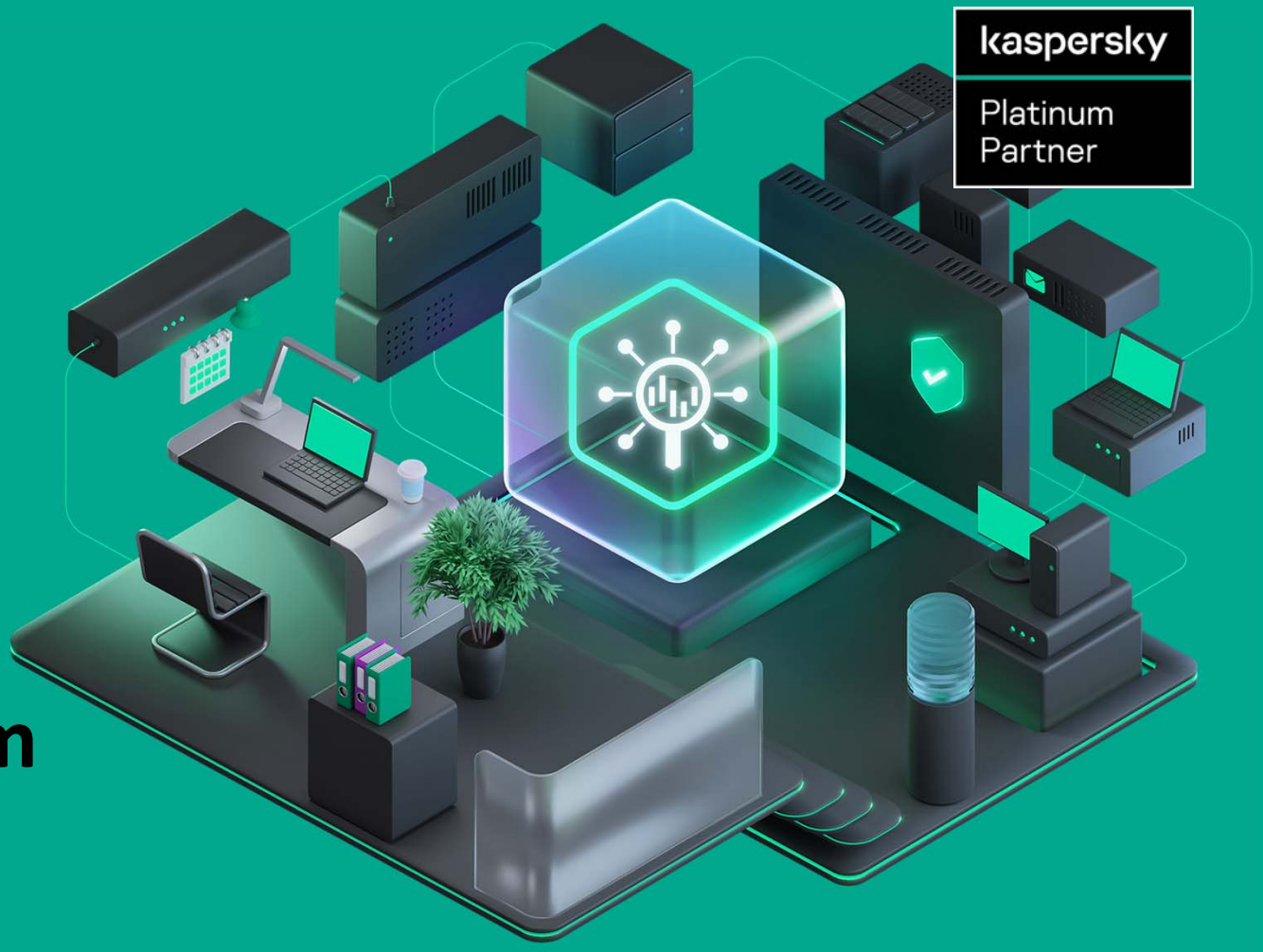
Kaspersky
Unified Monitoring and Analysis Platform



kaspersky
Platinum Partner

Руководитель направления решений
«Лаборатории Касперского»
Михаил Усачев

ПОЛИКОМ про

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Kaspersky Security
для бизнеса

Kaspersky
Endpoint Detection
and Response

Kaspersky
Anti Targeted Attack

Kaspersky Security
для интернет-шлюзов

Kaspersky Security
для почтовых серверов

Единая консоль мониторинга и анализа инцидентов ИБ

Kaspersky
Unified Monitoring and Analysis Platform

Решения сторонних производителей

Kaspersky
Security Center

Kaspersky
Threat Data Feeds

Kaspersky
CyberTrace

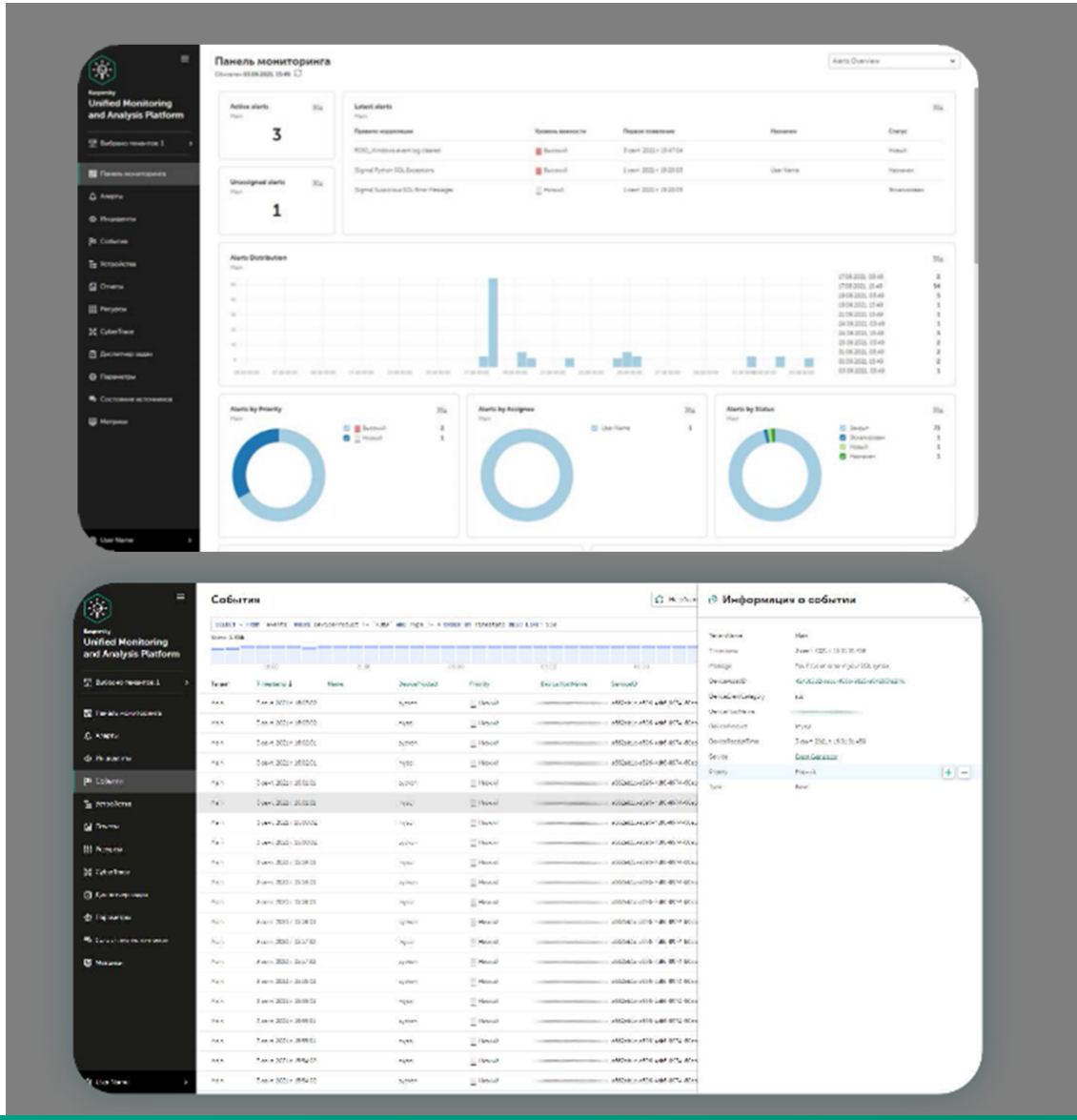
Kaspersky
Threat Loockup

Kaspersky
Industrial CyberSecurity

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

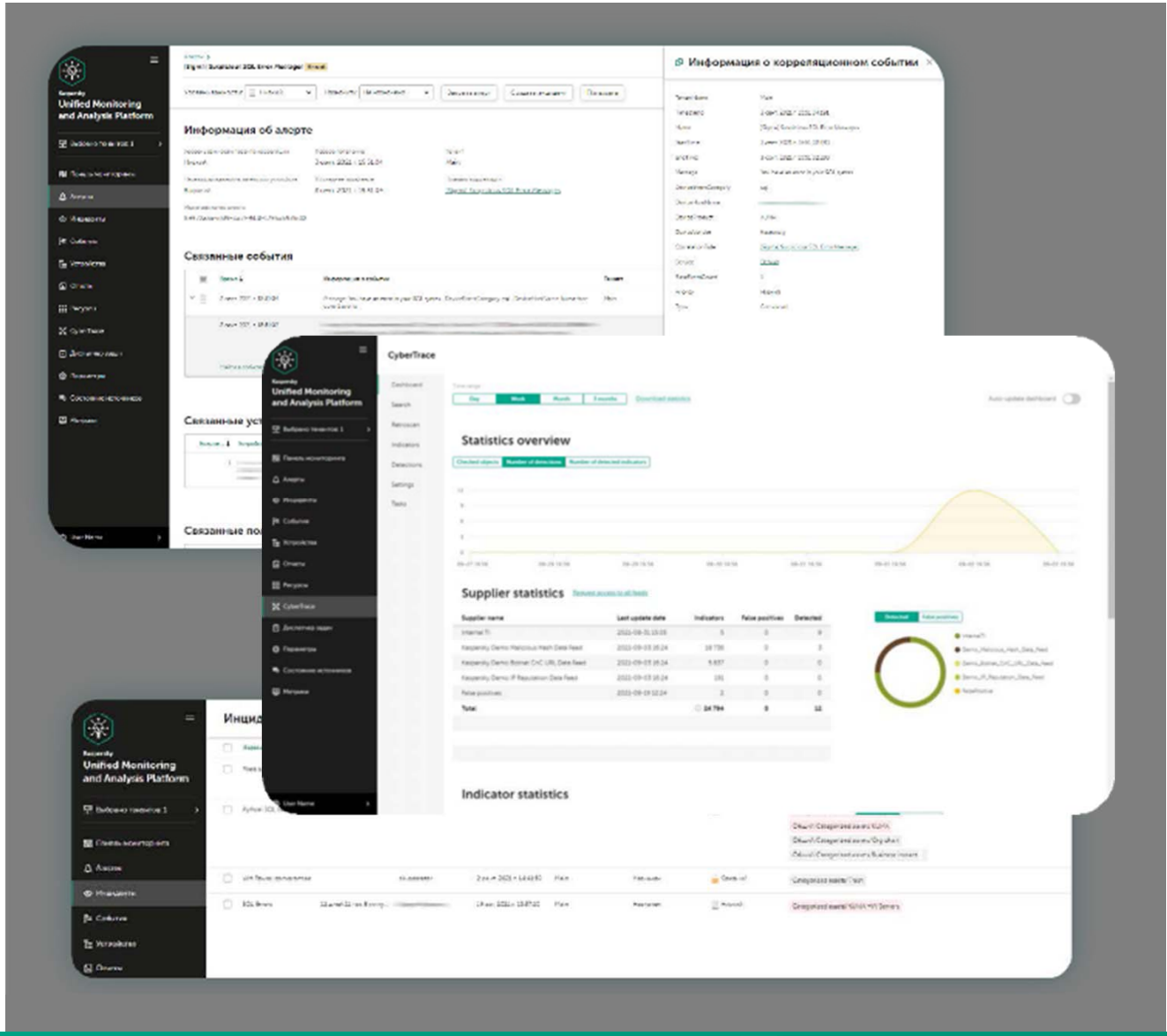
*Лицензируется дополнительно



Расследование инцидентов

Расследование

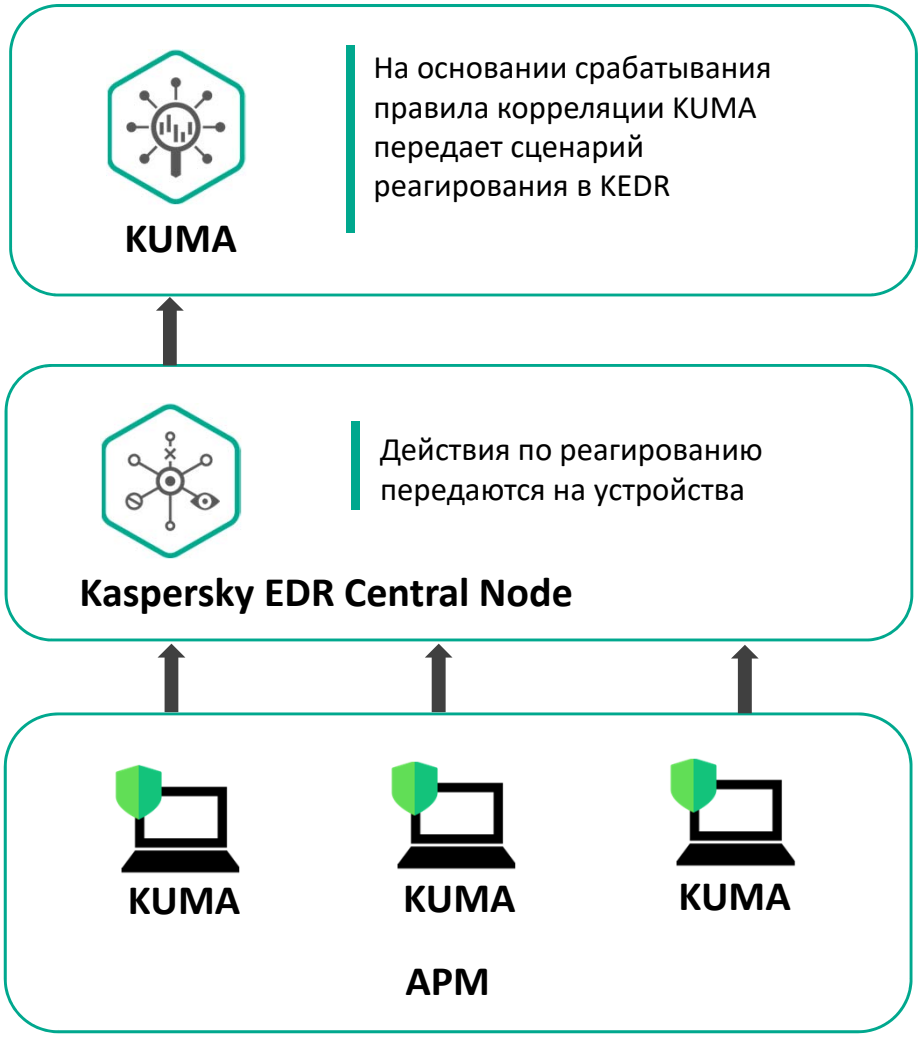
- Подробная информация об алертах, связанные события
- Приоритизация срабатываний и возможность объединения алертов в единый инцидент для ускорения процесса расследования
- Встроенный пакет правил корреляции с меппингом на MITRE ATT&CK
- Встроенная аналитика Threat Intelligence (Kaspersky Threat Lookup)*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



Реагирование на инциденты

Реагирование

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



Соответствие требованиям регуляторов

• Сбор и централизованное хранение данных и информации, связанной с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ, предоставляя им необходимую информацию об обнаруженных угрозах

• 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)

ГОССОПКА

Интегрированный модуль ГосСОПКА

Ключевые преимущества

Высокая производительность
300k +EPS на один узел

Низкие системные требования

Встроенное обогащение

Масштабируемость
Гибкая микросервисная архитектура

Интеграция «из коробки»
С продуктами сторонних поставщиков и решениями «Лаборатории Касперского»

Встроенные действия по реагированию

Примерный сайзинг

До 2k EPS
30 дней хранения

ALL-in-one
- CPU – 12vCPU
- RAM – 32 ГБ
- Storage – 4 ТБ

До 5k EPS
180 дней хранения

Коллектор
+ Коррелятор
+ Ядро
- CPU – 16 vCPU
- RAM – 32 ГБ
- Storage – 1.5 ТБ

Хранилище
- CPU – 16 vCPU
- RAM – 32 ГБ
- Storage – 20 ТБ

20k EPS
365 дней хранения

Ядро
- CPU: 8 Vcpu
- RAM: 12 GB
- Disk: 500 GB

Коррелятор
- CPU: 8 vCPU
- RAM: 32 GB
- Disk: 500 GB

Zookeeper – 3
- 4 vCPU
- 6 RAM
- 500 GB

Коллектор
- CPU: 8 vCPU
- RAM: 16 GB
- Disk: 500 GB

Хранилище x 4
- CPU: 32 vCPU
- RAM: 128 GB
- Disk: 57 TB

Kaspersky Symphony XDR

Защита конечных точек

Kaspersky Symphony EDR

Kaspersky
Endpoint Detection
and Response

+

Kaspersky Symphony Security

Kaspersky Endpoint Security
для бизнеса Расширенный

Kaspersky Security
для виртуальных
и облачных сред

Интеграция с решениями
сторонних производителей

Kaspersky
Unified Monitoring
and Analysis
Platform

Защита на уровне сети

Kaspersky
Anti Targeted Attack

Kaspersky Security
для почтовых серверов

Kaspersky Security
для интернет-шлюзов

Обучение пользователей

Kaspersky Automated Security
Awareness Platform

Threat Intelligence

Kaspersky
Cyber Trace

Kaspersky
Threat Data Feeds

Kaspersky
Cyber Trace

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