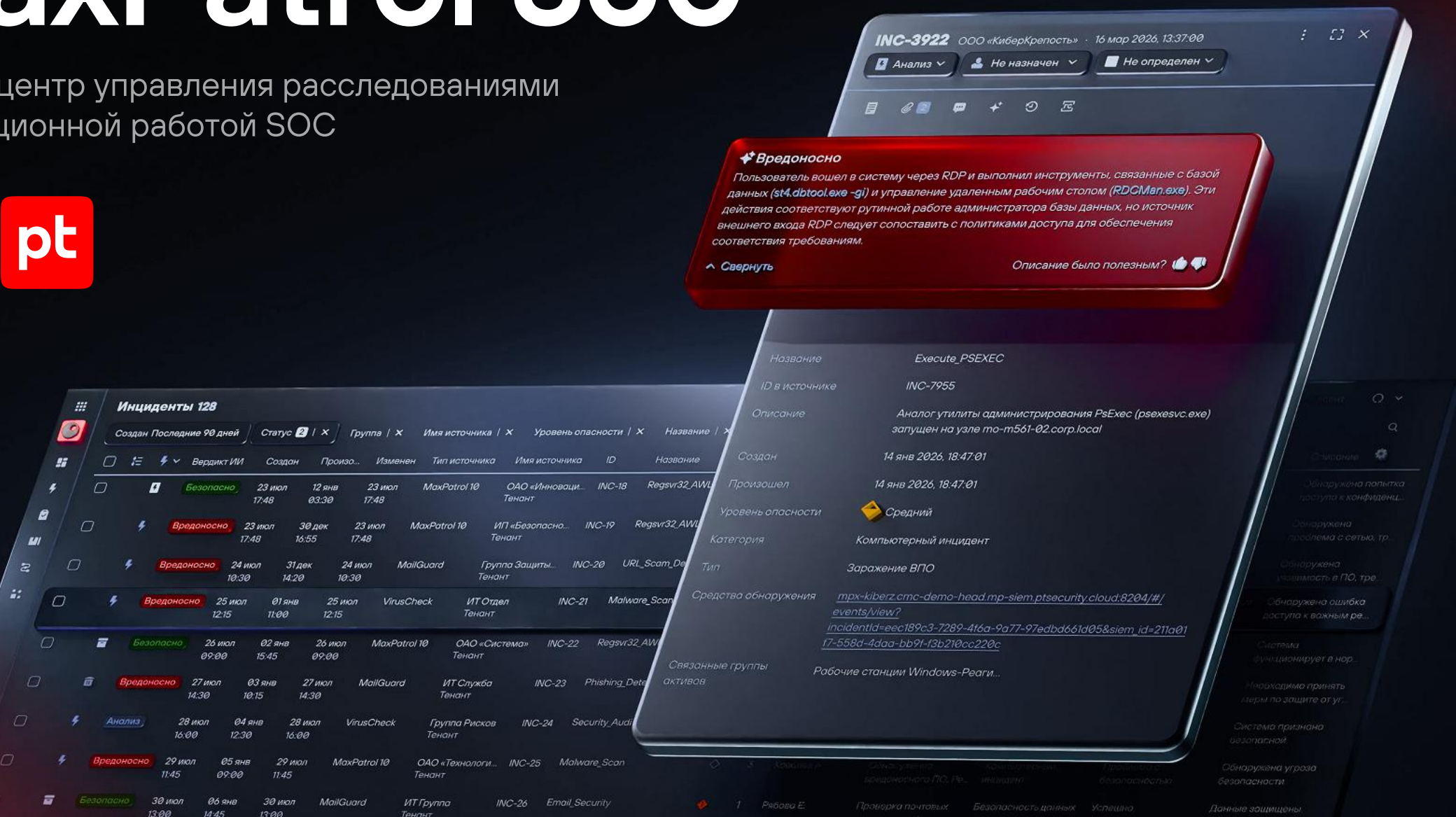


MaxPatrol 360

Единый центр управления расследованиями
и операционной работой SOC



Что такое SOC?

Security Operations Center

Центр Противодействия
Киберугрозам (ЦПК)



SOC – это структура, которая объединяет технологии, людей и процессы, чтобы вовремя выявлять риски и устранять последствия киберинцидентов до нанесения компании неприемлемого ущерба*

Иными словами, это подразделение в организации, которое постоянно отслеживает киберугрозы, оценивает их значимость, предотвращает, выявляет и реагирует на них по заранее заданным приоритетам, обеспечивая киберустойчивость организации

*то есть — до нарушения киберустойчивости или наступления недопустимого события (НС)



Сервисы



Процессы

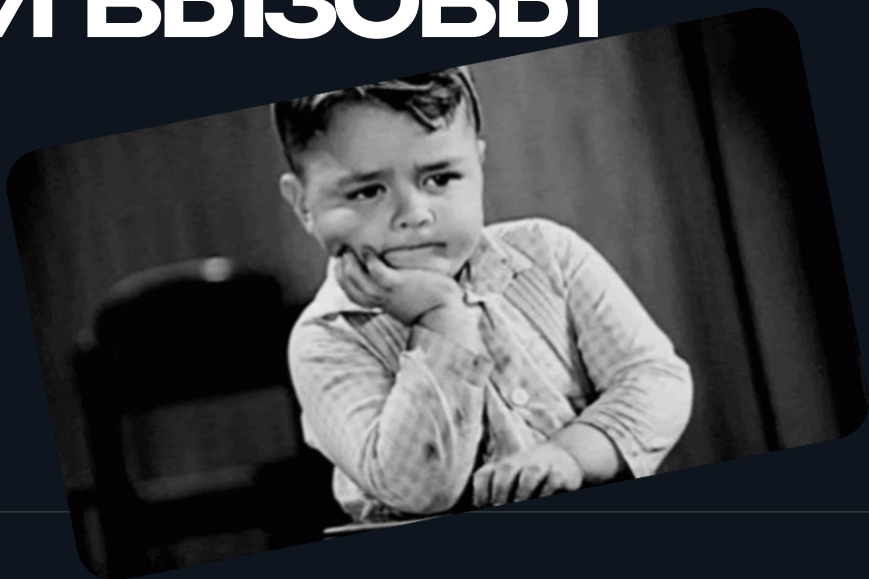


Люди и экспертиза



Технологии

Проблемы и вызовы



Фрагментация процессов ИБ

Большинство компаний используют более 10 систем безопасности/инструментов обеспечения ИБ. В крупных компаниях – более 40

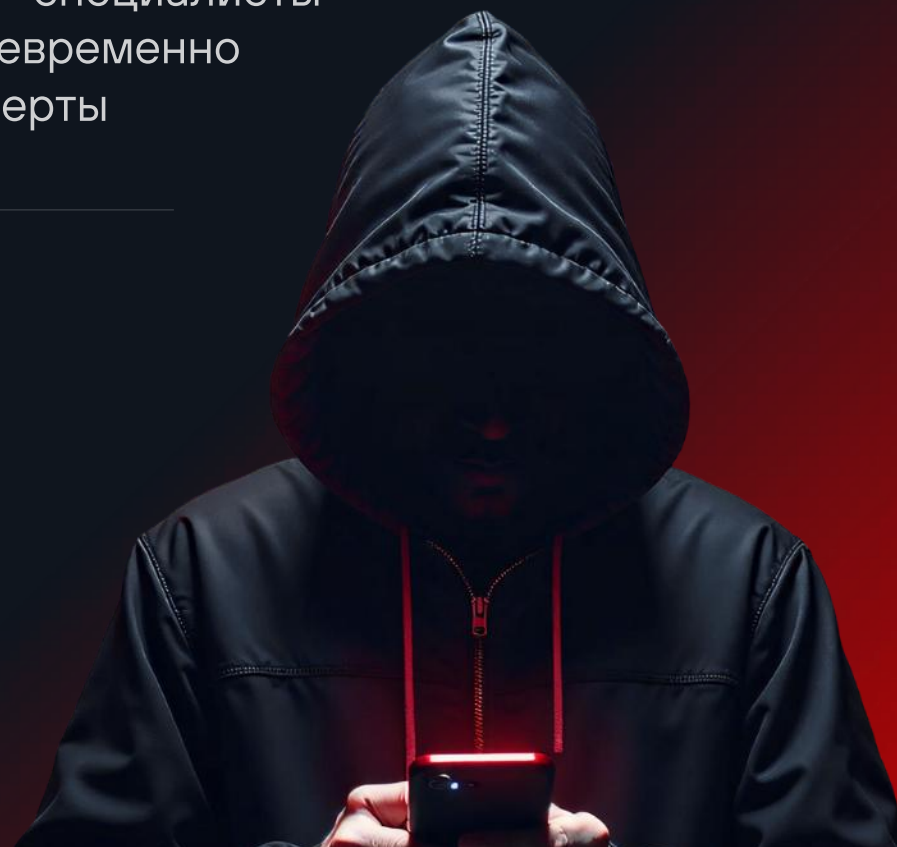
Alert fatigue

усталость от алертов – специалисты перегружены и несвоевременно разбирают security алерты

Недостаток контекста для принятия решений наряду с ручной обработкой инцидентов и недостаточной автоматизацией ведут к замедлению расследований

~40% специалистов долго расследуют кибератаки из-за нехватки контекста

Стремительно **«умнеющие» хакеры** и, соответственно, растущий спрос на «сервисную» безопасность и ассистентов: MDR, MSSP, холдинговые SOC и AI-driven расследования, реагирования.



Важно для SOC



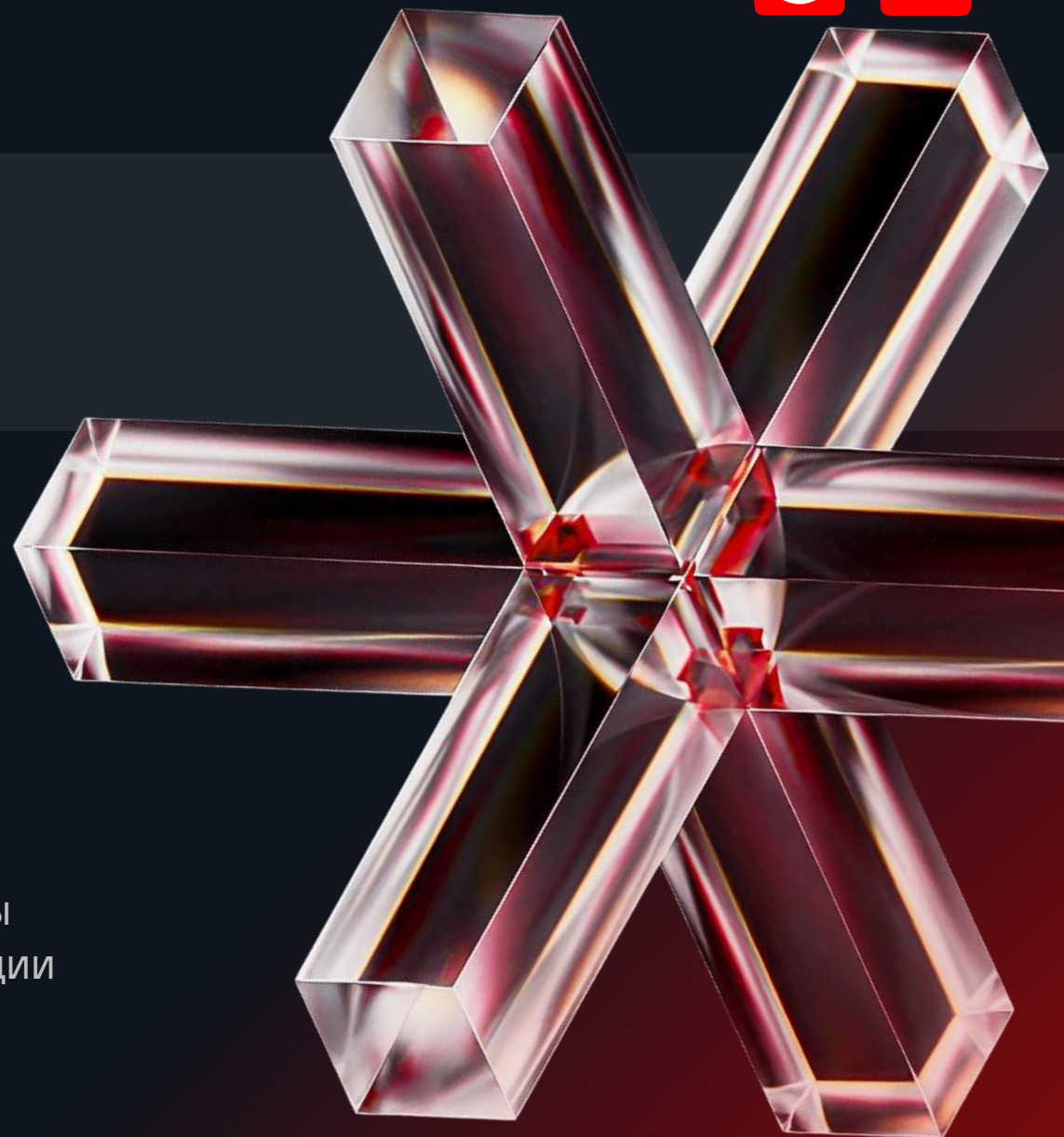
Оказывать качественный сервис
по обеспечению киберустойчивости

По данным исследований инцидентов, проведенных командой Positive Technologies*, доля проектов, в которых атака привела к нарушению внутренних бизнес-процессов, достигла 55%.

Это означает, что инциденты напрямую влияют:

- на производственные процессы
- клиентские сервисы
- логистику
- финансовые операции

* Исследование Positive Technologies: Итоги проектов по расследованию инцидентов и ретроспективному анализу — 2024–2025



MaxPatrol 360

В SOC



MaxPatrol 360



Управляет расследованиями SOC
в одной системе

Собирает события, инциденты,
расследования и действия аналитиков
в едином рабочем процессе



Автоматизирует реагирование
и рутинные операции

Плейбуки берут на себя типовые действия:
сбор данных, обогащение, уведомления
и запуск ответных мер



Масштабирует SOC
без роста штата сотрудников

Позволяет поддерживать мультитенантность
для централизованного управления десятками
инфраструктур внутри единой системы



Легко интегрируется

Подключается к продуктам не только
Positive Technologies, но и к другим решениям,
предоставляющим данные для сбора,
обогащения и реагирования на инциденты

Сценарии использования



Управление тенантами



Централизованный анализ инцидентов ИБ из разных тенантов



Автоматизированная обработка инцидентов



Реагирование



Распространение и установка экспертизы в разных тенантах



Бесшовный переход к исходным событиям с сохранением контекста



Дашборды



Контроль выполнения задач и коммуникация с клиентами



Широкие возможности по интеграции

Управление тенантами



- Тенанты объединяются в единую управляемую структуру, что дает оператору возможность единообразно управлять процессом обеспечения ИБ в этих тенантах из единого окна
- В таком формате упрощаются контроль обновлений, распространение экспертизы и проведение расследований инцидентов

Тенанты 12

ПодключенияДата добавления

Название	Описание	Подключенный MaxPatrol SIEM	Дата добавления
ЗАО «КиберСигнал»	Речная набережная, дом 9, Ростов-на-Дону, 344000	cyberkrepost.cloud.ru	22 апр
ООО «КиберКрепость»	Улица Мечты, дом 21, Нижний Новгород, 603000	cyberkrepost.cloud.ru	3 фев
ООО «ТехноЩит»	Улица Сосновая, дом 12, Уфа, 450000	oaoinava.app.ru	23 янв
ОАО «КБТехнологии»	Зеленая аллея, дом 3, Новосибирск, 630000	oaoinava.app.ru	23 янв
ИП «Защита»	Солнечный бульвар, дом 7, Екатеринбург, 620000	—	23 янв
ЗАО «Инновационные Решения»	—	—	20 янв
ИП «Безопасность Плюс»	Бульвар Радужный, дом 5, Челябинск, 454000	ipzashchitnik.app.ru	5 дек 2024
ОАО «Инновации»	Северный проспект, дом 8, Омск, 644000	ipbezopasnostbplus.cloud.ru	5 дек 2024
ООО «ЗащитаДанных»	Светлый переулок, дом 12, Санкт-Петербург, 190000	ipzashchitnik.app.ru	5 дек 2024
ИП «Страж»	Тихий проезд, дом 15, Челябинск, 454000	—	17 апр 2024
ИП «Защитник»	Уютный уголок, дом 15, Челябинск, 454000	ipbezopasnostbplus.cloud.ru	17 апр 2024
ИП «Даша КиберБез»	Спокойная улица, дом 15, Челябинск, 454000	—	17 апр 2024

ПодключенияДоступ+ Добавить

ООО «КиберКрепость»

Внутренний адресcyberkrepost.mp360.ru

Доступ30 пользователей

Дата добавления3 февраля, 15:25

MaxPatrol 10

КиберКрепостьcyberkrepost.cloud.ru:3334

Managament and Configuration27.4

Логинcmc_service_login

MaxPatrol 1027.4

Лицензиядо 1 июля 2030

Конвейерыconv-1.cyberkrepost.cloud.ru:8013conv-2.cyberkrepost.cloud.ru:8013

Knowledge Base27.4

Инциденты

Управление тенантами



Новый арендатор

Шаг 2 из 3

✕

Название

ООО «КиберКрепость»

Внутренний адрес

oookiberkrepost.mp360.softwaredomain.cloud

Описание

ул. Мечты, дом 21, Нижний Новгород, 603000

Пользователи

Иванов И. И. iivanov

Константинов В. К. vkonstantinov

Трудин Р. К. rtrudin

Жданов Л. С. lzdanov

Сергеев Е. А. esergeev

Показать

Интеграция с MaxPatrol 10

Подключение

КиберКрепость

Адрес

✓

 cyberkrepost.cloud.ru:3334

Версия 28.1

Арендатор MaxPatrol 10

КиберКрепость

Пользователи MaxPatrol 10

Админов А. ✕

Тулин Т. ✕

Приходько А. ✕

✕

✕

Прохоров И. ✕

Селютин А. ✕

Позитивный Т. ✕

Далее

Пропустить

Назад

Новый тенант

Шаг 3 из 3

✕

Подключение

Cyberkepost

Адрес  cyberkepost.cloud.ru:3334

Версия 28.1

Тенант MaxPatrol 10

Cyberkepost

Пользователи
MaxPatrol 10

Иванов И. И. iivanov
Константинов В. К. vkonstantinov
Трудин Р. К. rtrudin
Жданов Л. С. lzdанov
Сергеев Е. А. esergeev
[Показать](#)

Конвейеры

cybercastle-1-siem-1.security.ru
cybercastle-2-siem-1.security.ru
cybercastle-3-siem-1.security.ru

Инциденты

☒ Собирать инциденты 

Начало сбора

09.04.2025  12:30

Тип источника

MaxPatrol SIEM

Адрес

cyberkepost.cloud.ru:3334

Сохранить и завершить

Назад

Централизованный анализ инцидентов ИБ



- MaxPatrol 360 собирает из множества тенантов информацию об инцидентах ИБ, предоставляя оператору контекст для принятия решения
- При необходимости можно получить доступ к исходным событиям тенанта и просмотреть дополнительные данные по инциденту

Инциденты 128

Создан Последние 90 дней | Статус 2 x | Группа x | Имя источника x | Уровень опасности x | Название x | Вердикт x | +

☐			Создан	Произо...	Тип источника	Имя источника	ID	Название			Ответственный	Описание от ИИ	Категор
☐			23 июл 17:48	5 ноя 22:10	MaxPatrol 10	ОАО «КБТехно... Тенант	INC-20	Regsvr32_AWL_Bypass			Кузнецов И.	Подозрительная активность, связан...	Компьютерный инцидент
☐			14 янв 18:47	14 янв 18:46	MaxPatrol 10	ООО «КиберКр... Тенант	INC-2...	Execute_PSEXEC			Федоров В.	Обнаружено использование RD...	Компьютерный инцидент
☐			23 июл 17:48	30 дек 16:55	MaxPatrol 10	ИП «Безопасн... Тенант	INC-19	Regsvr32_AWL_Bypass			Смирнова Е.	Зафиксирован факт входа через RDP и...	Компьютерный инцидент
☐			23 июл 17:48	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-1	Regsvr32_AWL_Bypass			Вы Админист...	Использование RDP для доступа к инст...	Компьютерный инцидент
☐			23 июл 17:48	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-1	Regsvr32_AWL_Bypass			Вы Админист...	Активность указывает на потен...	Компьютерный инцидент
☐			23 июл 17:48	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-1	Regsvr32_AWL_Bypass			Вы Админист...	Пользователь	Компьютерный инцидент

INC-202 ООО «КиберКрепость» · 14 янв 2026, 18:47:01

Закрит | iprohorov | Подтвержден

Зафиксирована попытка удаления учетной записи proxied_user в MySQL на узле 127.0.0.1 (операция управления пользователями). Событие произошло вне подтвержденных работ. Признаки указывают на злоупотребление привилегиями локально на хосте либо компрометацию админских/сервисных учетных данных. Подтверждений успешного удаления в журналах не обнаружено — учётная запись сохранена.

Рекомендации

Выяснить инициатора (audit/binlog/syslog).
Сменить секреты proxied_user и админов; завершить активные сессии.
Запретить CREATE/DROP USER и GRANT ALL вне окна изменений.
Доступ к БД — только через бастион + MFA, именные учётки.
Включить аудит DDL/привилегий с алертами в SIEM.
Провести ревизию прав и настроить регулярную ротацию секретов (секреты в Vault).

Изменить

Всё | 4 | 3

14 янв 2026, 18:47:01 · correlationengine · Execute_PSEXEC

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

Attack · Defense Evasion · System Binary Proxy Execution: CMSTP

17 янв 2026, 14:05:27 · logcollector · endpoint_security · ms...

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

17 янв 2026, 14:05:27 · logcollector · endpoint_security · ...

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 (psexesvc.exe) запущен на узле mo-m561-02.corp.local

Attack · Defense Evasion · System Binary Proxy Execution: CMSTP

17 янв 2026, 14:05:27 · logcollector · endpoint_security · ms...

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 msiehcx.exe с привилегиями t1-gydzaniil при помощи утилиты администрирования PsExec или ее аналога на узле mo-m561-02.

Общие сведения

Название Execute_PSEXEC

ID в источнике INC-7955

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

Создан 14 янв 2026, 18:47:01

Произошел 14 янв 2026, 18:47:01

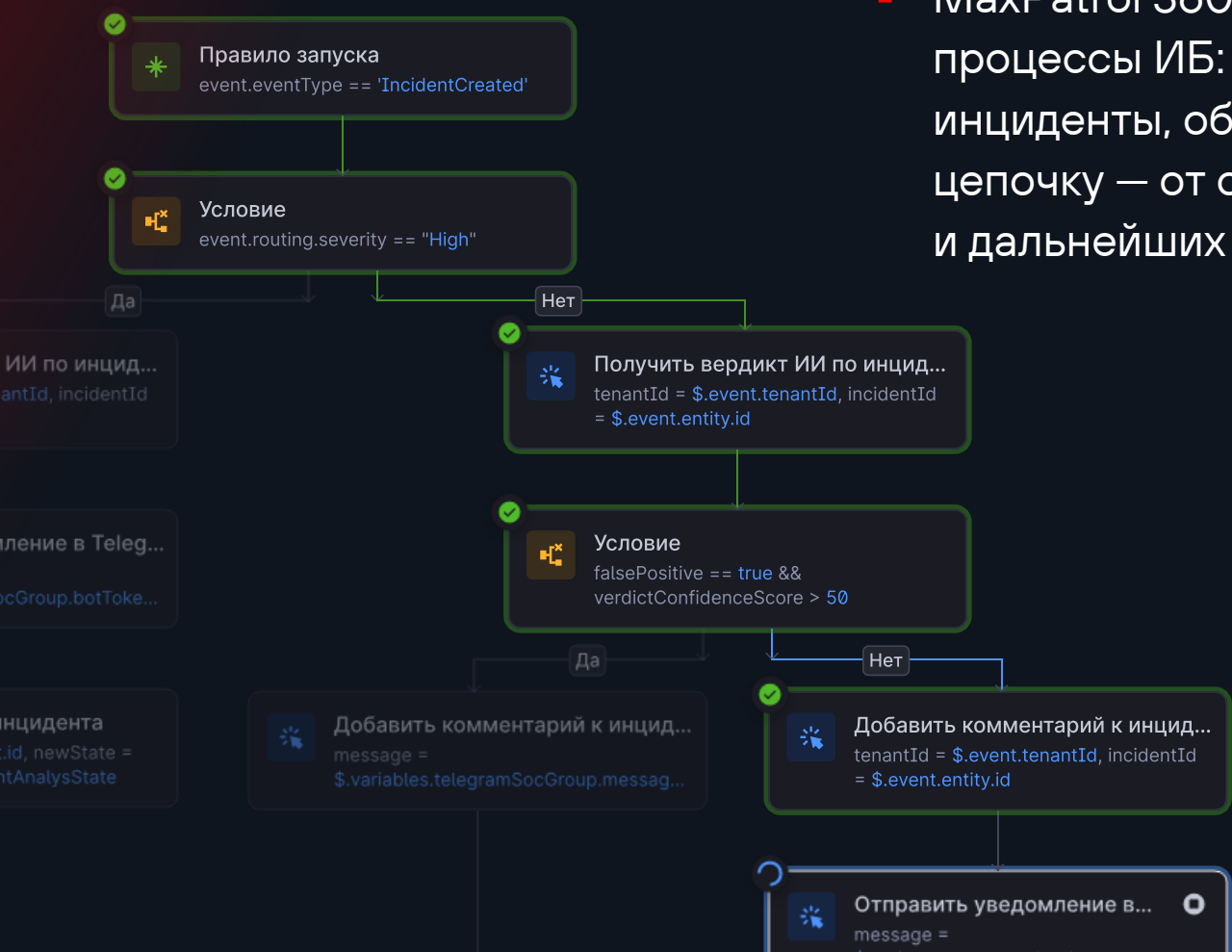
Уровень опасности Средний

Категория Компьютерный инцидент

Автоматизированная обработка инцидентов



- MaxPatrol 360 позволяет автоматизировано обрабатывать процессы ИБ: обогащать, менять статусы и реагировать на инциденты, обеспечивая непрерывную аналитическую цепочку — от обнаружения инцидента до принятия решения и дальнейших улучшений



Получить вердикт ИИ по инц...

Статус

В процессе

Запущен

21 июля, 17:30 / 25 мин, 30 сек

Журнал

Данные

Параметры

Входные данные

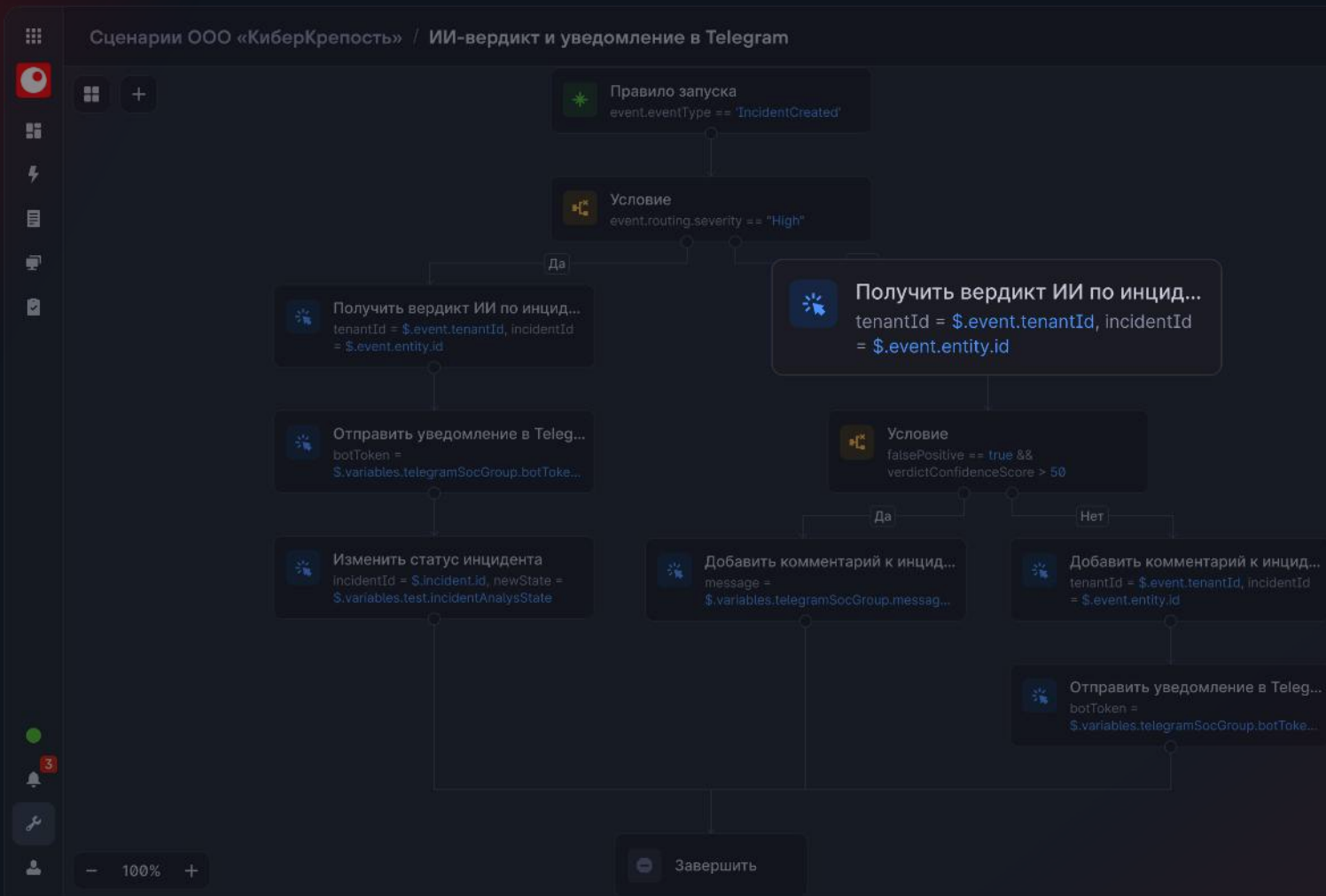
```
{  "tenantId": "tenant-42-prod",  "incidentId": "inc-2026-03-08-18421",  "patToken": "pat_x7Kf29LmQp81ZaBc",  "eventsCount": 37}
```

Автоматизированная обработка инцидентов



Сценарии ООО «КиберКрепость» 100							+ Создать	↑	↺
Статус Способ запуска Условие запуска							🔍		
☐ Название	Статус	Способ запуска	Условие запуска	Изменил	Дата изменения				
☐ Обогащение данных инцидента Автоматически обогащает инциденты данными из EDR системы	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Тулин Т.В.	11 фев 17:48				
☐ ИИ-вердикт и уведомление в Telegram Комплексная проверка индикаторов компрометации с развилками и уведомлениями	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Тулин Т.В.	11 фев 17:48				
☐ Фишинговая атака Автоматический анализ фишинговых писем и вложений	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Смирнов И.А.	10 фев 17:50				
☐ Malware - изоляция хоста Автоматическая изоляция зараженного хоста и создание тикета	▶ Включен	⚡ Вручную	—	Петрова А.С.	10 фев 17:51				
☐ Блокировка IP Блокирует IP адреса при обнаружении brute force атак...	■ Отключен	⚡ Вручную	—	Кириллов Д.Р.	10 фев 17:52				
☐ Повышение критичности - эскалация Сбор информации о подключённых устройствах	■ Отключен	⚡ Вручную	—	Семенова Л.Е.	4 янв 17:53				
☐ Обогащение данных о приложениях Анализ установленных приложений на устройстве	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Кузнецов В.Д.	3 янв 17:54				
☐ Мониторинг аномалий Выявление необычной активности в сети	■ Отключен	⚡ Вручную	—	Тихонов А.Ю.	24 ноя 2025 17:55				
☐ Анализ уязвимостей Сканирование систем на наличие известных уязвимостей	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Сидорова Е.Ф.	24 ноя 2025 17:56				
☐ Обнаружение DDoS атак Автоматическое обнаружение и смягчение DDoS атак	▶ Включен	⌚ Автоматически	event.eventType == 'IncidentCreated'	Лебедев А.П.	24 ноя 2025 17:57				
☐ Анализ сетевого трафика Мониторинг и анализ трафика для выявления угроз	■ Отключен	⌚ Автоматически	—	Климова М.И.	24 ноя 2025 17:58				
☐ Уведомление о подозрительных входах Оповещение пользователей о подозрительных входах	■ Отключен	⌚ Автоматически	—	Романов В.Е.	11 окт 2025 17:59				

Автоматизированная обработка инцидентов



Получить вердикт ИИ по инциденту



Получение вердикта ИИ-ассистента по инциденту

Название шага*

Получить вердикт ИИ по инциденту

Входные параметры

tenantId*

Идентификатор тенанта

\$.event.tenantId

incidentId*

Идентификатор инцидента

\$.event.entity.id

eventsCount*

Количество событий, связанных с инцидентом, которые ИИ-ассистент будет использовать для анализа ...

\$.event.tenantId

Выходные параметры ⓘ

☐ incidentId

Идентификатор инцидента

String

☒ autoFalse

Boolean

Реагирование



- MaxPatrol 360 позволяет автоматизировать реагирование, например, через MaxPatrol EDR или другие комлементарные решения (NTA-, SIEM-, VM-системы)

The screenshot displays the MaxPatrol 360 interface. On the left, a sidebar contains navigation icons. The main area is titled 'Инциденты 128' and features a table of incidents with columns for 'Создан', 'Произо...', 'Изменен', 'Тип источника', 'Имя источника', 'ID', and 'Название'. A modal window titled 'Реагирование на процесс' is open, showing details for incident 'INC-202' (dated 14 янв 2026, 18:47:01). The modal includes a 'Общие сведения' section with fields for 'Название' (Execute_PSEXEC), 'ID в источнике', 'Описание', 'Создан', 'Произошел', 'Уровень опасности', 'Категория', 'Тип', and 'Средства обнаружения'. Below this, there are tabs for 'Быстрые действия' and 'Рекомендованные сценарии'. The 'Быстрые действия' tab is active, showing a list of actions: 'Завершить процесс' (checked), 'Завершить все процессы (по имени / пути)', 'Завершить дерево процессов', and 'Запустить YARA-сканирование'. A 'Запустить' button is at the bottom of the modal. The background shows a list of incidents, with the first one being 'Regsvr32_AWL_Bypass' from 'MaxPatrol 10' on '23 июл 17:48'.

Создан	Произо...	Изменен	Тип источника	Имя источника	ID	Название
23 июл 17:48	5 ноя 22:10	23 июл 17:48	MaxPatrol 10	ОАО «КБТехно... Тенант	INC-20	Regsvr32_AWL_Bypass
23 июл 17:48	12 янв 03:30	23 июл 17:48	MaxPatrol 10	ОАО «Инновац... Тенант	INC-18	Regsvr32_AWL_Bypass
23 июл 17:48	30 дек 16:55	23 июл 17:48	MaxPatrol 10	ИП «Безопасн... Тенант	INC-19	Regsvr32_AWL_Bypass
23 июл 17:48	2 окт 19:20	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-16	Regsvr32_AWL_Bypass
23 июл 17:48	8 май 21:45	23 июл 17:48	MaxPatrol 10	im-mpx-debian... Тенант	INC-11	Regsvr32_AWL_Bypass
23 июл 17:48	14 июн 23:30	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-10	Regsvr32_AWL_Bypass
23 июл 17:48	23 июл 17:48	23 июл 17:48	MaxPatrol 10	ООО «КиберКр... Тенант	INC-1	Regsvr32_AWL_Bypass
23 июл 17:48	18 мар 12:00	23 июл 17:48	Ручное добав...	ОАО «Инновац... Тенант	INC-14	Regsvr32_AWL_Bypass
23 июл 17:48	15 авг 14:32	23 июл 17:48	Ручное добав...	ООО «КиберКр... Тенант	INC-13	Regsvr32_AWL_Bypass

Реагирование



Установка экспертизы в разных тенантах



- Позволяет централизованно определять состав пакетов экспертизы для тенантов
- Обеспечивает доставку и установку на тенанты, и отображает статус в едином окне

Распространение экспертизы 13

Пакет распространения	Статус	Тенанты	Дата отправки	Дата валидации	Дата созд
Базовый пакет для индивидуальн... 12.0	Доставлен	ООО «Сигнал»	11 ноя	11 ноя	11 ноя
Пакет для корпоративных систем	Отправляется	ЗАО «КиберСигнал», ООО «Кибе...	11 ноя	11 ноя	11 ноя
Экспертиза в защите корпорат... 15.0 ↑	Доставлен	ЗАО «КиберЩит», ОАО «Инновац...	11 ноя	11 ноя	11 ноя
Экспертиза по управлению сетево... 7.0	Доставлен	ООО «ЗащитаДанных»	11 ноя	11 ноя	11 ноя
Экспертиза в защите веб-приложе... 5.0	Валидируется	ОАО «Инновации»	11 ноя	11 ноя	11 ноя

ООО «КиберСигнал» Перейти

Статус	Пакет распространен...	Доставленная версия	Установка	Описание тенанта
В процессе	Пакет для КС	1.0	4 конвейера	Проспект Лунный, дом 22, Казань, 420000

Подготовка к установке

- Назначение установочной ветки cmc_content

Установка в конвейеры

- Cloud-conveyor-1.central-manageme...
- Cloud-conveyor-2.central-manageme...

Установка

Версия 2.0

Статус задачи: Выполнена

Дата запуска: 21 июля, 17:30

Дата завершения: 21 июля, 20:24

Длительность: 158 мин 30 с

Пакет для корпоративных систем

Версия 2.0

Статус: Отправляется

Дата валидации: 11 ноября, 11:24 (Тулин Т.В.)

Дата отправки: 12 ноября, 19:03 (Тулин Т.В.)

Тенанты 4

Название	Версия	Установка
ЗАО «КиберСигнал»	2.0	4 конвейера
ООО «КиберКрепость»	2.0	1 конвейер
ООО «ТехноЩит»	2.0	2 конвейера
ООО «КиберКрепость»	2.0	1 конвейер
ООО «ЗащитаТех»	2.0	Не требуется
ООО «Цифровая Защита»	2.0	1 конвейер
ООО «ТехноБлок»	2.0	2 конвейера

Установка экспертизы в разных тенантах



Распространение экспертизы 13						
СтатусДата отправкиДата валидацииДата созданияТенанты						
Пакет распространения	Статус	Тенанты	Описание	Дата отправки	Дата валидации	
Базовый пакет для ИП	12.0 ✔ Доставлен	ООО «Сигнал»	Описание пакета	11 ноя	11 ноя	
Пакет для КС	2.0 🔄 Отправляется	ЗАО «КиберСиг...	Описание пакета	11 ноя	11 ноя	
Экспертиза для защиты корпо...	15.0 ✔ Доставлен	ЗАО «КиберЩит...	Описание пакета	11 ноя	11 ноя	
Экспертиза для управления сетево...	7.0 ✔ Доставлен	ООО «ЗащитаДа...	Описание пакета	11 ноя	11 ноя	
Экспертиза для защиты веб-прило...	5.0 ✔ Доставлен	ОАО «Инноваци...	Описание пакета	11 ноя	11 ноя	
Экспертиза для анализа угроз	0.0 ⚠ Частично доставлен	«ТенКиБез»	Описание пакета	11 ноя	11 ноя	
Экспертиза для обеспечения безо...	2.0 ⚠ Ошибка доставки	«СПКиБ»	Описание пакета	11 ноя	11 ноя	
Экспертиза для мобильной безопа...	3.0 🔄 Отправляется	«Инновации Буд...	Описание пакета	11 ноя	11 ноя	
Экспертиза для ИП	11.0 🕒 Запланирована отпр	ИП «Страж»	Описание пакета	11 ноя	11 ноя	
Экспертиза для облачных техноло...	9.0 ➡ Готов к отправке	Тенант-1, Тенант...	Описание пакета	—	11 ноя	
Экспертиза для защиты данных	8.0 ⚠ Ошибка валидации	Тенант-1, Тенант...	Описание пакета	—	11 ноя	
Пакеты для облачных решений	6.0 🔄 Валидируется	Тенант-1, Тенант...	Описание пакета	—	11 ноя	
Пакеты для обеспечения безопас...	20.0 🔧 Требуется валидации	Тенант-1, Тенант...	Описание пакета	—	—	

Пакет для КС

Версия 2.0

🔗

➤ Отправить

⬇

✎

🗑

Статус

Дата валидации

Дата отправки

🔄 Отправляется

11 ноября, 11:24

12 ноября, 19:03

Тулин Т.В.

Тулин Т.В.

Тенанты 4

Название	Версия	Установка
🔄 ЗАО «КиберСигнал»	1.0	4 конвейера
✔ ООО «КиберКрепость»	1.0	1 конвейер
✔ ООО «ТехноЩит»	1.0	2 конвейера
✔ ОАО «КБТехнологии»	1.0	Не требуется

Информация о версии

Ветка базы знаний

Наборы для установки

SIEM_Content

Базовый набор

Табличные списки

Высоконагруженная система

Пакет SOC

Установка экспертизы в разных тенантах



☰

🔌

📄

🗨️

📁

← ООО «КиберСигнал» Перейти

Статус

В процессе

Пакет распространен...

Пакет для КС

Доставленная версия

1.0

Установка

4 конвейера

Описание тенанта

Проспект Лунный, дом 22, Казань, 420000

Доставка

Доставка пакета распространения
Версия 2.0

Подготовка к установке

Назначение установочной ветки
cmc_content

Cloud-conveior-1.central-manageme...
Конвейер

Подготовка набора для установки
Базовый набор, Высоконагруженная с...

Валидация
Версия SDK 103.40.60

Установка
Версия 2.0

Cloud-conveior-2.central-manageme...
Конвейер

Подготовка набора для установки
Табличные списки

Валидация
Версия SDK 103.40.60

Установка
Версия 2.0

Cloud-conveior-3.central-manageme...
Конвейер

Подготовка набора для установки
Базовый набор

Валидация
Версия SDK 103.40.60

Установка
Версия 2.0

Cloud-conveior-4.central-manage...
Конвейер

Подготовка набора для устан...
Высоконагруженная система, Пакет

Валидация
Версия SDK 103.40.60

Установка
Версия 2.0

Установка

✕

Версия 2.0

Статус задачи

✔ Выполнена

Дата запуска

21 июля, 17:30

Дата завершения

21 июля, 20:24

Длительность

158 мин 30 с

Журнал выполнения

17:30:10

Инициализация задачи

17:30:15

Проверка связи с конвейером "Cloud-conveior-4.central-management-hub.io:48140"

17:30:20

Связь установлена

17:34:15

Установочная ветка: OK

17:34:15

Набор для установки: OK

17:34:15

Запущен процесс установки

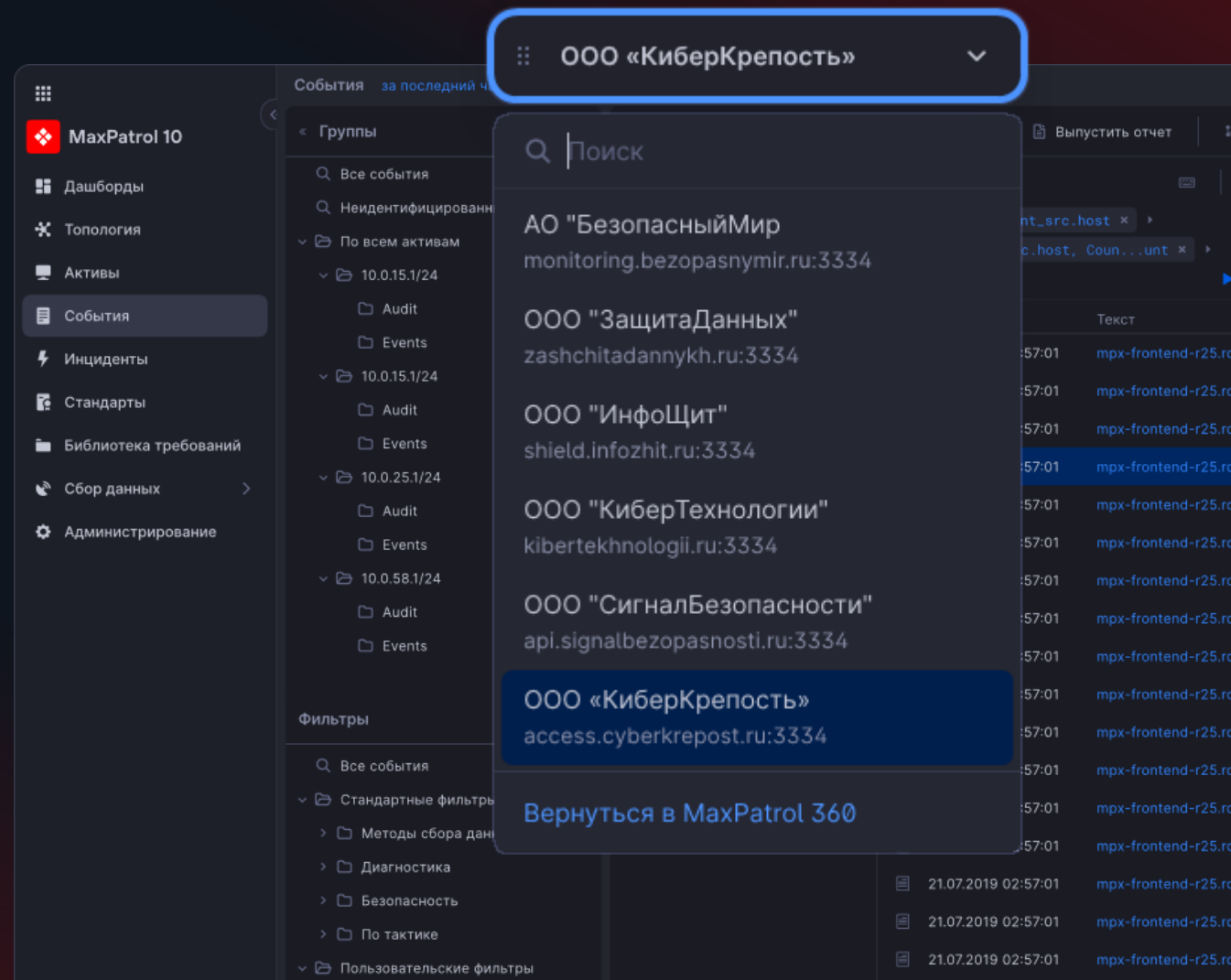
17:34:15

Набор установлен в конвейер "Cloud-conveior-4.central-management-hub.io:48140"

Бесшовный переход к исходным событиям



- MaxPatrol 360 обеспечивает бесшовный переход в подключенные тенанты для детального расследования инцидентов и переход между тенантами с сохранением контекста/состояния в режиме одного окна
- Для этого оператору предоставлен тенант-локатор, который отображает текущее рабочее пространство оператора



Запросы



- Раздел «Запросы» позволяет управлять коммуникацией по дополнительным. активностям, связанным с обработкой инцидента, например расследование подозрения на инцидент, координация устранения инцидента, проведение оценки риска в рамках инцидента и др.
- Запросы могут быть связаны как с конкретными инцидентами, так и использоваться автономно для выполнения иных задач

Запросы 128

Статус Создан Последние 90 дней x

Тенант

Приоритет

Ответственный

Срок выполнения +

Q

Создан	Изменен	Тенант	ID	Название	Ответственный
23 июл 17:48	23 июл 17:48	ООО «КиберКрепость»	REQ-001	Добавление IP в белый список...	Сидоров А.
26 июл 15:45	26 июл 15:45	ЗАО «КиберСигнал»	REQ-007	Фишинговая рассылка, очистка...	Тихонов Л.
26 июл 16:00	26 июл 16:00	ЗАО «КиберСигнал»	REQ-008	Макрос/loader из офисного файла	Соловьев М.
27 июл 10:10	—	ООО «КриптоТехнолог...	REQ-009	Успешный RDP-подбор и латера...	Смирнов Д.
27 июл 11:30	27 июл 11:30	ЗАО «ТехноЗащита»	REQ-010	Подозрительное OAuth-прилож...	Кузнецов В.
28 июл 12:15	28 июл 12:15	ООО «Сетевые Ресур...	REQ-011	Успешный RDP-подбор и латера...	Морозов Ж.
28 июл 13:40	28 июл 13:40	ЗАО «ИнфоТек»	REQ-012	Возможная эксфильтрация в об...	Ковалев Н.
29 июл 14:00	29 июл 14:00	ЗАО «КиберСигнал»	REQ-013	Вредонос в цепочке поставок (б...	Яковлев О.
24 июл 00:15	24 июл 00:15	ООО «ТехноСистемы»	REQ-003	Обновление ОС на сервере	Лебедев З.

Компрометация учётной записи, сброс токенов

REQ-002 · 22 ноября, 18:47:01 · ООО «КиберКрепость»

В работе Прохоров И.

Вы Прохоров И. 13 дек, 14:25

Добрый день! Пишу по инциденту ИБ: зафиксированы признаки компрометации учётной записи ivan.petrov@company.ru в вашем домене.

events_siem_22_10_2025.log

siemScreenshot.jpg

Вы Прохоров И. 13 дек, 12:00

Предлагаю короткий план из 6 шагов:

1. Заблокировать учётную запись в AD/IDM.

2. Принудительно выйти из всех сессий и сбросить refresh-токены / куки / OAuth-сессии.

3. Отозвать/удалить все активные API-токены и персональные ключи этого пользователя в критичных системах.

4. Сбросить пароль администратором, включить/создать включить MFA, передать новые данные по

Описание

Повод для расследования:

В логах — успешные входы/обновления токенов с нетипичных IP/устройств.

Есть действия от имени пользователя, которые он не подтверждает.

Область анализа:

Auth/SSO логи: login, mfa, token_issue/refresh, logout.

Audit log приложения, API Gateway/WAF (IP/UA).

Интервал: 26.12.2025 08:30–11:30 UTC + baseline 7 дней.

Дополнительно:

Ранее похожие кейсы: утечка refresh token/расширение браузера (пример).

Недавние изменения: политика сессий/MFA/TTL (если было).

Уже проверено: это не сервисный

Запросы



Для этого достаточно определить набор необходимых действий, задать приоритеты и сроки, назначить ответственных и отслеживать статус выполнения

Новый запрос

✕

Категория *

Расследование

Название *

Компрометация учётной записи, сброс токенов

Описание

Повод для расследования:

- В логах — успешные входы/обновления токенов с нетипичных IP/устройств.
- Есть действия от имени пользователя, которые он не подтверждает.

Наблюдаемые симптомы:

- Алерты: "new device / unusual location / impossible travel".
- Скачок token_refresh / проверок сессии.
- Audit: нетипичные действия (экспорт/изменение настроек/создание ключа — если применимо).

Ожидаемый результат расследования:

- Подтвердить/опровергнуть компрометацию.
- Понять вектор: пароль vs токен/сессия vs OAuth/ключ.
- Рекомендации по containment и предотвращению.

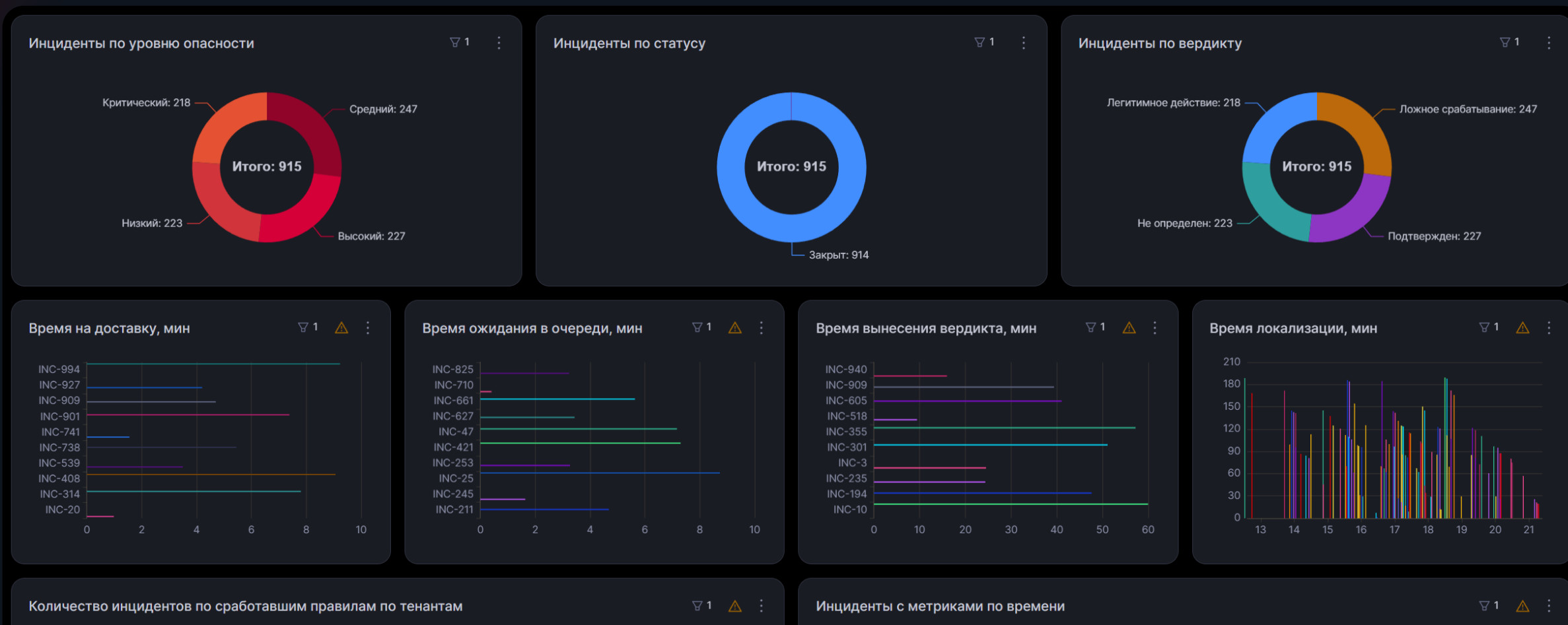
Ограничения и приоритет:

- Дедлайн: первичное заключение в течение 2 часов.
- Критичность: высокая → сразу ревокировать токены/сессии, step-up MFA/временная блокировка до выяснения.

Дашборды



- MaxPatrol 360 предоставляет возможность мониторинга ключевых метрик и их динамики на дашбордах, включая оценку текущего индекса защищенности, контроль инцидентов, находящихся в работе, а также скорость и качество их обработки



Дашборды



Инциденты по операторам



Количество инцидентов по дням по заказчикам



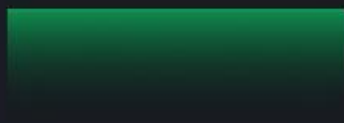
Среднее время
вынесения вердикта

59
минут



Процент выполнения
SLA для QWT

100



SLA для QWT



Поток обработки инцидентов

403

Среднее время
реагирования

97
минут

Широкие возможности по интеграции



- MaxPatrol 360 позволяет гибко подстраиваться под потребности любой IT-инфраструктуры за счет открытого API: сбор, обогащение, дополнительная аналитика

 **Swagger**
Supported by SMARTBEAR

Select a definition

v1

Incidents public API

v1 OAS 3.0

Authorize

.../app/im/api/incidents/swagger/v1/swagger.json

Incidents public API

Incidents

POST

/app/im/api/incidents/public/v1/incidents

Create incident from external source

🔒

▼

GET

/app/im/api/incidents/public/v1/incidents/{incidentId}

Get incident by id

🔒

▼

GET

/app/im/api/incidents/public/v1/incidents/{incidentId}/events

Get incident events

🔒

▼

POST

/app/im/api/incidents/public/v1/incidents/{incidentId}/artifacts

Add artifacts to incident

🔒

▼

GET

/app/im/api/incidents/public/v1/incidents/{incidentId}/tenant-id

Get incident tenant id

🔒

▼

Мониторинг и реагирование

Взаимодействие с CERT

Поиск угроз

Управление активными угрозами

SIEM



MaxPatrol 360

1

Охватывает ключевые процессы SOC

2

Агрегирует данные из всех источников

3

Собирает данные и события

Взаимодействие с внешними контрагентами

Взаимодействие с внутренними службами компании

Другие СЗИ

VM

Анализ рисков ИБ

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

Условия лицензирования

Базовая функциональность

Централизованная работа с инцидентами ИБ	₽ / актив
--	-----------

Централизованная работа с экспертизой	₽ / арендатор
---------------------------------------	---------------

Расширенная

Количество интеграций	₽ / интеграция
-----------------------	----------------

BI-дашборды	₽ / актив
-------------	-----------

Сценарии	₽ / актив
----------	-----------

Запросы (service desk)	₽ / арендатор
------------------------	---------------

Интеграция ГОССОПКА	₽ / коннектор
---------------------	---------------

Интеграция ФИНЦЕРТ	₽ / коннектор
--------------------	---------------



Roadmap MaxPatrol 360



Планы на Q2 2026

- Каталог действий для сценариев: реагирование через EDR
- Реализация тикет-системы: сервис «Запросы» для организации работ по инцидентам
- Разработка шаблонов уведомлений для реализации функции «Нотификации», в том числе для разных каналов информирования
- Базовые дашборды и возможность формирования отчетов по метрикам инцидентов
- Public API для работы с инцидентами и добавления инцидентов из сторонних источников
- Федерация MaxPatrol 360: синхронизации инцидентов между самостоятельными инсталляциями MaxPatrol 360



Roadmap MaxPatrol 360

2026

Беклог

- Импорт/экспорт инцидентов из UI
- Каталог действий для плейбуков: реагирование через AD, NGFW
- Каталог действий для плейбуков: расширение базового набора плейбуков
- Интеграции: внешние системы обогащения, расследования, реагирования
- Интеграции: подключение сторонних источников инцидентов
- Лицензирование MaxPatrol 360. Энфорсмент
- «Запросы». Расширение функционала. Интеграция с сервисом плейбуков
- Старая версия IM больше не включается в поставки MaxPatrol 10
- Централизованные дашборды с фильтрацией по тенантам
- Развитие AI/ML инструментов автоматизации расследования и реагирования
- Интеграция работы с активами в MaxPatrol 360

Планы, начинающиеся с третьего квартала 2026, гибко пересматриваются с учётом запросов рынка, бизнес-целесообразности и обратной связи клиентов и партнёров

Как попробовать?



Оставьте
заявку

на сайте
MaxPatrol 360
или свяжитесь
с вашим менеджером
в Positive Technologies

Подпишите NDA,
заполните анкету
по инфраструктуре

Разверните
MaxPatrol 360
в инфраструктуре:

установить и
настроить
систему помогут
наши
специалисты

Проведите
пилотный проект
и оцените результаты

вместе
со специалистами
Positive
Technologies

Вместо десятков инструментов – единый MaxPatrol 360



Оставить заявку
на пилот

