

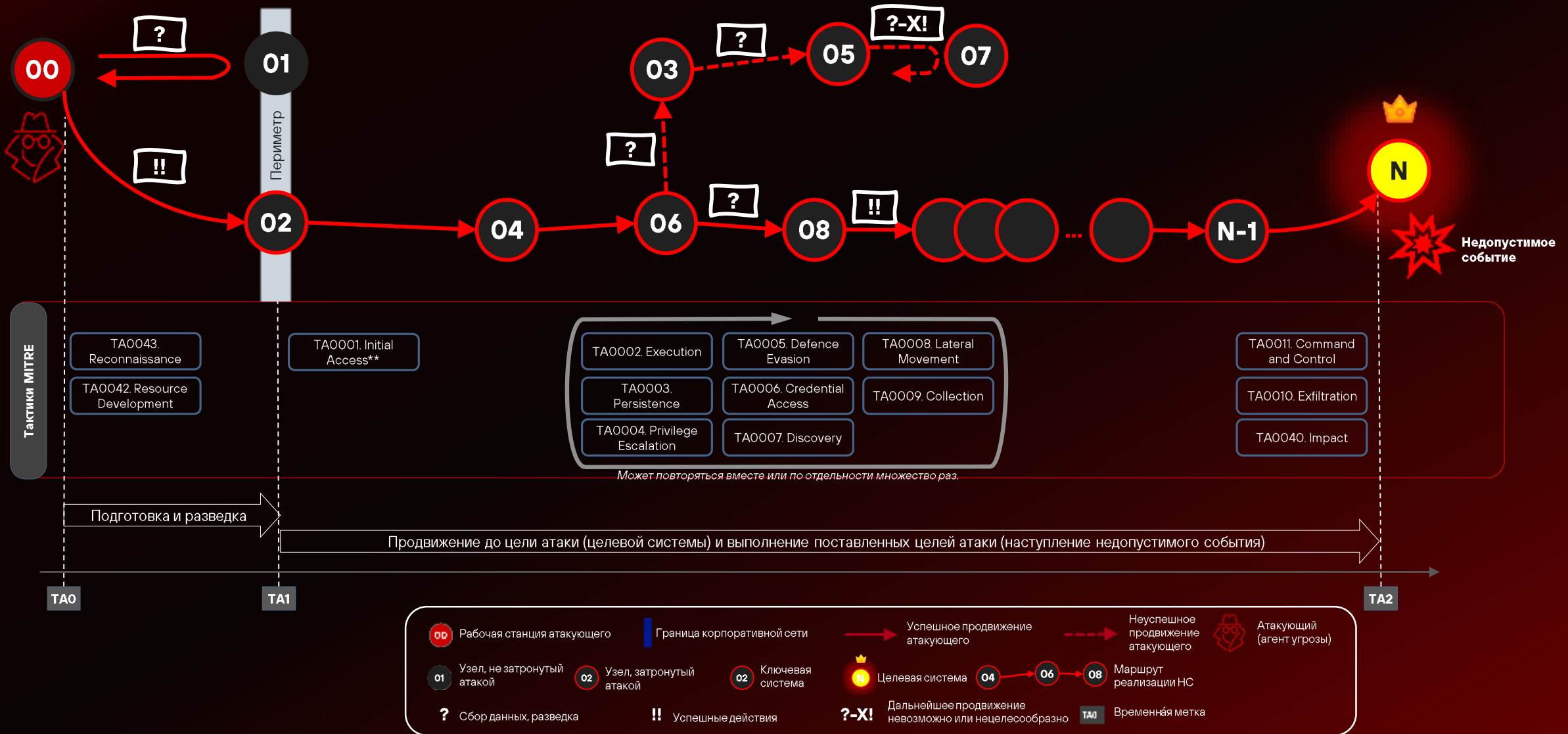
Кирилл Черкинский

Руководитель практики
защиты конечных устройств

pt

Защита конечных устройств с помощью MaxPatrol EDR

Инцидент и цепочка атаки



Что могло пойти не так?



Не отреагировали вовремя

+

Не подключили источники или собрали не всё

Не устранили уязвимости

→

Не было инструментов и процессов

Защита конечных устройств: чек-лист

СБОР ДАННЫХ

- События собираются со всех устройств?
- Достаточно ли этих событий для выявления атак?
- Вы можете оперативно корректировать профиль мониторинга?
- У вас есть информация о самих узлах? Кто за ними работает? Какой софт на них установлен? Как они настроены?
- А если сотрудники работают удаленно?

ВЫЯВЛЕНИЕ

- Есть ли у вас инструменты для оперативного выявления угроз?
- Вы уверены в качестве обнаружения?
- Можете обработать весь поток инцидентов и уведомлений?
- Достаточно ли быстро можете проанализировать ситуацию и подтвердить инцидент?

РЕАГИРОВАНИЕ

- Есть ли инструменты для реагирования? Достаточно ли вариантов действий?
- Можете ли локализовать инцидент быстро?
- Нужно ли привлекать ИТ или внешнего подрядчика?
- Можете ли автоматизировать реагирование?
- А в тех случаях, когда у агента нет связи с сервером?

СЛОЖНЫЙ КЕЙС

- Нужно защитить крупное международное мероприятие
- Часть инфраструктуры — удаленные площадки за периметром
- Другая часть регулярно обновляется
- Время решения инцидента — 2 часа



Как хакеры ПРОИГРАЛИ на «Играх Будущего»



Positive Technologies раскрыла подробности защиты мультиспортивного фиджитал-турнира «Игры Будущего» от кибератак

MaxPatrol EDR

Защитит конечные устройства от сложных и целевых атак

- **На ранних этапах выявляет атаки,** которые могут пропустить другие средства защиты устройств
- **Собирает максимум данных с узлов и обнаруживает киберугрозы**
- **Останавливает злоумышленников за считанные секунды**
- **Единый агент для продуктов Positive Technologies**



Экспертиза Positive Technologies уже на устройствах:

- Автономный поведенческий и корреляционный анализ, реагирование непосредственно на защищаемом устройстве
- Мощный корреляционный движок для поведенческого анализа угроз: 700+ правил PT ESC
- Покрывает 60% техник матрицы MITRE ATT&CK
- 6000+ YARA-правил
- Модули «Обнаружение подозрительных файлов» и «Проверка файлов по хеш-сумме» (65 000+ хеш-сумм в базе данных от PT ESC)
- В связке с PT Sandbox позволяет повысить качество проверки файлов даже из зашифрованных каналов (например, при отправке файла в Telegram)

Как устроен MaxPatrol EDR: архитектура



Как работает MaxPatrol EDR



На чем работает MaxPatrol EDR

CentOS 9	РЕД ОС 8	Альт Сервер 9	Astra Linux 1.8	RHEL 9	Ubuntu 24.04
Windows 10	Astra Linux 1.7	Oracle 9	Windows Server 2022	Альт Сервер 10.2	Альт Р. станция 9
РЕД ОС 7.2	Альт Р. станция 10.2	Debian 11	Альт Р. станция 10.1	Мос.ОС 12	CentOS 10
Debian 12	Windows Server 2019	RHEL 8	Ubuntu 22.04	ОСнова 2.0	macOS 14
Ubuntu 20.04	macOS 15	AlterOS 7.5	Windows 11	Альт Сервер 10.1	Astra Linux CE

...и ЭТОТ СПИСОК РАСТЕТ С КАЖДЫМ РЕЛИЗОМ

Политики MaxPatrol EDR

- Определяют набор модулей, устанавливаемых на агенты
- Хранят настройки, с которыми работают модули
- Можно сделать индивидуальными для каждой группы устройств
- Автоматизируют реагирование и сбор контекстных данных
- Упрощают взаимодействие между ИБ и ИТ департаментами:
 - Регулируют, каким образом и в каких случаях можно реагировать
 - Унифицируют профили сбора событий

The screenshot displays the MaxPatrol EDR Policy Editor interface. The main window is titled "default_Обнаружение угроз (Windows)". The interface is divided into several sections:

- Политики:** Shows the current policy name and options like "Связь с группами" and "Создать шаблон".
- Модули:** A list of modules under the "Включенные" (Enabled) tab, including "YARA-сканер", "Корреллятор (Windows)", "Проверка файлов в PT Sandbox", and "Проверка файлов по хэш-сумме". There is also a section for "Доступны для добавления" (Available for addition) with modules like "Antimal", "Завершение работы", "Интерпретатор языка Lua", "Корреллятор (Linux)", "Обнаружение подозрительных ф...", "Отправка событий на syslog-сер...", "Отправка файлов", "Сбор данных из файлов журналов", "Установщик auditd", and "Недоступны для добавления" (Not available for addition) with "ETW-трассировка событий Wind..." and "WinEventLog: сбор данных из жу...".
- Агенты:** Shows the "Корреллятор (Windows)" agent, which is "Включен" (Enabled) and has version "2.0.0". It includes a search field for "Common_whitelist_value".
- События:** A list of events with their MITRE ATT&CK coverage. The list includes:
 - AMSI Bypass via Powershell (T1542.001: Отключение или перенастройка средств защиты)
 - Abnormal Directory for Process (T1034.006: Подбор легитимного имени или расположения)
 - Abuse Kerberos RC4 (T1058: Кража или подделка билетов Kerberos)
 - Abusing CredSSP (T1003: Получение данных учетных данных)
 - Abusing Windows Telemetry Persist (T1051.005: Планирование заданий Windows)
 - Access PST file in share (T1039: Данные с области сетевых дисков)
 - Access System Credential Files via cmdline (T1552.001: Учетные данные в файлах, T1003.003: Файл ntls.dll, T1555: Учетные данные из хранилища паролей)

Развертывание не за часы, а за минуты

- Преднастроенные шаблоны «из коробки»
- Превращаем любую политику в шаблон
- Применяем шаблон к любой политике
- При необходимости экспортируем или импортируем шаблон

Шаблоны политик

Импортировать Экспортировать Удалить

Название или идентификатор

Тип	Название	Модули	ОС	Дата создания
П	Конфигуратор аудита Windows	Конфигуратор аудита Windows, Ядро (внутренний серв...	Все 2	20 мая, 15:33
П	Реагирование на угрозы (Windows)	Блокировка по IP-адресу, Блокировка учетных записей...	Все 9	20 мая, 15:33
П	Реагирование на угрозы (Linux)	Блокировка учетных записей, Завершение процессов, У...	Все 4	20 мая, 15:33
П	Интеграция с MaxPatrol VM	Сканирование в режиме аудита (MaxPatrol VM)		20 мая, 15:33
П	Обнаружение угроз (Windows)	YARA-сканер, Коррелятор (Windows), Проверка файлов ...	Все 4	20 мая, 15:33
П	Обнаружение угроз (Linux)	YARA-сканер, Коррелятор (Linux), Проверка файлов в P...	Все 4	20 мая, 15:33
П	Сбор данных с рабочих станций (Windows)	WinEventLog: сбор данных из журнала событий Window...	Все 3	20 мая, 15:33
П	Сбор данных с серверов (Windows)	WinEventLog: сбор данных из журнала событий Window...	Все 3	20 мая, 15:33
П	Сбор данных с контроллеров доменов (Windows)	WinEventLog: сбор данных из журнала событий Window...	Все 3	20 мая, 15:33
П	Сбор данных (Linux)	Нормализатор, Сбор данных из файлов журналов, Устан...	Все 3	20 мая, 15:33
П	Обнаружение угроз и реагирование (Windows)	YARA-сканер, Блокировка по IP-адресу, Блокировка уч...	Все 13	20 мая, 15:33
П	Обнаружение угроз и реагирование (Linux)	YARA-сканер, Блокировка учетных записей, Завершени...	Все 10	20 мая, 15:33

Всего 12 шаблонов

Реагирование на угрозы (Windows)

Параметры

Операционные системы

- Windows x86, x64
- Linux x86, x64
- macOS x64

Идентификатор: e975 a7b2-8dc5-ad98-172d-...-9b33-d601

Дата создания: 20 мая, 15:33

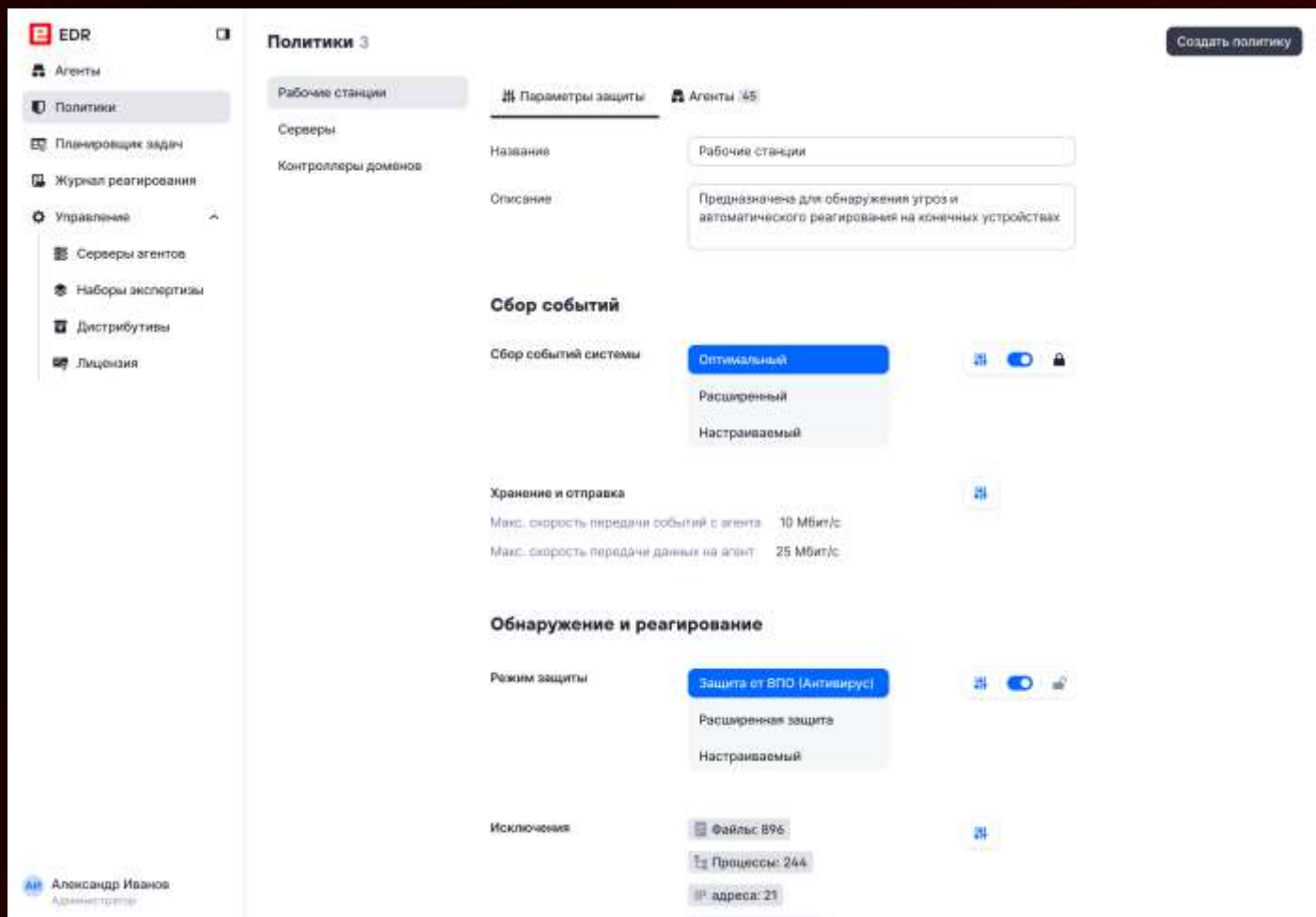
Описание: Политики на базе этого шаблона предназначены для лучшего реагирования на подозрительные или вредоносные действия на конечных устройствах под управлением Windows

Наборы экспертизы

Модули

- Блокировка по IP-адресу
- Блокировка учетных записей
- Завершение процессов
- Запуск командной оболочки
- Изоляция узлов
- Карантин
- Переадресация DNS-запросов (jshiba...
- Сбор данных о состоянии системы
- Удаление файлов

Обновления в следующих релизах



- Полная переработка логики работы с политиками
- Переход от компоновки политики модулями к выбору нужной функциональности
- Базовые «коробочные» профили не требуют конфигурирования
- Иерархичность политик с защитой параметров от изменения на вложенных уровнях

Готовые рецепты



Инвентаризация и сбор событий

- Минимум ресурсов на внедрение
- Минимальное влияние на производительность



Сбор данных и реагирование вручную

- Баланс между затратами на внедрение, функциональностью и нагрузкой на устройства



Сбор, обнаружение, реагирование

- Нужно «приучить» к инфраструктуре
- Агент EDR сильнее влияет на производительность устройства

СЦЕНАРИЙ 1

ИНВЕНТАРИЗАЦИЯ И СБОР СОБЫТИЙ

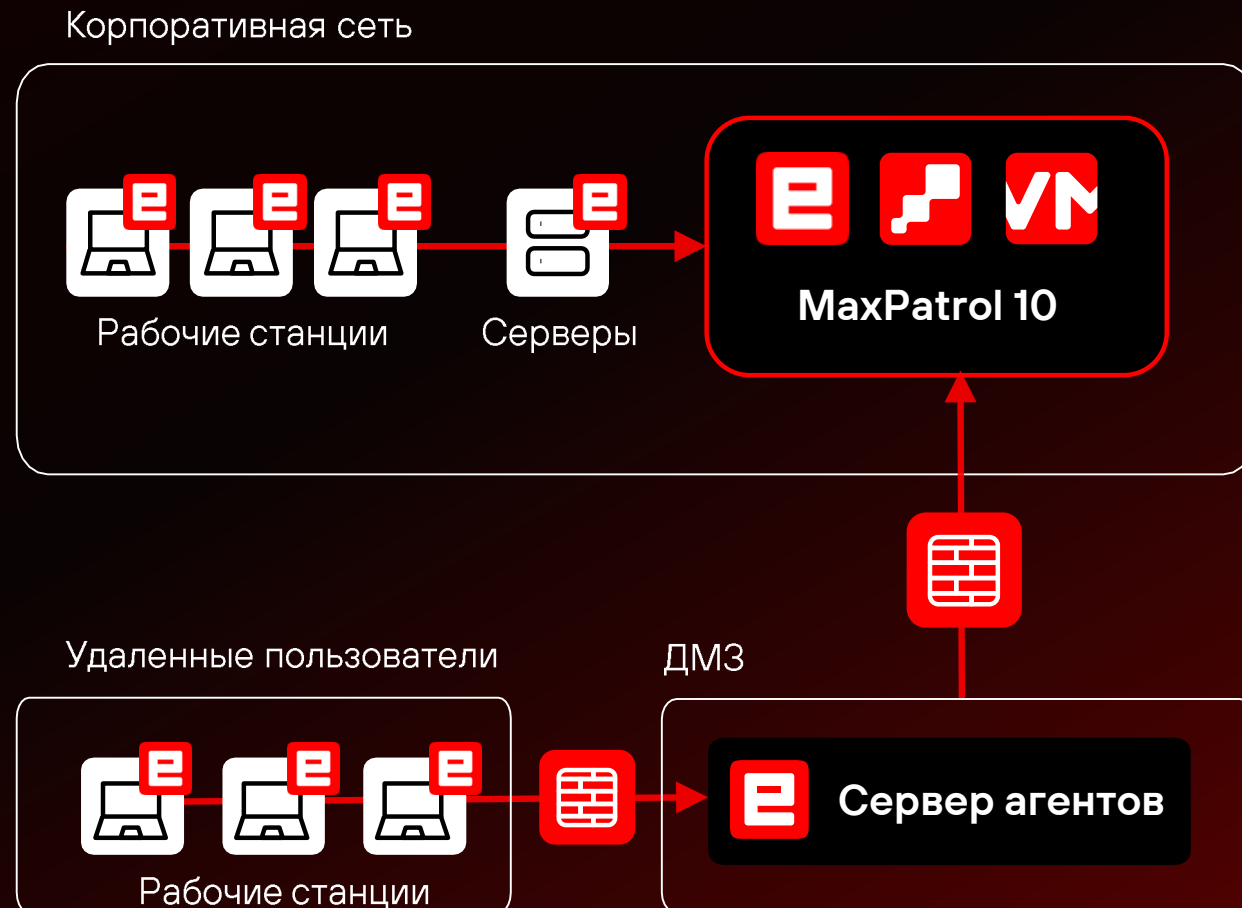
- Агент EDR отправляет события в MaxPatrol SIEM и помогает выстроить процесс управления уязвимостями
- Простое и быстрое внедрение, легкая настройка
- Синхронизация списков исключений с MaxPatrol SIEM



Управляемый сбор данных



- Конфигурируем и собираем:
 - Windows Eventlog
 - Sysmon
 - ETW
 - Auditd
 - eBPF** (Q3-Q4 2025)
 - Файлы журналов
- В том числе с устройств вне домена или периметра
- Сбор событий — непрерывно, сканирование — по расписанию
- Для сканирования не нужны учетные записи с повышенными привилегиями
- Более простая маршрутизация: все данные передаются через соединение агента



Конфигуратор аудита Windows

Конфигуратор аудита Windows ■ Отключить [↑](#) Сменить версию ⚙️ 🗑️

Включен · Версия: 1.0.0 · 🖥️ 📱 🍏

Вход учетной записи (Account Logon) ^

Аудит проверки учетных данных (Audit Credential Validation)

Контроллер доменов	Сервер	Рабочая станция
Успех <input type="checkbox"/> Отказ <input type="checkbox"/>	Успех <input type="checkbox"/> Отказ <input type="checkbox"/>	Успех <input type="checkbox"/> Отказ <input type="checkbox"/>

Аудит службы проверки подлинности Kerberos (Audit Kerberos Authentication Service)

Контроллер доменов	Сервер	Рабочая станция
Успех <input type="checkbox"/> Отказ <input type="checkbox"/>	Не настроено	Не настроено

Аудит операций с билетами службы Kerberos (Audit Kerberos Service Ticket Operations)

Контроллер доменов	Сервер	Рабочая станция
Успех <input type="checkbox"/> Отказ <input type="checkbox"/>	Не настроено	Не настроено

Аудит других событий входа учетных записей (Audit Other Account Logon Events)

Контроллер доменов	Сервер	Рабочая станция
Успех <input type="checkbox"/>	Успех <input type="checkbox"/>	Успех <input type="checkbox"/>

Управление учетными записями (Account Management) v

Настройка Sysmon и auditd на уровне политики

Установщик Sysmon

Включен · Версия: 1.0.0

Отключить Сменить версию

Основные параметры

Заменить исполняемый файл Sysmon на агенте

Да Нет

Заменить файл конфигурации на агенте

Да Нет

Файл конфигурации

```
<!--SYSMON EVENT ID 1 : PROCESS CREATION-->
<RuleGroup name="" groupRelation="or">
  <ProcessCreate onmatch="exclude">
    <CommandLine
condition="contains">:\Windows\system32\DllHost.exe /Processid</CommandLine>
    <CommandLine
condition="contains">:\Windows\system32\SearchIndexer.exe
/Embedding</CommandLine>
    <ParentCommandLine condition="begin
with">%%SystemRoot%\system32\csrss.exe
```

Установщик auditd

Включен · Версия: 1.0.0

Отключить Сменить версию

Основные параметры

Правила

```
# ignore errors
-i
# delete all rules
-D
# for busy systems
-b 8192

# disable kprint
```

Содержимое файла /etc/audit/audit.rules

Конфигурация auditd

```
#
# This file controls the
configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
```

Содержимое файла /etc/audit/auditd.conf

Заменить конфигурацию и правила auditd на агенте

Да Нет

ETW

Модули Зависимости Группы Агенты

Включенные

- ETW: трассировка событий Win... ⚠
- Конфигуратор аудита Windows ⚠
- WinEventLog: сбор данных из жу...
- Нормализатор
- Установщик Sysmon

Доступны для добавления

- [Устаревший] Драйвер сбора дан...
- Antimal
- Завершение работы
- Интерпретатор языка Lua
- Коррелятор (Linux)
- Обнаружение подозрительных ф...
- Отправка событий на syslog-сер...
- Отправка файлов
- Сбор данных из файлов журналов
- Сканирование в режиме аудита (...)
- Установщик auditd

Недоступны для добавления

- YARA-сканер
- Блокировка по IP-адресу
- Блокировка учетных записей
- Завершение процессов
- Запуск командной оболочки
- Изоляция узлов
- Карантин
- Коррелятор (Windows)

ETW: трассировка событий Windows Отключить Сменить версию

Включен · Версия: 1.0.0

Основные параметры

Microsoft-Windows-WMI-Activity

- Trace
- Operational
- Debug

Фильтр событий

* Обрабатываемые события

11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, 5857, 5858, 5859, 5860, 5861

Идентификаторы событий через запятую; * — все события

Исключения

Идентификаторы событий через запятую

Microsoft-Windows-Kernel-Process

- WINEVENT_KEYWORD_PROCESS
- WINEVENT_KEYWORD_THREAD
- WINEVENT_KEYWORD_IMAGE

Фильтр событий

Сохранить Отмена

- Технология ETW — это диагностическое средство ОС Windows, позволяющее получить огромное количество информации о службах, приложениях, драйверах
- Модуль создает ETW-сессию и подписывается на ETW события, публикуемые указанными провайдерами
- Сам проверяет активность созданной ETW сессии
- EDR - единственный поставщик ETW событий для обнаружения

Фильтрация событий

WinEventLog: сбор данных из журнала событий Windows Отключить Сменить версию

Включен · Версия: 1.0.0

Каналы журналов

Список каналов сбора данных

- Security
- Kaspersky Endpoint Security
- Kaspersky Event Log
- Microsoft-Windows-Windows Defender/Operational
- Microsoft-Windows-Sysmon/Operational
- Microsoft-Windows-PowerShell/Operational
- Microsoft-Windows-TaskScheduler/Operational
- System
- Application

* Канал

Microsoft-Windows-Sysmon/Operational

* Запрос для выбора событий (XPath 1.0)

*

Запрос для исключений (XPath 1.0)

*[System[EventID=7] and EventData[Data[@Name=SignatureStatus] = 'Valid'] and EventData[Data[@Name=Signatur

Сохранить Отмена

СЦЕНАРИЙ 2

ДОБАВЛЯЕМ РЕАГИРОВАНИЕ

- Модули реагирования только для ручного режима
- Появляется возможность локализовать и устранить инцидент
- Реагирование в два клика из карточки события



Ручное реагирование (+API)

→ Полная или частичная сетевая изоляция узлов

→ Завершение процессов

→ Удаление файлов

→ Блокировка соединений по IP-адресам

→ Перенаправление сетевых соединений (синкхолинг)

→ Блокировка учетных записей пользователей

→ Карантин файлов

→ Запуск командной оболочки

ГИБКОСТЬ НАСТРОЙКИ И УПРАВЛЕНИЕ НАГРУЗКОЙ

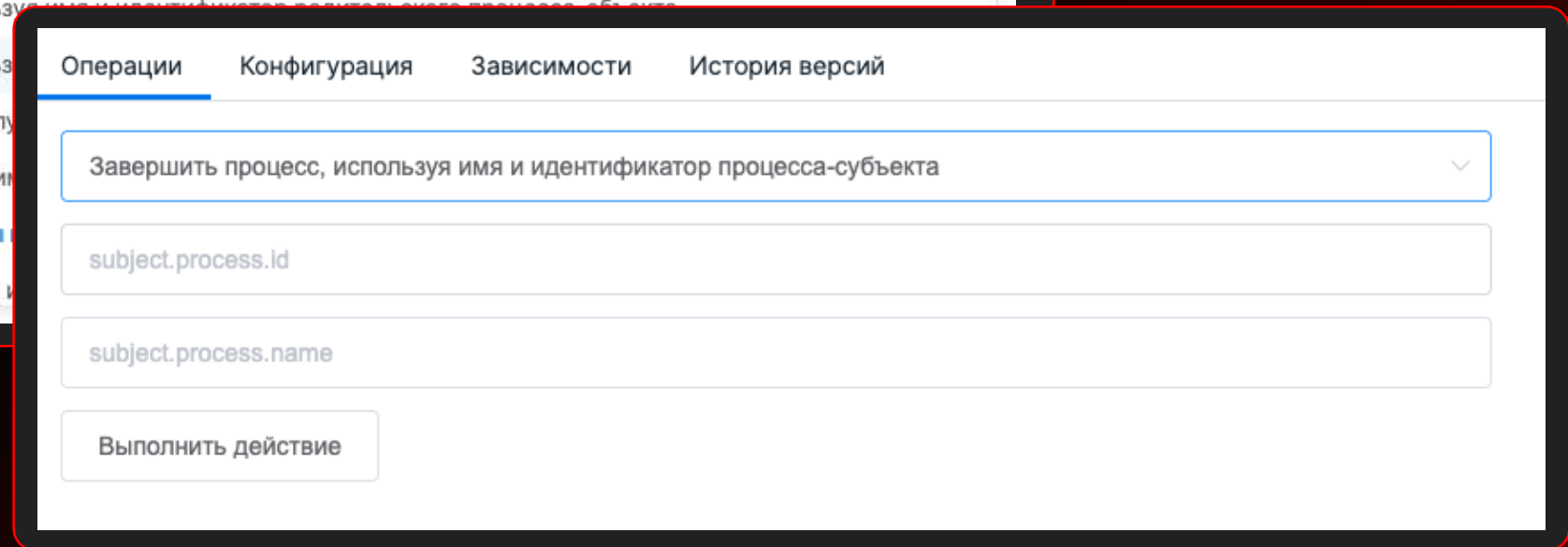
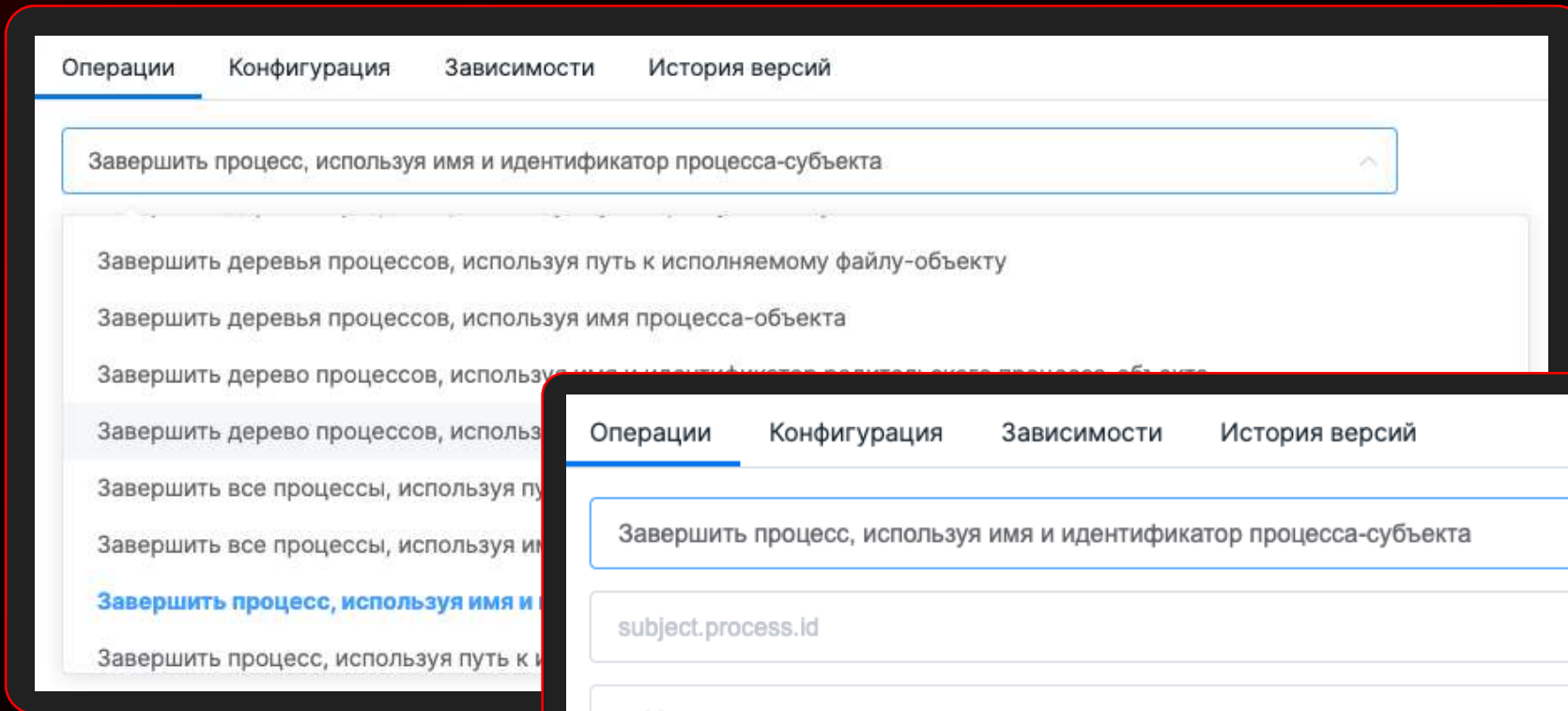
→ Настраиваемые
политики
реагирования

→ Модули
реагирования
в режиме ожидания
потребляют
минимум ресурсов

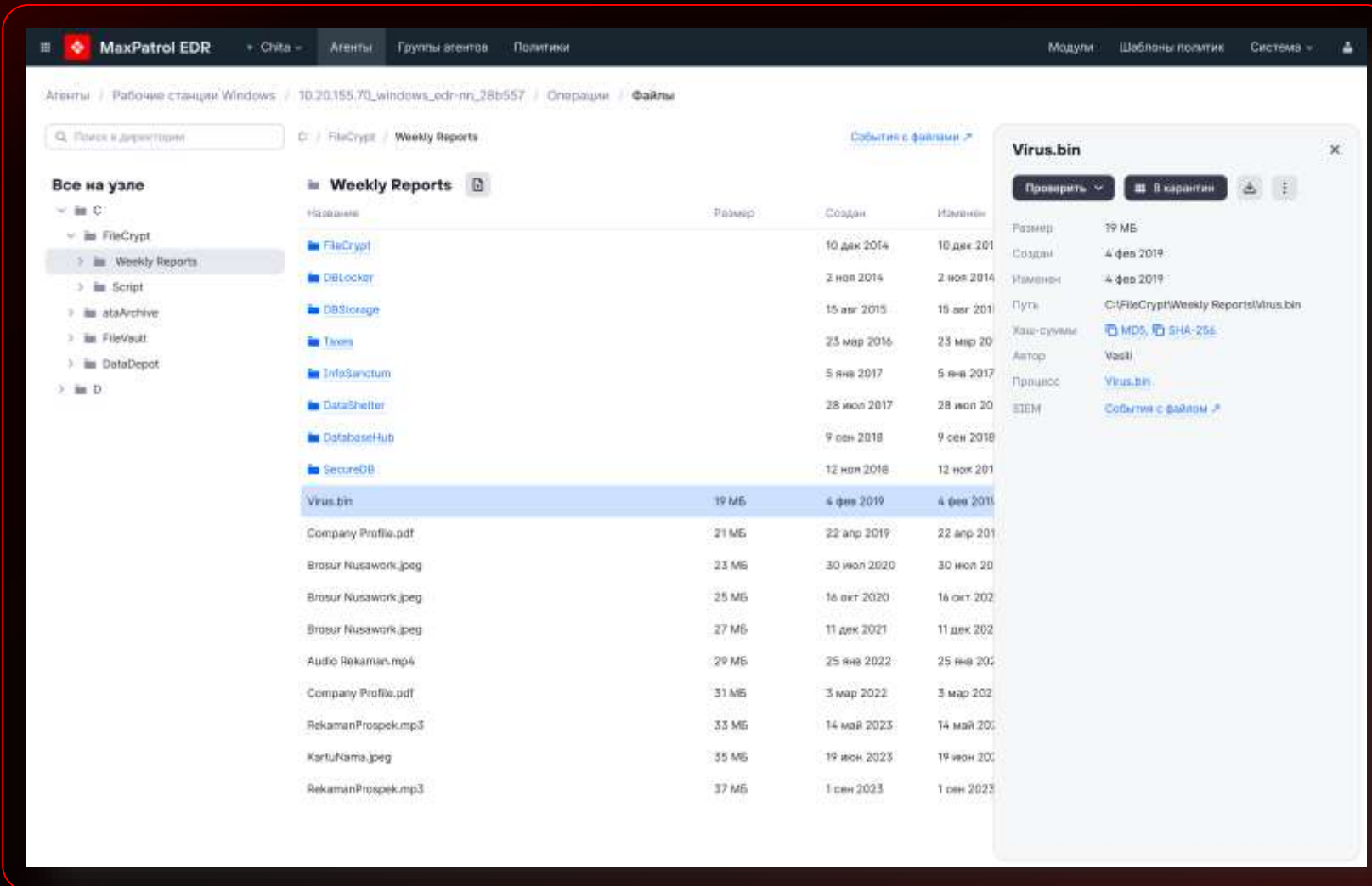
КОНТРОЛЬ УСТРОЙСТВ, НАХОДЯЩИХСЯ ВНЕ КОРПОРАТИВНОЙ СЕТИ

→ Реагирование
на устройствах вне
корпоративного
периметра

Реагирование из интерактива модуля



Обновления в следующих релизах



The screenshot displays the MaxPatrol EDR interface. The main window shows a file explorer view of the 'Weekly Reports' directory. The file 'Virus.bin' is selected, and a detailed view of the file is shown on the right. The interface includes a search bar, a navigation pane, and a main content area with a table of files.

Название	Размер	Создан	Изменен
FileCrypt		10 дек 2014	10 дек 2014
DBLocker		2 ноя 2014	2 ноя 2014
DBStorage		15 авг 2015	15 авг 2015
Taxim		23 мар 2016	23 мар 2016
InfoSanctum		5 янв 2017	5 янв 2017
DataShelter		28 июл 2017	28 июл 2017
DatabaseHub		9 сен 2018	9 сен 2018
SecureDB		12 ноя 2018	12 ноя 2018
Virus.bin	19 МБ	4 фев 2019	4 фев 2019
Company Profile.pdf	21 МБ	22 апр 2019	22 апр 2019
Brosur Nusawork.jpeg	23 МБ	30 июл 2020	30 июл 2020
Brosur Nusawork.jpeg	25 МБ	16 окт 2020	16 окт 2020
Brosur Nusawork.jpeg	27 МБ	11 дек 2021	11 дек 2021
Audio Rekaman.mp4	29 МБ	25 янв 2022	25 янв 2022
Company Profile.pdf	31 МБ	3 мар 2022	3 мар 2022
RekamanProspek.mp3	33 МБ	14 май 2023	14 май 2023
KartuNama.jpeg	35 МБ	19 июн 2023	19 июн 2023
RekamanProspek.mp3	37 МБ	1 сен 2023	1 сен 2023

The detailed view of 'Virus.bin' shows the following information:

- Проверить
- В карантин
- Размер: 19 МБ
- Создан: 4 фев 2019
- Именован: 4 фев 2019
- Путь: C:\FileCrypt\Weekly Reports\Virus.bin
- Хэш-суммы: MD5, SHA-256
- Автор: Vasil
- Процесс: Virus.bin
- ВЗЕМ

- Новый интерактив работы с файлами: выгрузка, загрузка, удаление, карантин, YARA и AV-сканы
- Новый интерактив для работы с процессами: завершить, просканировать, сделать дамп

Реагирование из карточки события в 2 клика

На агенте PT XDR dc-edr.edr2.local сработало правило корреляции Scheduled_task_Manipulation

Субъект	Действие	Объект	Статус	Источники
dc-edr.edr2	modify	schedule scan	success	192.168.55.150
subject account		object task	reason Task Modify	dc-edr.edr2.local (192.16...
mousocoreworker.exe		type Scheduled		
subject account		property command		
md5 57817AD88EBA2D8F14E8589...		value %systemroot%\system32\usd...		
sha1 50A2EE0F8C0F50D6826FC2B...		fullpath \microsoft\windows\updat...		
sha256 FA4917DC65B865CA31D1A...		state enabled		
lmphash 1BCF5F68943D3AA81D3...				

Реагировать

Реагирование

Название действия

Завершение процессов

- ▶ Завершить все процессы, используя имя процесса-субъекта mousocoreworker.exe
- Завершить все процессы, используя путь к файлу-объекту \microsoft\windows\updateorchestrator\schedule scan
- Завершить дерево процессов, используя имя и идентификатор родительского процесса-субъекта 3416 mousocoreworker.exe
- Завершить деревья процессов, используя имя процесса-субъекта mousocoreworker.exe
- Завершить деревья процессов, используя путь к файлу-объекту \microsoft\windows\updateorchestrator\schedule scan
- Завершить процесс, используя имя и идентификатор процесса-субъекта 3416 mousocoreworker.exe

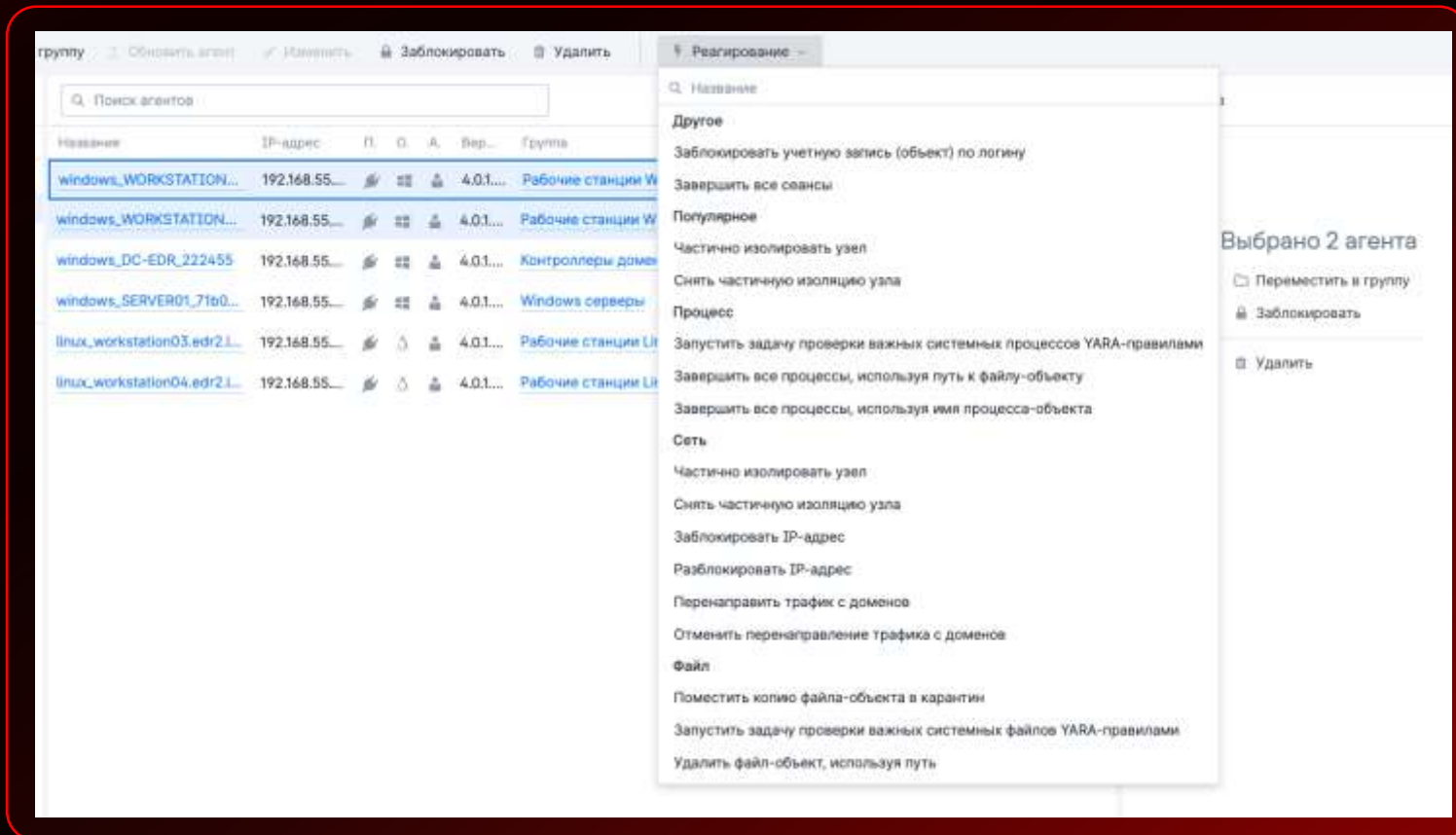
Изоляция узлов

- Полностью изолировать узел
- Снять частичную изоляцию узла
- Частично изолировать узел

Удаление файлов

- Удалить файл-объект, используя путь \microsoft\windows\updateorchestrator\schedule scan

Реагирование на множестве агентов



> Просто начать
и удобно продолжить

- В журнале реагирования отображаются статусы задач — понятная обратная связь по всем устройствам
- Можно повторить выполнение действий
- В пару кликов можно другое действие для выбранной группы или для некоторых агентов

Реагирование на множестве агентов

Журнал реагирования > Частично изолировать узел ↻ Повторить ⚡ Другое действие ▾

Результат

	Агент	П.	Последний раз в сети	Выполнено	Результат
Все 2					
Выполняется 1	windows_WORKSTATION...		Сегодня, 17:51		Применяется
Выполнено 1	windows_WORKSTATION...		Сегодня, 17:51	Сегодня, 17:51:52	Завершено
Ошибка 0					

Реагирование

Модуль
Изоляция узлов

Агенты
2

Инициировано
Сегодня, 17:51

СЦЕНАРИЙ 3

EDR НА МАКСИМАЛКАХ. ПРОКАЧИВАЕМ ОБНАРУЖЕНИЕ

- Обнаружение на агенте
- Многоэтапные проверки
- Автоматизация реагирования



MaxPatrol EDR: обнаружение

- Поведенческий анализ прямо на устройствах с помощью узлового коррелятора
- Статический анализ YARA-правилами для сканирования файлов и процессов
- Мониторинг появления опасных файлов и взаимодействия с ними
- Обнаружение наиболее актуальных вредоносных образцов по контрольным суммам
- Механизмы обнаружения работают на агенте, возможна работа **в автономном режиме**
- Дополнительные проверки артефактов во внешних системах (PT Sandbox, PT Multiscanner)

ОБНАРУЖИВАЕТ ПОПУЛЯРНЫЕ ТЕХНИКИ ИЗ МАТРИЦЫ MITRE ATT&CK

→ **600+ правил**
для Windows

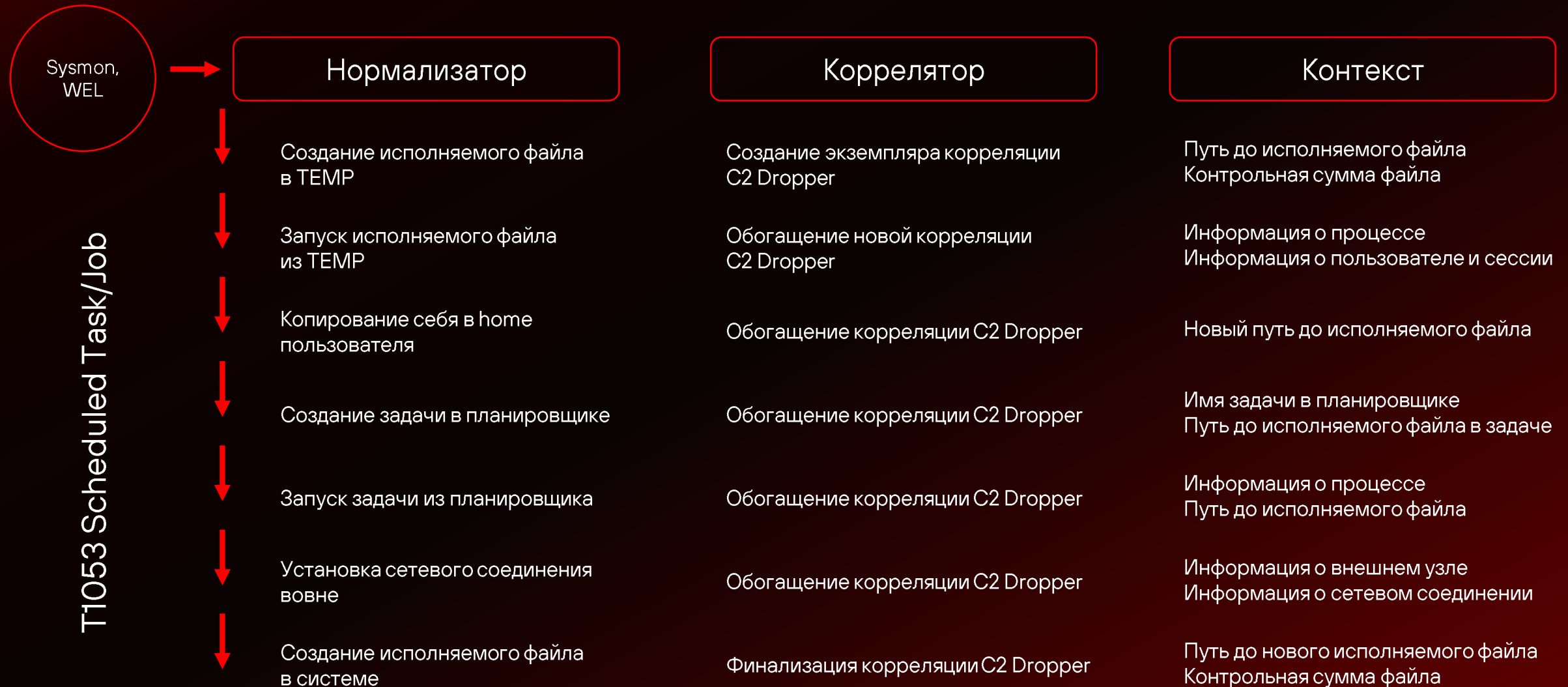
→ **150+ правил**
для Linux

ДАЕТ ВОЗМОЖНОСТЬ ГРАНУЛЯРНОЙ НАСТРОЙКИ СИСТЕМЫ

→ Баланс между глубиной детекта и нагрузкой на устройство

→ Уникальные политики обнаружения для разных групп активов

Корреляция на агенте



Пользовательская экспертиза

- Пользователи могут создавать в PT Knowledge Base (PT KB) свои наборы экспертизы для установки в MaxPatrol EDR
- Наборы экспертизы включают правила корреляции и нормализации, а также табличные списки
- Можно использовать отдельные наборы для разных политик

MaxPatrol EDR использует корреляционный движок, который работает **на агентах**.

Это позволяет выявлять техники злоумышленников локально. **Даже тогда, когда агент не подключен к серверу управления.**

Срабатывания коррелятора можно использовать как **триггеры для автоматизации действий** реагирования

Автоматизация действий

ЭКОНОМИЯ ВРЕМЕНИ И РЕСУРСОВ

→ Можно назначить разные сценарии для разных групп агентов

→ Действия выполняются даже в автономном режиме*

Мастер назначения действий · Шаг 2 из 2

События-триггеры для действия «Частично изолировать узел»

Все события	Выбранные
Быстрый поиск	Быстрый поиск
Abnormal Directory for Process +	Malware Trojan Dropper Script Generi... -
Abuse Kerberos RC4 +	Malware Trojan Ransom Win32 Generi... -
Abusing CredSSP +	Malware Trojan Ransom Win32 Generi... -
Abusing Windows Telemetry Persist +	Malware Trojan Win32 Generic a -
Access into Sensitive Files via Networ... +	Malware Trojan Win32 Generic o -
Access System Credential Files via cm... +	Malware Trojan Win32 Generic s -
Accessibility Feature Tool Abuse +	Metasploit Payload -
Account Discovery +	Mimikatz Command -
Account or Group discovery via SAM R +	Remote Password Dump -
Active Directory Snapshot +	Remoting Impacket PsExec -
ActiveDirectory Data Collection +	Remoting SysInternals PsExec -
ADCS Recon +	Remoting Windows Shell -
Add new user in commandline +	Remoting WinExec -
Alternate Data Stream +	Remoting WMI -
AMSI Bypass via Powershell +	Rubeus Usage -
AppCert DLLs Persist +	Run whoami as System -

Metasploit Payload

Metasploit_Payload

Описание	Действия	Переменные
Сохранить в БД	Коррелятор (Windows)	10
Отправить событие на syslog-сервер	Отправка событий на syslog-сервер	10
Частично изолировать узел	Изоляция узлов	50
Завершить дерево процессов, используя имя и идентификатор родительского процесса-объекта	Завершение процессов	74

Выбрать другое действие Сохранить Отмена

Автоматизация действий

ФИЛЬТРАЦИЯ ПО ТЕХНИКАМ MITRE

При настройке политик удобно фильтровать корреляционные правила по техникам, которые они покрывают.

Мастер назначения действий · Шаг 2 из 2

События-триггеры для действия «Удалить на уровне ядра исполняемый файл процесс...»

События

Быстрый поиск

- Abnormal Directory for Process +
- Access System Credential files via c... +
- Accessibility Feature Tool Abuse +
- Account Discovery +
- Active Directory Snapshot +
- Add new user in commandline +
- Alternate Data Stream +
- AMSI Bypass via Powershell +
- AppLocker Policies Discovery +

Выбрать другое действие

Искать тактику или технику

- TA0007: Изучение
 - T1046: Изучение сетевых служб
- T1087: Изучение учетных записей
 - T1087.002: Доменная учетная запись
 - T1087.001: Локальная учетная запись
- T1518: Изучение установленного ПО
 - T1518.001: Изучение средств защиты
- T1069: Изучение групп разрешений
 - T1069.002: Доменные группы
 - T1069.001: Локальные группы
- T1482: Изучение доверительных отношени...
- T1012: Запросы к реестру

Сбросить Применить Отмена

Abnormal Directory for Process

Abnormal Directory for Process

Действия Переменные

Исполнительный файл
process.name}} из
локального каталога на узле
{{src.host}} Высокая критичность;
точность

Используемые техники MITRE ATT&CK

5: Подбор легитимного имени
пользователя

Сохранить Отмена

MaxPatrol EDR + PT Sandbox для сложных случаев

- 1 Обнаруживаются файлы, скачиваемые, например, через Telegram, браузеры, P2P
- 2 Проводится подробный статический и поведенческий анализ
- 3 Реагирование выполняется автоматически в соответствии с параметрами политики



«Работодатель года».
Атака Lazarus Group



Объединенная консоль для работы с событиями

ИНСТРУМЕНТЫ ДЛЯ РАССЛЕДОВАНИЯ И THREAT HUNTING

- Группировка событий по активам и типам, предустановленные фильтры
- Настройка представления: фильтрация, выбор колонок, группировка и агрегация
- Интерактивное добавление условий в фильтры по клику
- Единый интерфейс для MaxPatrol EDR, MaxPatrol SIEM и MaxPatrol VM

The screenshot displays the MaxPatrol 10 interface. The main window shows a list of events with columns for ID, source, time, host, and text. A filter bar at the top allows for complex queries. A sidebar on the left provides a menu for filters and data collection methods. A detailed view of a specific event is shown on the right.

Filter Bar:

```

generator.type = "edr" > (|) time, event_src_host, text > (|) time (показываю только) >
event_src_subsys, COUNT(*) as Cnt > (|) Cnt (9 - 8) > 19888
  
```

Event List:

ID	event_src_subsys	time	event_src_host	text
9741	microsoft-windows-wmi-activity	16.07.2025, 17:45:00	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
3258	microsoft-windows-system/ops	16.07.2025, 17:44:12	workstation02.edr2.local	Обнаружено подключение с узла workstation02.ed...
1288	security	16.07.2025, 17:44:09	workstation01.edr2.local	На агенте PT XDR workstation01.edr2.local сработ...
383	audit	16.07.2025, 17:44:06	server01.edr2.local	На агенте PT XDR server01.edr2.local сработало пр...
318	microsoft-windows-wmi32k/trace	16.07.2025, 17:42:52	server01.edr2.local	Обнаружено подключение с узла server01.edr2.loc...
283	microsoft-windows-kernel-proca	16.07.2025, 17:40:43	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
364	microsoft-windows-task Schedul	16.07.2025, 17:40:33	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
97	cometlab	16.07.2025, 17:40:33	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
30	system	16.07.2025, 17:40:29	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
28	cometlab_inout	16.07.2025, 17:39:55	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
19	microsoft-windows-windows de	16.07.2025, 17:39:54	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
37	лет данных	16.07.2025, 17:39:50	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
17	microsoft-windows-wmi-activity	16.07.2025, 17:39:50	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
18	window powershell	16.07.2025, 17:39:49	dc-edr2.edr2.local	На агенте PT XDR dc-edr2.edr2.local сработало прав...
		16.07.2025, 17:37:00	server01.edr2.local	На агенте PT XDR server01.edr2.local сработало пр...
		16.07.2025, 17:36:26	dc-edr2.edr2.local	Обнаружено подключение по SMB от имени учетн...
		16.07.2025, 17:36:26	dc-edr2.edr2.local	Обнаружено подключение по SMB от имени учетн...
		16.07.2025, 17:36:07	server01.edr2.local	На агенте PT XDR server01.edr2.local сработало пр...

Filter Menu:

- Все события
- Стандартные фильтры
- Методы сбора данных:
 - Оконечные узлы
 - Все события
 - Файловые опера...
 - Сетевая активнос...
 - Процессы
 - Работа с реестр...
 - Сессии пользоов...
 - Журналы событий
 - Аутентификация...

Предотвращение известных угроз
на устройствах компании и сотрудников

MaxPatrol EPP

Модули MaxPatrol EPP



В разработке

Антивирусный движок

Молниеносное обнаружение и блокировка угроз на основе эмуляции поведения ВПО.



В разработке

Защита от шифровальщиков

Проактивная защита от шифровальщиков: мгновенная блокировка и восстановление.



В разработке

Контроль устройств

Ограничение доступа и предотвращение несанкционированного использования подключаемых устройств.



2026

Контроль приложений

Разрешение запуска только доверенных приложений.



2027

Защита от веб-угроз

Автоматическая блокировка доступа к опасным сайтам и предотвращение попыток заражения через интернет.



2027

Защита от сетевых угроз

Защита узла от сетевых атак: блокировка вредоносного трафика и подозрительной активности.

План развития в 2025 году

MaxPatrol EDR

MaxPatrol EDR 7.2 → 8.0 → 8.1

Улучшаем UX, управление агентами, выявление угроз, сбор событий
20 РКБ-проектов
Bug Bounty

Q1

Анонс M&A
Расширение команды
Стратегия развития

Q2

PHDays

22-24 мая

Демонстрация
антивирусной
технологии

Q3

Антивирусный
модуль (prevent)
в MaxPatrol EDR

Выпуск модуля
в коммерческое
пользование

Q4

PSD

Новый продукт
для защиты
устройств
класса EPP

Сертификат
ФСТЭК
по требованиям
САВЗ

MaxPatrol EPP

Дорожная карта EDR & EPP

	Q3 2025 – Следующий релиз	Q3–Q4 2025 – Бэклог со сквозным приоритетом (приоритет может меняться)
Версия	8.1	8.2–9.0
Product & agent management	<ul style="list-style-type: none"> Улучшение UX в части работы с агентами Темная тема интерфейса Браузер файлов и процессов с возможностью реагирования Расширение возможностей интеграции по протоколу Syslog Перенастройка политик безопасности в зависимости от принадлежности к сети 	<ul style="list-style-type: none"> Улучшение UX в части настройки политик и основной функциональности Оптимизация компонентов управляющего сервера: снижение требований к техническим характеристикам серверов, рост эффективности, работа с собственным хранилищем событий Повышение прозрачности состояния агентов (Health Check), расширение функций аналитики Развитие методов интеграции для обеспечения реагирования (в частности в PT NAD) Поддержка новых версий ОС на базе Linux
Detect & Response	<ul style="list-style-type: none"> Улучшение интеграции с PT Sandbox (поддержка нового контракта API) Стабилизация пользовательской экспертизы 	<ul style="list-style-type: none"> Расширение возможностей сбора событий с помощью eBPF-программ и различных файловых журналов Расширение возможностей сбора данных для расследования инцидентов Модернизация поведенческого обнаружения на конечном устройстве Передача файлов на конечное устройство Работа с пользовательскими списками IoC на хосте
EPP Endpoint Protection Platform NEW PT AV	<ul style="list-style-type: none"> Антивирусный модуль с защитой в реальном времени, сканирование по запросу или по расписанию Списки исключений (whitelists) Поддержка Windows, Astra Linux и РЕД ОС Обновленная антивирусная экспертиза от антивирусной лаборатории Positive Technologies 	<ul style="list-style-type: none"> Новый модуль Anti-Ransomware с автоматическим восстановлением поврежденных объектов (Alpha ver) Контроль устройств и приложений (Alpha ver) Развитие технологии превентивного обнаружения на базе антивируса
Цели	<p>Улучшение интеграционных сценариев</p> <p>Улучшение сценариев реагирования</p> <p>Поставка модуля антивирусной защиты в едином агенте</p>	<p>Развитие функций Endpoint Protection Platform</p> <p>Сертификация ФСТЭК по требованиям САВЗ</p> <p>Улучшение опыта управления агентами, улучшенное развертывание и мониторинг</p> <p>Усиление функций сбора событий</p> <p>Качественный рост детектирующих механик за счет новых технологий</p>



Кирилл Черкинский

Руководитель практики
защиты конечных устройств,
Positive Technologies



kcherkinskiy@ptsecurity.com

Спасибо!