



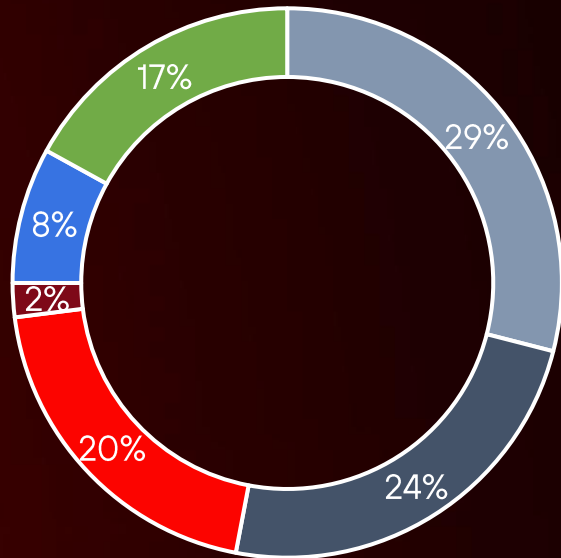
MaxPatrol SIEM



MaxPatrol SIEM

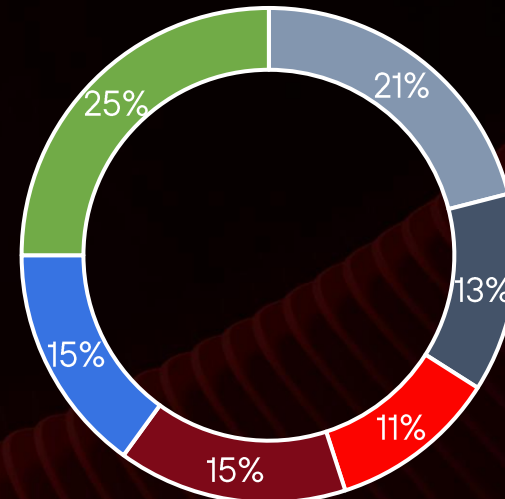
Результаты расследований инцидентов

Длительность атаки



- 5-7 дней
- 8-30 дней
- 1-3 месяца
- 4-6 месяцев
- 7-12 месяцев
- Более года

Время обнаружения с момента компрометации

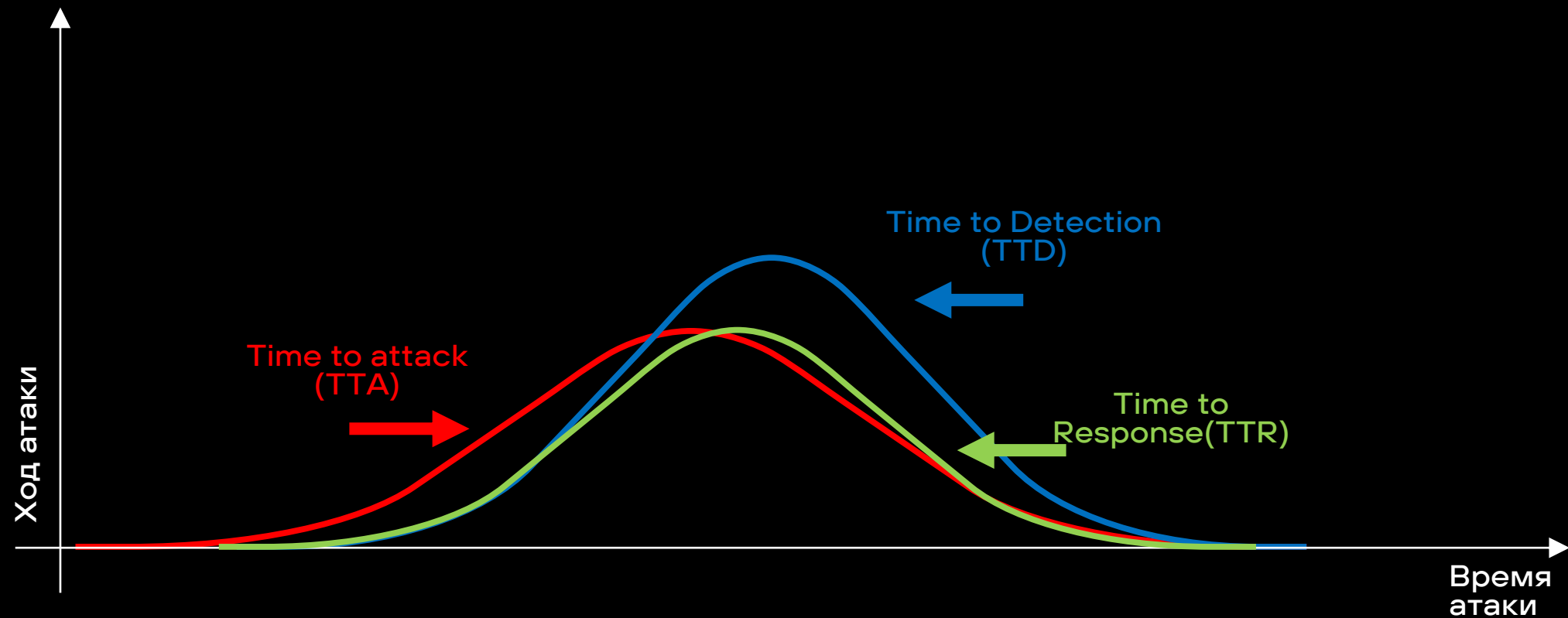


- Менее суток
- От 2 до 7 дней
- От 8 до 14 дней
- От 15 до 30 дней
- От 1 до 2 месяцев
- Более 2 месяцев



Итоги проектов 2023-2024 по расследованию инцидентов и ретроспективному анализу

Как обеспечить защиту инфраструктуры?



Что предлагает MP SIEM



Почему активы в SIEM-системе обязательны?

- Определение контекста при обнаружении и работе с инцидентами
критичность, роли узлов, принадлежность к периметру, пользовательские атрибуты актива
- Удобное управление доступом к событиям на базе групп активов
- Мониторинг источников – контроль полноты и качества сбора событий ИБ

A large, stylized DNA double helix structure is positioned on the right side of the slide. It is rendered in shades of red and white, with the two strands spiraling around each other. The helix is semi-transparent, allowing the background to be seen through it.

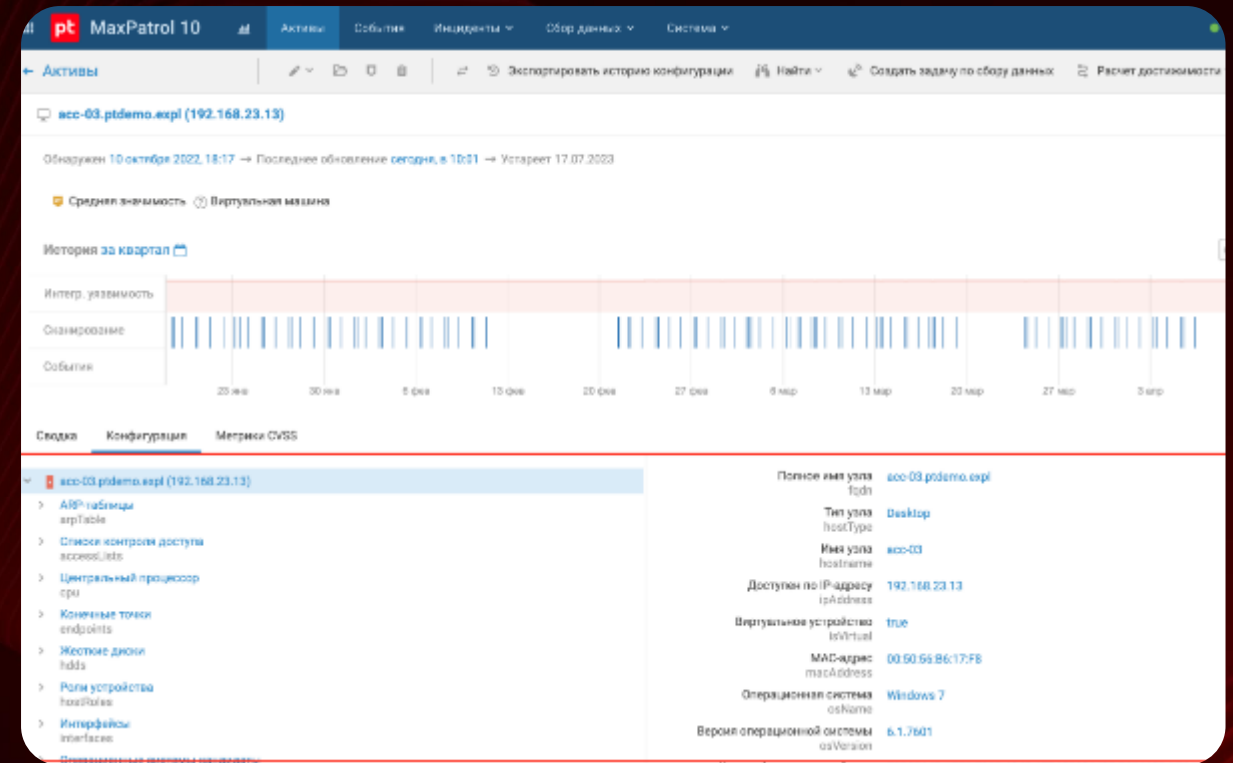
Активы

MaxPatrol
VM

MaxPatrol
SIEM

Учитывает изменения в IT-инфраструктуре

- MaxPatrol SIEM идентифицирует активы не только по FQDN, MAC- и IP-адресам, но и по дополнительным параметрам, таким как тип ОС, имя сетевого узла, признаки виртуальности узла.
- Благодаря этому при изменении IP- или MAC-адреса актива он не дублируется, данные о его состоянии продолжают фиксироваться в изначально созданной карточке.



Экспертиза в MaxPatrol SIEM

Более 70 экспертов PT Expert Security Center работают над написанием контента для MaxPatrol SIEM

350

источников «из коробки»

126

правил обогащений

9732

правил нормализации

292

табличных списка

1769

правил корреляции

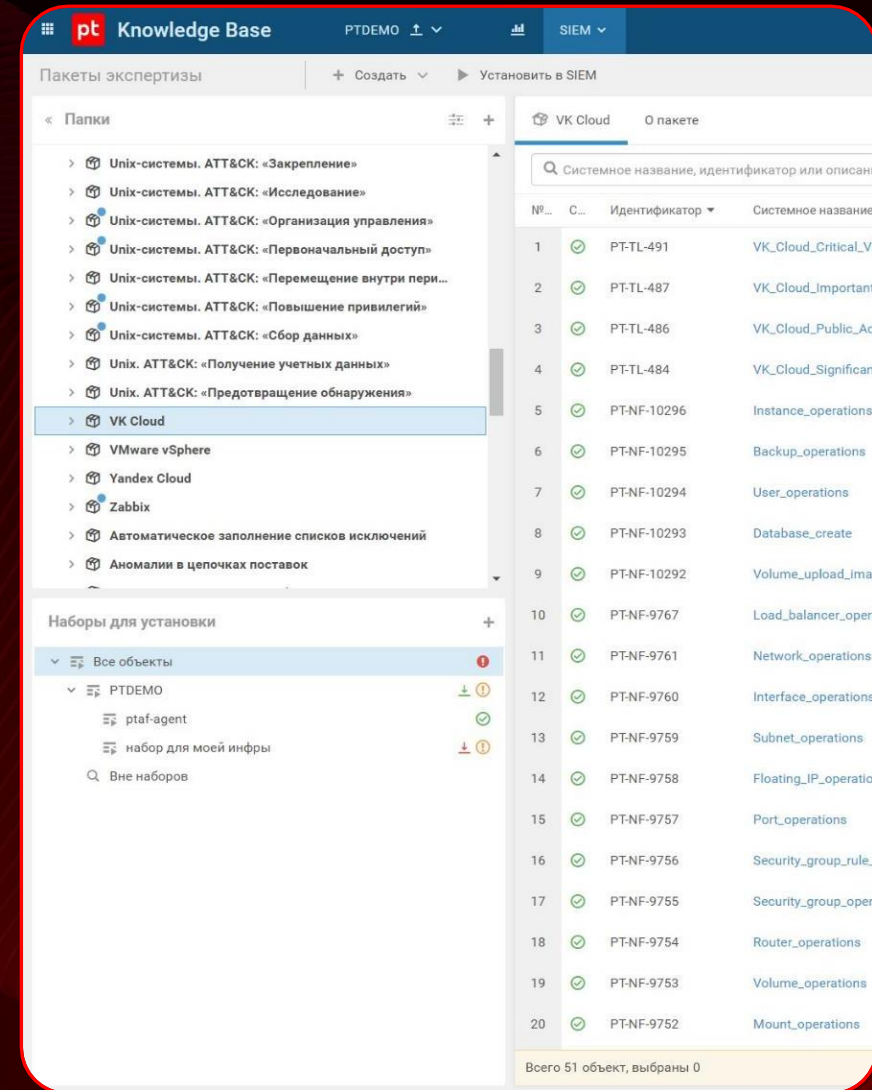
417

техник из матрицы MITRE
ATT&CK покрывает экспертиза
MaxPatrol SIEM «из коробки»

Новые пакеты экспертизы – два раза в месяц

Готовые к работе правила корреляции

Правила корреляции в составе пакетов экспертизы легко настроить под особенности IT-инфраструктуры благодаря подробным инструкциям и табличным спискам исключений, часть из которых предзаполнена экспертами Positive Technologies.



The screenshot displays the 'Knowledge Base' interface for 'PTDEMO'. The main section is titled 'Пакеты экспертизы' (Expert Packages) and shows a list of folders. The 'VK Cloud' folder is selected, and its contents are displayed in a table. The table has columns for '№...' (Number), 'С...' (Status), 'Идентификатор' (Identifier), and 'Системное название' (System Name). The table lists 20 items, all with a green checkmark in the status column. Below the table, there is a section for 'Наборы для установки' (Installation Sets) with a dropdown menu set to 'Все объекты' (All objects). The status bar at the bottom indicates 'Всего 51 объект, выбраны 0' (Total 51 objects, 0 selected).

№...	С...	Идентификатор	Системное название
1	✓	PT-TL-491	VK_Cloud_CriticalV...
2	✓	PT-TL-487	VK_Cloud_Important
3	✓	PT-TL-486	VK_Cloud_Public_Ac...
4	✓	PT-TL-484	VK_Cloud_Significan
5	✓	PT-NF-10296	Instance_operations
6	✓	PT-NF-10295	Backup_operations
7	✓	PT-NF-10294	User_operations
8	✓	PT-NF-10293	Database_create
9	✓	PT-NF-10292	Volume_upload_ima
10	✓	PT-NF-9767	Load_balancer_oper
11	✓	PT-NF-9761	Network_operations
12	✓	PT-NF-9760	Interface_operations
13	✓	PT-NF-9759	Subnet_operations
14	✓	PT-NF-9758	Floating_IP_operatio
15	✓	PT-NF-9757	Port_operations
16	✓	PT-NF-9756	Security_group_rule_
17	✓	PT-NF-9755	Security_group_oper
18	✓	PT-NF-9754	Router_operations
19	✓	PT-NF-9753	Volume_operations
20	✓	PT-NF-9752	Mount_operations

Обновления в документации к пакету экспертизы



- Информация о взаимосвязях контента упрощает работу с правилами корреляции
- Категоризация активностей.
- Добавление единого гайда по настройке ОС Windows.
- Рекомендация в методологии какие пакеты экспертизы подключать в зависимости от инфраструктуры.

Active Directory 0 пакете

Зависимости

В набор для установки нужно добавлять как сами правила корреляции, так и объекты базы данных PT KB, которые необходимы для работы этих правил. Перечень таких объектов для каждого правила указан ниже.

Примечание. Вы можете выбрать из пакета экспертизы те правила корреляции, которые хотите использовать, и добавить в набор для установки только их и те объекты базы данных PT KB, которые необходимы для работы этих правил.

Abuse_Kerberos_RC4

Правила нормализации:

- PT-NF-1904: PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested;
- PT-NF-1905: PT_Microsoft_Windows_eventlog_4769_Kerberos_service_ticket_requested;
- PT-NF-1907: PT_Microsoft_Windows_eventlog_4771_Kerberos_pre_authentication_failed;
- PT-NF-2611: PT_Microsoft_Windows_wmi_4771_Kerberos_pre_authentication_failed.

Active_Directory_Snapshot

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

ActiveDirectory_Data_Collection

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Пример экспертизы – Mimikatz

В пакет экспертизы входят:

- Правило корреляции
- Табличный список
- Правило нормализации
- Правило обогащение

```
correlation_rules 0 пакета



Правило корреляции Mimikatz_Command

1 event Mimikatz_in_Commandline:
2   key:
3     event_src.host
4   filter {
5     filter::NotFromCorrelator()
6     and filter::ProcessStart_Windows_any()
7     and (
8       regex(lower(object.process.cmdline), "\\b(privilege|crypto|sekurlsa|kerberos|lsadump|vault|token|misc|busylight|dpapi)::", 0) != null
9       or regex(lower(object.process.cmdline), "\\b(its::apphost\\b", 0) != null
10      or regex(lower(object.process.cmdline), "\\b(its::(multirdp|sessions|remote|logonpasswords)\\b", 0) != null
11      or regex(lower(object.process.cmdline), "\\b(its::(alias|group|serverinfo|session|share|stats|tod|user|wsession)\\b", 0) != null
12      or regex(lower(object.process.cmdline), "\\b(its::(exports|imports|list|resume|run|start|stop|suspend)\\b", 0) != null
13      or regex(lower(object.process.cmdline), "\\b(its::(close|connect|enum|server)\\b", 0) != null
14      or regex(lower(object.process.cmdline), "\\b(its::(add|clear|lookup|modify|patch|query)\\b", 0) != null
15      or regex(lower(object.process.cmdline), "\\b(its::(dump-(credentials|hashes))\\b", 0) != null
16      or regex(lower(object.process.cmdline), "\\b(its::(wmimikatz|\\b(its::(lsa|kerberos|smbapi|users|token|process|dpapi|smb|ldap|crypto|registry))\\b", 0) != null
17    )
18    and filter::CheckWL_Process_Creation("Mimikatz_Command", lower(object.process.cmdline))
19  }
20
```





tabular_lists 0 пакета

Windows_Hacktools (справочник)

Известные утилиты для взлома ОС Windows

Идентификатор PT-TL-200
Поставщик Positive Technologies
Папка Атаки с помощью специализированного ПО/tabular_lists
Наборы для установки не задано
Статус валидации 
Статус установки 

+ Добавить запись ✎ Редактировать 🗑 Удалить 🔄 Активировать ⏸ Деактивировать 📄 Импорт 📄 Экспорт

binary_name	binary_description	commandline	hash	event_type	event_importance	event_description	Источник
gs-netcat.exe			1756b5d536035347fb...	event	medium	Утилита для создания...	
rvb3v\$V1.0.exe			79ac42b885de9e7bf59...	incident	high	Утилита для взаимоде...	
sharpefspotato.exe	\\bsharpefspotato\b		239a78582fe7a8648ca...	incident	high	Утилита SharpEfsPotat...	
sweetpotato.exe	\\bsharppotato\b		fdbaf19ed6f0a2d7a5da...	incident	high	Утилита SweetPotato д...	

Пример экспертизы – Mimikatz

В пакет экспертизы входят:

- Рекомендации по созданию задачи на сбор
- Как правильно установить пакет
- Как настроить источники/MP SIEM
- Помощь в расследовании

Настройка источников

Настройку источников на активе нужно выполнять от имени учетной записи, добавленной в группу Administrators на контроллере домена, в котором расположен актив.

Внимание! При использовании в IT-инфраструктуре организации межсетевое экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом MP 10 Collector. Используются системный TCP-порт 135 и динамические TCP-порты 49152–65535.

Внимание! При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений «Удаленное управление журналом событий (именованные каналы – входящий)» (Remote Event Log Management (NP-In)), «Удаленное управление журналом событий (RPC)» (Remote Event Log Management (RPC)), «Удаленное управление журналом событий (RPC-ERMAP)» (Remote Event Log Management (RPC-ERMAP)).

Источниками событий для правил корреляции пакета экспертизы на активе служат операционная система Windows и служба Microsoft Sysmon. События обоих источников сохраняются в журнале событий Windows.

На активе необходимо установить службу Microsoft Sysmon или, если служба установлена, изменить параметры конфигурации службы.

Для настройки Windows на контроллере домена актива нужно:

1. Настроить аудит Windows PowerShell с помощью групповой политики.

Регистрация событий аудита Windows PowerShell доступна в Windows 7, Windows Server 2008 R2 и в более поздних версиях.

Внимание! Для работы правил корреляции пакета экспертизы на источнике должна быть установлена оболочка командной строки Windows PowerShell версии

Расследование инцидента

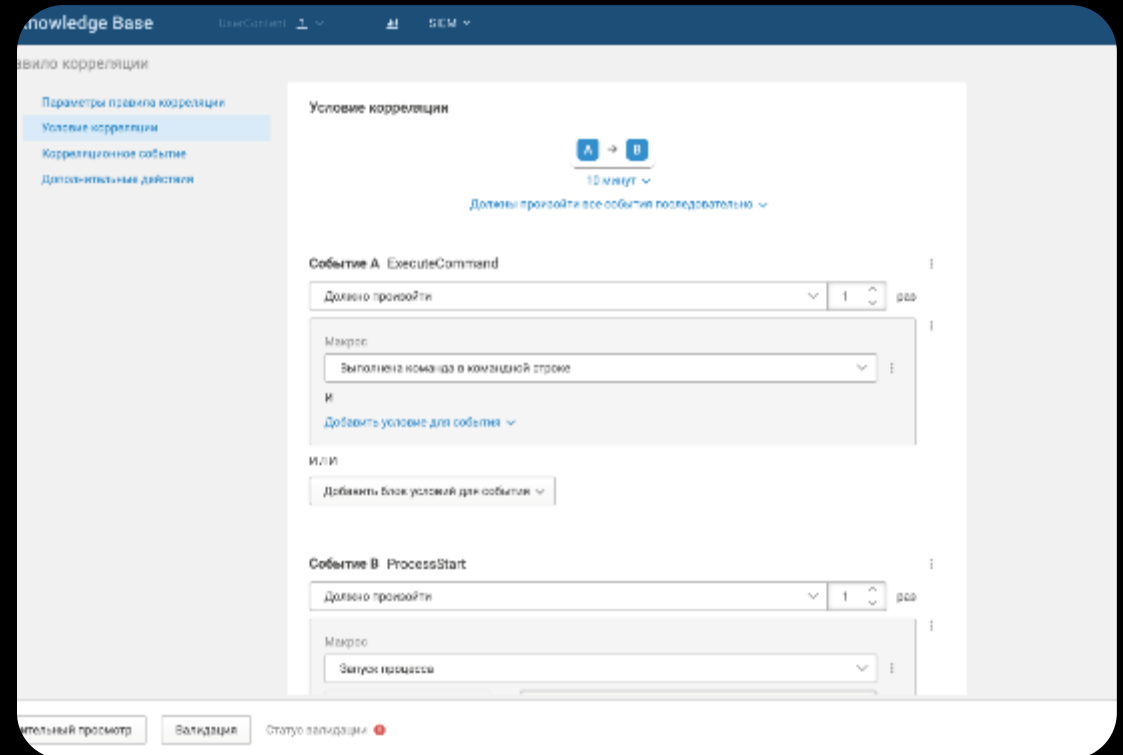
В расследовании инцидента помогает анализ связанного с ним события ИБ. По значениям полей события вы можете определить:

- `dst.ip`, `dst.fqdn` или `dst.host` – IP-адрес и полное доменное имя (FQDN) узла внутри контролируемого периметра, на который направлена атака, или узла во внешней сети, используемый злоумышленником для обмена данными (`dst.port` – порт подключения);
- `src.ip`, `src.fqdn` или `src.host` – IP-адрес и полное доменное имя (FQDN) узла, с которым связана подозрительная активность;
- `subject.account.id`, `subject.account.name`, `subject.account.domain` – идентификатор, логин и домен учетной записи, с которой связана подозрительная активность.

Помогает создавать правила корреляции

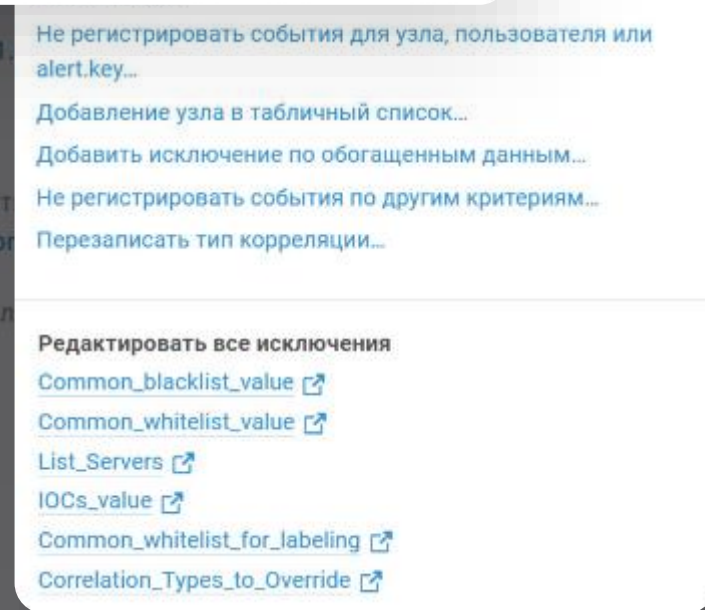
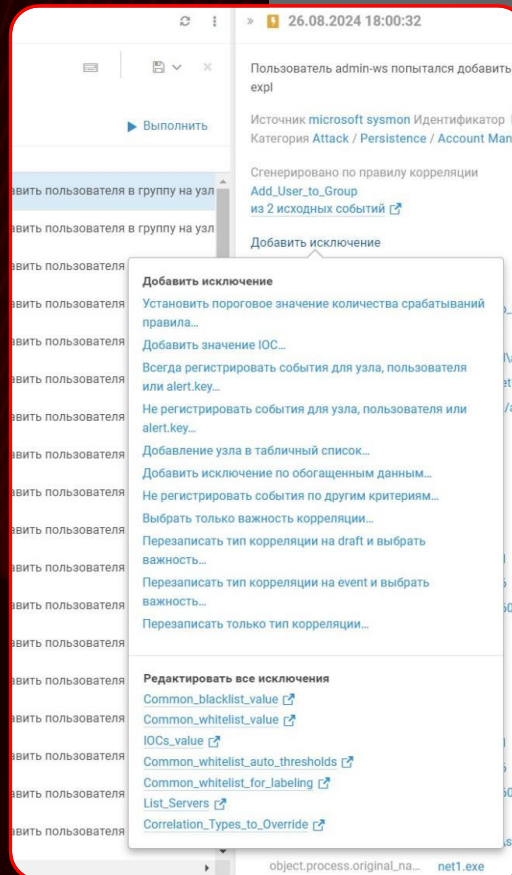
Чтобы создать собственные правила корреляции:

1. Выберите события, условия и подходящий макрос.
2. Настройте последовательность событий.
3. Задайте условия срабатывания.
4. Установите новые правила в MaxPatrol SIEM.



Вайтлистинг

- Пользователи MaxPatrol SIEM могут добавлять исключения для правил обнаружения угроз, чтобы предотвратить повторные ложные срабатывания.
- Достаточно отметить параметры событий, на которые правило не должно реагировать, например адрес сетевого узла или имя конкретного пользователя.
- Для создания исключений выполняется обогащение карточки события и используются данные обогащения

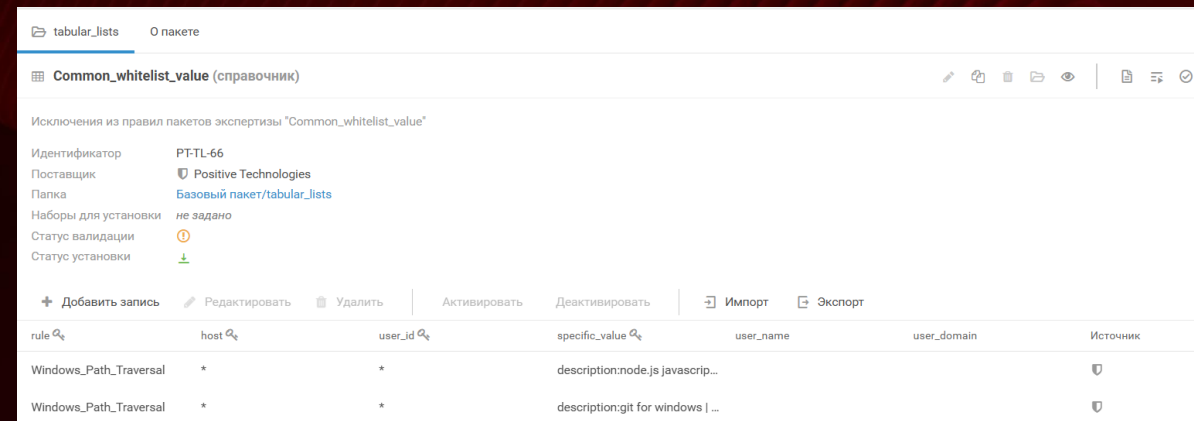
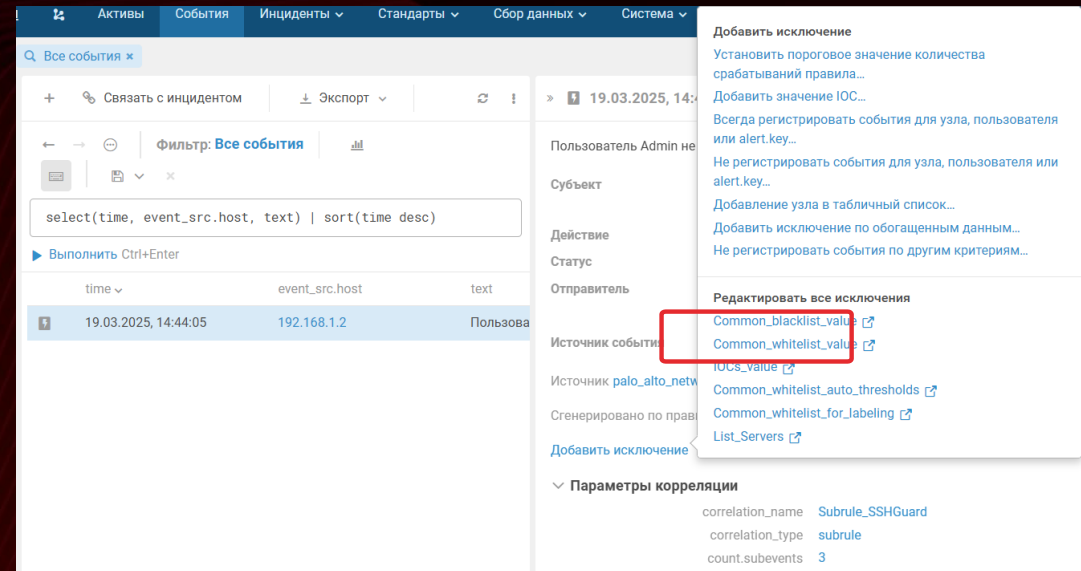


Механизмы вайтлистинга

Автоматическое заполнение белых (черных) списков исключений

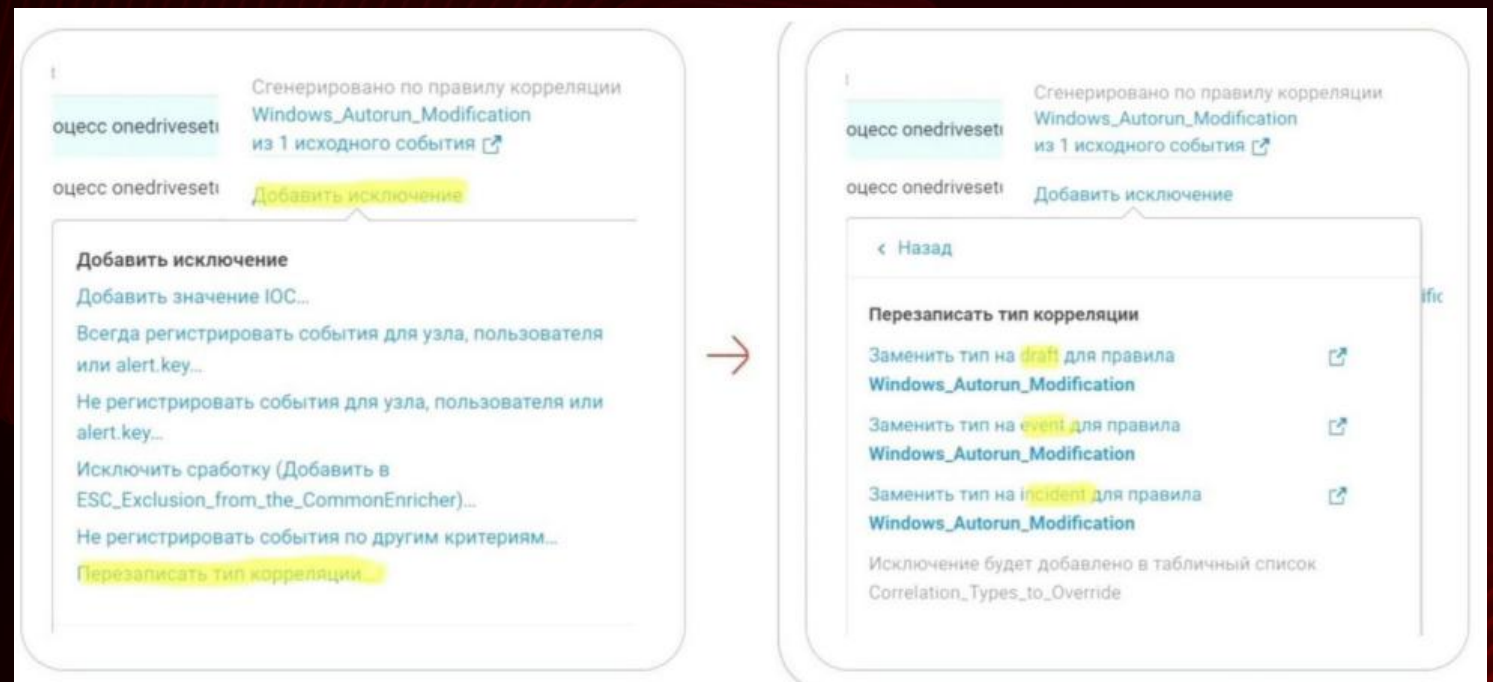
Примеры таких активностей:

- Фоновая активность операционной системы
- Работа скриптов администрирования ИТ-инфраструктуры
- Регулярный запуск процессов (по расписанию)



Механизмы вайтлистинга

Изменение типа
корреляции



Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

оцесс onedriveset

оцесс onedriveset **Добавить исключение**

Добавить исключение

- Добавить значение IOC...
- Всегда регистрировать события для узла, пользователя или alert.key...
- Не регистрировать события для узла, пользователя или alert.key...
- Исключить сработку (Добавить в ESC_Exclusion_from_the_CommonEnricher)...
- Не регистрировать события по другим критериям...
- Перезаписать тип корреляции...**

→

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

оцесс onedriveset

оцесс onedriveset **Добавить исключение**

< Назад

Перезаписать тип корреляции

- Заменить тип на **draft** для правила Windows_Autorun_Modification
- Заменить тип на **event** для правила Windows_Autorun_Modification
- Заменить тип на **incident** для правила Windows_Autorun_Modification

Исключение будет добавлено в табличный список Correlation_Types_to_Override



Функционал расследования и реагирования

Карточка события

- Фокус на данных, обязательных для понимания контекста происходящего
- Возможность изменить карточки событий выбранных типов, чтобы сделать работу отдельных пользователей удобнее
- Контекстные экшны

> 19.10.2023 13:43:44

Пользователь admin-acc01 запустил подозрительный процесс p.exe, метаданные или хеш которого совпадает с системным процессом psexec.exe, на узле acc-01.ptdemo.expl

17 Оценка риска

Субъект  admin-acc01 acc-01  13
subject account

Действие  start

Объект  p.exe  20
object process
fullpath c:\tmp\p.exe
hash F8DBABDFA03068130C277CE49C60E35C029FF29D...
 admin-acc01 acc-01  14977
 cmd.exe  21
fullpath c:\windows\system32\cmd.exe


Статус  success

Отправитель  mp10-agt3 (192.168.55.21)  1435

Источник события  mp10-agt3 (192.168.55.21)  1435

 Реагировать












Источник microsoft sysmon Идентификатор
Microsoft-Windows-Sysmon/Operational
Категория Attack / Defense Evasion / Rename System Utilities

Сгенерировано по правилу корреляции
Copied_or_Renamed_Executable
из 1 исходного события 

Работа с деревом гипотез

Алерты с узлами, файлами, процессами и учетными данными сгруппированы для быстрого анализа

Алерты с процессом cmd.exe

-  [20.10.2023 16:00:44](#)
Обнаружена попытка получить информацию о версиях системы, приложений и включенных компонентах на узле acc-01.ptdemo.expl
-  [20.10.2023 16:00:44](#)
Обнаружена попытка получить информацию о версиях системы, приложений и включенных компонентах на узле acc-01.ptdemo.expl
-  [20.10.2023 16:00:15](#)
Пользователь system выполнил скрипт на узле acc-01.ptdemo.expl
-  [20.10.2023 15:29:56](#)
Обнаружена попытка получить информацию о состоянии средств защиты и мониторинга на узле acc-01.ptdemo.expl
-  [20.10.2023 15:29:56](#)
Обнаружена попытка получить информацию о состоянии средств защиты и мониторинга на узле acc-01.ptdemo.expl
-  [20.10.2023 15:29:55](#)
Обнаружена попытка получить информацию о состоянии средств защиты и мониторинга на узле acc-01.ptdemo.expl
-  [20.10.2023 15:29:55](#)
Обнаружена попытка получить информацию о состоянии средств защиты и мониторинга на узле acc-01.ptdemo.expl
-  [20.10.2023 15:22:29](#)
Обнаружена попытка получить список учетных записей на узле acc-01.ptdemo.expl
-  [20.10.2023 15:22:29](#)
Обнаружена попытка получить список учетных записей на узле acc-01.ptdemo.expl
-  [20.10.2023 10:17:35](#)
Обнаружена попытка выполнить потенциально опасную команду на узле acc-01.ptdemo.expl
-  [20.10.2023 08:13:34](#)
Обнаружена попытка выполнить потенциально опасную команду на узле acc-01.ptdemo.expl

Реагирование на инцидент

- Реагирование на инциденты на уровне узла*
- Процессы, файлы и узлы — под контролем

* С использованием агента MaxPatrol EDR и встроенной интеграции

» 19.10.2023 13:43:44

Пользователь admin-acc01 запустил подозрительный процесс p.exe, метаинформация или хеш которого совпадает с системным процессом psexec.exe, на узле acc-01.ptdemo.expl

subject account

Действие ▶ start

Объект 📄 p.exe 🚩 25

object.process.name

p.exe

Реагировать

Удалить исполняемый файл процесса-объекта

Завершить все процессы, используя путь к исполняемому файлу процесса-объекта

Завершить процесс, используя путь к исполняемому файлу и идентификатор процесса-объекта

Завершить все процессы, используя имя процесса-объекта

Завершить процесс, используя имя и идентификатор процесса-объекта

Завершить деревья процессов, используя путь к исполняемому файлу-объекту

Завершить дерево процессов, используя путь к исполняемому файлу и идентификатор родительского процесса-объекта

Завершить деревья процессов, используя имя процесса-объекта

Завершить дерево процессов, используя имя и

> Параметры корреляции

> Адресаты

MaxPatrol EDR + MaxPatrol SIEM

Экосистема
Positive
Technologies

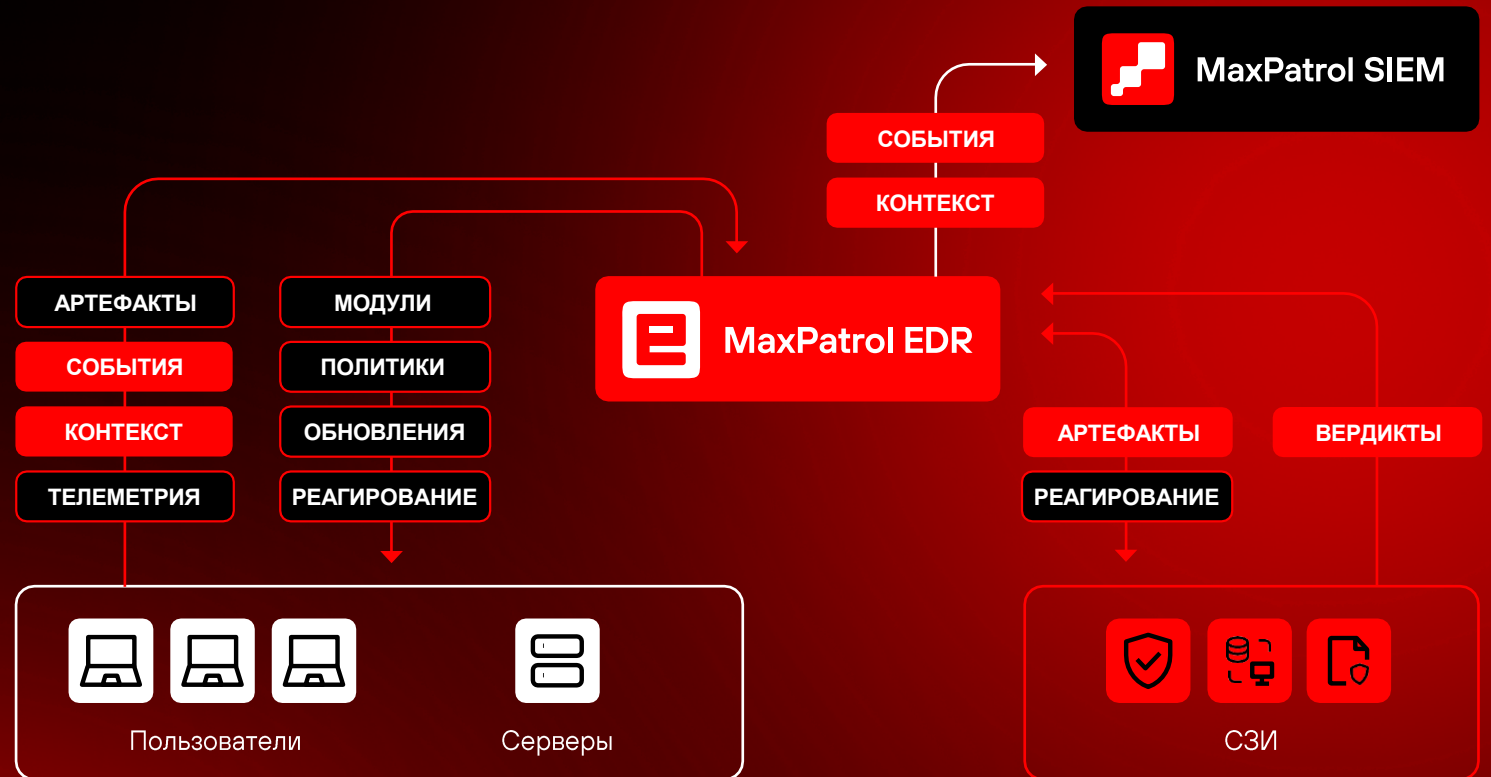
1 Дает дополнительный контекст — вне узла (для точного обнаружения)

2 Реагирование на угрозы в едином интерфейсе

3 Оптимизация архитектуры MaxPatrol SIEM

(события собираются централизованно через серверы агентов)

- Сбор событий с устройств, не подключенных к корпоративной сети
- Возможность фильтровать события при чтении из журналов
- Управление в единой консоли



Мониторинг источников 2.0



MaxPatrol SIEM не даст злоумышленнику использовать слепые зоны в мониторинге для обхода защиты



Рекомендации PT ESC

Какие источники необходимо мониторить и какие требования к контролю необходимы



- Контроль активности источника
- Контроль потока событий (допустимый диапазон, отклонение от среднего)
- Контроль задержки
- Контроль необходимых идентификаторов в потоке событий
- Настройка автогенерации событий, связанных с нарушением проверок
- Настройка уведомлений при нарушении политики мониторинга источников

Мониторинг источников 2.0



Политики

+ Создать правило Редактировать Копировать

« Список политик

- Активы
 - Значимость активов
 - Сроки актуальности (аудит)
 - Сроки актуальности (пентест)
- Мониторинг источников
 - Активность активов**
 - Поток событий с источников
 - Форвардеры
- Стандарты
 - Соответствие стандартам
 - Статусы несоответствий
- Уязвимости
 - Статусы уязвимостей
 - Отметка важная

Активность активов

Порядок	Состояние	Название
1	▶	Рабочие станции Windows
2	▶	Сетевые устройства
3	▶	Контроллеры домена
4	▶	Серверы Windows
5	▶	Активность Sandbox

Активы

Группы активов: Root x

Фильтр активов: `Host.HostType = 'Desktop' and WindowsHost and Host.@IpAddresses.Item in 192.168.22.0/24`

3 актива соответствуют запросу

Контроль активности активов

Частота проверки: 4 минуты

Часовой пояс: UTC+3

Период контроля: Круглосуточно Заданные периоды

08:00 - 19:00

Добавить

Контроль задержки

Время между появлением события на источнике и получением его конвейером обработки событий

Допустимая задержка: 5 минут

Мониторинг источников 2.0



The screenshot displays the MaxPatrol 10 interface for monitoring sources. The main view shows details for the host **dc01.ptdemo.expl (192.168.31.1)**. The status is **Активность** (Active) and **Задержка** (Delay). The delay is 3 minutes and 19 seconds, which is within the 6-minute norm. The last check was at 14:38 today. The rule applied is **Контроллеры домена** (Domain Controllers).

Below this, a table lists various monitoring rules for different sources:

Источник	Правило	Период контроля	Частота проверки	Допустимый поток	Поток
microsoft Microsoft-Windows	Серверы Windows	00:00-00:00	00:00-14:34	200-4000 событий за период	0 событий за период (ниже допустимого)
microsoft AD FS	Контроллеры домена поток сс	00:00-00:00	14:34-14:35	Более 1 EPS	0 EPS (ниже допустимого)
microsoft System	Серверы Windows	00:00-00:00	14:34-14:35	-15..+10 %	0 событий за период
microsoft AD FS 2.0	Контроллеры домена поток сс	00:00-00:00	14:34-14:35	Более 1 EPS	0 EPS (ниже допустимого)
microsoft Security	Серверы Windows	00:00-00:00	14:34-14:35	1-10 EPS	0 EPS (ниже допустимого)
microsoft Active Directory W	Контроллеры домена поток сс	00:00-00:00	14:34-14:35	Более 1 EPS	0 EPS (ниже допустимого)
microsoft event_id 4672,467	-	-	-	-	0,017 EPS(14:33-14:34)
microsoft event_id 5140	-	-	-	-	0,1 EPS(14:31-14:32)
microsoft event_id 4688	-	-	-	-	0,033 EPS(13:44-13:45)

On the left, the 'Фильтры' (Filters) section shows: 'Все активы' (All active) with 1 item, 'Без правил' (No rules) with 1 item, and 'С правилами' (With rules) with 3 items for active violations, 5 for flow violations, and 3 for delay violations.



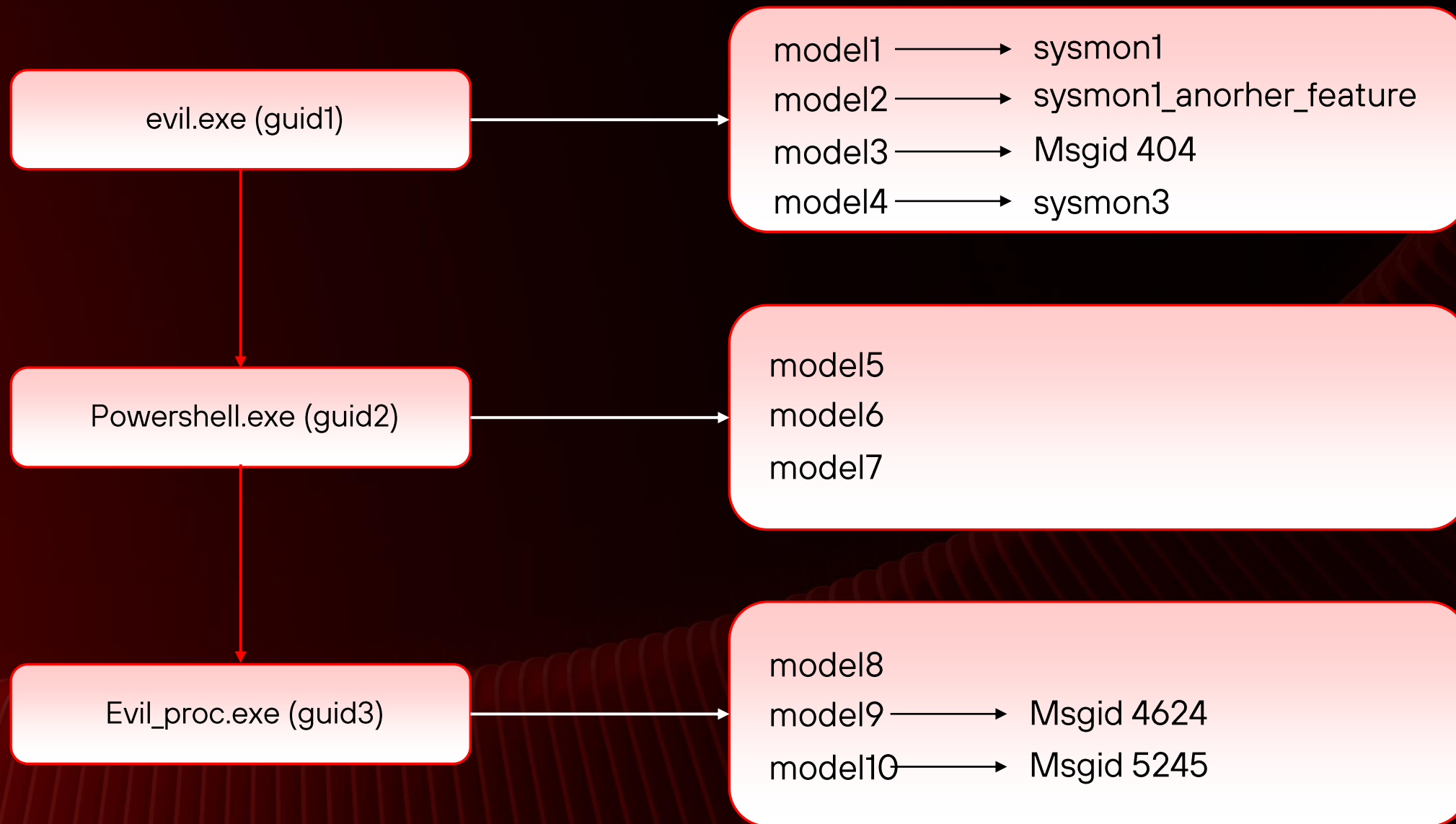
ML-модуль Behavioral Anomaly Detection (BAD) в MP SIEM

Область обнаружения угроз



Увеличиваем область обнаружения угроз

Пример работы



ВAD сегодня

72

ML- модели

Выявление аномалий
на базе событий из **14** типов систем

Windows + Sysmon

KSC

SQL Server

TeamCity

1C Enterprise

Keycloak

Password

AuditD

vSphere (ESXi)

Check Point Gaia

Cisco (IOS, ASA, FWSM, PIX)

FortiGate

OpenVPN

Artifactory

ML-модуль BAD

Behavioral Anomaly Detection (BAD) –
высококвалифицированный помощник:



Приоритизирует работу оператора — **акцентирует внимание** на событиях MaxPatrol SIEM с **наиболее высоким уровнем риска**, опираясь на вердикт ML-моделей

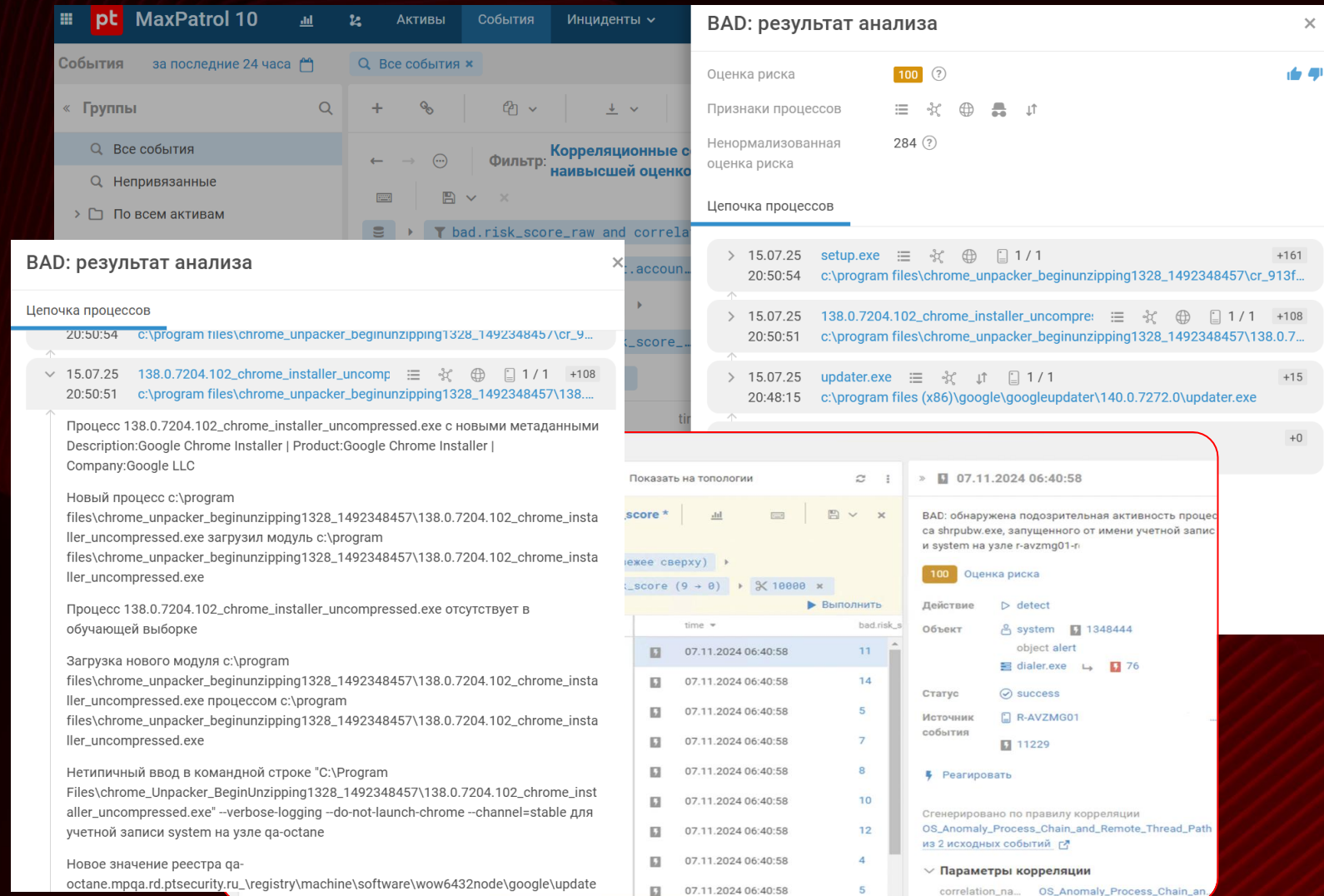


Расширяет возможности MaxPatrol SIEM — работает как **второй эшелон** защиты, **самостоятельно обнаруживает** скрытые и **целенаправленные атаки**



Приоритизация работы оператора

Подсвечивает приоритетные для обработки корреляционные события и дает дополнительный **контекст**

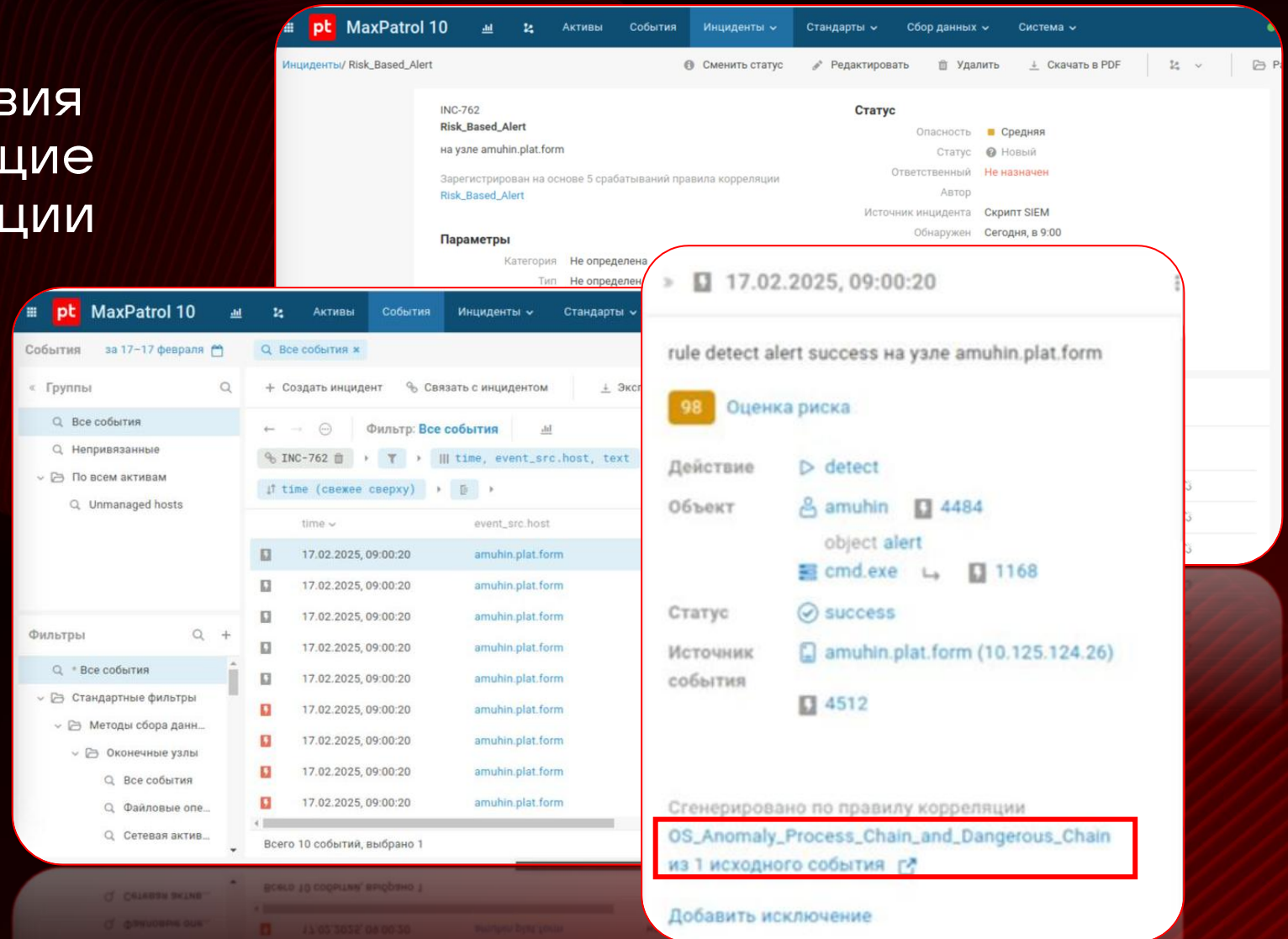


The screenshot displays the MaxPatrol 10 interface with several panels:

- Top Panel:** MaxPatrol 10 header with navigation tabs: Активы, События, Инциденты.
- Event List:** Filtered by "Корреляционные с наивысшей оценкой".
- BAD: результат анализа (Left Panel):**
 - Цепочка процессов: 15.07.25 138.0.7204.102_chrome_installer_uncomp (Risk: +108).
 - Процесс 138.0.7204.102_chrome_installer_uncompressed.exe с новыми метаданными: Description: Google Chrome Installer | Product: Google Chrome Installer | Company: Google LLC.
 - Новый процесс c:\program files\chrome_unpacker_beginunzipping1328_1492348457\138.0.7204.102_chrome_installer_uncompressed.exe загрузил модуль c:\program files\chrome_unpacker_beginunzipping1328_1492348457\138.0.7204.102_chrome_installer_uncompressed.exe.
 - Процесс 138.0.7204.102_chrome_installer_uncompressed.exe отсутствует в обучающей выборке.
 - Загрузка нового модуля c:\program files\chrome_unpacker_beginunzipping1328_1492348457\138.0.7204.102_chrome_installer_uncompressed.exe процессом c:\program files\chrome_unpacker_beginunzipping1328_1492348457\138.0.7204.102_chrome_installer_uncompressed.exe.
 - Нетипичный ввод в командной строке "C:\Program Files\chrome_Unpacker_BeginUnzipping1328_1492348457\138.0.7204.102_chrome_installer_uncompressed.exe" --verbose-logging --do-not-launch-chrome --channel=stable для учетной записи system на узле qa-octane.
 - Новое значение реестра qa-octane.mpqa.rd.ptsecurity.ru\registry\machine\software\wow6432node\google\update.
- BAD: результат анализа (Right Panel):**
 - Оценка риска: 100.
 - Признаки процессов: 284.
 - Цепочка процессов: 15.07.25 setup.exe (Risk: +161), 15.07.25 138.0.7204.102_chrome_installer_uncomp (Risk: +108), 15.07.25 updater.exe (Risk: +15).
- Bottom Panel:** "Показать на топологии" section with a table of correlation events and a detailed view of a specific event (07.11.2024 06:40:58) with a risk score of 11.

Второй эшелон защиты

Обнаруживает действия хакера, не подпадающие под правила корреляции



The image displays three overlapping screenshots of the MaxPatrol 10 SIEM interface. The top screenshot shows an incident detail view for 'INC-762 Risk_Based_Alert' on host 'amuhin.plat.form', with a status of 'Средняя' (Medium) and 'Новый' (New). The middle screenshot shows a list of events for the date '17-17 февраля', with a filter for 'Все события' (All events) and a table of events. The bottom screenshot shows a detailed view of an event with a risk score of 98, action 'detect', and object 'amuhin.plat.form'. A red box highlights the correlation rule used: 'OS_Anomaly_Process_Chain_and_Dangerous_Chain'.

MaxPatrol 10 | Инциденты / Risk_Based_Alert

INC-762
Risk_Based_Alert
на узле amuhin.plat.form

Статус: Опасность **Средняя**, Статус **Новый**, Ответственный **Не назначен**, Автор, Источник инцидента **Скрипт SIEM**, Обнаружен **Сегодня, в 9:00**

Параметры: Категория **Не определена**, Тип **Не определен**

17.02.2025, 09:00:20

rule detect alert success на узле amuhin.plat.form

98 Оценка риска

Действие: **detect**

Объект: **amuhin** **4484**, **object alert**, **cmd.exe** **1168**

Статус: **success**

Источник события: **amuhin.plat.form (10.125.124.26)** **4512**

Сгенерировано по правилу корреляции
OS_Anomaly_Process_Chain_and_Dangerous_Chain
из 1 исходного события

Добавить исключение

Преимущества



Фокус на критичных инцидентах

Снижает шум и позволяет сосредоточиться на действительно опасных событиях. Корреляция отсекает очевидное, BAD классифицирует сложное.

Видит то, что не ловит корреляция

Обнаруживает аномалии, которые невозможно поймать с помощью стандартных правил и сигнатур. Выявляет нетипичное поведение в инфраструктуре, расширяя зону контроля за счёт поведенческого анализа.

Работает без ручной настройки

Не требует обновлений правил или постоянной ручной донастройки. автономные процессы обнаружения снижают необходимость ручного контроля. Первые релевантные результаты — через 1–2 недели (оптимально – 1 месяц)

Подстраивается под инфраструктуру

Система адаптирует логику детекта и переобучается на данных, снижая количество ложных срабатываний.



Алия Рахматуллина

Лидер продуктовой практики
MP SIEM, MP BAD, MP IM
Positive Technologies



arakhmatullina@ptsecurity.com

Спасибо!