



Перезагрузка SOC

Новый взгляд на привычные инструменты

Порошин Вадим
ЛПП During Attack

Что нужно SOC сегодня?



Полнота аудита
инфраструктуры
и контроль сбора
событий



Качество
обнаружения,
в том числе
целенаправленных
атак



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

Знать,
где искать



Знать,
что искать



Знать,
что делать дальше



Результат

Что мешает SOC быть более эффективными?



1

Потоки событий
и ИТ-инфраструктура растут

2

Усложняются техники
и тактики злоумышленников

3

Нехватка
человеческого ресурса

Нужны решения, содержащие экспертизу и возможности автоматизации задач SOC и способные:

- оперативно обнаруживать сложные атаки на ранних этапах — угрозы, которые обойдут базовые средства;
- уверенно реагировать и автоматизировать рутинные операции;
- учитывать особенности инфраструктуры и процессы построения ИБ в организации.

Chapter 1. Снижаем порог входа и автоматизируем рутину



MaxPatrol 360

Единый центр управления
расследованиями и контентом
инсталляций SIEM



PT Naira

Ассистент аналитика SOC



MaxPatrol 02

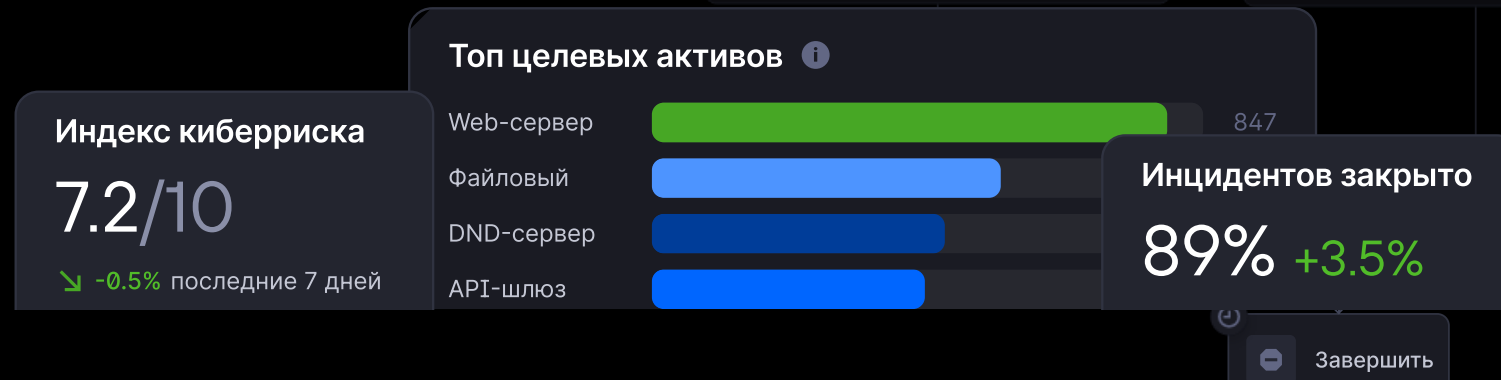
Замена L1-L2 SOC,
авторасследование,
сбор контекста и вердикты
с помощью ML от PT



Снижаем порог входа и автоматизируем рутину



- Управление тенантами
- Распространение и установка экспертизы в разных тенантах
- Централизованный анализ инцидентов ИБ из разных тенантов
- Бесшовный переход к исходным событиям с сохранением контекста
- Автоматизированное реагирование на инциденты на базе сценариев



Результат MaxPatrol 360



Единое окно

Команда SOC работает в едином интерфейсе, без переключения между системами



Автоматизация

Рутинные задачи автоматизируются и ускоряются через плейбуки и единое окно работы с инцидентами



Полный цикл

Инциденты проходят полный цикл — от обнаружения события до устранения



Ускорение

Сокращается время расследования и реагирования

PT Naira — простым языком о сложном



✦ AI-помощник

✕

AI-помощник использует облако Positive Technologies. Если поля события содержат конфиденциальную информацию, удалите ее перед отправкой запроса

Описание процесса

Чтобы составить запрос для AI-помощника, заполните поля:

Процесс

object.process

subject.process

object.process.name

lsass.exe

object.process.meta

Необязательно

object.process.fullpath

\\?\volume{ba3380f3-de5c-468c-9a78-cafc60eed812}\

Необязательно

object.process.chain

{lsass.exe} ← <unknown process>

Необязательно

object.process.parent.name

Необязательно

object.process.parent.fullpath

Необязательно

Отправить запрос

✦ AI-помощник
✕

Administrator · Сегодня, 12:30

Опиши этот процесс с точки зрения ИТ и ИБ.

object.process.name	lsass.exe
object.process.meta	—
object.process.fullpath	\\?\volume{ba3380f3-de5c-468c-9a78-cafc60eed812}\windows\system32\lsass.exe
object.process.chain	{lsass.exe} ← <unknown process>
object.process.parent.name	—
object.process.parent.fullpath	—

✦ Помощник · 12:31

1. Установлено ли приложение по умолчанию в операционной системе?
 Да. `lsass.exe` поставляется со всеми версиями Microsoft Windows и устанавливается вместе с ОС.
2. Относится ли приложение к числу системных процессов, необходимых для работы операционной системы?
 Да. Это системный процесс, без которого работа механизмов аутентификации и политики безопасности невозможна.
3. Какое целевое предназначение у исполняемого файла. Приведи основные примеры использования данного процесса.
`lsass.exe` – Local Security Authority Subsystem Service. Он отвечает за:
 - проверку учётных данных при входе в систему (логон);
 - создание и управление токенами доступа;
 - применение локальных и доменных политик безопасности;
 - обработку протоколов аутентификации (Kerberos, NTLM, Negotiate);
 - управление паролями, изменениями учётных записей и аудитом безопасности.
4. Какие стандартные пути к исполняемому файлу на жестком диске?

✦ AI-помощник

✕

```
serialization issue. (#141)* Update-ModuleManifest should add
ExternalModuleDependencies value as a collection. (#129)##
1.1.3.1New features* Added 'PrivateData' field to ScriptFileInfo.
(#119)Bug fixes## 1.1.2.0Bug fixes## 1.1.1.0Bug fixes##
1.1.0.0* Initial release from GitHub.* PowerShellCore support.##
For full history of release notes see
changelog:https://github.com/PowerShell/PowerShellGet/blob/
master/CHANGELOG.md@}) HelpInfoURI =
'http://go.microsoft.com/fwlink/?linkid=2113539')# SIG # Begin
signature block# MljKQYJKoZIhvcNAQcColjg
```

✦ Помощник · 12:24

1. Потенциальный результат запуска

При загрузке (например, `Import-Module PowerShellGet`) будет создан модуль PowerShellGet 2.2.5. Он добавит в текущую сессию набор команд (`Find-Module`, `Install-Module`, `Publish-Module` и др.), позволит управлять репозиториями, искать, устанавливать, обновлять и публиковать модули/скрипты из PowerShell Gallery и частных источников.

2. Параметры и флаги (все поля манифеста)

- `RootModule` = 'PSModule.psm1'
- `ModuleVersion` = '2.2.5'
- `GUID` = '1d73a601-4a6c-43c5-ba3f-619b18bbb404'
- `Author` = 'Microsoft Corporation'
- `CompanyName` = 'Microsoft Corporation'
- `Copyright` = '(c) Microsoft Corporation. All rights reserved.'
- `Description` = 'PowerShell module with commands for discovering, installing, updating and publishing the PowerShell artifacts...'
- `PowerShellVersion` = '3.0'
- `FormatsToProcess` = 'PSGet.Format.ps1xml'
- `FunctionsToExport` = @('Find-Command', 'Find-DSCResource', 'Find-Module', 'Find-RoleCapability', 'Find-Script', 'Get-CodeExecutionProvider', 'Get-InstallModule', 'Get-

MaxPatrol O2



1 **Обнаруживает**
злоумышленника
и определяет, до каких ресурсов
ему удалось добраться

2 **Расследует**
путь продвижения
злоумышленника
в ИТ-инфраструктуре путь

3 **Реагирует**
на атаку до того, как
организации будет нанесен
непоправимый ущерб



MaxPatrol O2

сегодня



1

Облачная технология

2

Центральная консоль
для управления
инцидентами

3

AI

Автоматизированные
расследования
инцидентов

4

AI

Центральная консоль
для управления
инцидентами

Как это выглядит?



Вердикт от ИИ

Последовательность инцидента

События, «подтянутые» в рамках автоматического расследования

INC-202

ООО «КиберКрепость»

22 ноября, 18:47:01

Закрывает

iprohorov

Легитимное действие

Заключение ещё не добавлено

Добавить

Легитимное действие

Пользователь вошел в систему через RDP и выполнил инструменты, связанные с базой данных (st4.dbtool.exe -gi) и управление удаленным рабочим столом (RDCMan.exe). Эти действия соответствуют рутинной работе администратора базы данных, но источник внешнего входа RDP следует сопоставить с политиками доступа для обеспечения соответствия требованиям.

Общие сведения

1. Временной период: 2025-04-21T14:01:02.406Z to 2025-04-21T14:01:04.341Z

2. Пользователь: aamelinaadm@plat.form (тип входа 10, доступ RDP)

3. Задействованные устройства:

а. Источник: dc1-bst-srv-01.plat.form (10.125.130.4)

б. Цель: dc3-d-st4app-01.plat.form (10.125.100.3)

4. Активность: Выполнение st4.dbtool.exe -gi и RDCMan.exe из локального пути на рабочем столе, с внутренними сетевыми соединениями к SQL Server и веб-сервисам.

Общие сведения

Название

Execute_PSEXEC

ID в источнике

INC-7955

Описание

Аналог утилиты администрирования PsExec (psexecvc.exe) запущен на узле mo-m561-02.corp.local

Создан

17 ноя 2025, 14:05:29

Произошел

13 дек 2025, 18:47:01

Уровень опасности

Средний

Все

4

3

17 ноя, 14:05:27 · correlationengine · Execute_PSEXEC

Аналог утилиты администрирования PsExec (psexecvc.exe) запущен на узле mo-m561-02.corp.local

Attack · Defense Evasion · System Binary Proxy Execution: CMSTP

17 ноя, 14:05:27 · logcollector · endpoint_security · msg_id:...

Запущен процесс std.exe с привилегиями system при помощи утилиты администрирования PsExec или ее аналога на узле mo-m561-02.corp.local

17 ноя, 14:05:29 · logcollector · endpoint_security · msg_id:...

Запущен процесс std.exe с привилегиями system при помощи утилиты администрирования PsExec или ее аналога на узле mo-m561-02.corp.local

17 ноя, 14:07:27 · XDR · Execute_PSEXEC

Аналог утилиты администрирования PsExec (psexecvc.exe) запущен на узле mo-m561-02.corp.local

Attack · Defense Evasion · System Binary Proxy Execution: CMSTP

17 ноя, 14:07:27 · logcollector · endpoint_security · msg_id:...

Запущен процесс std.exe с привилегиями system при помощи утилиты администрирования PsExec или ее аналога на узле mo-m561-02.corp.local

17 ноя, 14:07:32 · NAD · Execute_PSEXEC

Запущен процесс msiehex.exe с привилегиями t1-guzdanil при помощи утилиты администрирования PsExec или ее аналога на узле mo-m561-02.corp.local

Attack · Defense Evasion · System Binary Proxy Execution: CMSTP

Chapter 2.

Улучшаем детект



Смещение акцента на сенсоры SOC

- MaxPatrol EDR — хостовой детект и доверенный сбор логов
- PT NAD сетевой контекст кибератаки и удобное расследование



Повышаем видимость за счет ML

MaxPatrol BAD дает ML-детект, основанный на выявлении аномалий в событиях хостов и сети с выдачей скоринга критичности



Экспертиза в MaxPatrol SIEM

- Приоритизация контента, разделение на базовый детект и hunting с ежемесячным обновлением
- ML-детект как замена классическому, там где это оправдано

MaxPatrol SIEM. Полная видимость IT-инфраструктуры



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



MaxPatrol BAD



ML-модуль поведенческого анализа (Behavioral Anomaly Detection) в MaxPatrol SIEM, предназначенный для выявления сложных, скрытых и нетипичных атак и последующего скоринга за счет технологий машинного обучения



Анализирует поток событий и обогащает сработки правил корреляции оценкой риска



Использует ML-модели для поиска поведенческих аномалий и нетипичной активности — работает как автономный сенсор, независимо от правил корреляции



Обнаруживает:

- сложные целенаправленные атаки, в том числе с использованием техник обхода правил корреляции;
- новые тактики, техники и процедуры, ещё не покрытые детектами;
- постэксплуатацию ранее неизвестной уязвимости.

PT Network Attack Discovery



PT NAD эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий хакеров в трафике



Точно определяет действия атакующих внутри сети на ключевых этапах атаки за минимальное

PT NAD внедряется за один час и в режиме близкому к реальному времени увидит точки проникновения в инфраструктуру и масштаб атаки за счет объединения восемь методов обнаружения угроз, из которых пять уникальных.



Выбор экспертов — незаменимый инструмент для ретроспективного анализа и расследований

- Технология DPI детально разбирает корпоративный сетевой трафик на любых скоростях, а данные используются для ручного анализа и автоматического обнаружения аномалий.
- Это позволяет выявлять угрозы, которых нет в базах данных сигнатур IDS/IPS и NGFW



Оперативно выявляет актуальные для рынка России угрозы

- Экспертный центр PT ESC поставляет индикаторы компрометации, правила, поведенческие и статистические модули, нацеленные на выявления популярных атак на территории России.
- Крупный бизнес из разных отраслей России защищен от кибератак с помощью PT NAD

Chapter 3.

Храним и обрабатываем события оптимальным способом



MaxPatrol SIEM

- Повышение производительности от 35% до 50%
- Вынесение нормализации на коллектор и балансировка потока



MaxPatrol Log Management

Снижение нагрузки на SIEM, обработка до 100k+ событий на одном конвейере, хранение, ретро корреляция и поиск индикаторов



PT Security Lakehouse

Lake House, хранящий любые объемы и форматы данных на базе S3

MaxPatrol SIEM + Log Management



Изменение архитектуры за счет появления возможности распределения потоков и повышение производительности



Вынесение нормализации на SIEM Collector с одновременным распределением потока на SIEM и LM/SDL



Появление MaxPatrol Log Management:

- До 120к EPS на конвейер (standalone) с значительным снижением стоимости решения
- Умное и ручное распределение потоков — фильтрация по дереву корреляции и из UI
- Единая с MP SIEM консоль поиска событий



Повышение производительности конвейера SIEM до 80к EPS и снижение нагрузки на CPU, RAM на 35-50% на текущих инсталляциях

PT Security Lakehouse



- Интеграция в качестве точки сбора и хранения всех возможных событий и логов (EDR, сетевая телеметрия, другие ИБ/ИТ системы) любых вендоров
- Нормализация экспертизой Positive Technologies
- Интеграция с BI системами и с любыми другими аналитическими продуктами

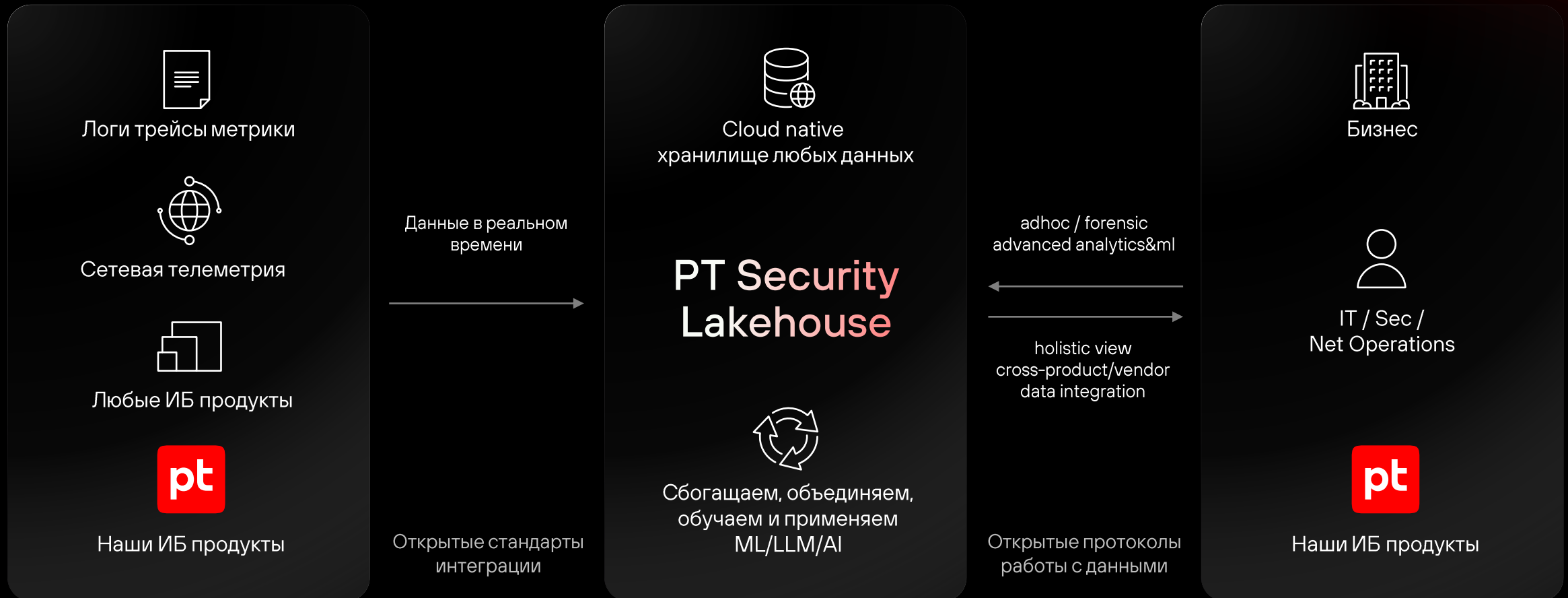
Платформа централизованного
Log Management

Решение сложностей
масштабирования хранилищ СЗИ

Поставщик данных для ML

Расширенная, в том числе
кросс-продуктовая аналитика

PT Security Lakehouse



Действительно ниже TCO (при условии если cloud инфраструктура уже есть)

- Стандартизация железа
- Эластичность: можно отдавать ресурсы обратно в облако когда нет нагрузки
- S3 на шпинделях: высокоплотные производительные хранилки
- Self healing механизмы → меньше сил на сопровождение
- Write once, read many → все текущие и будущие кейсы на одной платформе

Открытая архитектура

- Интеграции: открытые стандарты как на заливку данных, так и на чтение
- Данные: даже отказаться от лицензий — данные в открытом формате на S3 останутся, никакой боли и вендор-лока

Вендор агностик

весь зоопарк данных можно хранить и анализировать на одной платформе

Future-proof

архитектура, готовая к AI-SOC и прочему

Задай
вопрос
спикеру





Спасибо!