

MaxPatrol 360

Единый центр управления расследованиями
и операционной работой SOC

MaxPatrol 360 помогает команде ИБ быстрее
расследовать инциденты, снижать объем ручных
операций и централизованно управлять
безопасностью в распределенной инфраструктуре.



Что меняется после внедрения

-  Команда SOC работает в едином интерфейсе,
без переключения между системами
-  Инциденты проходят полный цикл —
от обнаружения события до устранения
-  Рутинные задачи автоматизируются
через плейбуки
-  Сокращается время расследования
и реагирования

Прирост
эффективности
команды ИБ*

+50%

Как работает

Встроенные интеграции

API

Что умеет



MaxPatrol SIEM

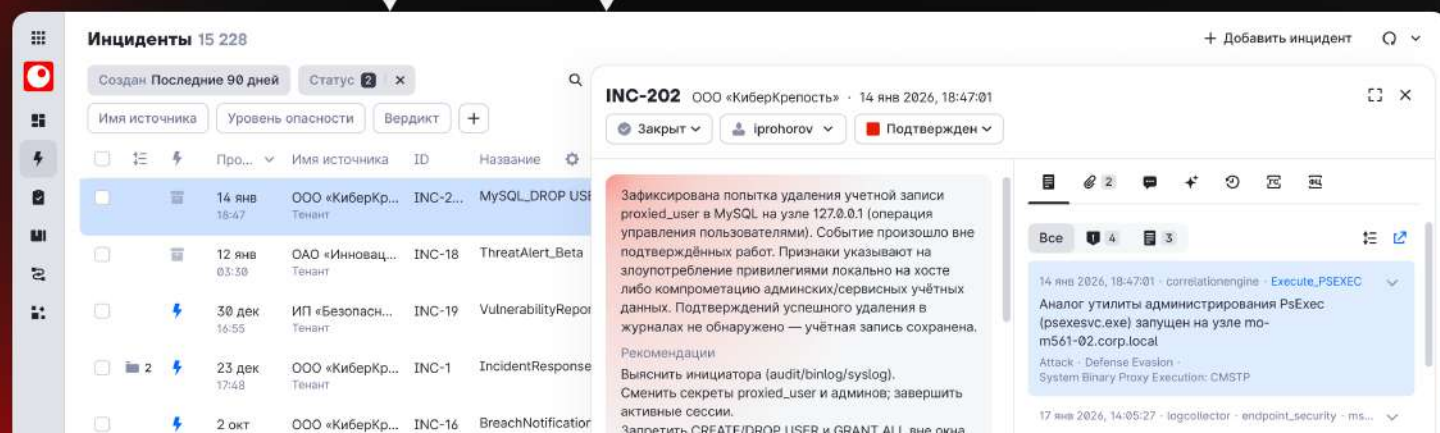
-  MaxPatrol EDR
-  MaxPatrol VM
-  PT NAD



Другие
системы

-  Прозрачность
-  Обнаружение
-  Восстановление
-  Защита
-  Реагирование
-  Консолидация

MaxPatrol 360



Инциденты 15 228

Создан Последние 90 дней Статус 2 x

Имя источника Уровень опасности Вердикт +

	Про...	Имя источника	ID	Название
☐	14 янв 18:47	ООО «КиберКр... Тенант	INC-2...	MySQL_DROP US...
☐	12 янв 03:30	ОАО «Инновац... Тенант	INC-18	ThreatAlert_Beta
☐	30 дек 16:55	ИП «Безопасн... Тенант	INC-19	VulnerabilityRepo
☐	23 дек 17:48	ООО «КиберКр... Тенант	INC-1	IncidentResponse
☐	2 окт	ООО «КиберКр... Тенант	INC-16	BreachNotification

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

Закрыт iprohorov Подтвержден

Зафиксирована попытка удаления учетной записи proxied_user в MySQL на узле 127.0.0.1 (операция управления пользователями). Событие произошло вне подтверждённых работ. Признаки указывают на злоупотребление привилегиями локально на хосте либо компрометацию админских/сервисных учётных 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.

Заполнить CREATE/DROP USER и GRANT ALL в базе...

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

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

Attack - Defense Evasion - System Binary Proxy Execution: CMSTP

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

Какие задачи решает MaxPatrol 360



Управление расследованиями SOC в одной системе

Все события, инциденты, расследования и действия аналитиков собираются в едином рабочем процессе



Масштабирование SOC без роста штата

Поддержка мультитенантности позволяет централизованно управлять десятками инфраструктур внутри одной системы



Автоматизация реагирования и рутинных операций

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



Интеграция решений

Синергия с продуктами экосистемы Positive Technologies и другими решениями, предоставляющими информацию об инцидентах

Кому подойдет



Крупному бизнесу
с распределенной
инфраструктурой



Провайдерам услуг
безопасности
(MSSP)



Организациям — субъектам КИИ,
обязанным организовать взаимодействие
с НКЦКИ

Узнайте обо всех
возможностях MaxPatrol 360

