPI
- Нагрузку на сеть и систему в организации
- Важность источников информации об уязвимостях

Плановая обработка уязвимостей



Два пути обработки уязвимостей



Процесс VM

Плановая обработка уязвимостей

- В IT-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с IT-отделом

Особо опасные уязвимости

- Фокус смещается на трендовые уязвимости и на те, что имеют эксплойт и расположены на важных активах
- О сроках устранения каждой уязвимости служба ИБ и IT-отдел договариваются отдельно

Контроль устранения



Статусы уязвимостей

Исключена

Новая

В работе

Исправляется

Требуется проверка

Просрочена

Устранена

Значимость актива

Высокая

Средняя


Низкая

Плановое устранение


Вчера

Уязвимости с отметкой «важная»


Активы высокой значимос...

813 -340  99



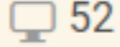
110  703 

Активы средней значимос...


0  0

Остальные уязвимости


Активы высокой значимос...

31 K -17023  52



31 K 

Активы средней значимос...

72 -52  1




72 

Трендовые уязвимости


Вчера


Актуальные

Активы высокой значимос...


2,3 K +29  131



114  2,2 K 


12 

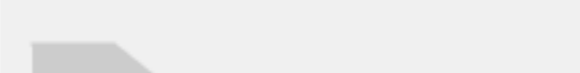
Остальные активы

0  0

Исправленные


Исключенные

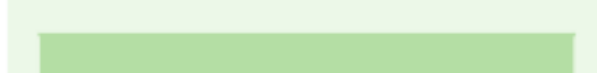
0 -8  0






Устраненные

3,7 K  73





 Важная

Уязвимости можно автоматически присваивать отметку «Важная» в зависимости от критериев (например, наличие эксплойта) или актива, на котором она была обнаружена

■ Уязвимость CVE-2024-20359 CVE-2024-20359 Cisco Cisco ASA

🔥 Есть эксплойт

🔧 Можно исправить

1 | 0 | 0

Уязвимость микропрограммного обеспечения межсетевых экранов Cisco Adaptive Security Appliance (ASA) и Cisco Firepower Threat Defense (FTD) связана с неверным управлением генерацией кода. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код с привилегиями root с помощью специально созданного файла

Дата публикации

24 апреля 2024, 00:00

Как исправить

Использование рекомендаций производителя: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h>

Ссылки

<https://bdu.fstec.ru/vul/2024-03264> ↗

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h> ↗

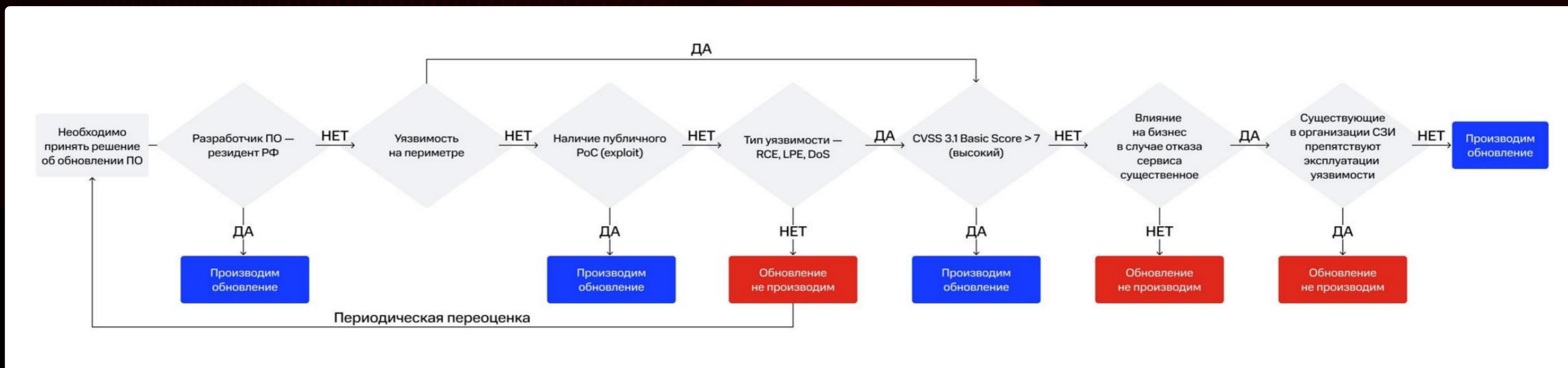
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog> ↗

Статус	Уязвимость на активе	Обнаружена
Новая	🚩 fw10.company.com (192.168.0.231) ↗ Устранение: Нет политики Cisco Cisco ASA 9.12(3)12	6 сен 2024, 05:33

Другие возможности MaxPatrol VM

- Рекомендации НКЦКИ для принятия решения по обновлению критически значимого ПО
- Оценка уязвимостей по методике ФСТЭК

Алгоритм принятия решения по обновлению ПО



Скачать документ
с рекомендациями



Алгоритм принятия решения по обновлению ПО



Уязвимости

Группы активов

Фильтр активов

Фильтр уязвимостей

```
Host.Softs.@Vulners and  
  
(Host.Softs.Vendor not in ["Communigate Systems", "Crypto-Pro", "Doctor  
Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive  
Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex",  
"CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go",  
"Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media  
Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project",  
"OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin",  
"PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTY", "Python Software  
Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid",  
"SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total  
Commander", "TrueCrypt Foundation", "University Of Cambridge",  
"VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl",  
"vsFTPd"])  
  
and (Host.Softs.@Vulners.Metrics.Exploitable = false)  
  
and not (Host.Softs.@Vulners.Name like "%Remote Code Execution%" or  
Host.Softs.@Vulners.Name like "%Удаленное%выполнение%" or  
Host.Softs.@Vulners.Name like "%Повышение%привилеги%" or  
Host.Softs.@Vulners.Name like "dos%" or Host.Softs.@Vulners.Name like  
"%Отказ%в%обслуживании%")
```

Ctrl + Enter для проверки запроса

✓ 9398 уязвимостей соответствуют запросу

Уязвимость **не** на периметре

Разработчик ПО **не** резидент России

Публичный эксплойт **отсутствует**

Тип уязвимости **не** RCE, LPE, DoS

Оценка уровня опасности уязвимостей по методике ФСТЭК

$$V = I_{cvss} \times I_{infr}$$

где I_{cvss} – показатель, характеризующий уровень опасности уязвимости;
 I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

2.6. Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1¹.

Ссылки

<https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/#CVE-2019-9799>

Оценка по CVSS v3

Общая **6.5**
 Базовая **7.5** – AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
 Временная **6.5** – E:U/RL:O/RC:C

2.7. Показатель I_{infr} определяется по следующей формуле:

$$I_{infr} = k * K + l * L + p * P, \text{ где}$$

K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

k, l, p – весовые коэффициенты показателей.

№ п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1	$7,0 \leq V \leq 10,0$	Критичный
2	$4,5 \leq V < 7,0$	Высокий
3	$1,5 \leq V < 4,5$	Средний
4	$V < 1,5$	Низкий

Оценка уязвимостей по методике ФСТЭК в MaxPatrol VM



The screenshot displays the MaxPatrol 10 interface with a query for vulnerability assessment using the ФСТЭК methodology. The main table shows the following data:

Узел	Уязвимость	Оценка уязвимости	Уровень критичности уязвимости
srv13.company.com (192.168.2.8)	Неподдерживаемая версия	6,4	High
srv6.company.com (192.168.0.11)	Неподдерживаемая версия	6,4	High
srv10.company.com (192.168.2.15)	Неподдерживаемая версия	6,4	High
srv10.company.com (192.168.2.15)	Неподдерживаемая версия	6,4	High
sccm.ptrevenge.stf (10.144.0.105)	Неподдерживаемая версия	6,4	High
srv6.company.com (192.168.0.11)	Неподдерживаемая версия	6,4	High
1c-srv.ptrevenge.stf (10.144.1.231)	Неподдерживаемая версия	6,4	High
srv13.company.com (192.168.2.8)	Неподдерживаемая версия	6,4	High
col-vm (10.144.1.67)	Неподдерживаемая версия	6,4	High
srv4.company.com (192.168.1.9)	Неподдерживаемая версия	6,4	High
wec (10.144.0.120)	Неподдерживаемая версия	6,4	High
srv5.company.com (192.168.1.10)	Неподдерживаемая версия	6,4	High
1c-db.ptrevenge.stf (10.144.1.230)	Неподдерживаемая версия	6,4	High
dc.ptrevenge.stf (10.144.0.102)	Неподдерживаемая версия	6,4	High
col-vm (10.144.1.67)	Неподдерживаемая версия	6,4	High
adcs2.ptrevenge.stf (10.144.0.104)	Неподдерживаемая версия	6,4	High
srv6.company.com (192.168.0.11)	Неподдерживаемая версия	6,4	High
dc.ptrevenge.stf (10.144.0.102)	Неподдерживаемая версия	6,4	High
dc-2.ptrevenge.stf (10.144.0.103)	Неподдерживаемая версия	6,4	High
sccm.ptrevenge.stf (10.144.0.105)	Неподдерживаемая версия	6,4	High
srv2.company.com (192.168.0.6)	Неподдерживаемая версия	6,4	High
exchange.ptrevenge.stf (10.144.0.106)	Неподдерживаемая версия	6,4	High
srv3.company.com (192.168.2.7)	Неподдерживаемая версия	6,4	High

The interface also shows a detailed view for the selected host **srv13.company.com (192.168.2.8)**, including system information, network configuration, and a list of the most dangerous vulnerabilities.

Информация о системе

- OS: Windows 2012 R2 6.3.9600
- BIOS: Phoenix Technologies LTD PhoenixBIOS 4.0 Release 6.0
- CPU: Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz
- MB: Intel Corporation
- RAM: 8
- HDD: \\.\PHYSICALDRIVE0, \\.\PHYSICALDRIVE1
- Ethernet: vmxnet3 Ethernet Adapter
- Domain: company.com

Самые опасные уязвимости

- Неподдерживаемая версия
- Неподдерживаемая версия
- Неподдерживаемая версия
- Неподдерживаемая версия
- Неподдерживаемая версия
- Неподдерживаемая версия
- Удаленное выполнение кода
- Повышение привилегий
- Повышение привилегий
- Удаленное выполнение кода

Уязвимости ОС и ПО

ПО	Кол-во	Состояние
Windows 2012 R2 6.3.9600	3287	Критично
ПО		
Microsoft Internet Explorer	1394	Критично
Microsoft .NET Framework	108	Критично
Microsoft Exchange	88	Критично
OpenSSL	38	Критично
VMware Tools	9	Внимание
Adobe Flash Player for Microsoft Edge and Internet Explorer	2	Критично

Спасибо!



Олег Кочетов

Лидер продуктовой практики
MaxPatrol VM, MaxPatrol HCC

✉ okochetov@ptsecurity.com

☎ +7 905 783 90 46

📍 @Bednight



Новости о продуктах
Positive Technologies:
t.me/ptproductupdate



Telegram-чат о MaxPatrol VM,
MaxPatrol SIEM и PT XDR:
t.me/MPSIEMChat

