kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Unified Monitoring
and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform

Сложность и масштаб кибератак, а также ущерб от них растут с каждым днем. Злоумышленники используют все более изощренные техники и тактики для проникновения в ИТ-инфраструктуру организации и сокрытия факта компрометации. Разрозненные средства защиты информации оказываются малоэффективны против хорошо скоординированных атак. Для противодействия современным угрозам система информационной безопасности должна функционировать как единое целое – подобно иммунной системе организма.

Более 20 лет практического опыта «Лаборатории Касперского» и технологии в области создания средств защиты информации, противодействия целевым атакам и анализа вредоносного ПО легли в основу решения Kaspersky Unified Monitoring and Analysis Platform (KUMA). Решение является одним из основных компонентов единой платформы безопасности для обнаружения и анализа современных сложных атак и угроз ИБ и реагирования на них.

Ключевые преимущества

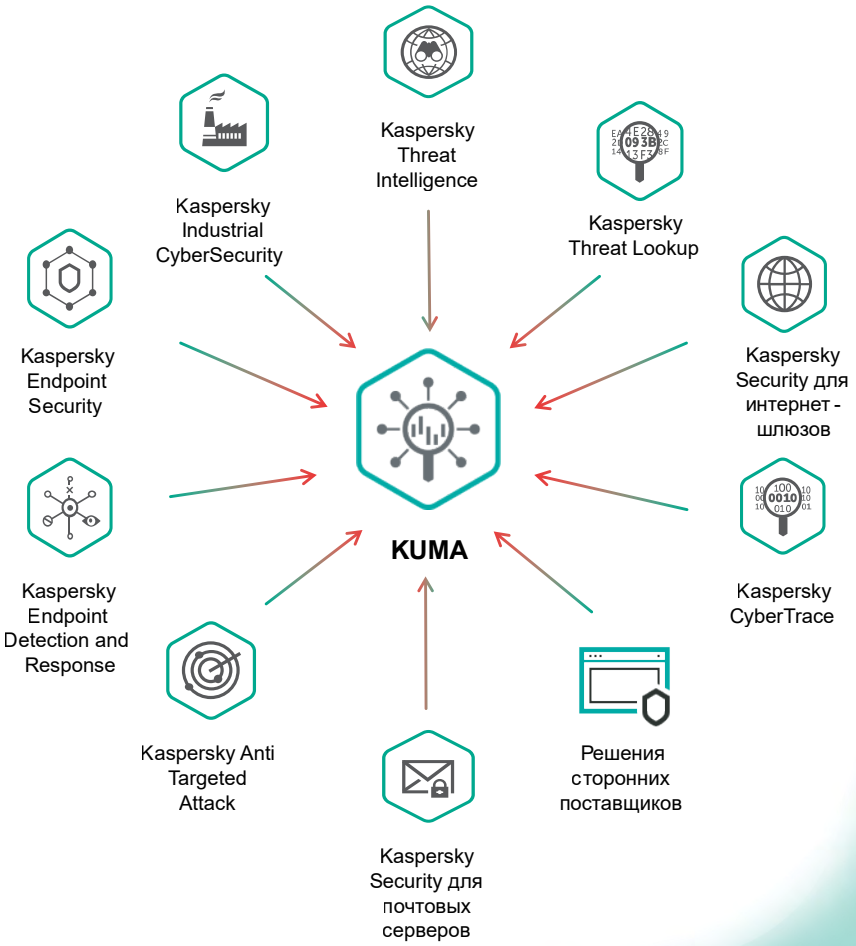
Комплексная экосистема безопасности
Kaspersky Unified Monitoring and Analysis Platform (KUMA) – решение класса SIEM (Security information and event management), предназначенное для централизованного сбора, анализа и корреляции событий информационной безопасности с различных источников данных. Решение обеспечивает единую консоль мониторинга, анализа и реагирования на угрозы ИБ, объединяя как решения «Лаборатории Касперского», так и сторонних производителей.

Система поддерживает интеграцию с следующими продуктами «Лаборатории Касперского»:

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection & Response
- Kaspersky Security Center
- Kaspersky Security для бизнеса
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов
- Kaspersky CyberTrace
- Kaspersky Threat Data Feeds
- Kaspersky Threat Lookup
- Kaspersky Industrial Cybersecurity for Nodes
- Kaspersky Industrial Cybersecurity for Networks

А также с решениями сторонних поставщиков, например:

- Windows Event Log
- Palo Alto NGFW, Panorama
- Check Point R80.20
- Cisco ASA, WSA
- FortiGate UTM
- FortiAnalyzer
- Windows OS
- VipNet Coordinator
- Dovecot
- VmWare
- Linux
- FreeBSD
- Exim
- Squid

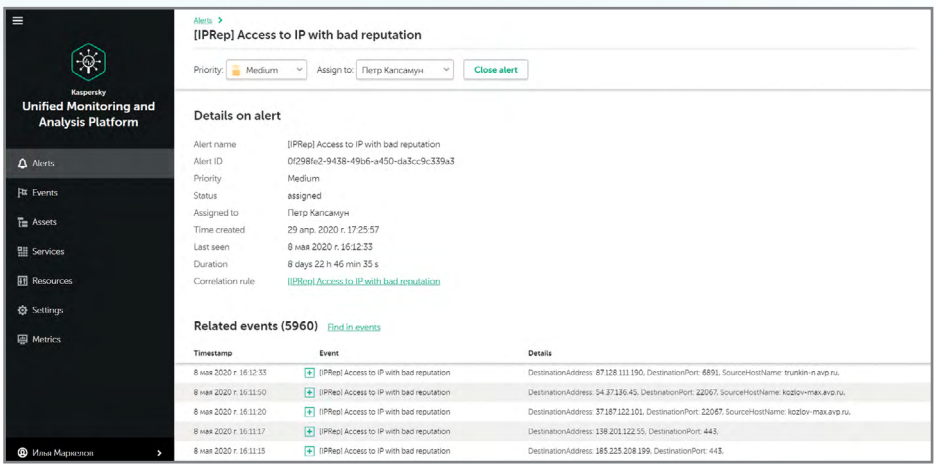


Помимо этого, благодаря наличию у решения гибкого API, возможна интеграция с продуктами сторонних поставщиков, такими как платформы реагирования на инциденты, системы регистрации и учета заявок, сканеры защищенности и другими.

Потоковая корреляция в реальном времени

Решение Kaspersky Unified Monitoring and Analysis Platform обеспечивает централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ в реальном времени и своевременное оповещение об инцидентах.

Высокопроизводительный потоковый движок корреляции обеспечивает производительность более 300 тысяч событий в секунду (EPS) на один узел корреляции. Модульная архитектура решения позволяет еще больше увеличить общую производительность за счет балансировки и распределения нагрузки между компонентами.



Модульная архитектура

Решение Kaspersky Unified Monitoring and Analysis Platform было специально разработано для работы в современных динамично изменяющихся и высоконагруженных ИТ-средах.

Модульная микросервисная архитектура решения позволяет легко изменять конфигурацию системы, обеспечивая масштабируемость, отказоустойчивость и гибкость вариантов развертывания.

Интеграция с Kaspersky Threat Intelligence

«Лаборатория Касперского» обладает одной из наиболее полных и достоверных баз данных Threat Intelligence. Глобальная база Kaspersky Threat Intelligence постоянно обновляется данными из облачной репутационной сети Kaspersky Security Network (более чем 100 млн сенсоров в 200+ странах), результатами ручного анализа APT, оперативными данными из Даркнета, результатами анализа новых экземпляров вредоносного программного обеспечения (более 400 тысяч в сутки).

Решение поддерживает интеграцию «из коробки» с платформой Kaspersky CyberTrace для агрегации и управления потоками данных об угрозах, а также с облачной онлайн-платформой для расследования инцидентов и анализа угроз Kaspersky Threat Intelligence Portal.

Доступ к экспертизе «Лаборатории Касперского»

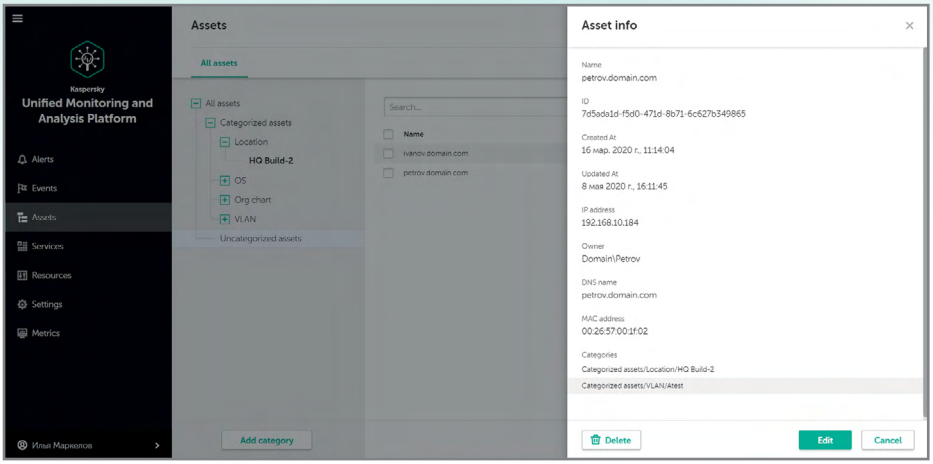
Kaspersky Unified Monitoring and Analysis Platform поставляется с готовым набором детектирующей логики. Аналогичная детектирующая логика и правила корреляции используются как в SOC «Лаборатории Касперского», так и в коммерческих сервисах Threat Hunting.

В отличие от стандартных правил корреляции, детектирующая логика KUMA основана на практическом опыте «Лаборатории Касперского» по противодействию самым изощренным угрозам и многократно подтвердила свою эффективность в реальной инфраструктуре.

Автоматический сбор информации о конечных точках

Одна из самых актуальных проблем при расследовании инцидентов – недостаток информации и контекста об информационных активах организации.

Автоматизированное обнаружение и инвентаризация хостов в сети позволяет решить эту проблему. Решение Kaspersky Unified Monitoring and Analysis Platform с помощью агента Kaspersky Endpoint Security в автоматизированном режиме получает полную информацию о конечных точках (в том числе сведения о уязвимостях на рабочих станциях), а также любых изменениях, произошедших с ними. Данная информация может использоваться для корреляции событий ИБ с учетом контекста, а также и при расследовании инцидентов.



Автоматизированное реагирование на инциденты

В ситуациях критических инцидентов, таких как, например, массовое распространение шифровальщиков в инфраструктуре – счет идет на секунды. Важно максимально быстро локализовать инцидент и тем самым ограничить ущерб для организации.

Интеграция системы KUMA с решением Kaspersky Endpoint Detection and Response позволяет организовать автоматическое или полуавтоматическое реагирование (решение принимает оператор) на критические инциденты и минимизировать ущерб для бизнес-процессов организации.

Решения для крупного бизнеса:
kaspersky.ru/enterprise

www.kaspersky.ru