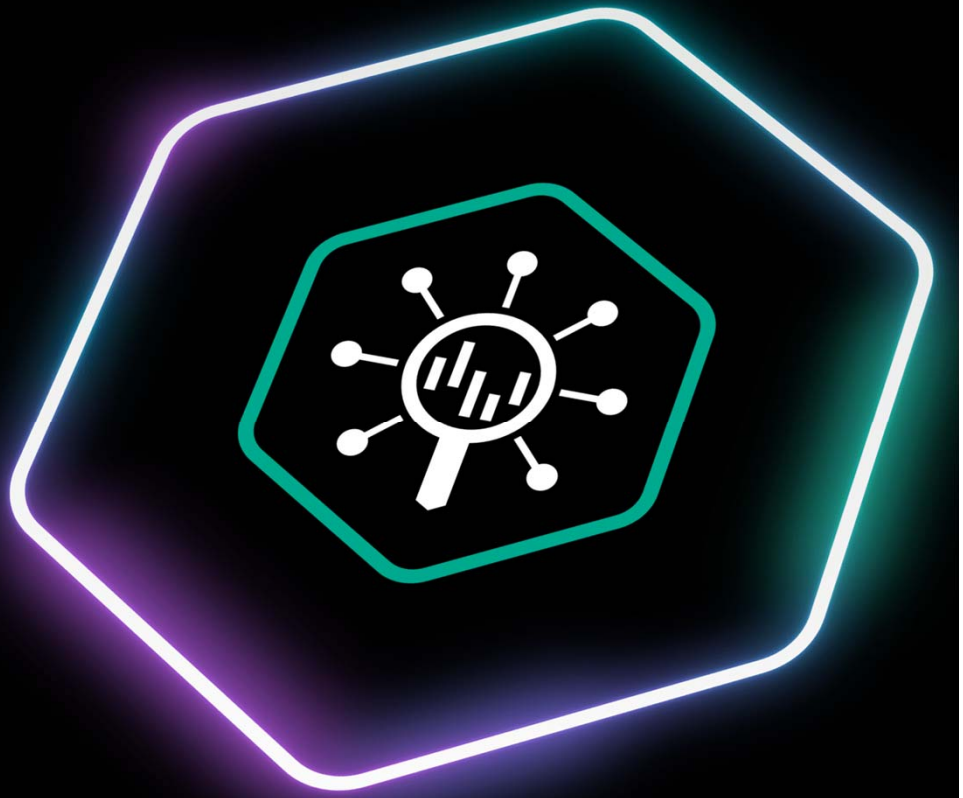
Kaspersky Unified Monitoring and Analysis Platform

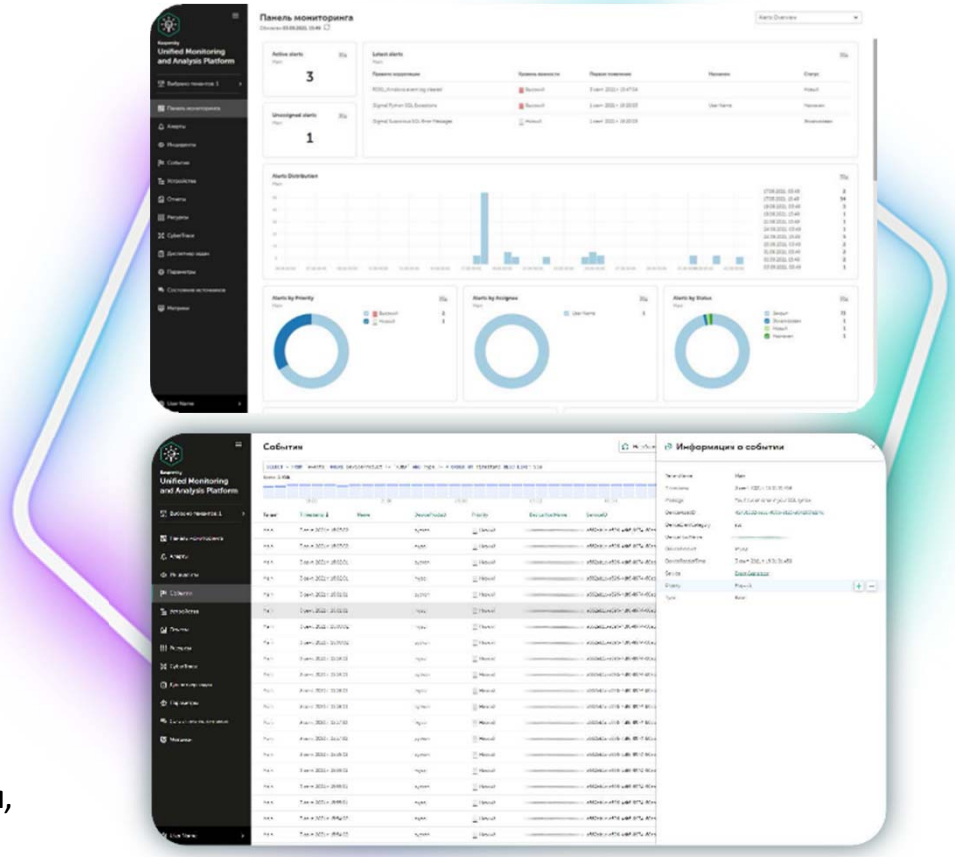


Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Мониторинг ИБ

- Сбор событий со всех подключенных источников данных в инфраструктуре
- Универсальный инструмент по нормализации, фильтрации и агрегации данных
- Встроенное потоковое обогащение исходных событий аналитическими данными об угрозах (Kaspersky Cybertrace*, Threat data feeds*)
- Корреляция событий и выявление комплексных инцидентов ИБ
- Интуитивно понятный интерфейс для обнаружения, расследования и реагирования на инциденты ИБ



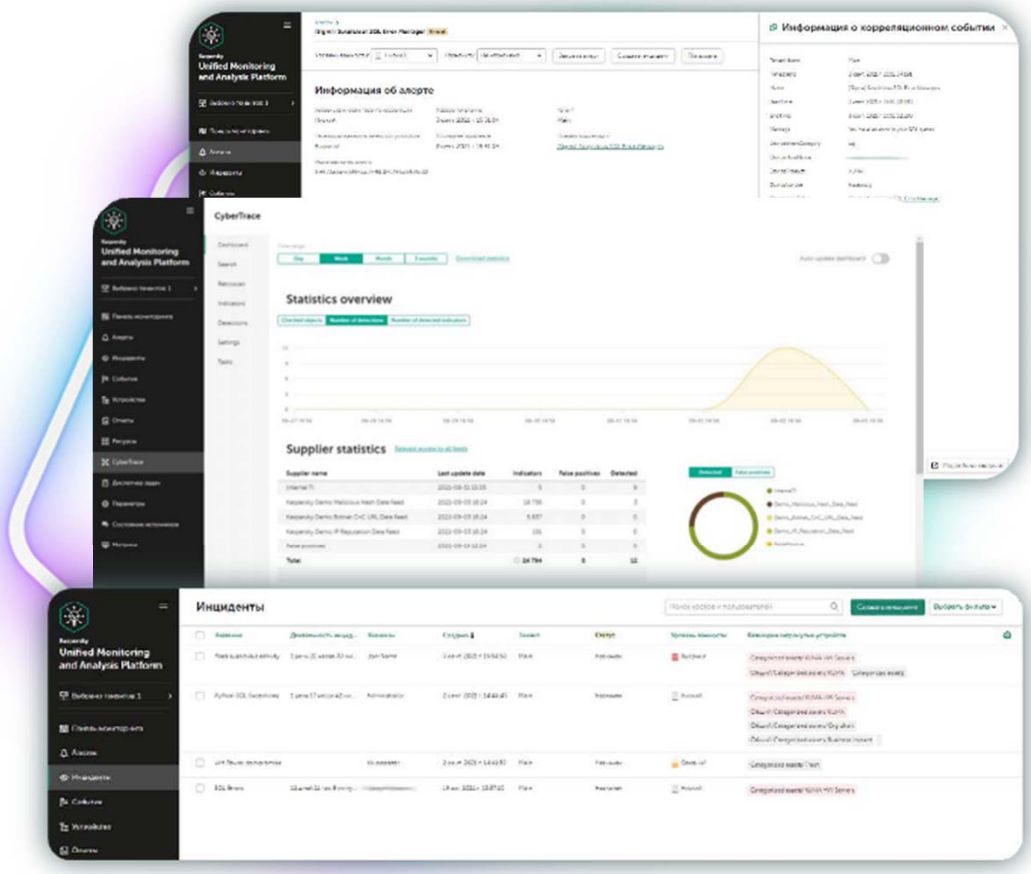
*Лицензируется дополнительно

ПОЛИКОМ про

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Расследование инцидентов

- Подробная информация об алертах, связанные события
- Приоритизация срабатываний и возможность объединения алертов в единый инцидент для ускорения процесса расследования
- Встроенный пакет правил корреляции с меппингом на MITRE ATT & CK
- Встроенная аналитика Threat Intelligence (Kaspersky Threat Lookup)* для повышения эффективности расследования



*Лицензируется дополнительно

ПОЛИКОМ про

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Реагирование на инциденты

- Оперативное уведомление об случившихся инцидентов на почту
- Управление агентами на рабочих местах для реагирования на выявленные инциденты через KSC
- Интеграция с Kaspersky EDR* обеспечивает Возможность централизированного автоматического реагирования на конечных устройствах по результатам расследования инцидента
- Возможность интеграции с решениями сторонних поставщиков для обеспечения автоматического реагирования

*в ближайших планах разработки

ПОЛИКОМ про

Соответствие требованиям регуляторов

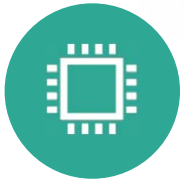
Соответствие

- Сбор и централизованное хранение данных и информации, связанными с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ
- Интегрированный модуль ГосСОПКА
- Обеспечение части мер по обеспечению безопасности для значимых объектов КИИ (ФСТЭК №239)
- Соблюдение рекомендаций со стороны ФинЦЕРТ
- Помощь в соответствии требованиям ГОСТ 57580.1 – 2017 (безопасность финансовых (банковских) операций

Интегрированный модуль ГосСОПКА

ПОЛИКОМ про

Ключевые преимущества



Высокая производительность

300k+EPS на один узел

Масштабируемость

гибкая микросервичная архитектура

Низкие системные требования

Интеграция «из коробки»

с продуктами сторонних поставщиков и решения «Лаборатории Касперского»

Встроенное обогащение

Встроенные действия по реагированию

ПОЛИКОМ про

kaspersky
Platinum Partner

Благодарю за внимание!

Руководитель направления решений
«Лаборатории Касперского»
Михаил Усачёв

тел: + 7 (812) 325 84 00
моб: + 7 911 929 60 04

e-mail: Mikhail.Usachev@polikom.ru

ПОЛИКОМ про