



Экспертная защита для
вашего бизнеса

Kaspersky Unified Monitoring and Analysis Platform

kaspersky

АКТИВИРУЙ
БУДУЩЕЕ

Экспертная защита для вашего бизнеса

Актуальные ИБ-задачи

Противодействие сложным угрозам
в киберагрессивной среде

Замещение ушедших поставщиков
в сжатые сроки

Соответствие требованиям
регуляторов

Решение KUMA

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — высокопроизводительное решение класса SIEM российского производства, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации.

Комплексная защита

Kaspersky Unified Monitoring and Analysis Platform объединяет продукты «Лаборатории Касперского» и сторонних поставщиков в единую систему ИБ и является ключевым компонентом на пути реализации комплексного защитного подхода, способного обезопасить от актуальных киберугроз не только по отдельности корпоративную или промышленную среду, но и наиболее эксплуатируемый злоумышленниками стык IT/OT-систем.

Также Kaspersky Unified Monitoring and Analysis Platform помогает подойти комплексно к вопросу соответствия требованиям законодательства в области обеспечения безопасности объектов КИИ. В частности, встроенный модуль ГосСОПКА позволяет напрямую обмениваться данными об инцидентах с НКЦКИ.

Кибербезопасность
на стыке IT / OT-систем



Корпоративная
безопасность



Kaspersky
Symphony

XDR



Kaspersky
Unified Monitoring
and Analysis



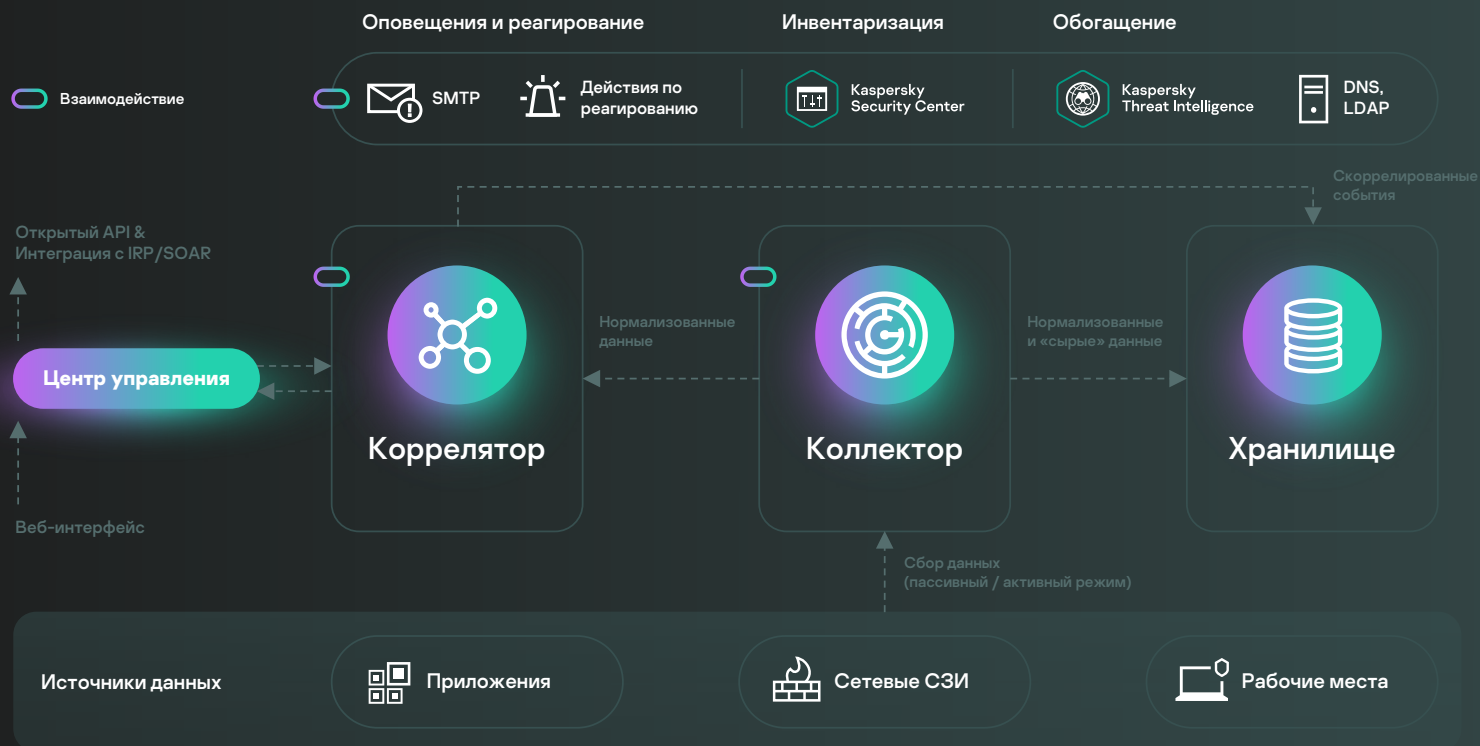
Промышленная
безопасность



Kaspersky
Industrial
CyberSecurity

XDR

Архитектура решения



Интеграция «из коробки»

Kaspersky Unified Monitoring and Analysis Platform поддерживает следующую интеграцию:

Программное обеспечение с открытым исходным кодом

Unbound, Dovecot, Nginx, Apache, DNS BIND, pfSense (с OpenVPN), Exim, Squid, Postfix и др.

Ключевые продукты от различных поставщиков

Microsoft, Palo Alto Networks, Cisco, Juniper, TrendMicro, VMWare, «Код безопасности», CheckPoint, Fortinet, Positive Technologies, Infotecs, InfoWatch, «Бастия», Huawei, Oracle, MikroTik, «Бифит», 1С, «С-Терра» и др.

Операционные системы

Windows, Linux, FreeBSD

Интеграция IRP / SOAR

Security Vision, R-Vision

Поддерживаемые способы сбора и получения событий

Netflow, Kafka, NATS, SQL, TCP, UDP, HTTP, Files, SNMP, WMI и др.

Благодаря наличию у решения гибкого API возможна интеграция с широким набором продуктов сторонних поставщиков, в том числе с платформой реагирования на инциденты, системой регистрации и учета заявок, сканером защищенности и многими другими продуктами.



Интеграция с продуктами «Лаборатории Касперского»

Kaspersky Unified Monitoring and Analysis Platform обменивается информацией с решениями и технологиями «Лаборатории Касперского», что позволяет связать установленные у вас продукты «Лаборатории Касперского» и сделать их работу **еще эффективнее.**

Решение

Как связано с KUMA



Kaspersky
Security Center

Автоматический сбор инвентаризационной информации: установленное ПО, уязвимости, оборудование, владелец актива и т. д. Агрегация оповещений об угрозах, а также управление агентами на рабочих местах для реагирования на выявленные инциденты. Установка патчей для выявленных уязвимостей



Kaspersky
Total Security
для бизнеса

Оповещения об угрозах, обнаруженных на рабочих станциях



Kaspersky
EDR Expert

Централизованный сбор оповещений о продвинутых угрозах и АPT-атаках на уровне рабочих мест, а также поддержка передачи сырой телеметрии для более широких возможностей по расследованию и проактивному поиску угроз. В рамках лицензии Kaspersky Symphony XDR предоставляется реагирование с использованием возможностей EDR-агентов как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции)



Kaspersky
Anti Targeted
Attack

Централизованный сбор оповещений о продвинутых угрозах и АPT-атаках на уровне сети



Kaspersky
Security для
интернет-шлюзов

Оповещения об угрозах, обнаруженных веб-шлюзом



Kaspersky
Security для
почтовых серверов

Оповещения об угрозах, обнаруженных почтовым шлюзом



Kaspersky
CyberTrace

Потоковое обогащение событий ИБ контекстом и предоставление информации в интерфейсе Kaspersky Unified Monitoring and Analysis Platform. Накопление собственных знаний об угрозах, полученных в процессе расследования инцидентов, и управление этими знаниями



Kaspersky
Threat Data
Feeds

Источник контекстной информации по новым угрозам, индикаторам компрометации, тактикам и техникам злоумышленников, а также доступ к аналитическим отчетам об АPT-угрозах, об угрозах для финансовых организаций и промышленных предприятий



Kaspersky
Threat Lookup



Kaspersky
Industrial
CyberSecurity

Оповещения об угрозах, обнаруженных в промышленных технологических сетях, а также поддержка сценариев инвентаризации активов и реагирования



Всесторонняя защита

Это комплексное решение помогает ИБ-службам отражать продвинутые кибератаки на всех уровнях значительно быстрее и с меньшими усилиями благодаря оптимально настроенной автоматизации защитных действий, кросс-продуктовому взаимодействию, обогащению достоверной аналитикой о киберугрозах и многоуровневому контролю потенциальных точек входа злоумышленников

Плавный переход к XDR-концепции

Kaspersky Symphony XDR

Kaspersky Unified Monitoring and Analysis Platform является центральным элементом в решении класса XDR (Extended Detection and Response) – Kaspersky Symphony XDR.

Kaspersky Symphony XDR – это все, что сегодня нужно ИБ-экспертам, чтобы успешно отражать сложные кибератаки.

Решение объединяет технологии EPP и EDR, почтовый и интернет-шлюзы, песочницу, инструменты анализа сетевого трафика, платформу повышения осведомленности сотрудников, аналитические данные о киберугрозах и систему мониторинга и корреляции событий безопасности (SIEM). Все элементы Kaspersky Symphony XDR взаимосвязаны между собой, дополняют друг друга и входят в одну лицензию.

Kaspersky Symphony XDR

Защита конечных точек

Kaspersky Symphony EDR



Kaspersky
EDR Expert



Kaspersky Symphony Security



Kaspersky
Endpoint Security
для бизнеса
Расширенный



Kaspersky
Security для виртуальных
и облачных сред



Kaspersky
Unified Monitoring
and Analysis

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
Threat Lookup



Kaspersky
Threat Data
Feeds



Kaspersky
CyberTrace



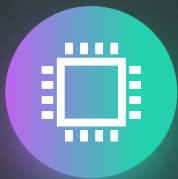
Интеграция с решениями
сторонних поставщиков

Ключевые преимущества



Масштабируемая архитектура и низкие системные требования

Решение создано 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



Высокая производительность

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



Потоковая корреляция в реальном времени

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



Автоматический сбор информации о конечных точках и реагирование

Автоматический сбор инвентаризационной информации (установленное ПО, уязвимости, оборудование, владелец актива и т. д.) может использоваться для корреляции событий ИБ с учетом контекста, а также при расследовании инцидентов. Управление агентами на рабочих местах помогает в процессе реагирования на выявленные инциденты



Тесное взаимодействие с Kaspersky Threat Intelligence

«Лаборатория Касперского» является одним из лидеров в области сервисов оперативного информирования о киберугрозах. Решение Kaspersky Unified Monitoring and Analysis Platform тесно интегрировано с богатым портфолио сервисов Kaspersky Threat Intelligence, что позволяет выявлять и приоритизировать угрозы и в один клик получать доступ к контекстной информации по новым атакам, индикаторам компрометации, тактикам и техникам злоумышленников



Интегрированный модуль ГосСОПКА

Обеспечение соответствия требованиям регуляторов

Решение помогает организациям соответствовать действующему законодательству РФ в сфере безопасности объектов КИИ. В частности, оно позволяет выполнить требования в части обнаружения, предупреждения и ликвидации последствий атак, информирования о компьютерных инцидентах, а также установления причин и условий их возникновения. Встроенный модуль ГосСОПКА напрямую обменивается данными об инцидентах с НКЦКИ



Создавая безопасность

25 лет практического опыта «Лаборатории Касперского» в области создания средств защиты информации, противодействия целевым атакам и анализа вредоносного ПО легли в основу решения Kaspersky Unified Monitoring and Analysis Platform

А также:

Предоставление высокопроизводительного решения в условиях политики импортозамещения

Ценность решения для бизнеса



Сокращение прямых потерь от целенаправленных действий злоумышленников



Снижение рисков информационной безопасности



Объединение в целостную систему ИБ интегрированных решений «Лаборатории Касперского» и сторонних производителей и плавный переход к XDR-концепции



Повышение продуктивности работы ИБ-служб по выявлению, расследованию и реагированию на сложные киберинциденты



Обеспечение помощи в соответствии требованиям внутренних политик безопасности и внешних регулирующих органов



**Kaspersky
Unified Monitoring
and Analysis
Platform**

Подробнее

www.kaspersky.ru

© 2023 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Запросить демонстрацию решения

#kaspersky
#bringonthefuture

kaspersky