



MaxPatrol SIEM



MaxPatrol SIEM

Как выбрать SIEM

Выбор есть всегда

Важно не ошибиться в критериях:

«Бесплатный» долгострой
имени главного
специалиста по ИБ



Для формального
выполнения требований
регуляторов



Устанавливается
на «оптимальные»
с точки зрения заказчика
аппаратные ресурсы



«Недорогой»



Совсем «зеленый» SIEM:
много обещает, мало может



**Работает
на результат**



Критерии выбора SIEM-системы

Полнота аудита
инфраструктуры
и контроля сбора
событий



Качество
обнаружения,
в том числе
целенаправленных
атак



Полнота
интеграций
со смежными
продуктами
и «встройка» в процесс
обеспечения ИБ



Стабильность работы
при любой нагрузке



Стоимость
владения



Удобство
использования



Знание продукта
на рынке,
большое количество
специалистов, имеющих
экспертизу работы
данной системой



Гибкость
и масштабируемость
решения



Критерии выбора SIEM-системы



Знаем,
где искать



Полнота аудита инфраструктуры и контроля сбора событий

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



Активы

MaxPatrol
VM

MaxPatrol
SIEM

Мониторинг источников



Политики

« 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

+ Создать правило

✎ Редактировать

📄 Копировать

Активность активов

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

Активы

Группы активовRoot x

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

3 актива соответствуют запросу

Контроль активности активов

Частота проверки4 минуты

Часовой поясUTC+3

Период контроляКруглосуточно Заданные периоды

08:00 - 19:00

Добавить

Контроль задержки

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

Допустимая задержка5 минут

Мониторинг источников



MaxPatrol 10

Активы События Инциденты Стандарты Сбор данных EDR Система

Мониторинг источников Показывать: активы за последние 30 дней

Источники

Неидентифицированные 2

Все активы

- ActiveDirectory
- audit
- Docker
- PT Demo
 - AD Groups
 - High&Medium with Tr...
 - (file) FileServer(SMP)

Фильтры

Все активы

Без правил 1

С правилами

- С нарушениями активн... 3
- С нарушениями потока 5
- С нарушениями задержк... 3

Активы: 13 x Источники Форвардеры

192.70.197.182 Активность Задержка Источники: Check Point Gaia Cisco ASA Cisco IOS Cisco IOS XE

dc01.ptdemo.expl (192.168.31.1) Активность Задержка Источники: microsoft Microsoft-Windows-Sysmon/Operational microsoft AD FS microsoft

Узел активен
Период контроля: 14:30–14:35, частота проверки — 5 минут
Последнее событие: Сегодня, 14:34
Правило: Контроллеры домена

Задержка в норме
Задержка 3 минуты, 19 секунд, норма — до 6 минут
Последняя проверка: Сегодня, 14:38
Правило: Контроллеры домена

Источник	Правило	Период контроля	Частота проверки	Допустимый поток	Поток
microsoft Microsoft-Windows-Sysmon/Operational	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)

https://mp10-core.ptdemo.local/#/management/policies/list?policyId=sourceMonitoring&ru...

Знаем,
что искать



Качество
обнаружения

Экспертиза в MaxPatrol SIEM

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

335

источников «из коробки»

99

правил обогащений

9127

правил нормализации

203

табличных списка

1306

правил корреляции

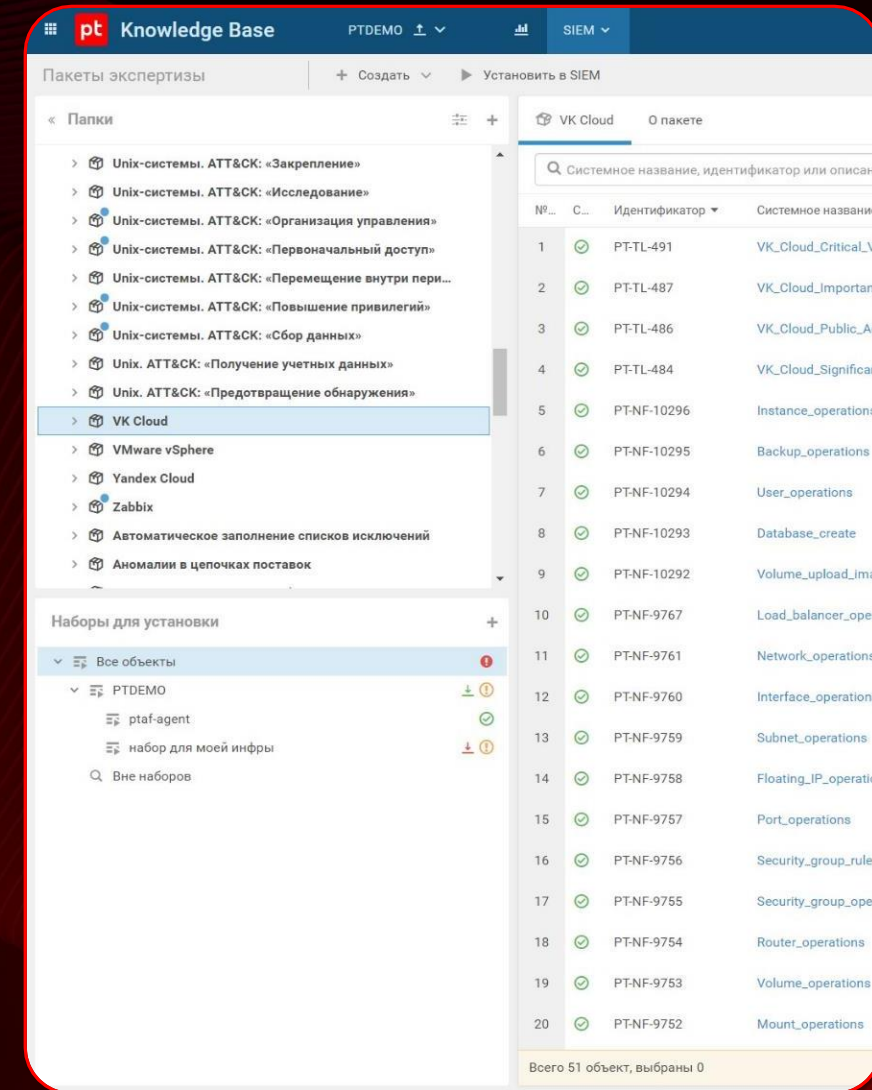
287

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

Новые пакеты экспертизы – раз 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.



Как понять, что событие ИБ-инцидент

Не требует глубоких знаний
специалистов и помогает
на каждом этапе
обнаружения кибератак

Пакеты экспертизы содержат не только описание
правил корреляции, но и рекомендации
по расследованию инцидентов

1С:Предприятие 8.3 и Битрикс24 О пакете

Расследование инцидента

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

- `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.

Примечание. Вы можете получить дополнительную информацию о действиях злоумышленника из анализа событий, связанных с его учетной записью и узлом, на котором была обнаружена подозрительная активность.

Реагирование на инцидент

Если обнаруженная активность не является для учетной записи ожидаемой и легитимной, рекомендуется принять меры к блокировке учетной записи и (или) изоляции узла, с которого производилась атака.

При выявлении ложного срабатывания необходимо настроить механизм обработки ложных срабатываний. Для этого данные связанного с инцидентом события ИБ необходимо внести в табличный список для исключений.

Вы можете использовать белые списки `Common_whitelist_value`, `Common_whitelist_regex` и черные списки `Common_blacklist_value`, `Common_blacklist_regex`. Табличные списки с постфиксом `value` вы можете заполнять по ссылке из сводки о событии ИБ в интерфейсе MaxPatrol SIEM или вручную, табличные списки с постфиксом `regex` — только вручную. Исключения, указанные в черных списках, обладают более высоким приоритетом по сравнению с исключениями в белых списках.

При ручном заполнении табличных списков в колонках нужно указать:

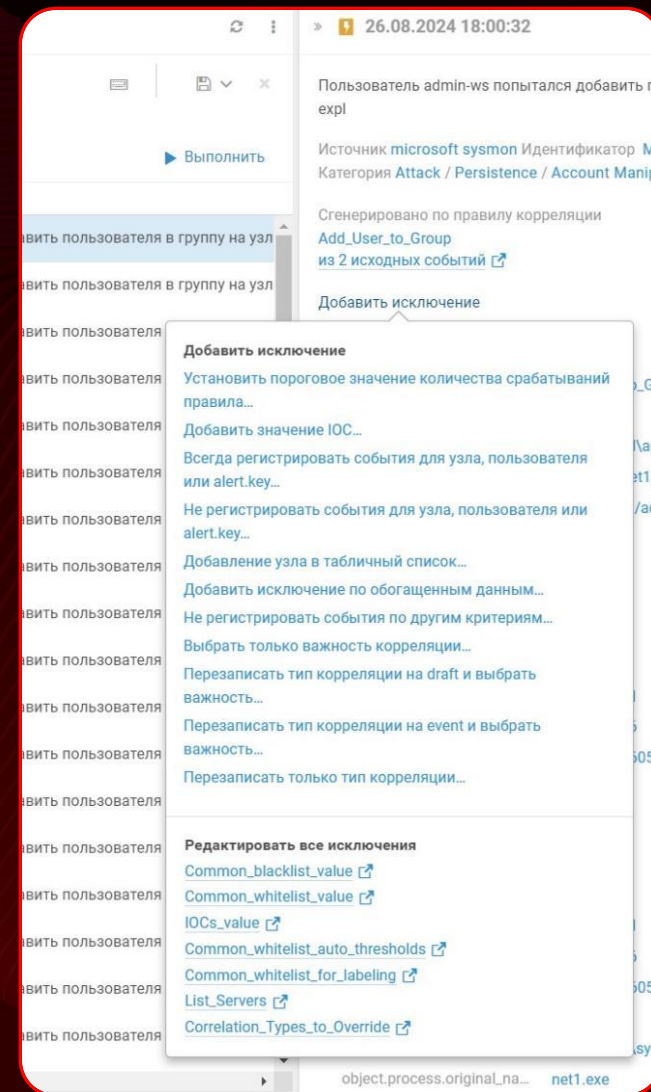
- **rule** — имя правила корреляции, по которому зарегистрировано событие (указано в поле события `correlation_name`).

Примечание. Буквы во все колонки табличного списка, кроме колонки **rule**, нужно вводить только в нижнем регистре. Кроме того, если данные в колонках могут принимать любые значения, необходимо ввести звездочку (*) в колонки с типом данных String и ноль в колонки с типом данных Number.

- **host** — имя узла, на котором зарегистрировано событие (указано в поле `event_src.host`).
- **user_id** — идентификатор учетной записи, с которой связана подозрительная активность (указан в поле `subject.account.id`).
- **specific_value** — дополнительную информацию о событии (указана в поле `alert.key`).

Универсальная схема правила

- 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.
- Обогащение карточки события и использование данных обогащения для создания исключений



ML-модуль BAD



**Ваш высококвалифицированный
ПОМОЩНИК:**



Помогает избежать ошибочного
вайтлистинга



Выдает второе мнение в виде Risk score
по событию, акцентируя внимание оператора
на наиболее рискованных событиях



Обнаруживает целенаправленные атаки,
выступая вторым эшелоном защиты



Неутомимый работник

59

ML-моделей



График работы
24x7



ФОТ ~ = зарплата
студента 2-3 курса



Рабочее место
1-2U 19" Rack mount

14

ТИПОВ СИСТЕМ

Windows + Sysmon

Security Center

SQL Server

1C Enterprise

Keycloak

Passwork

Auditd

vSphere (ESX)

Checkpoint Gaia

Cisco (IOS, ASA, FWASM, PIX)

FortiGate

OpenVPN

Artyfactory

TeamCity

BAD в SIEM-системе



Второе мнение
внутри карточки
события —
false positive

04.06.2024 10:29:51

Обнаружена попытка обойти запрет на запуск приложений с помощью встроенной утилиты Microsoft Windows "regsvr32" на узле

15 Оценка риска

Субъект 0
subject account

Действие start

Объект regsvr32.exe **19**
object process
fullpath c:\windows\system32\regsvr32.exe
hash 022CB167A29A32DAE848BE91AEF721C74F1975AF151...
 0
 diagplugin_user.001915.exe **0**
fullpath c:\use downloads\diagplugin_user.0019...

Статус success
reason User execution

Источник события 188.246.191.162 **1** 431

Источник microsoft sysmon Идентификатор Microsoft-Windows-Sysmon/Operational
Категория Attack / Defense Evasion / System Binary Proxy Execution: Regsvr32

Сгенерировано по правилу корреляции
Regsvr32_AWL_Bypass
из 2 исходных событий

Пользователь создал новый процесс regsvr32...

Назад Подтвердить Отклонить

Оценка риска **15** Событие **18** Узел **25** Пользователь

Сработавшие модели (10)

Нетипичная цепочка запусков процессов (windows): Аномальный переход от процесса к процессу: regsvr32.exe ser.001915.exe (current process)

Нетипичный процесс для пользователя (windows): Запуск процесса regsvr32.exe не является типичным для учетной записи исходя из ее поведенческой активности (current process), Запуск процесса diagplugin_user.001915.exe не является типичным для учетной записи исходя из ее поведенческой активности (parent process)

Нетипичный ввод в командной строке для пользователя на данном узле (windows): Нетипичный ввод в командной строке "C:\windows\System32\regsvr32.exe" /s /n /i:user "C:\Users\ AppData\Local\SkbKontur\DiagPlugin\3.0.27.723\kdaxapi64.dll" для учетной записи на узле NB-MP2D1W33 (current process), Нетипичный ввод в командной строке "C:\Users\ Downloads\DiagPlugin_user.001915.exe" для учетной записи на узле NB-MP2D1W33 (parent process)

Аномальная активность родительских процессов: 0

Активность в локальной сети родительских процессов: 0

Интернет-активность родительских процессов: 1

Аномальные прокси-соединения у родительских процессов: 0

Сетевая активность процесса: 0

Число узлов с активным текущим именем процесса: 2627

Число узлов с хэш-значением текущего процесса: 2533

Сработавшие правила (3)

OS_Process_Chain_Anomaly_Detection_Rule_Proxemic_Interaction

OS_Process_Chain_Anomaly_Detection_and_User_Command_Line_Input_On_Host

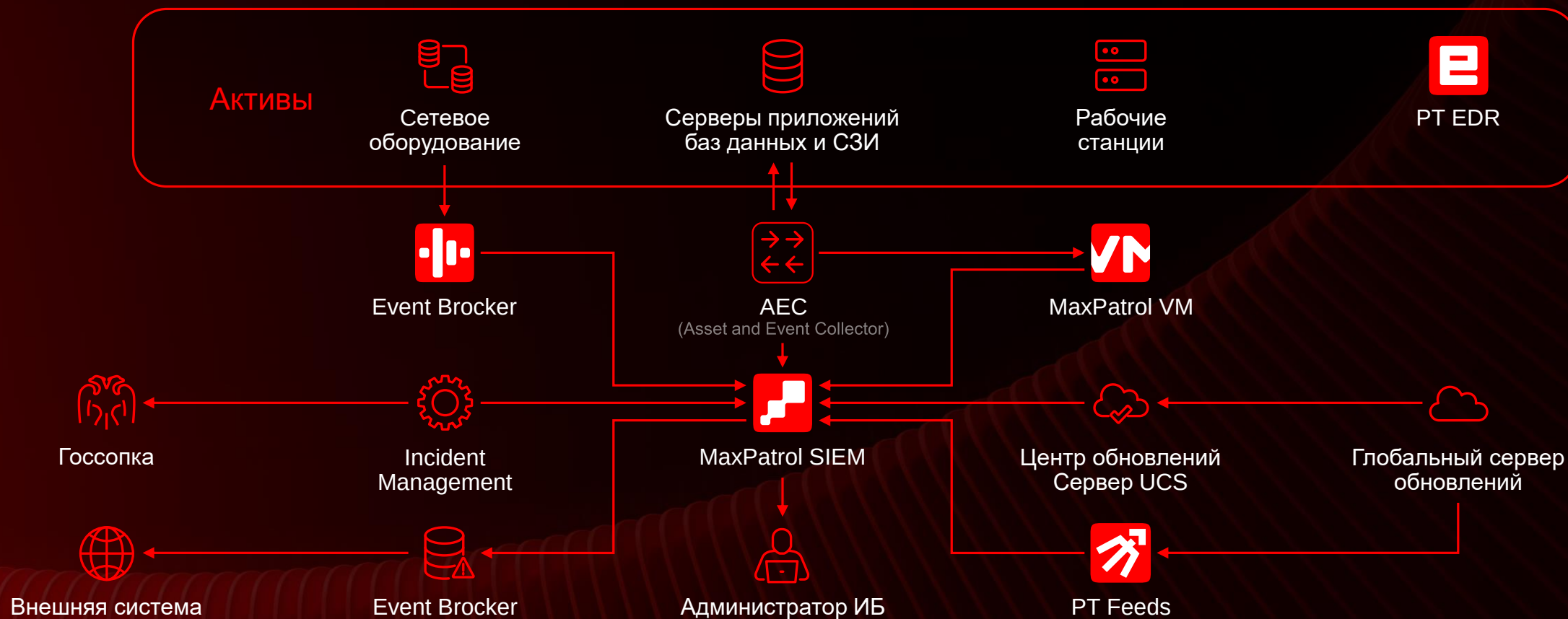
OS_Anomaly_Process_and_User_Command_Line_Input_On_Host

Знаем,
что дальше
делать



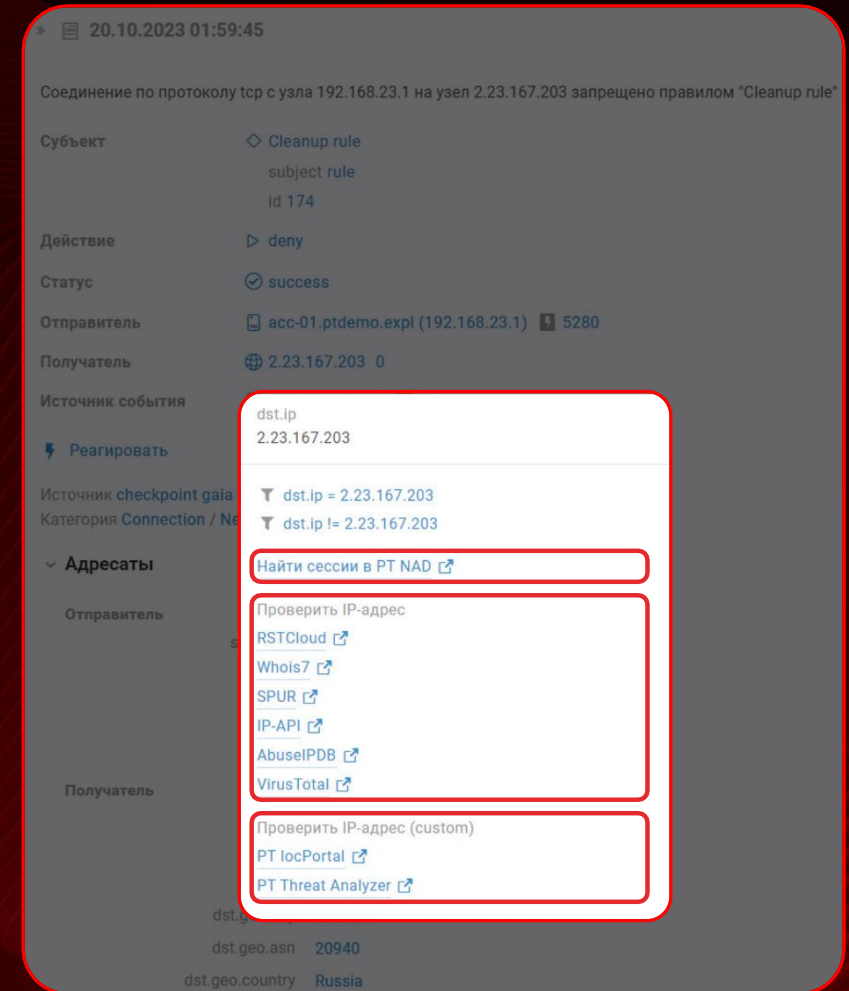
Интеграции
и экосистема

MaxPatrol SIEM – ядро экосистемы



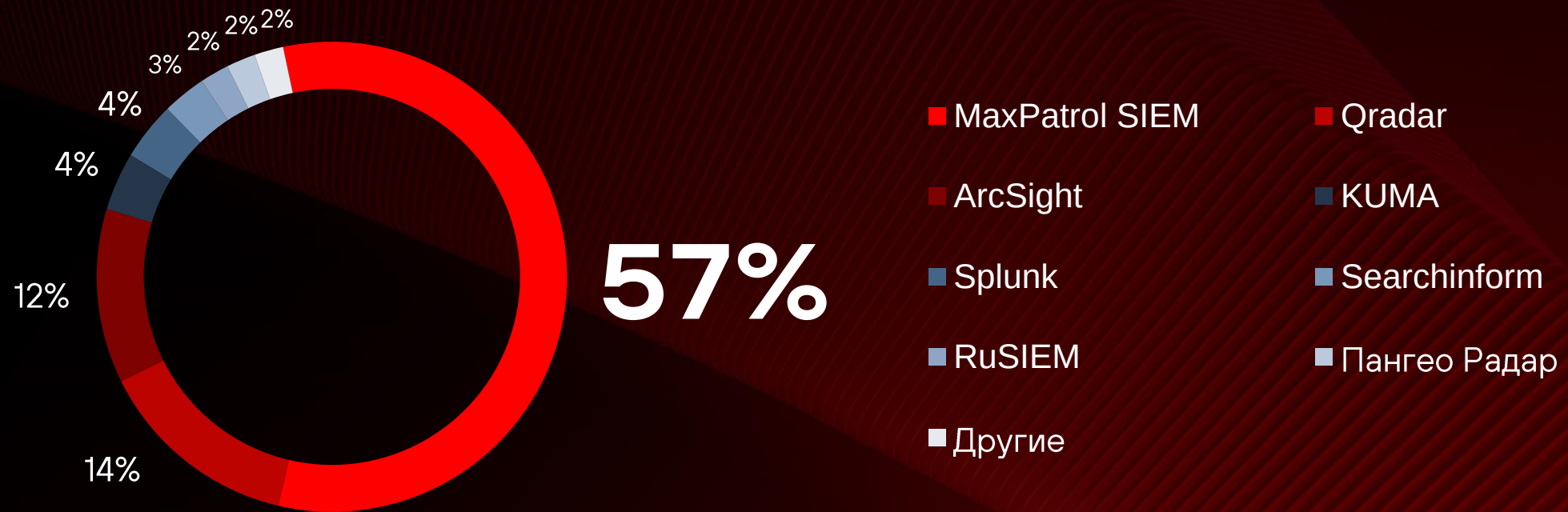
MaxPatrol SIEM знает, что делать дальше

- Репутация IP адреса, домена или файла за секунды
- Реагирование на инциденты из карточки*
- Любые внешние или внутренние сервисы в контексте события
- Кастомизация карточки для выбранных типов событий и удобства работы отдельных пользователей



* С использованием MaxPatrol EDR агента и встроенной интеграции

MaxPatrol SIEM — лидер на российском рынке SIEM-систем



Преимущества MaxPatrol SIEM



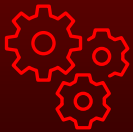
Актуальная экспертиза

Каждый месяц MaxPatrol SIEM автоматически пополняется пакетами экспертизы для обнаружения новых атак. Плюс мы постоянно обновляем и улучшаем ранее загруженные правила.



Помощь в принятии решений

В MaxPatrol SIEM встроен ML-помощник BAD (Behavioral Anomaly Detection). Это система second opinion, повышающая эффективность обнаружения атак за счет альтернативного метода оценки событий.



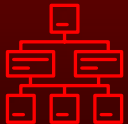
Enterprise-производительность

Архитектура MaxPatrol SIEM позволяет из единого окна проводить мониторинг ИБ в сложных инфраструктурах масштаба государства, показывает стабильность при работе даже на больших потоках — более 540 000 событий в секунду



Быстрый результат

Оперативно разворачивается и запускает мониторинг инфраструктуры за счет более 350 коннекторов и более 1100 экспертных правил «из коробки».



Адаптация к изменениям

Продукт быстро адаптируется к изменениям в инфраструктуре и четко идентифицирует ИТ-активы. Классификация активов по группам облегчает настройку правил корреляции.



Простота и удобство

MaxPatrol SIEM экономит время аналитику на сбор контекста атаки. Связанные события, второе мнение ML-модуля BAD и проверка опасных файлов — все в одном окне.

Присоединяйтесь к нам в Telegram



**Более
5000 участников**