Центральный элемент
вашей ИБ-системы

# Kaspersky Unified Monitoring and Analysis Platform

kaspersky активируй будущее

## Приоритизация событий с помощью ИИ

Разработанный в «Лаборатории Касперского» модуль машинного обучения поможет приоритизировать срабатывания. Он анализирует, насколько характерна та или иная активность, связанная с различными активами — рабочими станциями, виртуальными машинами, мобильными телефонами и так далее. Если алерт, выявленный системой в результате корреляции событий, не является типичным для актива, на котором он обнаружен, такое срабатывание помечается в интерфейсе дополнительным статусом. Таким образом, аналитик быстрее видит инциденты, которые требуют первостепенного внимания.

В KUMA также доступен ассистент аналитика KIRA — Kaspersky Investigation and Response Assistant. Интеграция с KIRA позволит работать с системой профильным сотрудникам с разным уровнем подготовки. Так, опираясь на анализ от ИИ, начинающие специалисты смогут принимать более быстрые и точные решения по реагированию на инциденты.

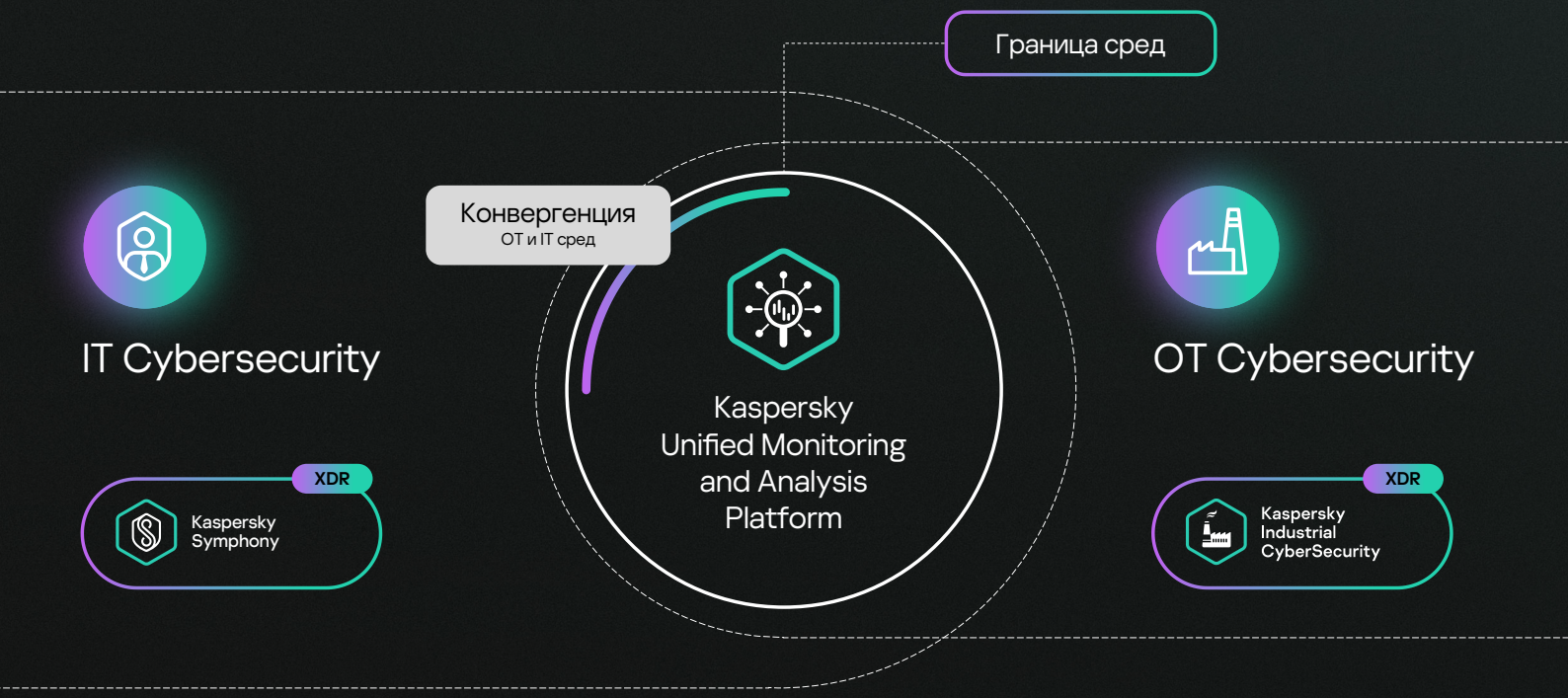
# Центральный элемент вашей системы ИБ-безопасности

## О решении

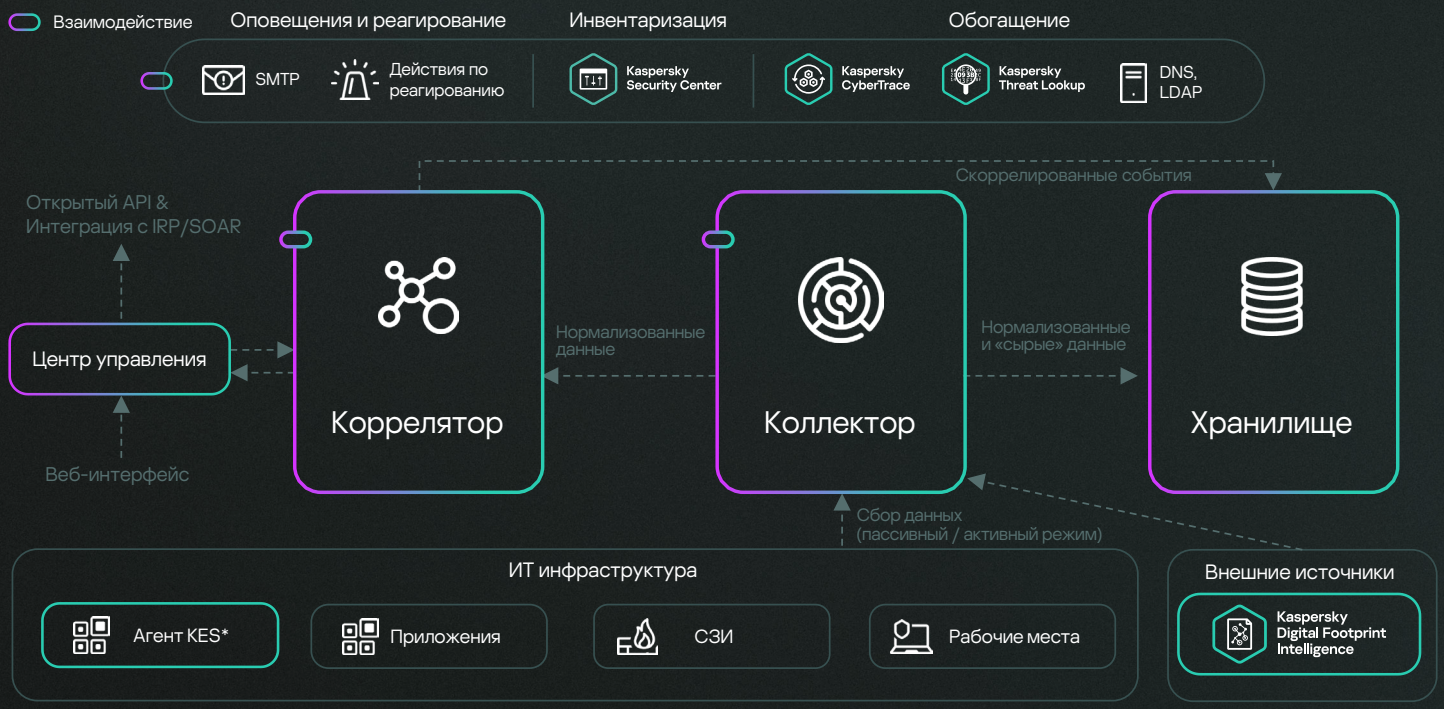
Kaspersky Unified Monitoring and Analysis Platform (KUMA) — высокопроизводительное решение класса SIEM российского производства, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации.

## Центральный элемент комплексной защиты

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 корпоративную или индустриальную среду, но и наиболее инфраструктуру на стыке 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.



# Архитектура KUMA




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 «из коробки»

Kaspersky Unified Monitoring and Analysis Platform поддерживает следующую интеграцию:

### ПО с открытым исходным кодом

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

### Поддерживаемые способы сбора и получения событий

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

### Интеграция IRP / SOAR

Security Vision, R-Vision

### Операционные системы

Windows, Linux, FreeBSD и др.

### Свыше 350 продуктов различных поставщиков

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

# Возможности интеграции с другими продуктами «Лаборатории Касперского»

KUMA интегрируется с другими продуктами «Лаборатории Касперского», что открывает новые возможности для MSSP-партнеров

### 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 Endpoint Detection and Response Expert

Централизованный сбор оповещений о продвинутых угрозах и APT-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 NGFW

Межсетевой экран нового поколения для защиты российских компаний от современных сетевых угроз, реализованный как программно-аппаратный комплекс, который устанавливается в инфраструктуре компании на границе сети или внутри нее

### Kaspersky Industrial CyberSecurity

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

### Kaspersky Threat Lookup

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

### Kaspersky Digital Footprint Intelligence

Предоставляет комплексную защиту от цифровых рисков, которая помогает компаниям отслеживать свои цифровые активы и обнаруживать угрозы в даркнет-ресурсах (deep web, darknet и dark web)

### Kaspersky Anti Targeted Attack

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

### Kaspersky CyberTrace

### Kaspersky Threat Data Feeds

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 Security для почтовых серверов

Оповещения об угрозах, обнаруженных почтовым шлюзом

### Kaspersky Security для интернет-шлюзов

Оповещения об угрозах, обнаруженных веб-шлюзом

### Kaspersky Security для бизнеса

Оповещения об угрозах, обнаруженных на рабочих станциях

# Плавный переход к XDR-концепции

## 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.

## Kaspersky Symphony XDR

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

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.

# Ключевые преимущества

Масштабируемая архитектура и низкие системные требования

Высокая производительность

Потоковая корреляция в реальном времени

Автоматический сбор информации о конечных точках и реагирование

Тесное взаимодействие с Kaspersky Threat Intelligence

Интегрированный модуль ГосСОПКА

# Ключевые возможности KUMA 4.2

| Категория | Основные нововведения |
|---|---|
| Обнаружение кражи учетной записи с помощью ИИ | ML-алгоритмы позволяют обнаруживать потенциальные кейсы Lateral Movement, сравнивания текущую активность пользователя с обученным профилем его стандартной исторической активности. |
| Коррелятор 2.0 Beta | Улучшение производительности в 5 раз и новый функционал: новый технологический стек (Rust), PCRE вместо RE2, отказоустойчивость, скользящее окно корреляции и др. |
| Гибкая ролевая модель | Создание настраиваемых ролей по доступам и возможностям к разделам в KUMA. |
| Управление пользовательскими поисковыми запросами | Возможность остановки «тяжелых» запросов в хранилище, а также возможность выполнения пользовательских запросов с низким приоритетом. |
| Резервное копирование / восстановление событий из архивов | Поддерживается экспорт данных о событиях в архивные файлы. Это позволяет осуществить длительное хранение данных, что является важным требованием для расследований и соблюдения нормативных требований.<br>Импортирование событий из другой инсталляции KUMA. |
| Использование S3 как холодного хранения ClickHouse | В качестве холодного хранения сейчас доступны диски и HDFS. |

## Стрим «Четвертая стена киберзащиты: что нового в KUMA 4.0?»

Подробнее

# Ценность решения для бизнеса

Почти 30 лет практического опыта «Лаборатории Касперского» в области создания средств защиты информации, противодействия целевым атакам и анализа вредоносного ПО легли в основу решения Kaspersky Unifed Monitoring and Analysis Platform. Промышленные компании по-разному подходят к защите IT- и OT-сред. Большинство компаний давно используют проверенные системы обнаружения угроз и реагирования на инциденты в корпоративных сетях.

## Снижение рисков

Снижение рисков информационной безопасности

## Сокращение потерь

Сокращение прямых потерь от целенаправленных действий злоумышленников

## Эффективное решение

Предоставление высокопроизводительного решения в условиях политики импортозамещения

## Единая платформа безопасности

Объединение в целостную платформу безопасности интегрированных решений «Лаборатории Касперского» и сторонних производителей

## Повышение продуктивности

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

## Соответствие требованиям

Обеспечение помощи в соответствии требованиям внутренних политик безопасности и внешних регулирующих органов (в частности, требованиям ФЗ-187 и приказа ФСТЭК России №239)

# Покрытие матрицы MITRE ATT&CK

MITRE ATT&CK — это публичная база знаний, в которой собраны тактики и техники целевых атак, применяемые различными группировками киберпреступников. Сегодня она считается общемировым отраслевым стандартом и включает сотни техник и подтехник и тысячи процедур. Выбирая направления развития SIEM-системы Kaspersky Unified Monitoring and Analysis Platform, мы во многом опираемся именно на базу знаний MITRE. Мы начали включать в KUMA разметку текущих правил в соответствии с методами и тактиками атак MITRE, чтобы расширить возможности по анализу угроз и визуализировать степень защиты. Мы также ориентируемся на MITRE, когда разрабатываем OOTB (Out-of-the-box) контент нашей SIEM-платформы.

## Сколько техник покрывает KUMA?

KUMA покрывает более 62% матрицы, а при использовании продуктов «Лаборатории Касперского» этот показатель становится значительно выше.

Подробнее

# Kaspersky Unified Monitoring and Analysis Platform

Подробнее

www.kaspersky.ru



#kaspersky
#активируйбудущее