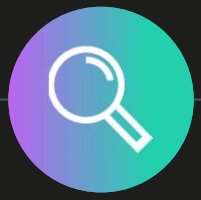
Kaspersky Unified Monitoring and Analysis Platform

Продуктовая презентация

kaspersky

Актуальные ИБ-задачи

Противодействие сложным угрозам в киберагрессивной среде



ИБ-замещение ушедших поставщиков в короткие сроки

Соответствие требованиям регуляторов

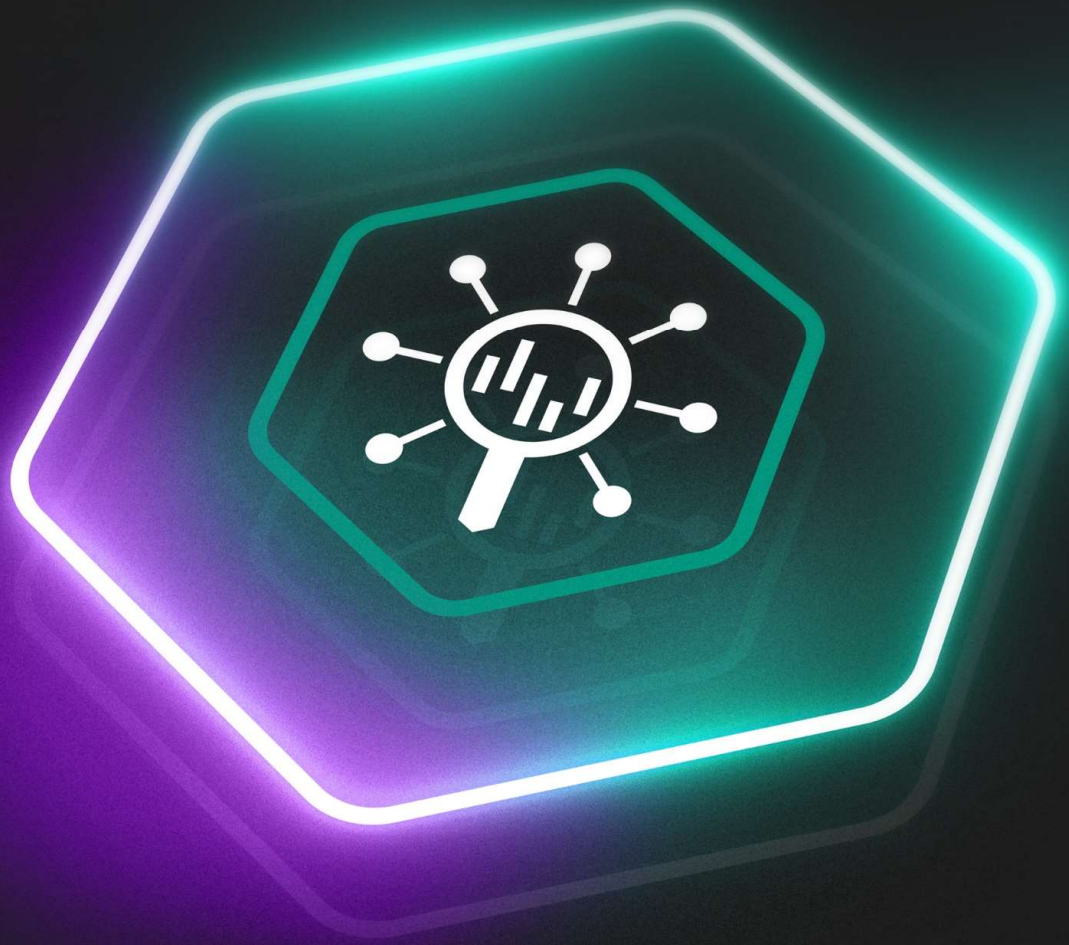
52%

организаций считают, что процесс работы с инцидентами стал труднее, чем два года назад

Сегодня обнаружение и реагирование труднее осуществлять, чем два года назад, по следующим причинам:

41%	Стремительное расширение и изменение ландшафта угроз
40%	Расширение поверхности атак
39%	Постоянное изменение поверхности атак
37%	Рост количества и сложности оповещений об инцидентах безопасности

Kaspersky Unified Monitoring and Analysis Platform



Актуальные ИБ-вызовы, в т.ч. связанные с SIEM

Разрозненные средства защиты, которые усложняют работу специалистов ИБ, отнимают много ресурсов и повышают стоимость владения

Необходимость получения контекстной информации о событиях безопасности для упрощения процесса реагирования

Высокие требования к производительности SIEM-систем как ключевое требование

Поиск альтернативных SIEM-систем в условиях политики импортозамещения

Необходимость соответствовать требованиям в области безопасности КИИ, в том числе взаимодействовать с НКЦКИ — получать и отправлять данные об инцидентах

Необходимость плавного перехода к XDR-концепции и всеобъемлющей безопасности в рамках всей инфраструктуры

Объединение существующих решений в единую систему ИБ для увеличения эффективности анализа данных

Обеспечение единой концепции кибербезопасности

Решение Kaspersky Unified Monitoring and Analysis Platform (KUMA) — обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, объединяет решения «Лаборатории Касперского» и продукты сторонних поставщиков, в т. ч. в единую XDR-систему Kaspersky Symphony XDR, и помогает подойти комплексно к защите бизнеса не только корпоративного сегмента, но и индустриального (стык OT/IT) и вопросу соответствия требованиям внешних регулирующих органов.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Security для бизнеса

Kaspersky Security для интернет-шлюзов

Kaspersky Security Center

Kaspersky Threat Data Feeds

Kaspersky Anti Targeted Attack

Kaspersky Security для почтовых серверов

Kaspersky CyberTrace

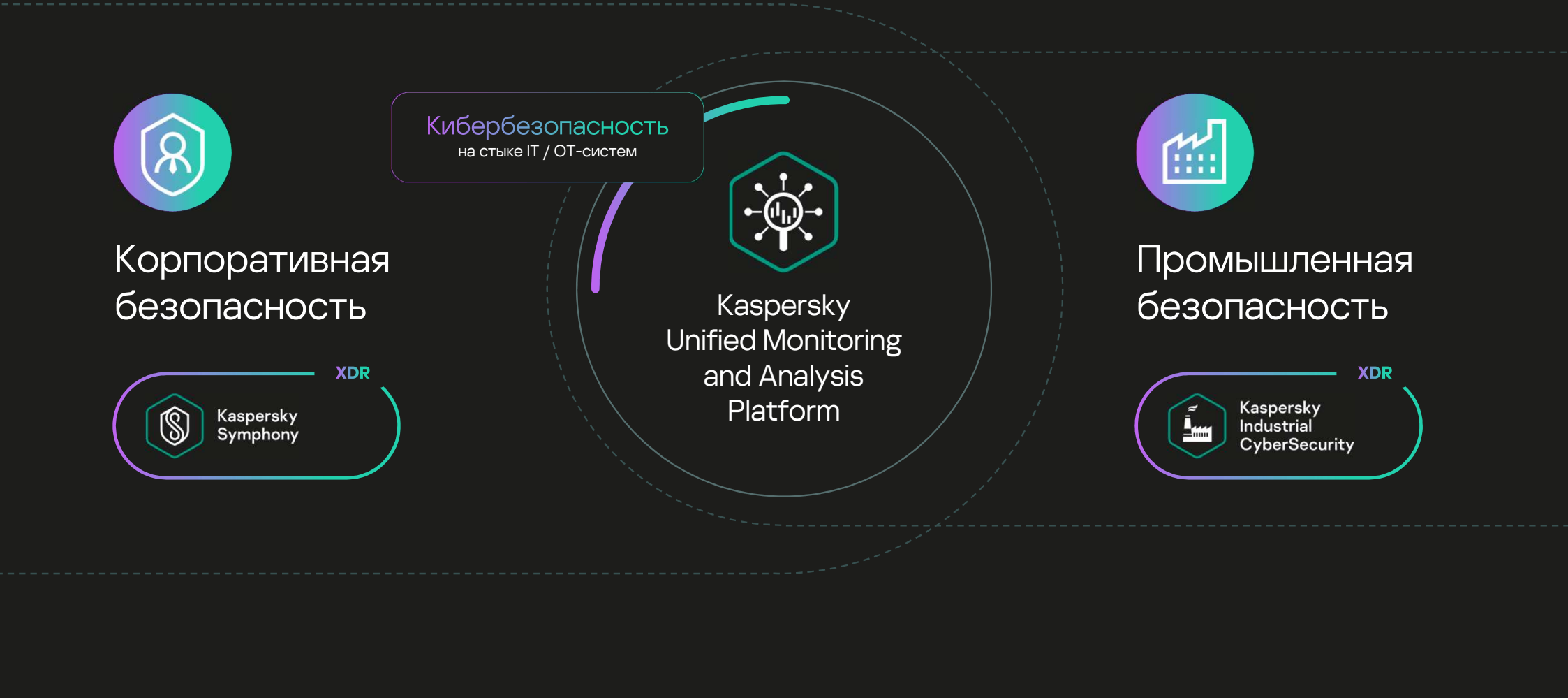
Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity

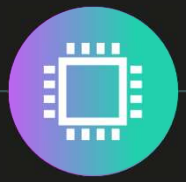
Kaspersky EDR Expert

Решения сторонних поставщиков

Kaspersky Unified Monitoring and Analysis Platform



Ключевые преимущества



Высокая производительность

300k+ EPS на один узел

Низкие системные требования

Современный язык

Эффективное хранилище

Масштабируемость

Гибкая микросервисная архитектура

Единый интерфейс веб-консоли

Все настройки в одном окне

Интеграция «из коробки»

С продуктами сторонних поставщиков и решениями «Лаборатории Касперского»

Низкий порог входа

Не требует знания специальных языков запросов или написания правил

Сертификат ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4455

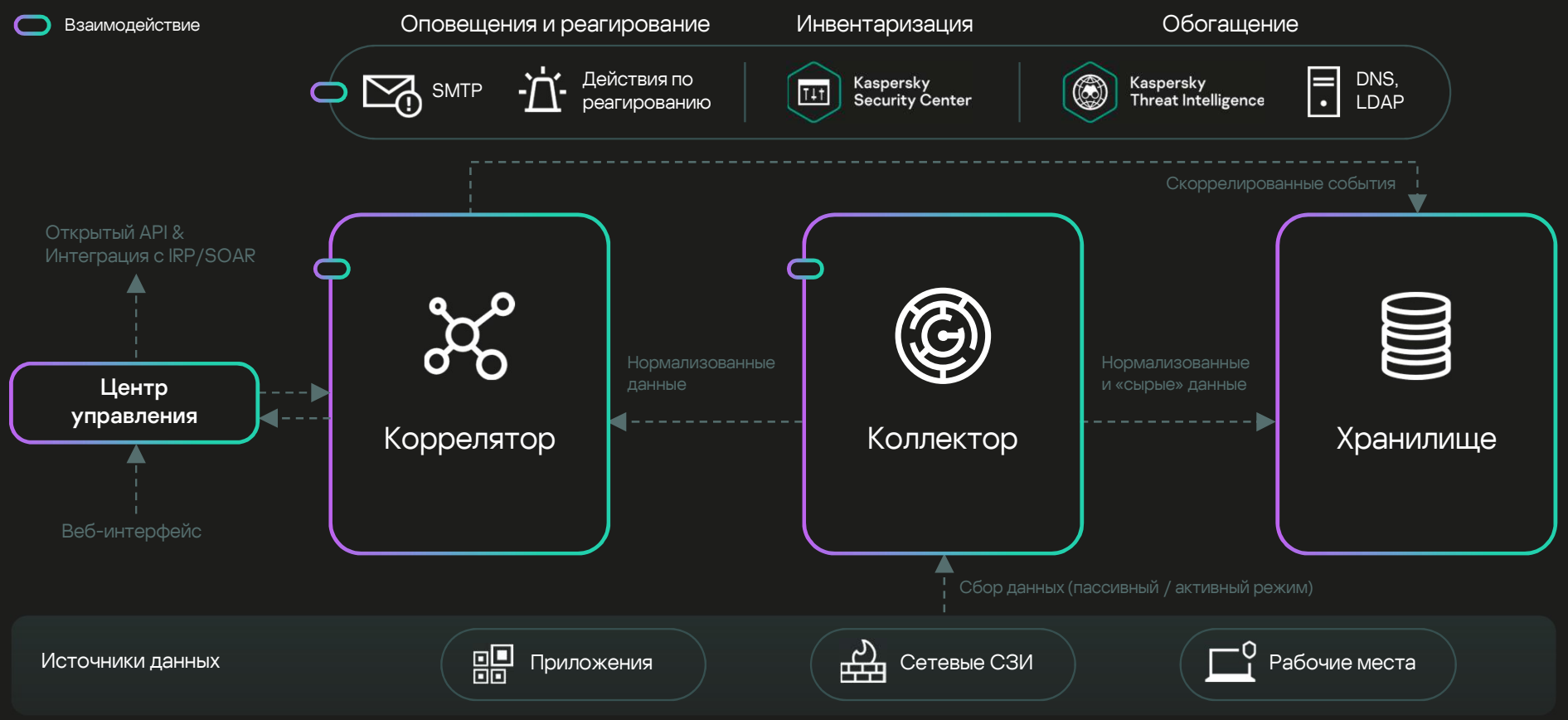
Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
28 сентября 2021 г.

Выдан: 28 сентября 2021 г. Переоформлен: 7 ноября 2022 г.
Действителен до: 28 сентября 2026 г.

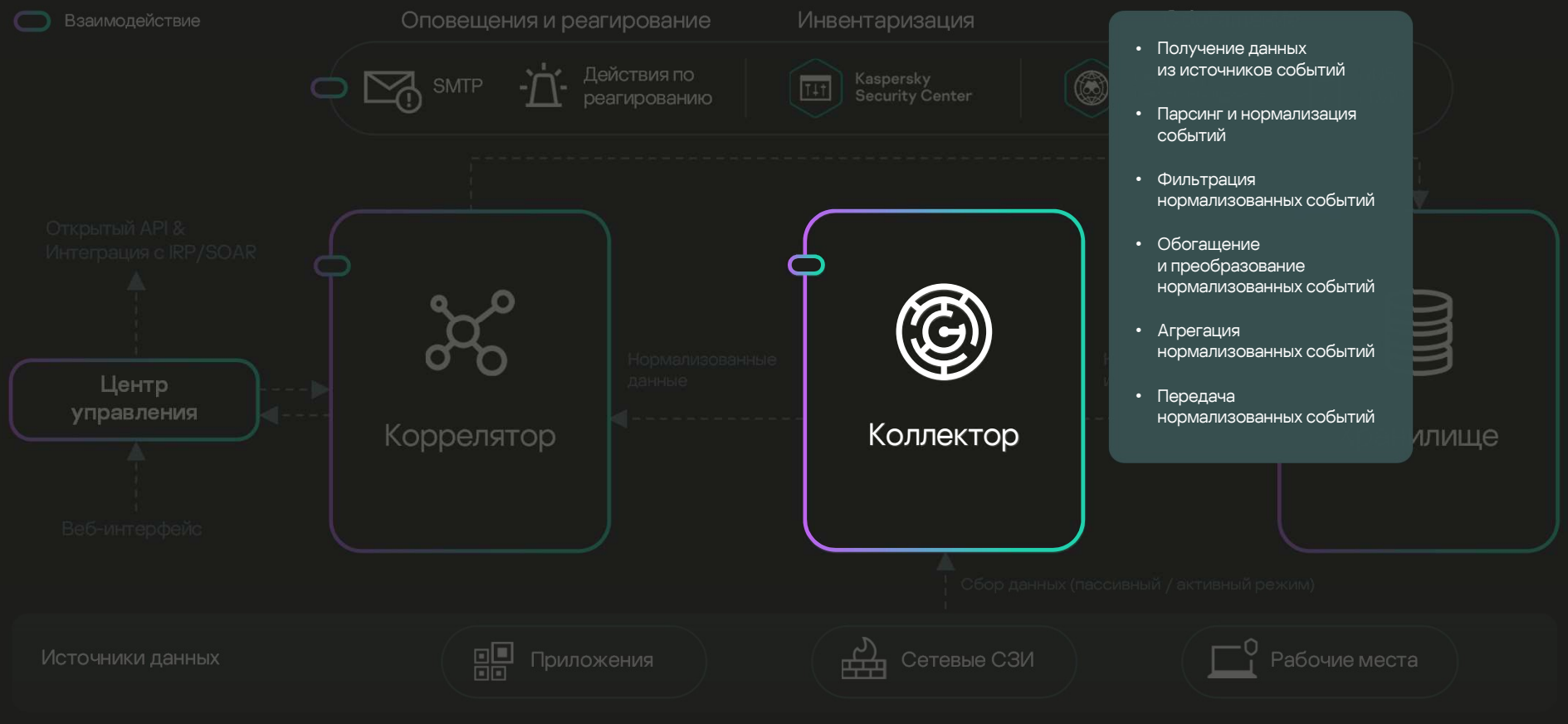
Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Unified Monitoring and Analysis Platform»**, разработанное и производимое АО «Лаборатория Касперского», является системой управления событиями информационной безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и технических условиях ТУ 643.46856491.00116-03 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00116-03 30 01.

Архитектура KUMA

Архитектура KUMA

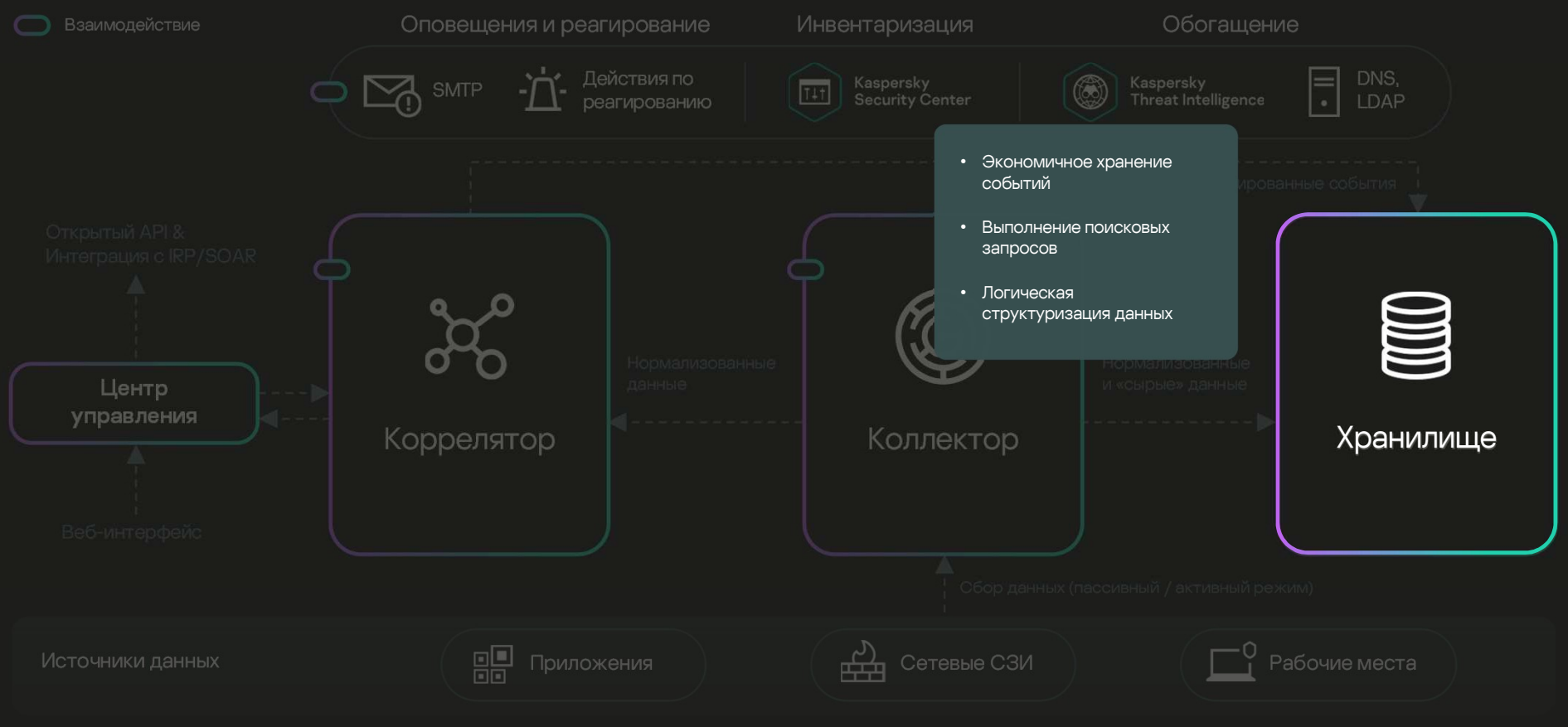


Архитектура KUMA

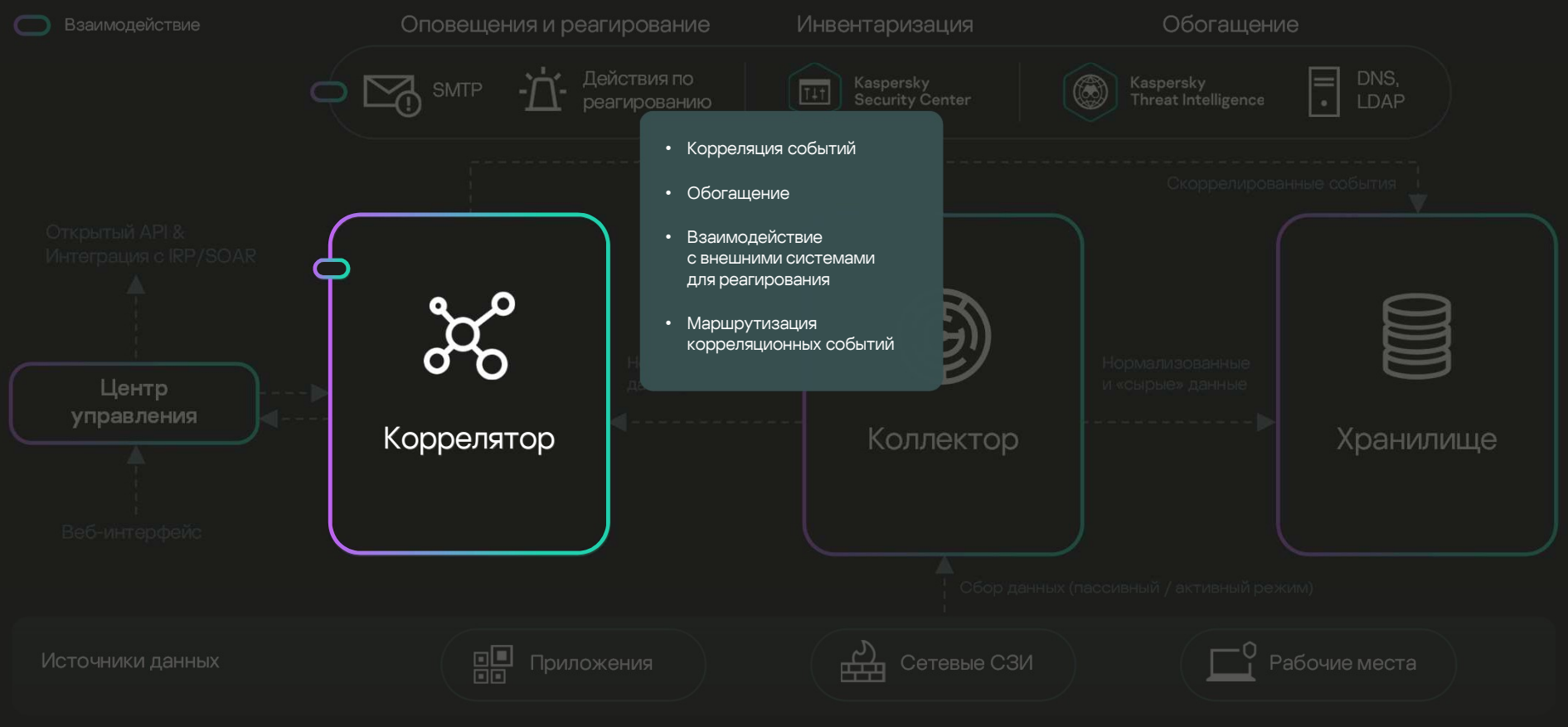


- Получение данных из источников событий
- Парсинг и нормализация событий
- Фильтрация нормализованных событий
- Обогащение и преобразование нормализованных событий
- Агрегация нормализованных событий
- Передача нормализованных событий

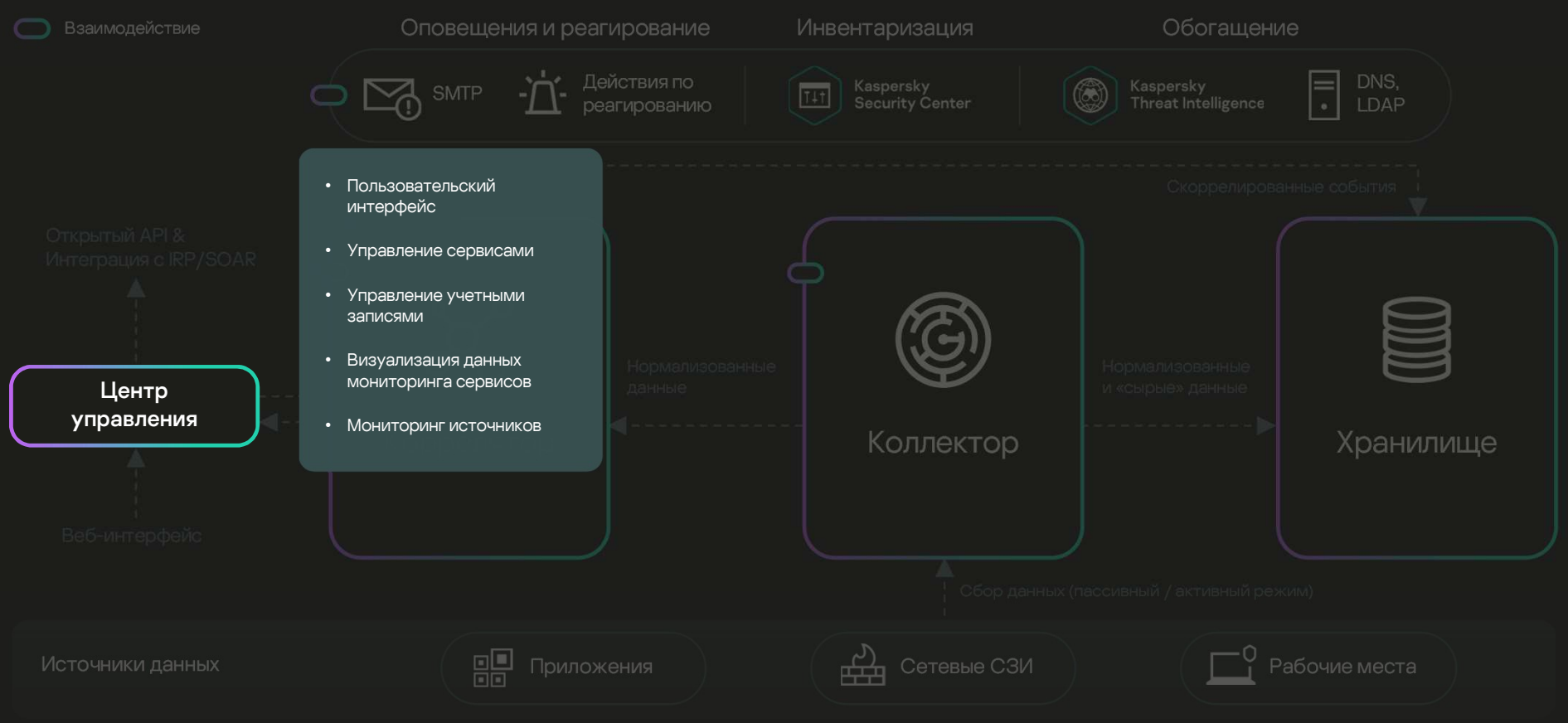
Архитектура KUMA



Архитектура KUMA



Архитектура KUMA



Поддерживаемые источники данных «из коробки» и другие интеграции

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, Бастион, Huawei, Oracle, MikroTik, Бифит, 1С, С-Терра и др.

Поддерживаемые способы сбора и получения событий

Netflow, Kafka, NATS, SQL, TCP, UDP, HTTP, Files, SNMP, WMI

Операционные системы

Windows, Linux, FreeBSD

Интеграция IRP / SOAR

Security Vision, R-Vision

Коннекторы и нормалайзеры (парсеры)

Коннекторы

TCP listener

UDP listener

Netflow v9/10

NATS

Kafka

HTTP

File

SQL

sFlow

SNMP

WMI

Netflow Ipfix

Нормалайзеры

JSON

CEF

CSV/TSV

Key/Value
ключ-значение

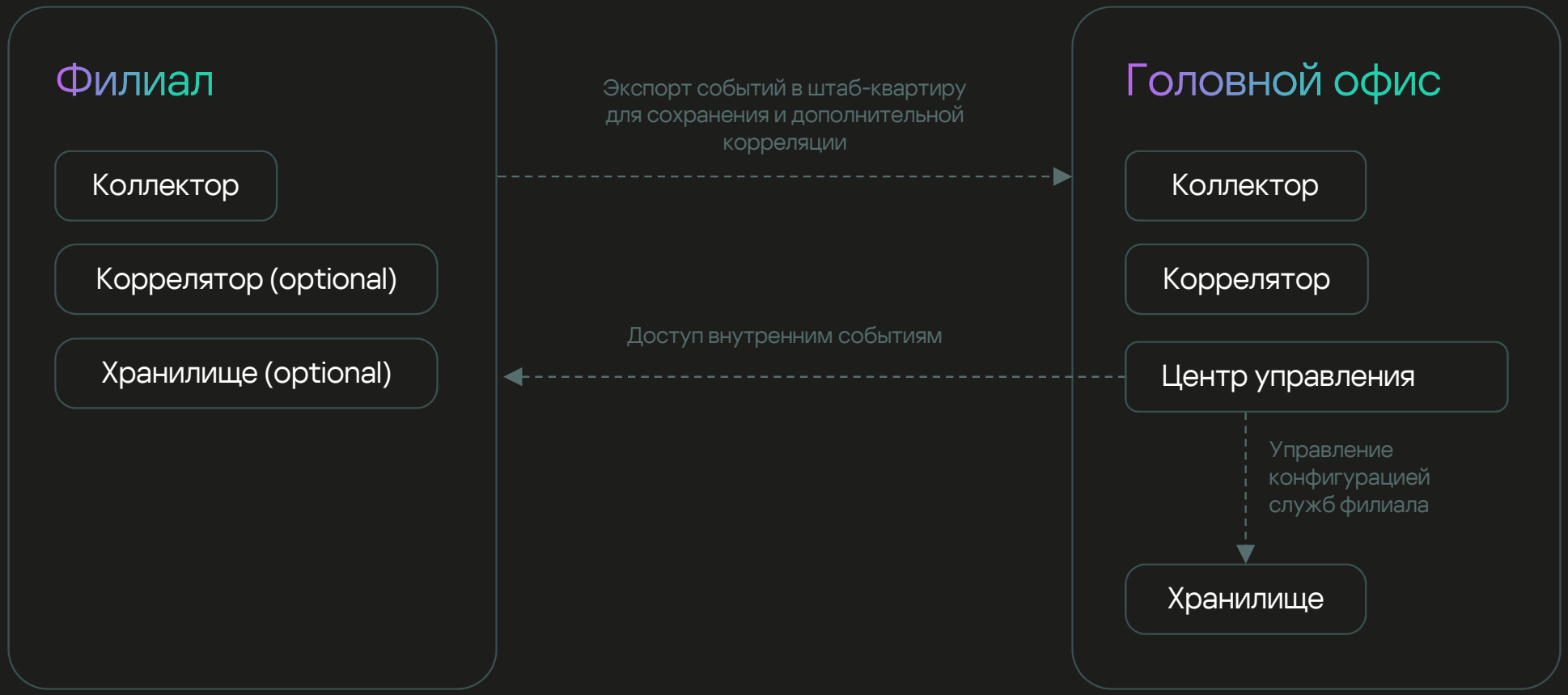
Regexp
(регулярные выражения)

Syslog (RFC3164 & RFC5424)

XML

Windows Event Log

Распределенная инфраструктура

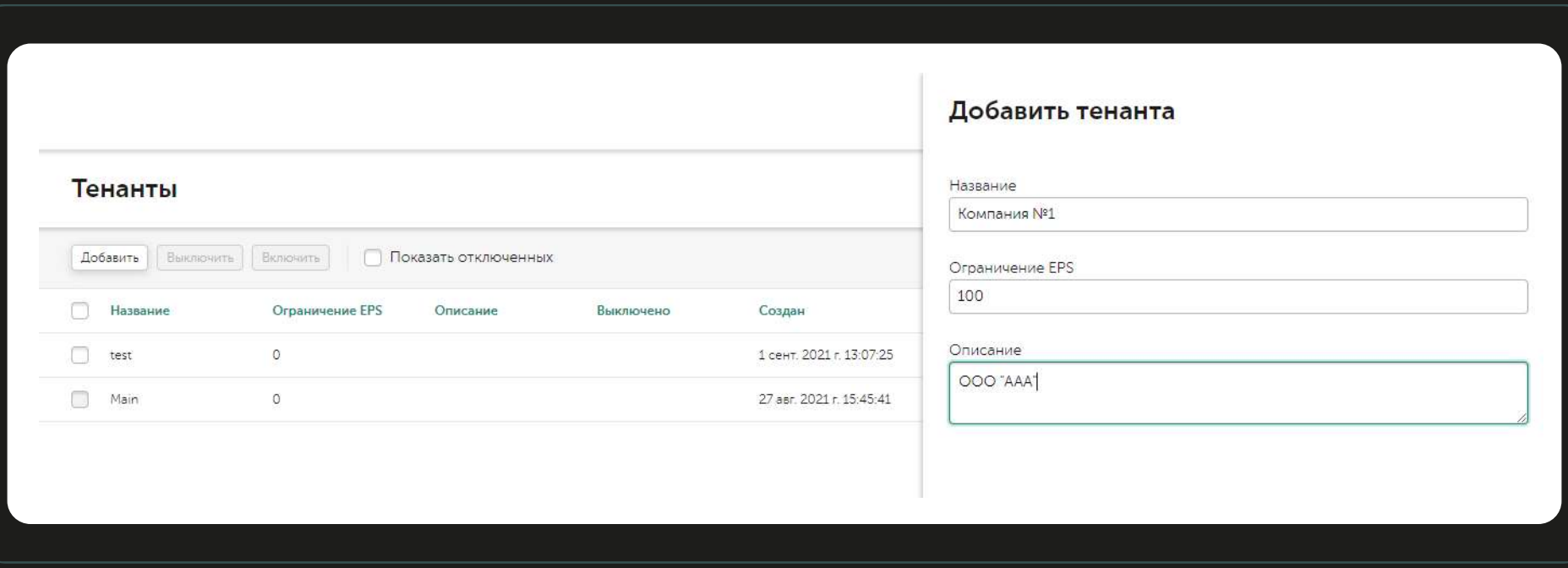


Поддержка Multitenancy

Разделение данных,
конфигурации и прав доступа

Возможность ограничения EPS
для каждого тенанта отдельно

Целевой сценарий для MSSP
и центров ГосСОПКА



Примеры сайзинга

Примерный сайзинг — 1 вариант

~ 5k EPS

90 дней хранения

All-in-one

CPU – 16 CPU

RAM – 32 ГБ

Storage – 16 ТБ

Примерный сайзинг — 2 вариант

~ 20k EPS 180 дней хранения

* Объем хранилища зависит от длительности хранения событий

Коллектор	Коррелятор	Центр управления	x2 Хранилище событий
CPU – 8 CPU RAM – 16 ГБ Storage – 500 ГБ	CPU – 8 CPU RAM – 32 ГБ Storage – 500 ГБ	CPU – 8 CPU RAM – 12 ГБ Storage – 500 ГБ	CPU– 24 CPU RAM – 64 ГБ Storage – 62* ТБ

Примерный сайзинг — 3 вариант

~ 40k EPS 180 дней хранения

* Объем хранилища зависит
от длительности хранения событий

x2 Коллектор	Коррелятор	Центр управления	x4 Хранилище событий
CPU – 8 CPU RAM – 16 ГБ Storage – 500 ГБ	CPU – 8 CPU RAM – 32 ГБ Storage – 500 ГБ	CPU – 8 CPU RAM – 12 ГБ Storage – 500 ГБ	CPU– 24 CPU RAM – 64 ГБ Storage – 62* ТБ

Оптимизация стоимости оборудования за счет стоимости разделение хранения на этапы

Передача «исторических» данных на менее производительное оборудование через заданный интервал.

Единый поиск со всеми поддерживаемыми возможностями SQL по всем данным независимо от того, на каком хранилище события находятся.

Лицензирование

Шаг по

100 EPS

Учет по количеству «чистых» EPS

Минимальная лицензия от

500 EPS

Дополнительные модули

- ГосСОПКА
- Netflow
- Threat Intelligence

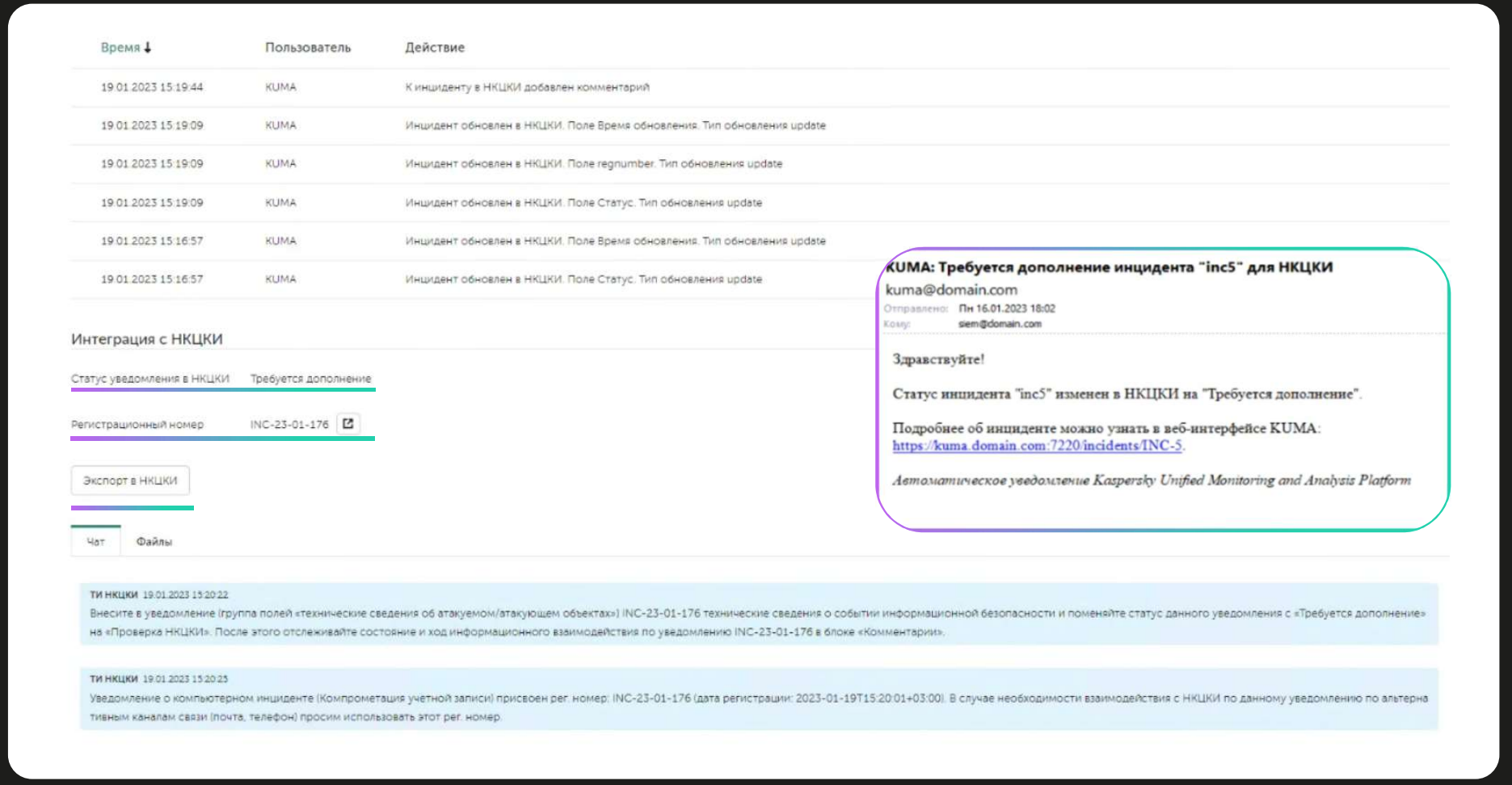
Срок действия

- 1 год
- 2 года
- 3 года

Интеграция с ГосСОПКА

- Синхронизация статусов инцидентов
- Категоризация активов в соответствии с КИИ-категориями
- Возможность приложить файл к инциденту
- Интерактивный чат со специалистами НКЦКИ
- Сравнение актуальных значений параметров инцидентов в KUMA со значениями, переданными в ГосСОПКА
- Осуществлена передача инцидентов в режиме иерархии инсталляций KUMA – родительские узлы KUMA смогут информировать НКЦКИ об инцидентах, выявленных на подчинённых системах

Работа с инцидентом. Отслеживание статуса и обратная связь



Время	Пользователь	Действие
19.01.2023 15:19:44	KUMA	К инциденту в НКЦКИ добавлен комментарий
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле Время обновления. Тип обновления update
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле regnumber. Тип обновления update
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле Статус. Тип обновления update
19.01.2023 15:16:57	KUMA	Инцидент обновлен в НКЦКИ. Поле Время обновления. Тип обновления update
19.01.2023 15:16:57	KUMA	Инцидент обновлен в НКЦКИ. Поле Статус. Тип обновления update

KUMA: Требуется дополнение инцидента "inc5" для НКЦКИ

kuma@domain.com

Отправлено: Пн 16.01.2023 18:02

Кому: siem@domain.com

Здравствуйте!

Статус инцидента "inc5" изменен в НКЦКИ на "Требуется дополнение".

Подробнее об инциденте можно узнать в веб-интерфейсе KUMA:
https://kuma.domain.com:7220/incidents/INC-5.

Автоматическое уведомление Kaspersky Unified Monitoring and Analysis Platform

Синергия SIEM и TI-платформы

KUMA

+ TI

Kaspersky
Unified Monitoring
and Analysis Platform

- Сбор событий
- Нормализация
- Обогащение
- Корреляция
- Хранение

Kaspersky
CyberTrace

Платформа управления потоками данных об угрозах

Kaspersky
Threat Intelligence

- Ransomware URL
- Botnet URL
- Malicious URL
- Phishing URL
- IP Reputation

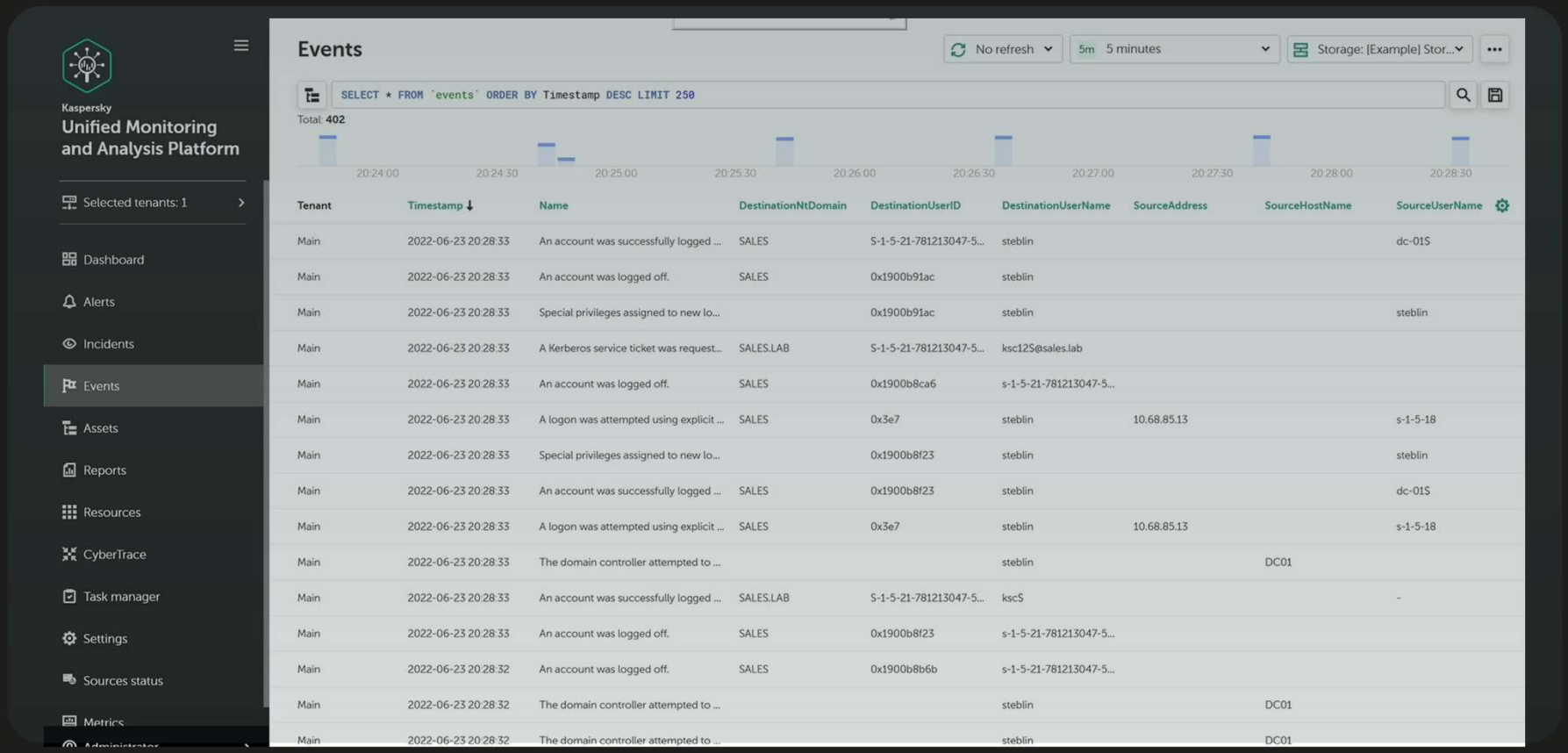
Техническая поддержка

		Premium	Premium Plus
Каналы связи	Company account (веб-портал, уведомления через почту)	●	●
	Телефон	●	●
Время реакции в зависимости от уровня критичности	Критический (24/7)	2 часа	0,5 часа
	Высокий (в рабочие часы)	6 часов	4 часа
	Средний (в рабочие часы)	8 часов	6 часов
	Низкий (в рабочие часы)	10 часов	8 часов
Доступные услуги	Программные исправления	●	●
	Удаленное подключение для диагностики проблем	●	●
	Постпроектная поддержка	●	●
	Частные исправления	●	●
	Рекомендации по оптимизации	●	●
	Персональный технический менеджер		●
	Регулярные статус-встречи с TAMом для ретроспективного анализа зарегистрированных инцидентов, связанных с ТП		Ежеквартальный отчет
	Парсеры логов под заказ	10	20
	Количество включенных часов Professional Services (не менее 2 часов на 1 сессию)	0	16 часов (2 дня)

Примеры функционала

Пример 1. Инвентаризация информационных активов

Демонстрация



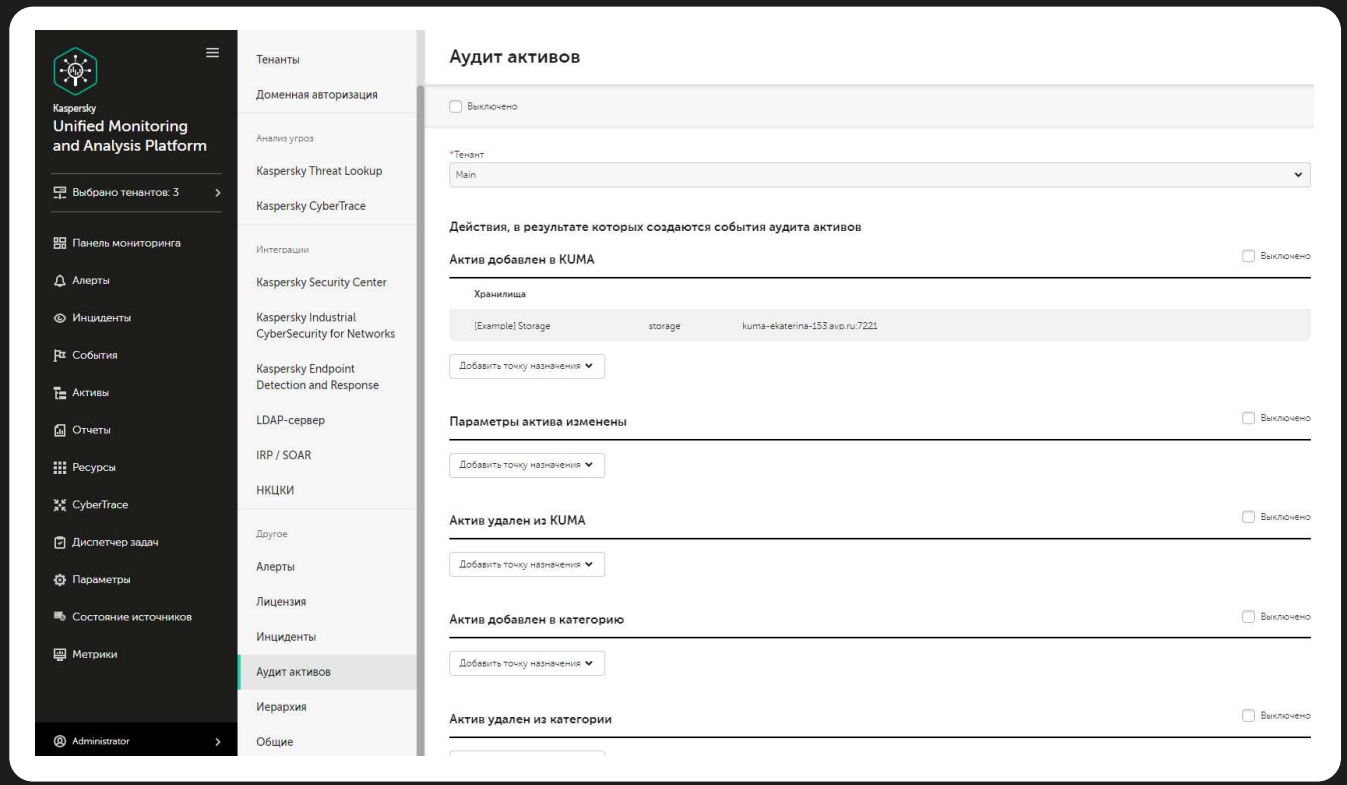
Tenant	Timestamp ↓	Name	DestinationNtDomain	DestinationUserID	DestinationUserName	SourceAddress	SourceHostName	SourceUserName
Main	2022-06-23 20:28:33	An account was successfully logged ...	SALES	S-1-5-21-781213047-5...	steblin			dc-01$
Main	2022-06-23 20:28:33	An account was logged off.	SALES	0x1900b91ac	steblin			
Main	2022-06-23 20:28:33	Special privileges assigned to new lo...		0x1900b91ac	steblin			steblin
Main	2022-06-23 20:28:33	A Kerberos service ticket was request...	SALES.LAB	S-1-5-21-781213047-5...	ksc12$@sales.lab			
Main	2022-06-23 20:28:33	An account was logged off.	SALES	0x1900b8ca6	s-1-5-21-781213047-5...			
Main	2022-06-23 20:28:33	A logon was attempted using explicit ...	SALES	0x3e7	steblin	10.68.85.13		s-1-5-18
Main	2022-06-23 20:28:33	Special privileges assigned to new lo...		0x1900b8f23	steblin			steblin
Main	2022-06-23 20:28:33	An account was successfully logged ...	SALES	0x1900b8f23	steblin			dc-01$
Main	2022-06-23 20:28:33	A logon was attempted using explicit ...	SALES	0x3e7	steblin	10.68.85.13		s-1-5-18
Main	2022-06-23 20:28:33	The domain controller attempted to ...			steblin		DC01	
Main	2022-06-23 20:28:33	An account was successfully logged ...	SALES.LAB	S-1-5-21-781213047-5...	ksc$			-
Main	2022-06-23 20:28:33	An account was logged off.	SALES	0x1900b8f23	s-1-5-21-781213047-5...			
Main	2022-06-23 20:28:32	An account was logged off.	SALES	0x1900b8b6b	s-1-5-21-781213047-5...			
Main	2022-06-23 20:28:32	The domain controller attempted to ...			steblin		DC01	
Main	2022-06-23 20:28:32	The domain controller attempted to ...			steblin		DC01	

Аудит активов

События аудита
для каждого тенанта

Можно направить
в коррелятор
и создавать алерты
на появление
уязвимостей

Можно строить
графики анализа
состояния активов

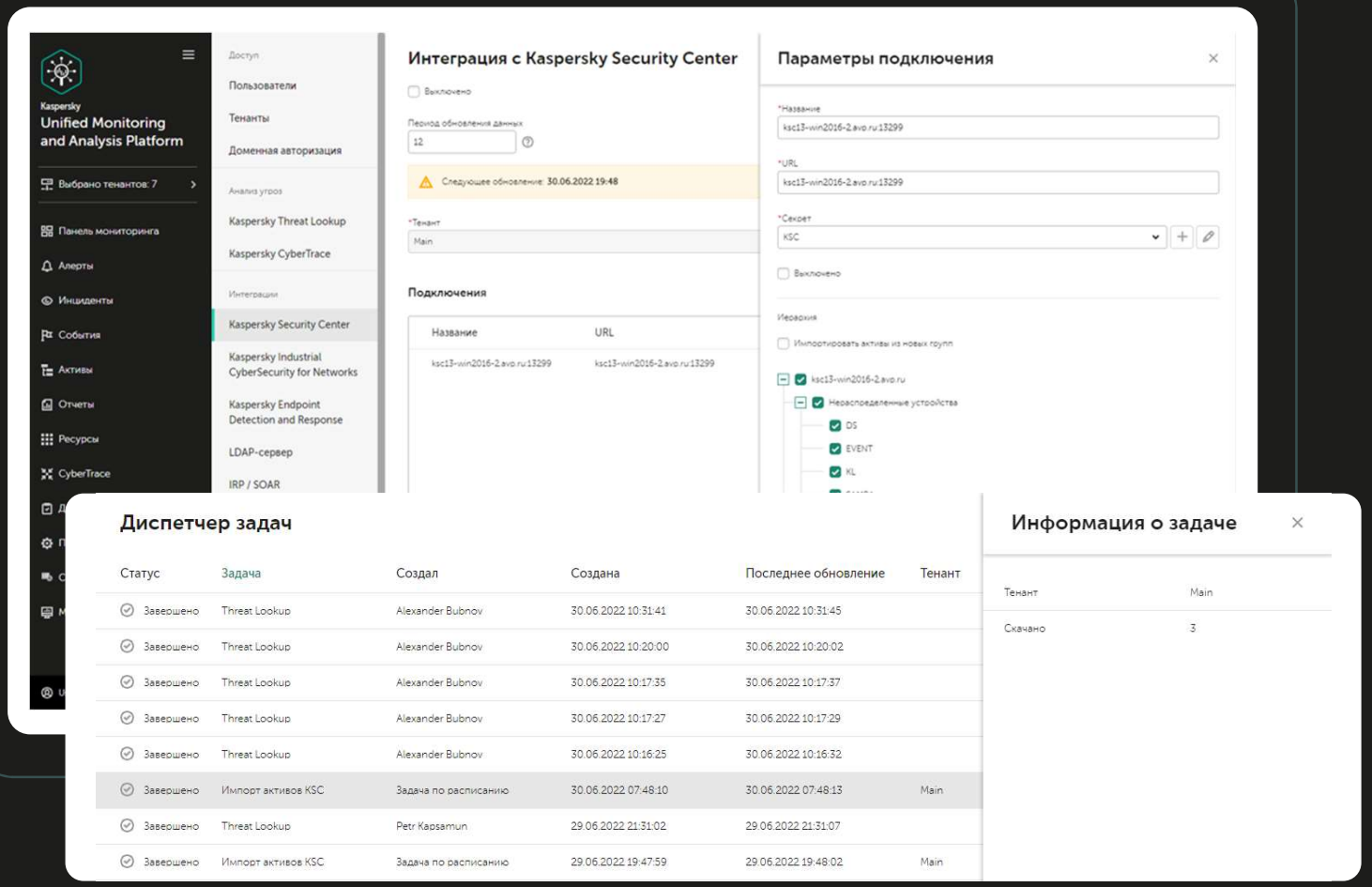


Импорт активов

с фильтрацией по структуре серверов на уровне иерархии KSC и групп администрирования

с настройкой расписания

с выводом результатов в менеджере задач



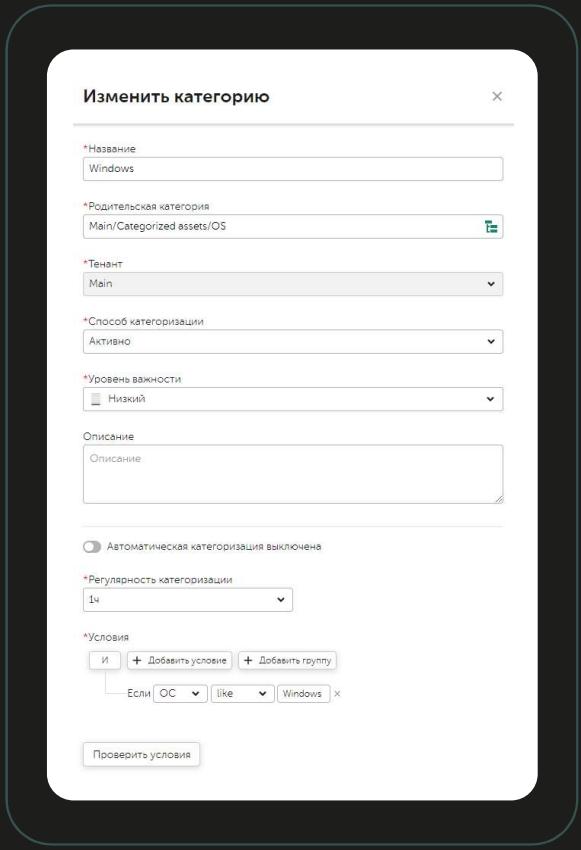
Динамическая категоризация по:

FQDN | IP | CVE | ОС | Расширенный статус KSC

ПО | КИИ | Статус Endpoint Sensor

Логические операторы
AND, OR, NOT и группировки

Возможность
проверки условий



Пример 2. Сбор и анализ расширенной телеметрии

Единый агент EPP+EDR

Драйвер сети

Драйвер перехвата OS API

Драйвер мониторинга файловой системы

Драйвер мониторинга процессов и сервисов

Обогащение и фильтрация

~15k EPD

Создание, модификация файлов и т .д.

Запуск, инъекция процессов и т.д.

Сетевые соединения, DNS-запросы, скачивание файла, e-mail и т.д.

Изменение реестра, Event logs, WMI, автозапуск и т.д.

Инциденты AV, DeviceControl и т.д.

GERT
Группа реагирования

SOC Team

GREAT
Центр глобальных исследований и анализа угроз

EDR Central Node

Обогащение

Визуализация

Корреляция

+ Инциденты EDR

Threat Intelligence

3rd party
Сторонние события

KUMA

Обогащение

Визуализация

Корреляция

Пример 3. Потоковое «обогащение» событий

Решения

«Лаборатории Касперского»

Логи

Алерты

Телеметрия

+

Источники данных
передают «сырые» события

Приложения

АРМ

Сетевые СЗИ

Коллектор

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky CyberTrace

Kaspersky Threat Data Feeds

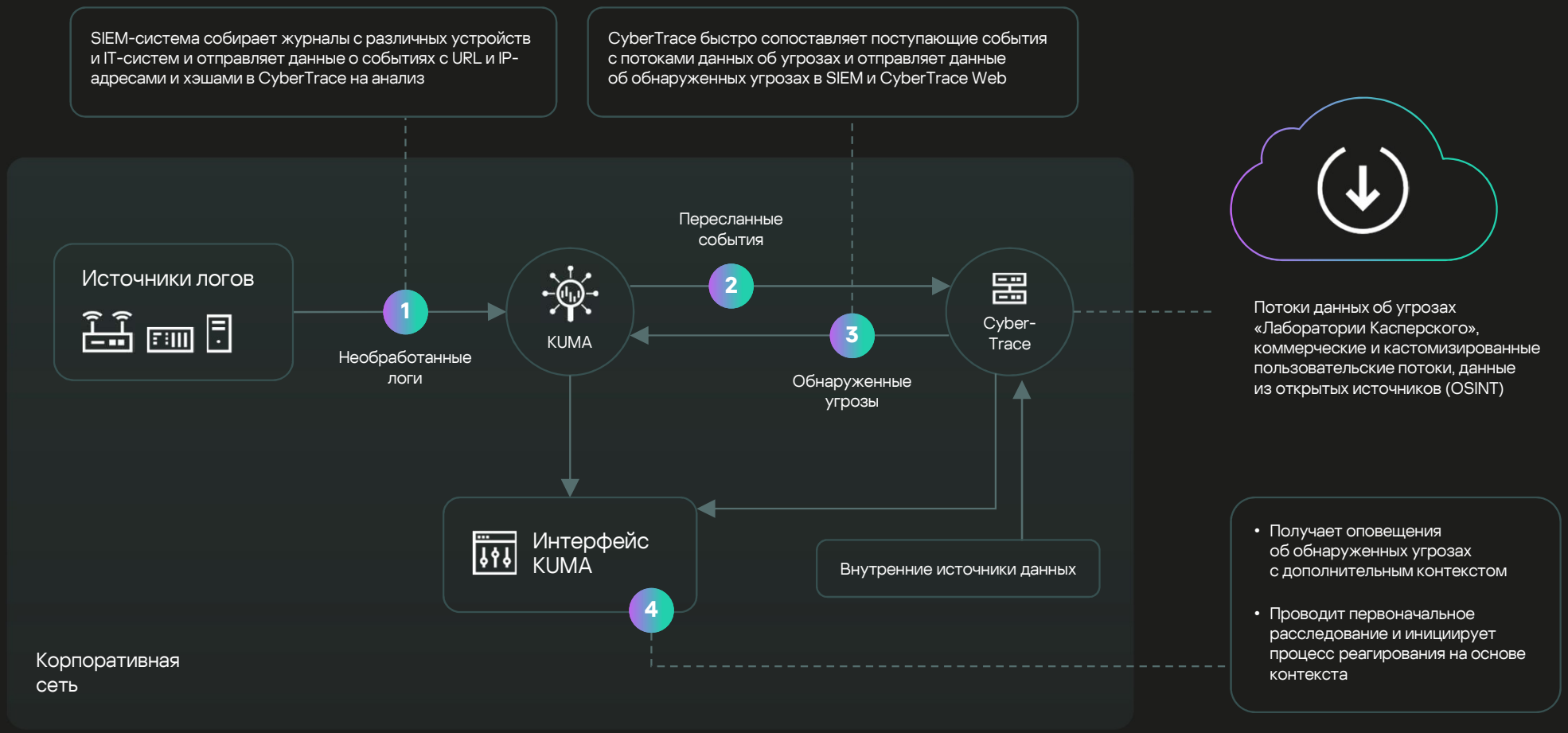
«Обогащение» событий

Коррелятор

Kaspersky Unified Monitoring and Analysis Platform

«Обогащенные» события

Kaspersky CyberTrace — платформа для управления данными о киберугрозах



Kaspersky CyberTrace

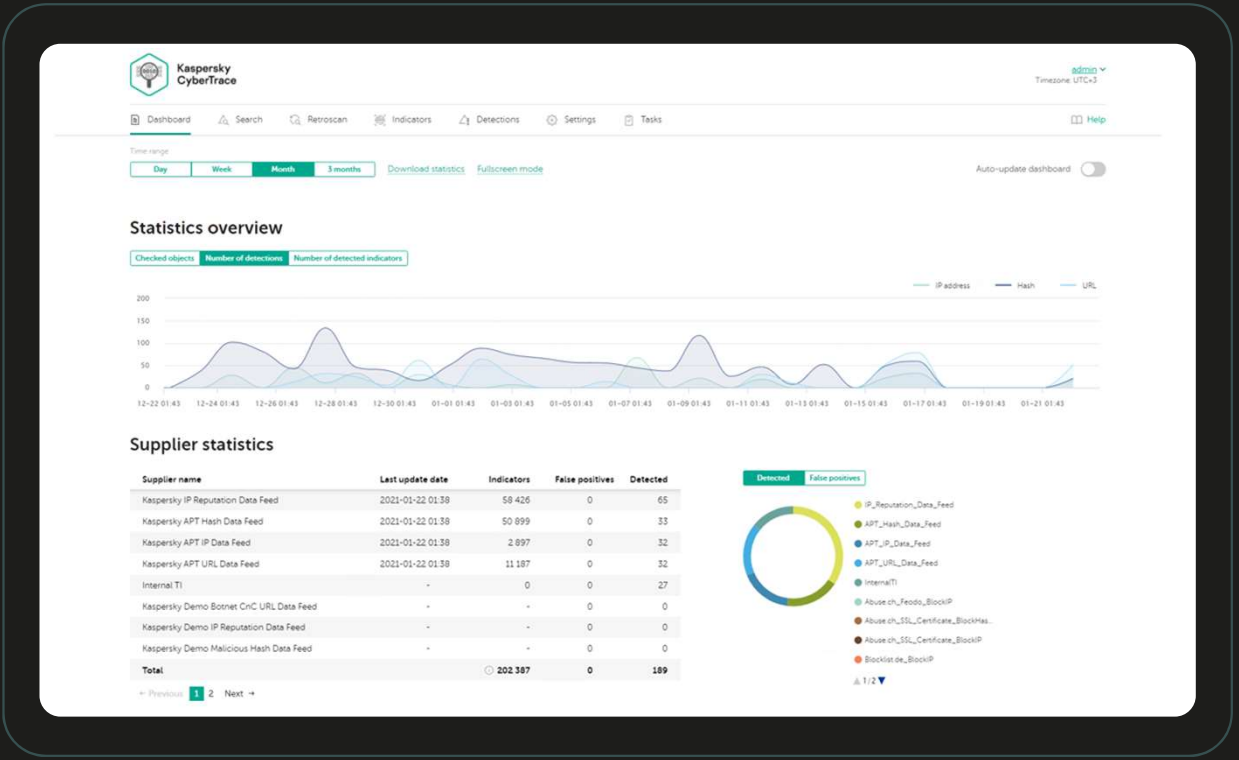
База данных для хранения
и поиска по данным (+ retroscan)

Агрегация, дедупликация,
нормализация и обмен данными

Статистика обнаружений
и матрица пересечений
по потокам данных

Публичный API (для интеграции и
автоматизации)

Мультитенантность для MSSP
и крупных предприятий



Потоки данных об угрозах

Kaspersky Threat Data Feeds

- IP reputation feed
- Hash feed (Win / *nix / MacOS / Androidos / iOS)
- URL feeds (malicious, phishing and C&C)
- Ransomware URL feed
- APT IoC feeds
- Vulnerability feed
- Passive DNS (pDNS) feed
- IoT URL feed
- Whitelisting feed
- ICS hash feed
- И другое

Потоковое обогащение событий ИБ контекстом и представление информации в интерфейсе KUMA. Накопление собственных знаний об угрозах, полученных в процессе расследования инцидентов и управление этими знаниями

Парсинг событий

Для CyberTrace не нужно отдельно настраивать регулярные выражения

Расследование

Результаты обогащения пишутся сразу в исходное событие

Логика обнаружения

Создание кастомного индикатора из инцидента и добавление его в базу CyberTrace в едином интерфейсе

Пример 4. «Обогащение» событий по запросу

Запрос по индикатору

(вручную / авто)

Пример -URL: “example.com”)

Запрос по индикатору
(url, hash, domain, ip)

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Threat Lookup

Карточка инцидента

Имя: «Обнаружено взаимодействие с CnC сервером»
Описание:.....
Связанные события: .....
Связанные IP: 1.2.3.4, 2.3.4.5, ...
Связанные пользователи: i.Ivanov, a.petrov, ...
.....

“Обогащение” карточки инцидента данными из Kaspersky Threat lookup

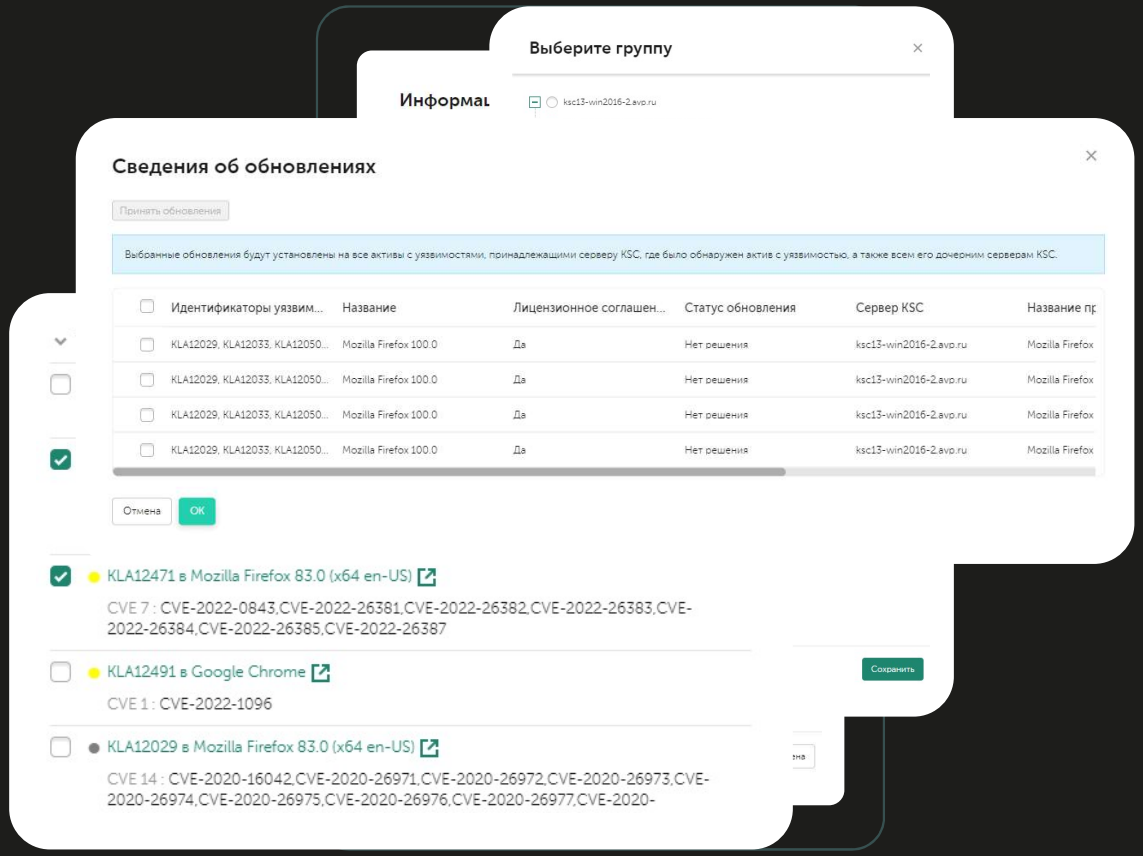
Ответ на запрос

URL: «example.com»
first seen: “2016-08-10”
last seen:” 2020-03-01”
Связанные хэш-суммы вредоносных файлов MD5:”.....”
SHA-1: “.....”
SHA256:” ”
Связанные вредоносные URL: “....”
Связанные IP: 1.2.3.4, 2.3.4.5, ...

Реагирование из карточки

Перемещение в группу администрирования (влияет на политику антивируса)

Установка патчей для уязвимостей



Пример 6. Автоматизированное реагирование на инциденты KES/KEDR Expert

Пример 7. Скрипты для автоматического реагирования

KEDR Response (script)

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути
- Логирование реагирования в системном журнале

Telegram Response

Оповещения об алерте в телеграм

KWTS

- Блокировка по IP
- Блокировка по URL
- Блокировка по Домену

AD Response (script)

- Блокировка УЗ и разблокировка
- Выход пользователя из активных сессий
- Добавление УЗ в группу и исключение из группы

UserGate Response

- Блокировка по IP
- Блокировка по URL
- Блокировка по Домену

KSMG

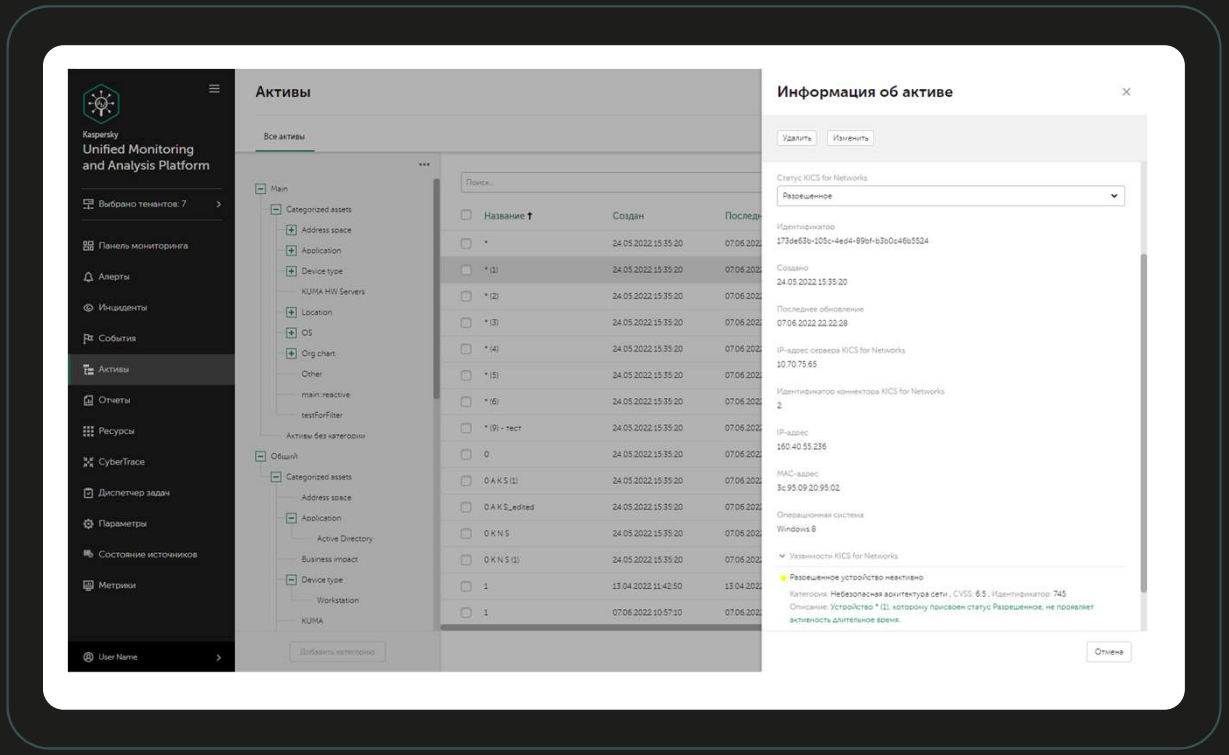
- Блокировка по email-адресу
- Блокировка по IP

Пример 8. Интеграция с Kaspersky Industrial CyberSecurity

Kaspersky
Industrial CyberSecurity
for Networks

Импорт активов вместе
с уязвимостями

Реагирование вручную
из карточки



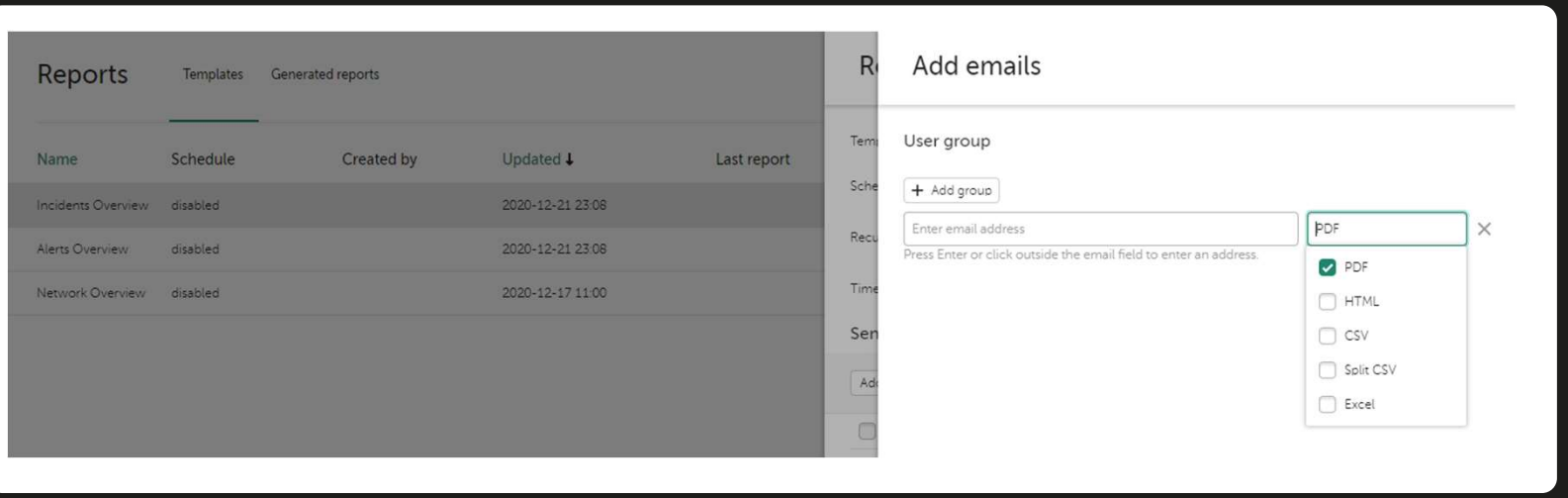
Визуализация
и отчетность

EO36

Генерации отчётов

Доступны следующие форматы:

HTML | PDF | CSV | раздельный CSV | Excel



Slide 52

EO36 Изменить логику подачи

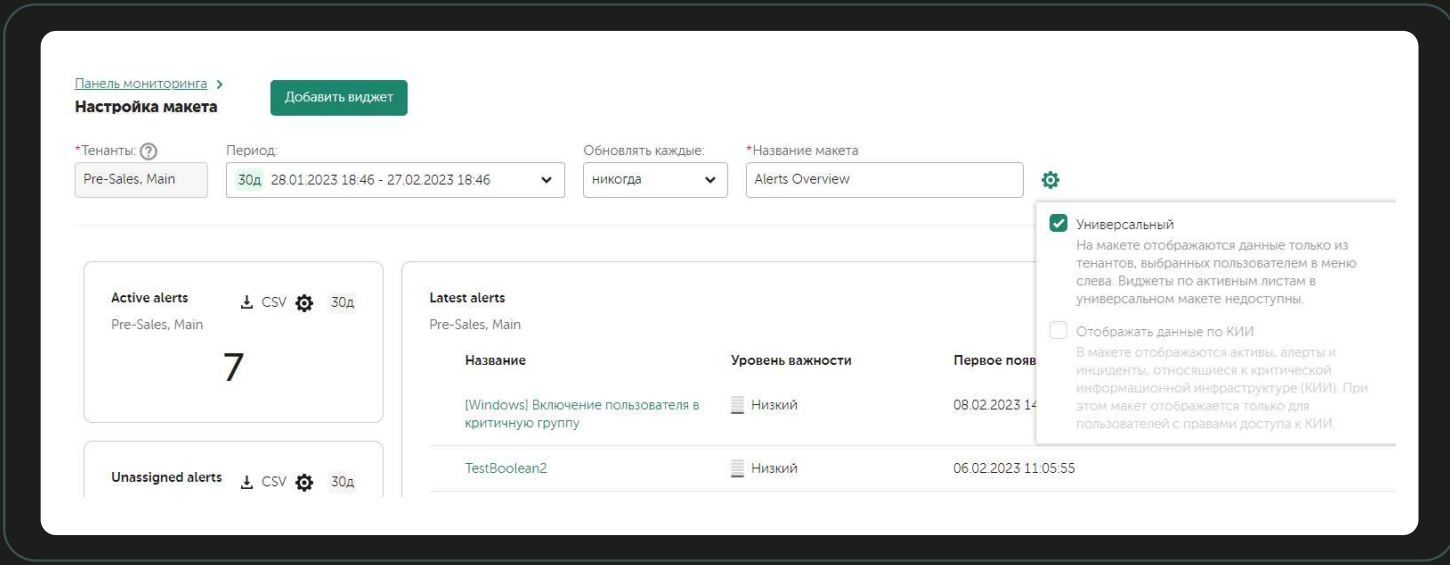
Elizaveta Orzhekovskaya; 28.09.2023

EO37

Обновления в дашбордах

Единые для всех тенантов (общие) шаблоны дашбордов

Скачивание данных в CSV

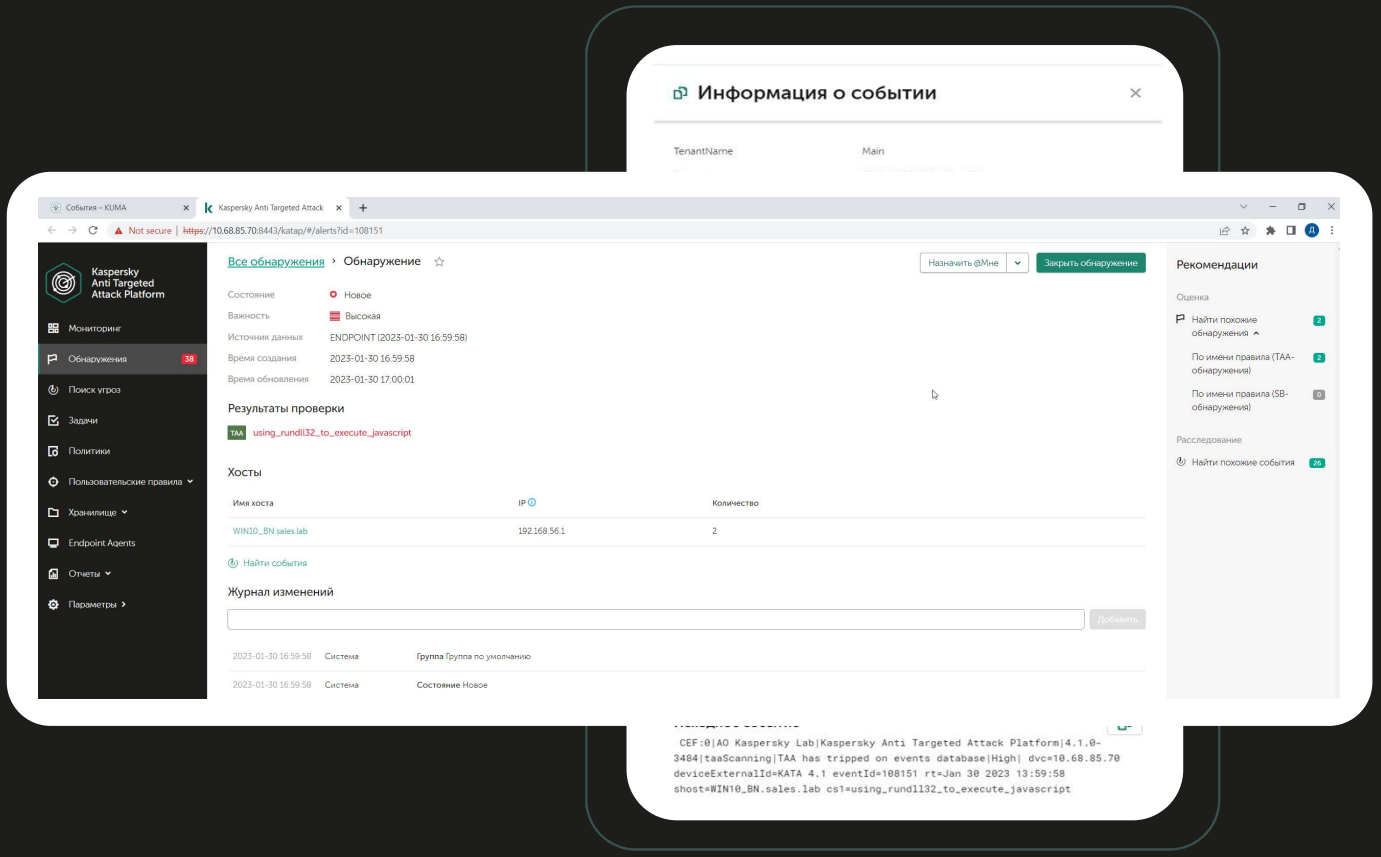


EO37 Изменить логику подачи

Elizaveta Orzhekovskaya; 28.09.2023

Расширенная интеграция KES / KEDR Expert / KATA

Для событий
о срабатываниях
KATA/EDR
добавлена ссылка,
позволяющая
перейти на
карточку алерта
в KATA/EDR



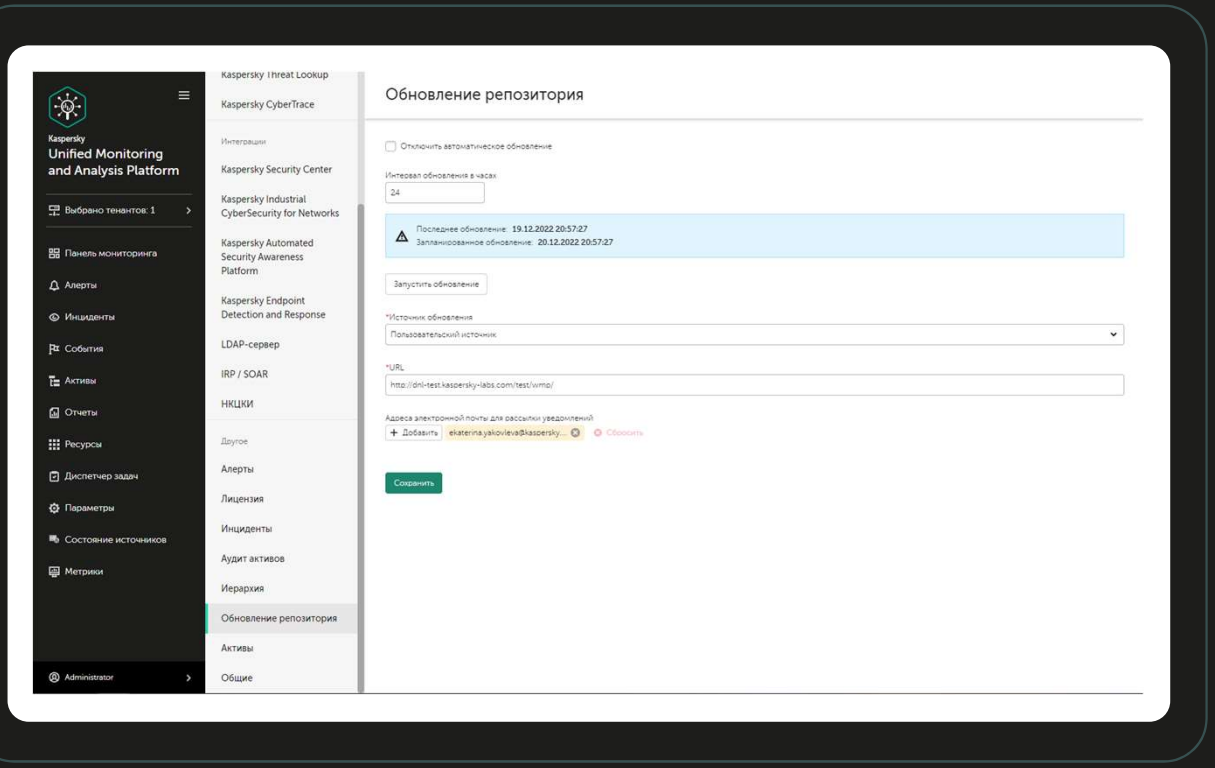
Централизация
и унификация

Подсистема обновления

оперативно получает информацию о доступных обновлениях контента

анализирует содержимое каждого обновления

в том числе без прямого доступа к интернету с использованием механизма «зеркала обновления»



KUMA — **лидирующее SIEM** решение в РФ и центральный элемент XDR

Эффективность команд SOC

Автореагирование, единый список событий для расследования и хантинга

Гибкость

Сложные схемы развёртывания, широкие возможности корреляции, мощный поиск

Производительность

KUMA — центральный элемент XDR

Технологическое ядро Kaspersky Symphony XDR

Сильные стороны Kaspersky Symphony XDR

Kaspersky Symphony

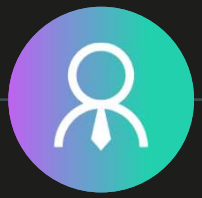
XDR

Фокус на конечные точки

Включен EDR в синергии с EPP – они уже защищают более чем 60 миллионов корпоративных рабочих мест по всему миру

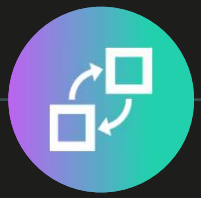
Фокус на аналитику об угрозах

Включена признанная лучшей в мире аналитика об угрозах (по результатам Forrester Wave: External Threat Intelligence Services 2021)



Фокус на киберграмотность

Включены модуль контроля и повышение осведомленности рядовых сотрудников



Фокус на взаимодействие

Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии, гибкость сетевой защиты (Netflow, движки KATA, загрузка TI в сторонние инструменты – IDS&APT фиды). Взаимодействие с решениями сторонних поставщиков

Фокус на соответствие

Помогает обеспечить соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА

Фокус на качество

В состав входят продукты, заслужившие признание аналитиков, независимых лабораторий и клиентов по всему миру

SE Labs AAA December 2021 ADVANCED SECURITY (EDR)

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

AV TEST

FORRESTER®

Цифры говорят больше слов

>25 лет

«Лаборатория Касперского» в сфере информационной безопасности

>400 млн

Пользователей используют наши защитные решения

>240 тыс.

Компаний по всему миру мы оберегаем от киберугроз

>$10 трлн

Сумма бизнес-активов, защиту которых мы обеспечиваем

>380 тыс.

Уникальных вредоносных объектов мы обнаруживаем ежедневно

>650 млн

Кибератак было остановлено нашими решениями в 2022 году

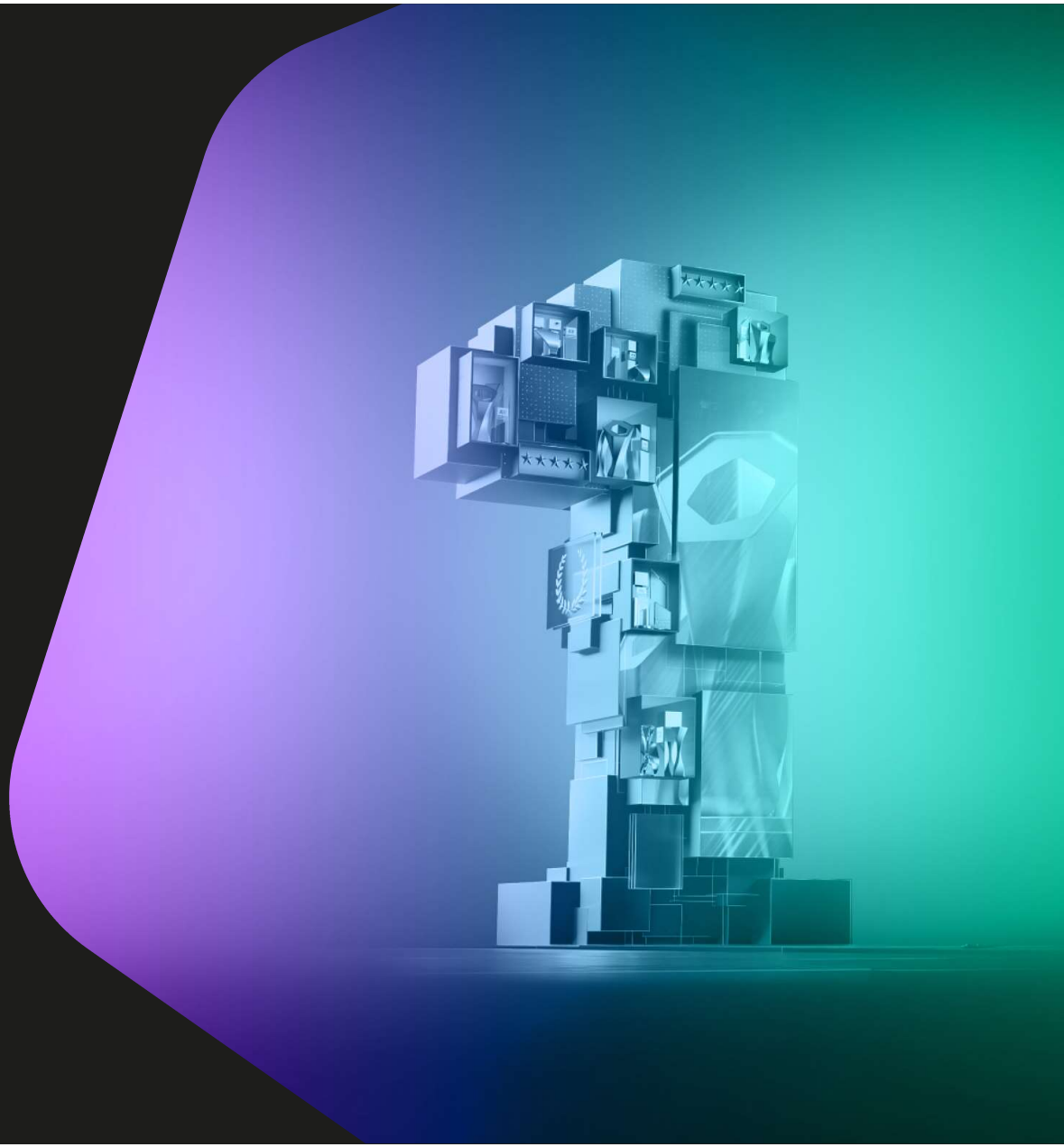
Фокус на экосистемность

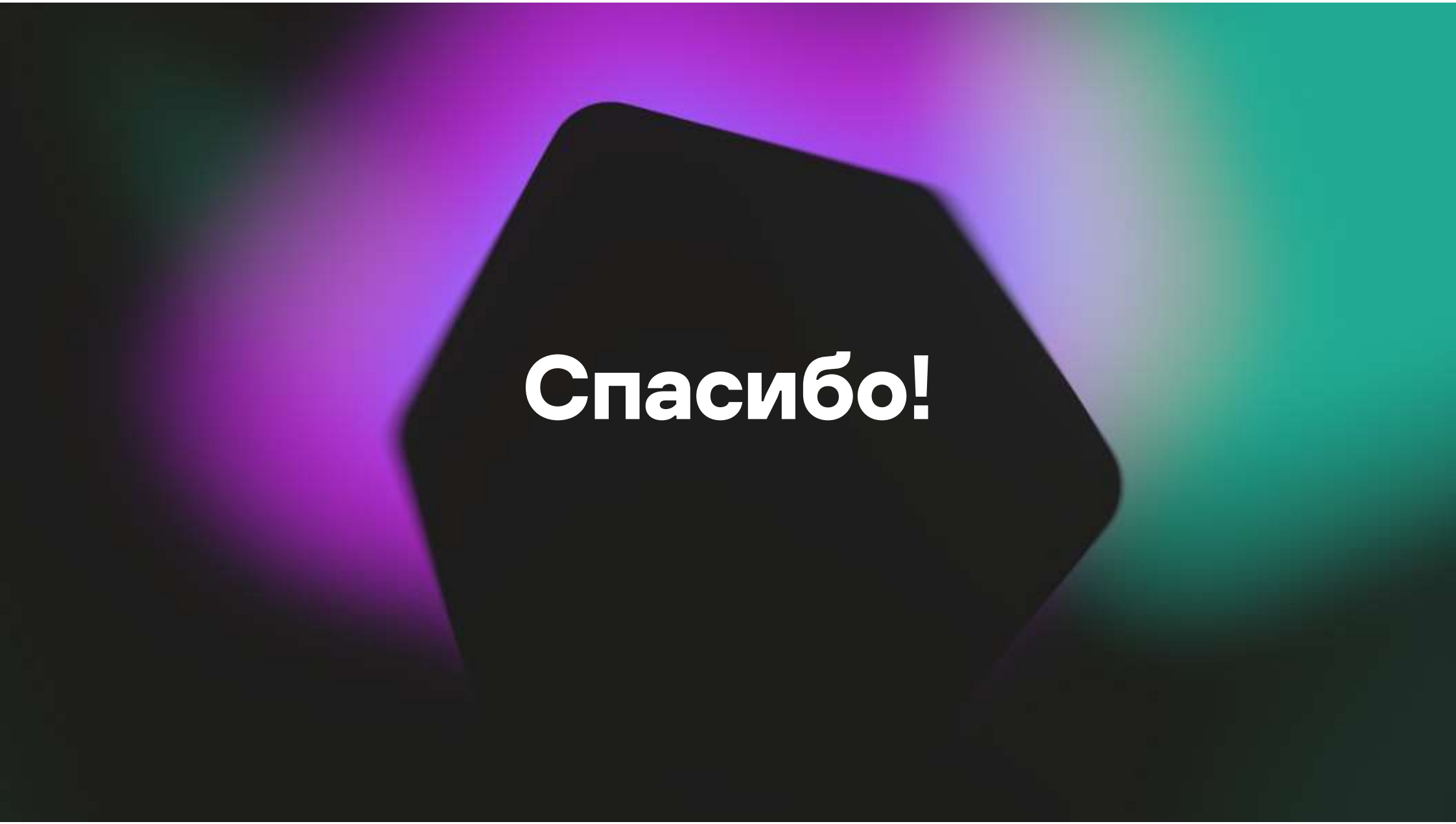
Единый партнер по кибербезопасности

Обеспечение комплексной защиты

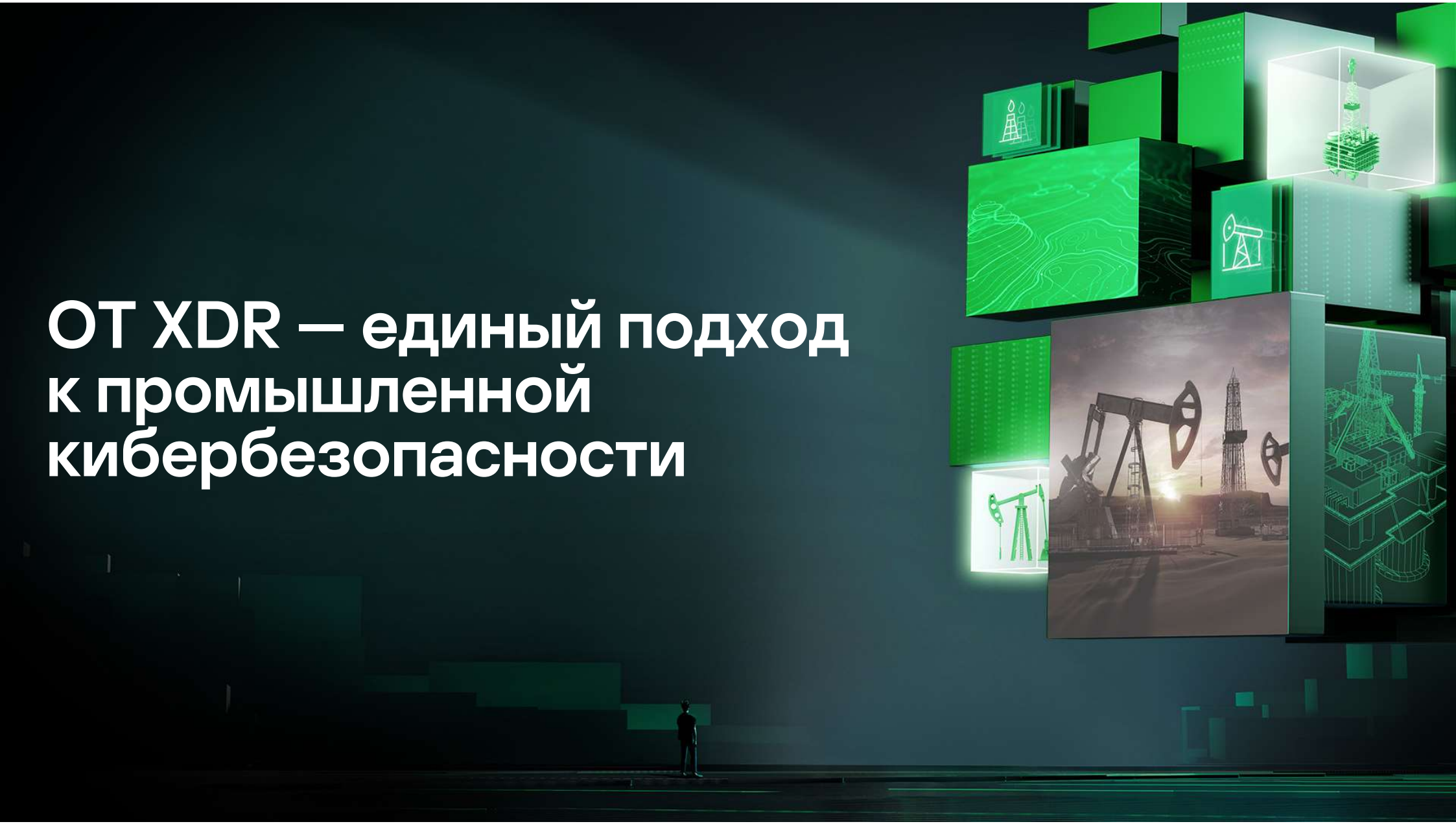
Единая точка взаимодействия

Надежность и уверенность




Спасибо!

OT XDR — единый подход к промышленной кибербезопасности



Архитектура платформы и основные функции

Kaspersky Industrial CyberSecurity

Управление активами и рисками

Пассивное обнаружение компонентов OT и уязвимостей. Опциональный активный опрос, ориентированный на риски, ситуационная осведомленность и отчетность

Детектирование и реагирование на уровне сети

Анализ сетевого трафика для обнаружения вторжений на самом низком уровне (протоколы ICS, DPI и сигнатуры IDS)

Детектирование и реагирование на уровне конечных узлов

Защита от вредоносных программ, контроль доверенных устройств и ПО. ICS EDR позволяет анализировать первопричины инцидентов в OT

Kaspersky Industrial CyberSecurity for Nodes

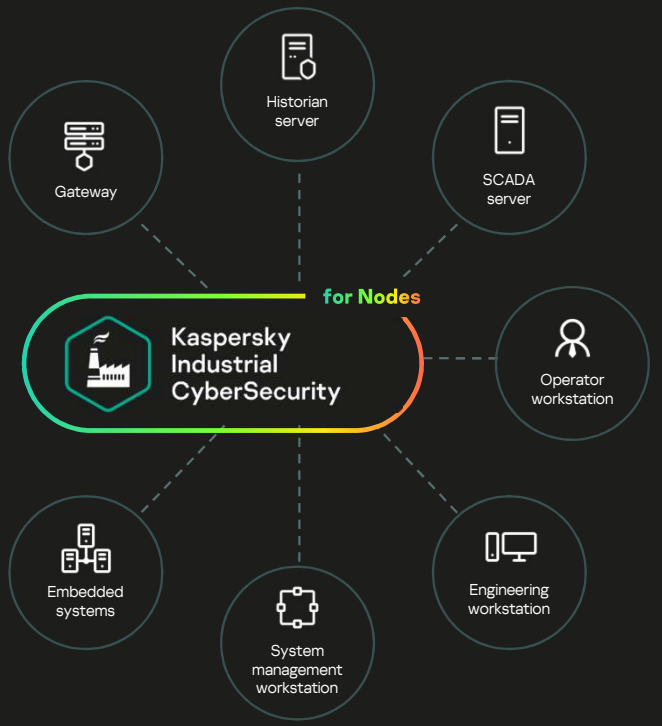
Промышленная защита конечных точек,
средство EDR и сенсор телеметрии

KICS for Nodes компоненты

Windows Nodes

- Антивирус
- Контроль запускаемых приложений
- Контроль устройств
- Контроль целостности файлов
- Контроль целостности ПО ПЛК
- Защита от шифрования сетевых папок
- Защита от эксплойтов
- Защита от сетевых угроз
- Анализ журналов Windows
- Управление Firewall
- Мониторинг доступа к реестру
- Портативный сканер
- Аудит безопасности
- EDR агент
- Сенсор телеметрии (Интеграция с KICS for Networks)

Industrial Endpoint Protection



Отраслевая специфика: целостность ПО ПЛК и ICS coverage

Контроль целостности ПО ПЛК

Контроль проекта ПЛК и отслеживание изменений

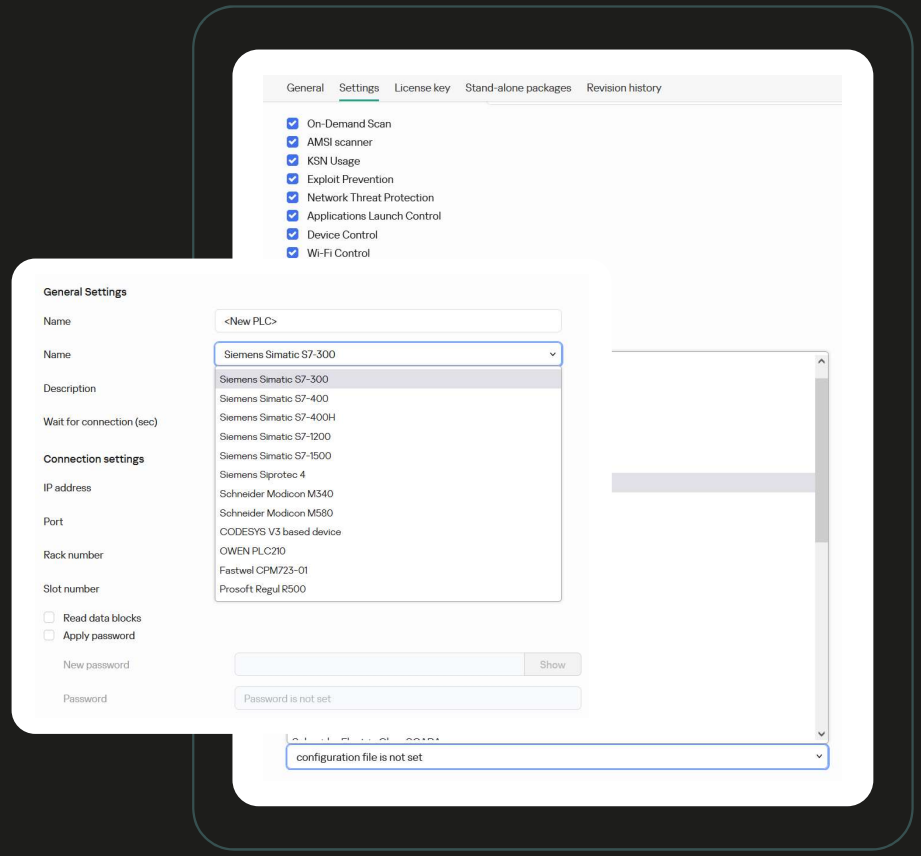
Проверка совместимости

Сотрудничество с поставщиками промышленной автоматизации, проведение сертификации и тестов на совместимость, подготовка совместных эталонных моделей и интеграция наших различных продуктов и решений

Профили безопасности для конечных устройств

Рекомендуемые настройки доверенной зоны и исключения процессов доступны из коробки и применяются прямо на этапе установки:

- Экспертиза, основанная на результатах тестирования совместимости
- Руководства администратора на системы АСУТП



KICS for Nodes: Портативный сканер

Решает задачи:

- Сканирование или защита автономных систем
- Сканирование или защита систем, в которых использование антивирусного программного обеспечения запрещено из-за рисков совместимости или нарушения целостности
- Позволяет проводить проверку безопасности ноутбуков гостей или субподрядчиков перед выполнением работ на месте

- Преобразуйте флэш-накопитель в портативный сканер KICS for Nodes
- Используйте этот портативный инструмент на нескольких узлах ICS, даже с устаревшей ОС
- Подход, не требующий установки и не влияющий на работу технологического узла
- Режимы блокировки или «только уведомлять»
- Отчеты для всех хостов, хранящиеся на портативном накопителе сканера

KICS for Nodes с KICS Portable лицензией

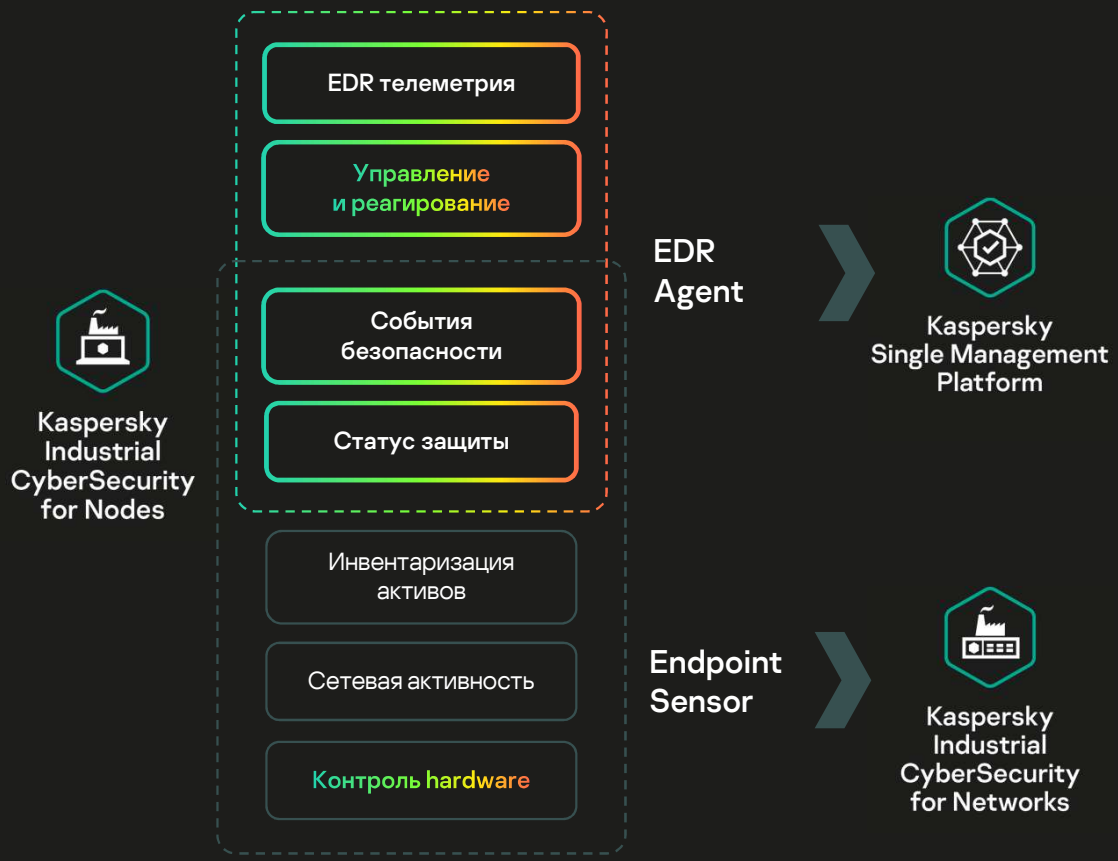
Любой USB флэш-накопитель

- Защита от копирования
- Работа с командной строкой
- Не требует установки

- Сканирование узла, не позволяющего установить какое-либо дополнительное ПО

- Отчет о сканировании сохраняется на флэш-накопитель.
- Сканирование узлов один за другим одним флэш-накопителем

Больше чем просто Защита конечных устройств



Kaspersky Industrial CyberSecurity for Nodes

Многофункциональное решение

EPP, EDR агент с возможностью инвентаризации и аудита

Промышленный EDR

Обнаружение и телеметрия для анализа первопричин, реагирования при необходимости

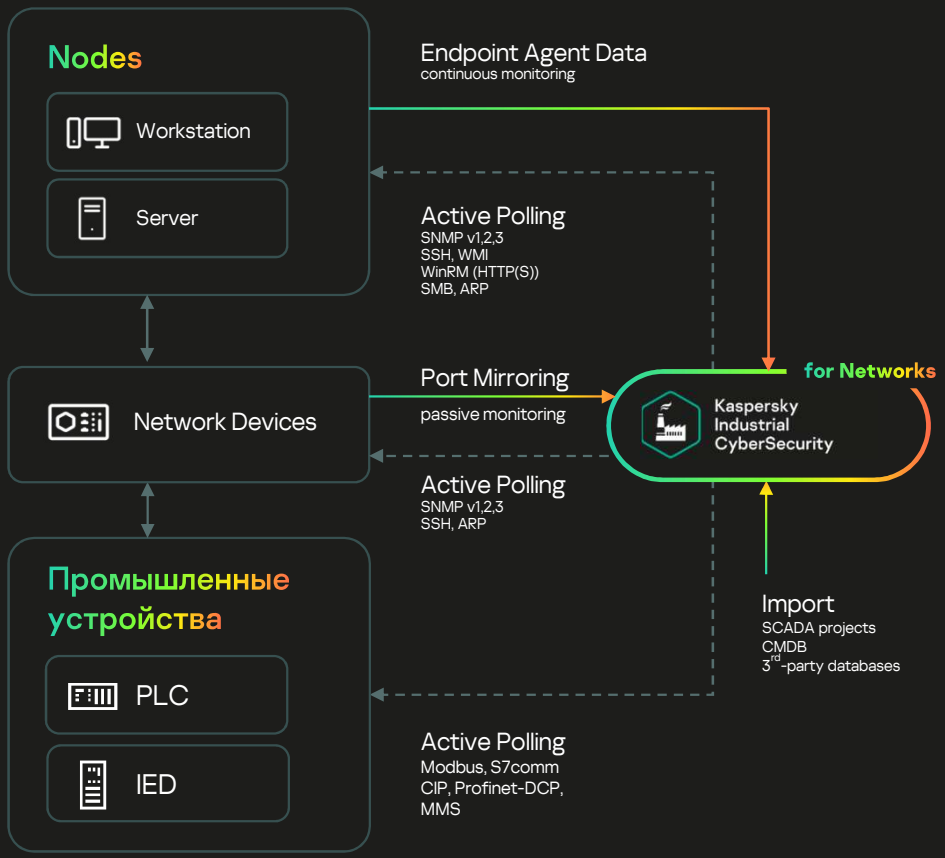
Телеметрия с конечного узла

Полная видимость и ситуационная осведомленность благодаря обнаружениям и обогащению данных с конечного узла

Kaspersky Industrial CyberSecurity for Networks

Обнаружение и визуализация промышленных сетей,
управление рисками и обнаружение угроз

Инвентаризация устройств



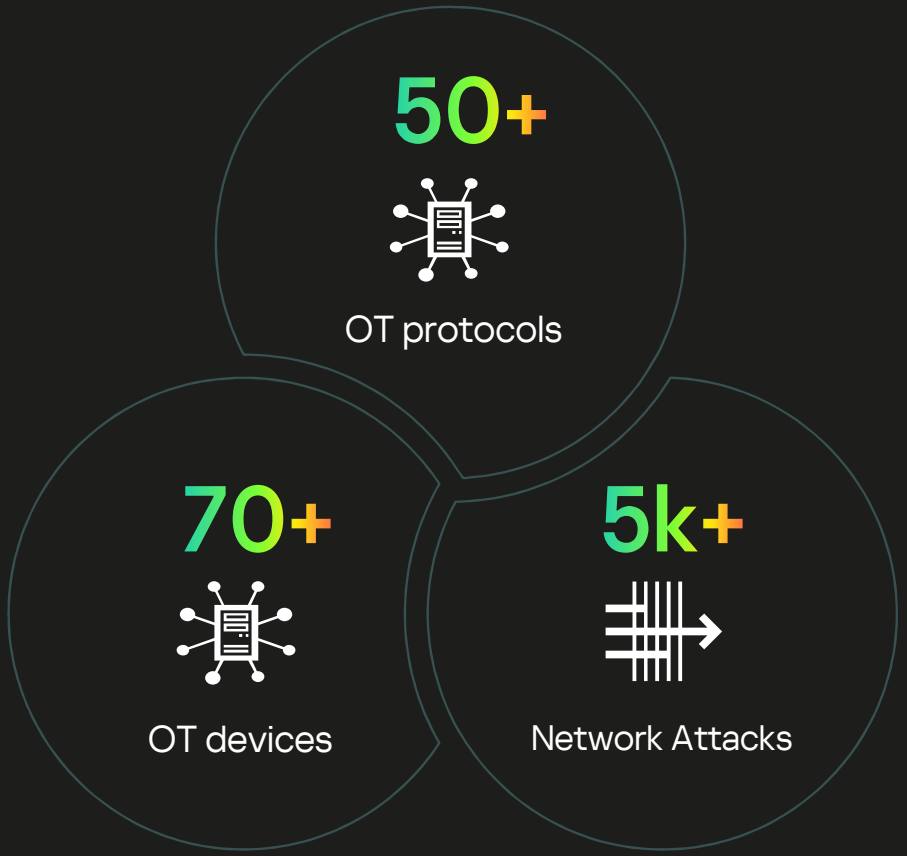
Методы инвентаризации сети

1. Пассивный мониторинг (SPAN сессия)
2. Телеметрия с агента на узле
3. Активный опрос
4. Импорт конфигураций SCADA / DSC / PLC проектов

Ключевые преимущества

- Автоматическая инвентаризация и категоризация устройств, анализ рисков и аудит безопасности
- Вариативность методов и комбинированный подход к инвентаризации активов
- Эффективный подход для любой ситуации, в зависимости от этапа производства на объекте
- Инвентаризация без SPAN сессии
- Автоматическое определение активного метода опроса по категории устройства, только протоколы и порты, поддерживаемые устройством, без вредоносного сканирования

Поддержка промышленных устройств и протоколов



- Глубокая проверка пакетов для протоколов OT и IT
- Поддержка новых устройств и протоколов предоставляется с обновлениями, без переустановки продукта и не в качестве дополнительного экспертного пакета
- Автоматическое определение и отслеживание значений тегов, автоматическая генерация правил процесса, готовых к включению
- Импорт SCADA-проектов для устройств и меток
- Пассивная проверка целостности проекта ПЛК

Централизованная система аудита узлов промышленной сети

Ключевые преимущества

Аудит безопасности для узлов на Windows, Linux и сетевого оборудования

Задачи для одного узла или групповые, запускаемые вручную или по расписанию

Полнофункциональный редактор для проверок и параметров безопасности

Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT

Стандарт индустрии – Open Vulnerability and Assessment Language (OVAL) + XCCDF

Поддержка сторонних и пользовательских баз OVAL

Отчёты, результаты аудита и история проверок доступны в одном месте

Защищённое хранилище секретов для безагентского аудита

Централизованная система автоматизированного аудита безопасности

Аудит безопасности

SSH

Удаленный

Настройка рабочих станций и серверов:

Настройки безопасности Linux

Конфигурация сетевых устройств:

Активное сетевое оборудование

Агент (KICS for Nodes)

Настройка рабочих станций и серверов:

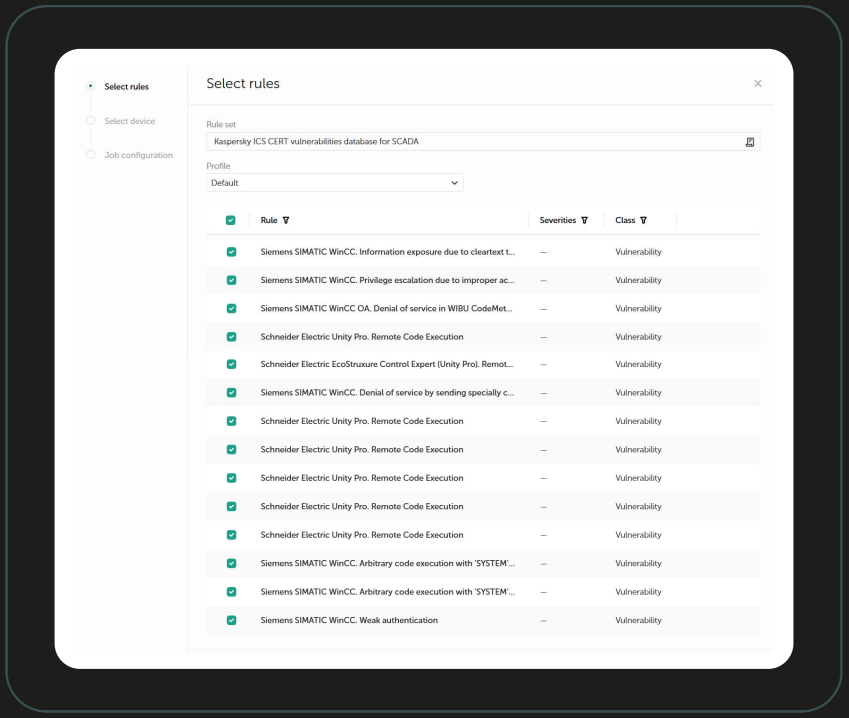
Настройки безопасности Windows

Уязвимости:

Инвентаризация промышленного ПО и обнаружение уязвимостей

Правила аудита безопасности

Мастер выполнения задач аудита с базой данных Kaspersky ICS



Набор конфигураций аудита безопасности, предоставляемых из коробки

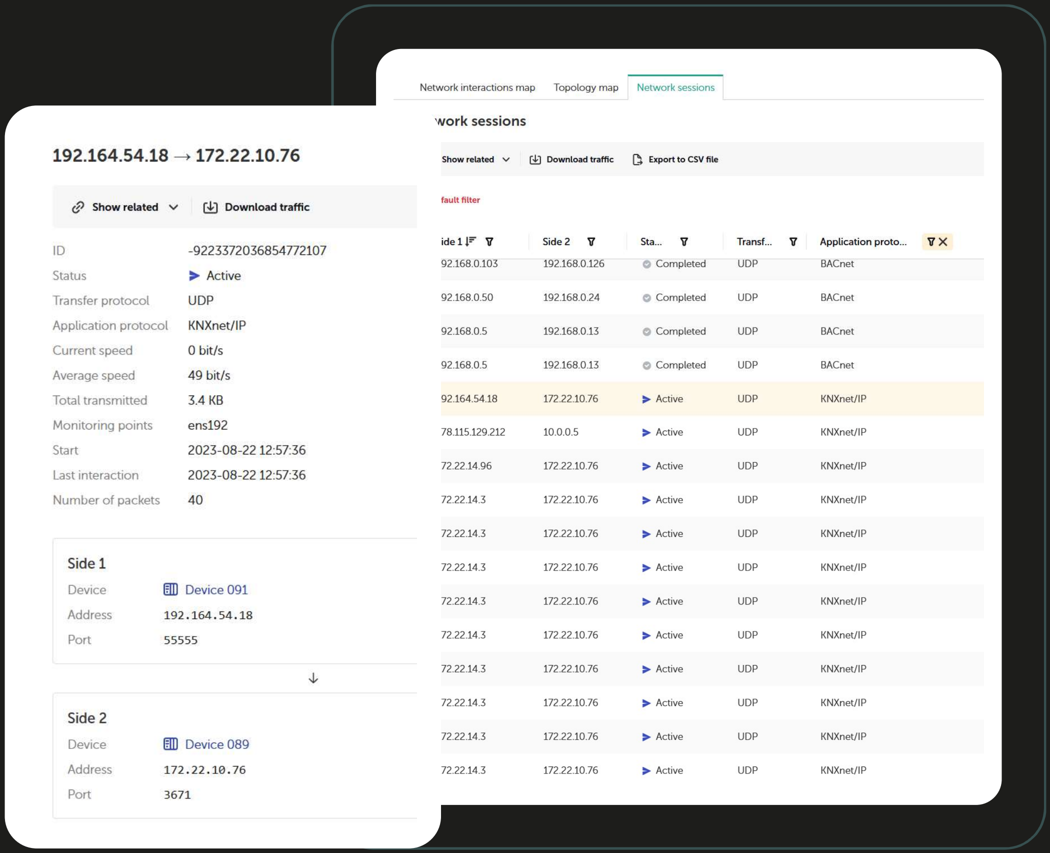
База данных уязвимостей Kaspersky ICS CERT для SCADA

- Общие настройки безопасности для for Windows XP/7/8.1/10/11
- Общие настройки безопасности для Window Server 2012/2012 R2/2016/2019/2022
- Общие настройки безопасности для Debian
- Общие настройки безопасности для Red Hat Enterprise Linux, CentOS, Oracle Linux
- Общие настройки безопасности для Ubuntu
- Общие настройки безопасности для SUSE Linux Enterprise, openSUSE
- Уровень безопасности -1 для маршрутизаторов и коммутаторов Cisco
- Уровень безопасности -2 для маршрутизаторов и коммутаторов Cisco
- Общие настройки безопасности для FortiGate

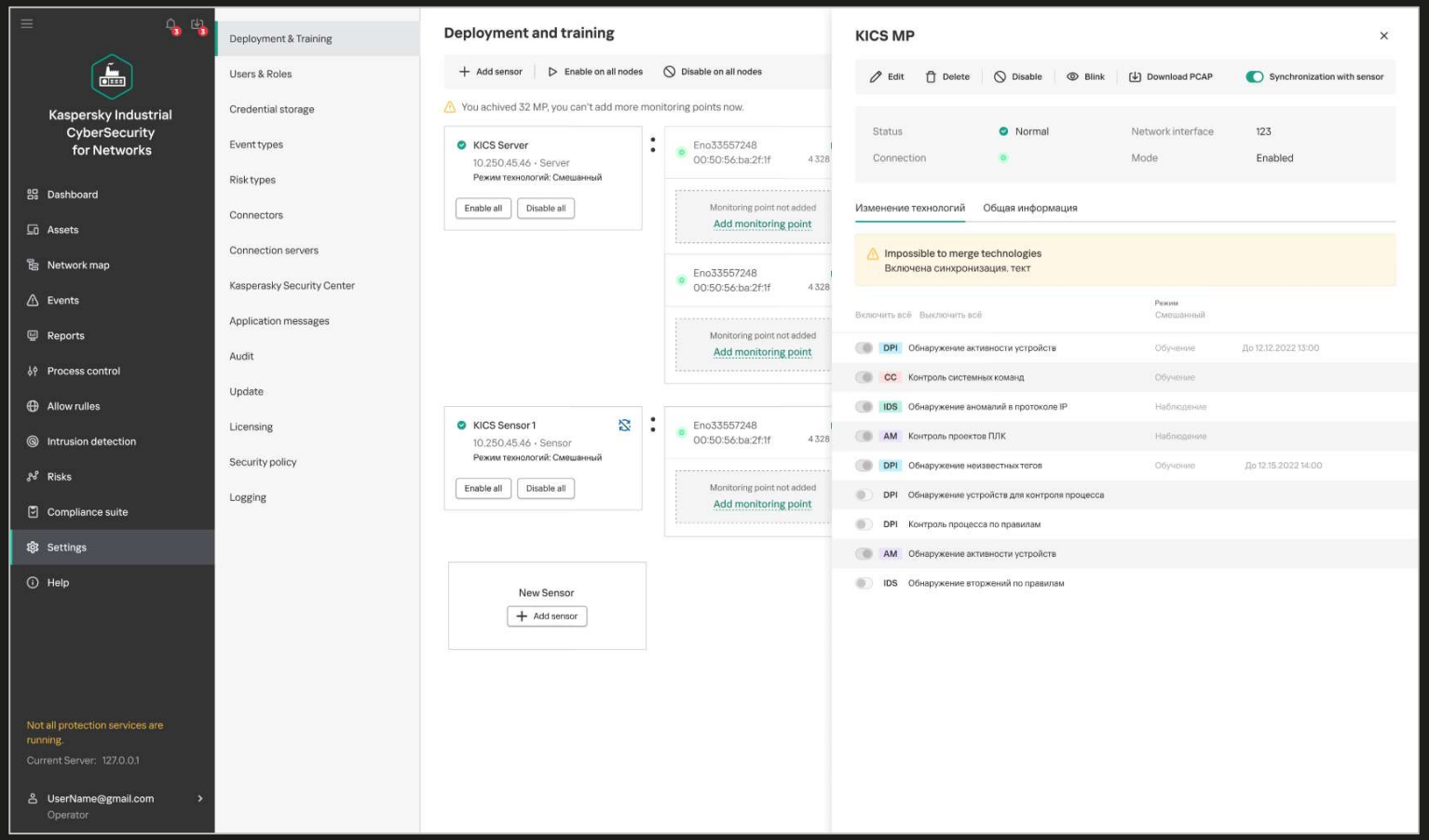
Новые конфигурации будут поставляться вместе с обновлениями продукта, также может быть запрошен конкретный набор правил для поддержки.

Сетевые сессии

- Статус сессий (Активная / Закрытая)
- Направление коммуникаций
- Транспортный и прикладной уровень протоколов
- Статистическая по сессиям (скорость, объем)
- Загрузка трафика для выбранных сессии

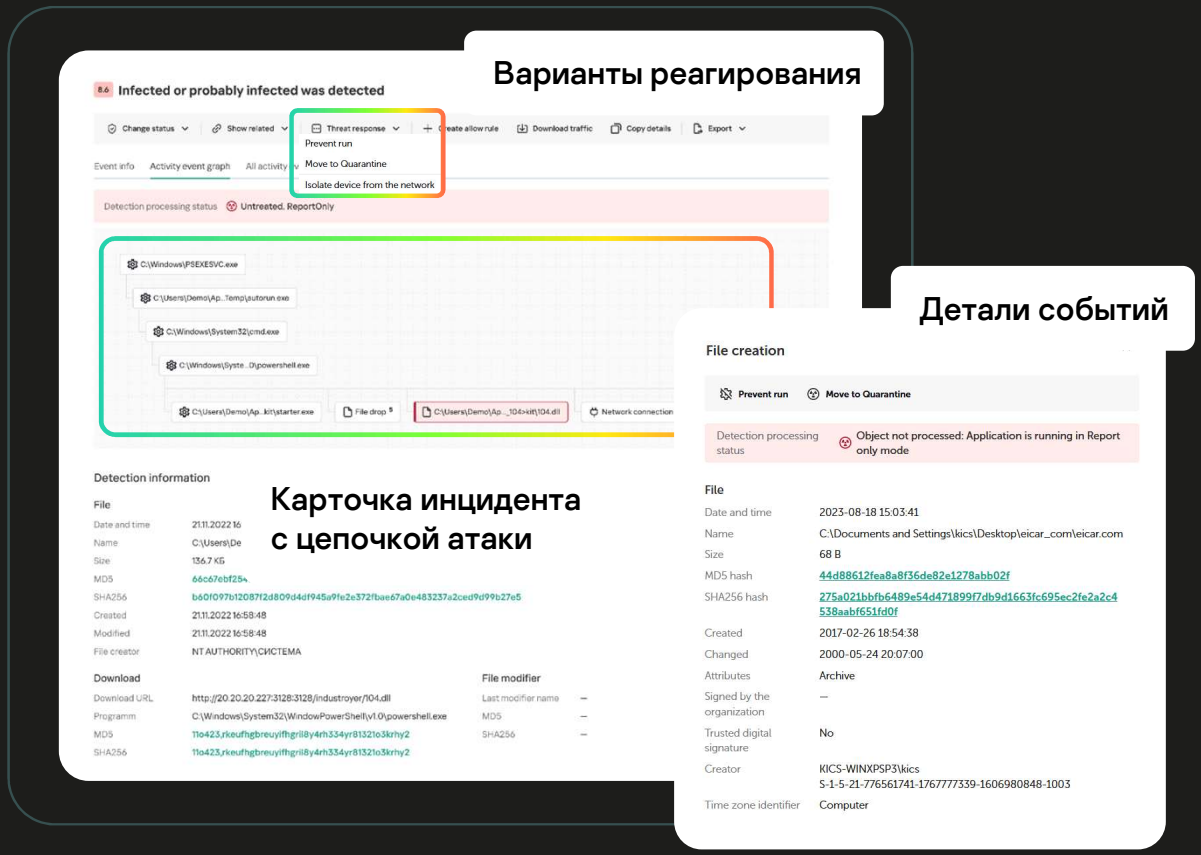


KICS for Networks: Гранулярное обучение



- Гибкость настройки режима работы для сервера, сенсоров, точек мониторинга
- Удобный выбор режима для новых сенсоров
- Разные комбинации режимов работы для технологий
- Расписание для режимов работы

KICS XDR: телеметрия с узла, обнаружение и реагирования

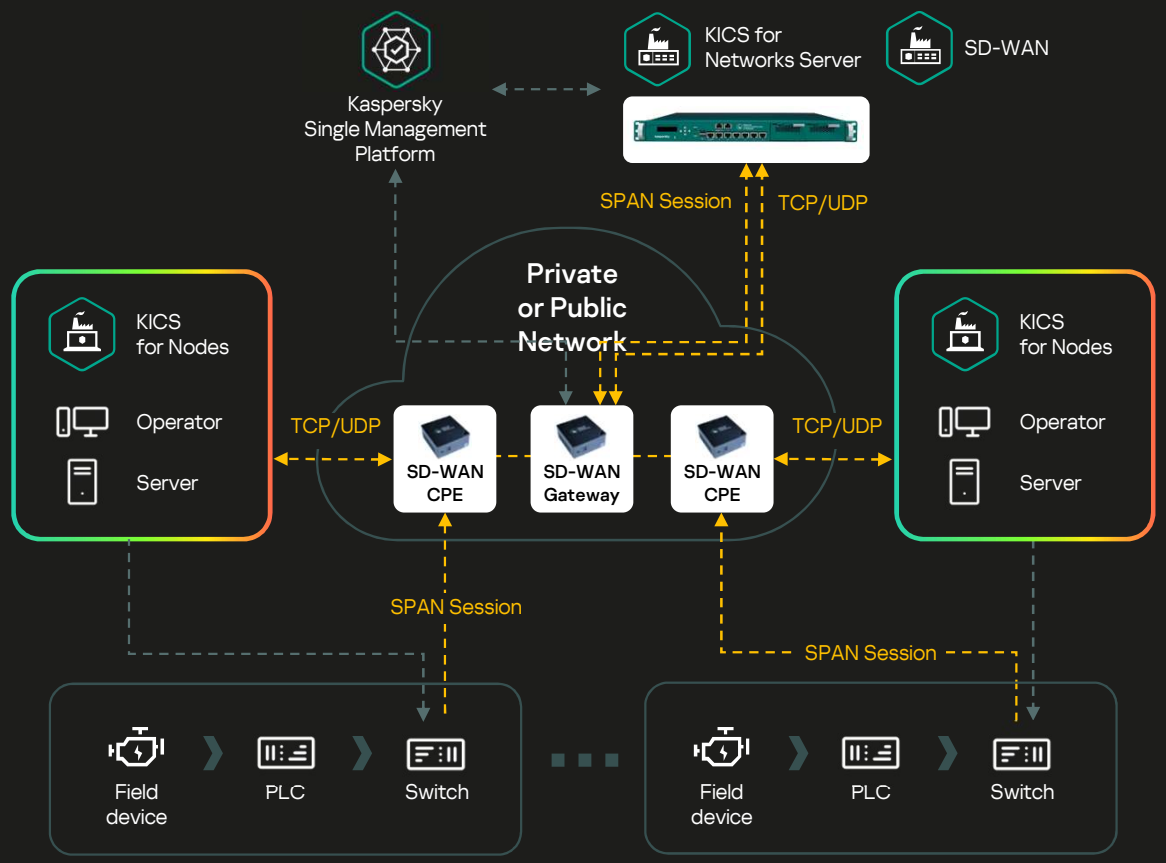


Нативный XDR для расследования инцидентов и реагирования на них

- KICS for Networks – универсальный инструмент для агрегирования информации об обнаружениях, обнаруженных в сети и на конечных узлах
- Телеметрия, связанная с инцидентами, доступна в единой консоли для анализа, включая формат цепочки атаки
- Возможность точечного реагирования

Кросспродуктовые интеграции

Сеть в рамках 1 АСУТП: KICS + SD-WAN

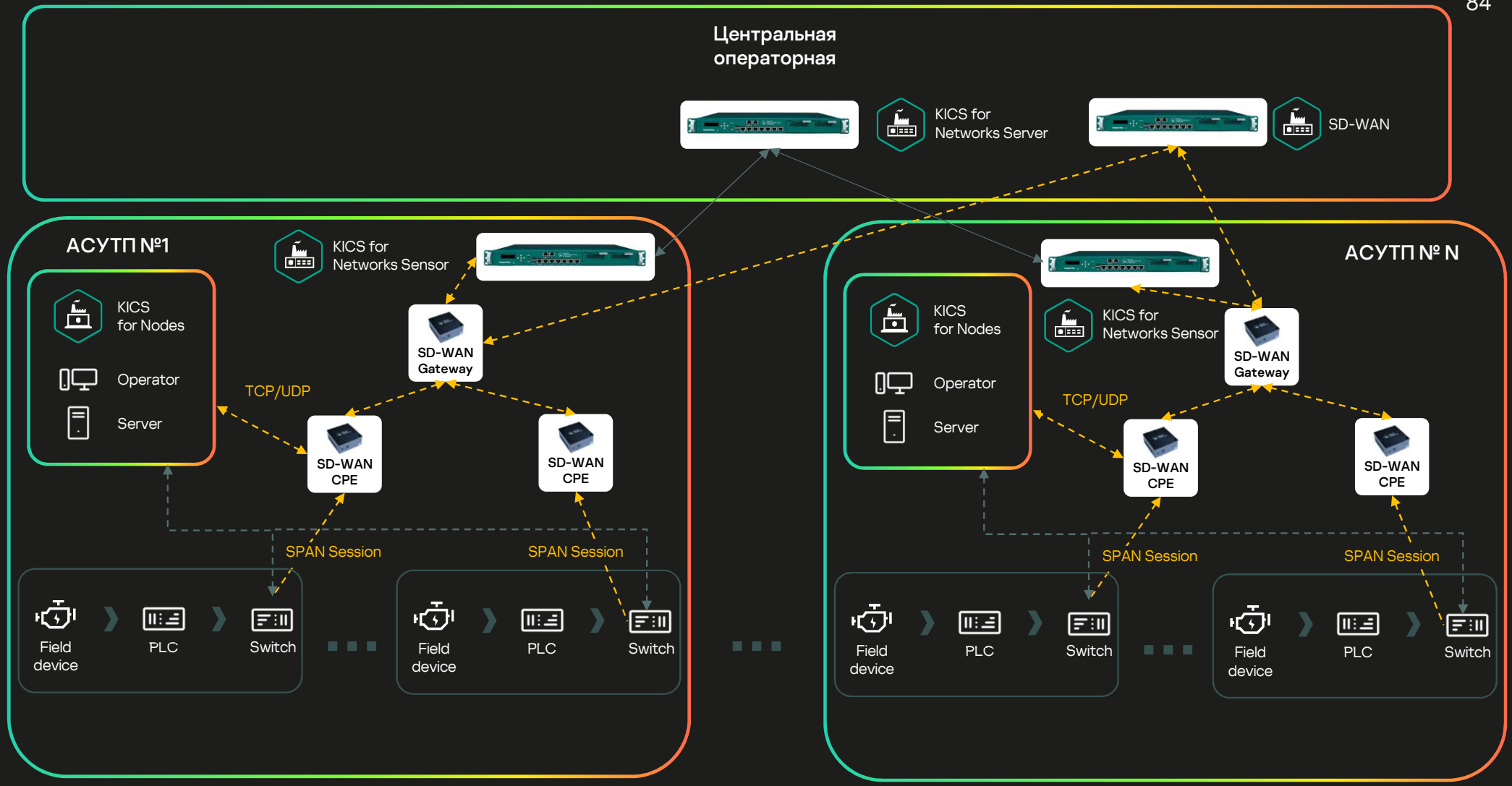


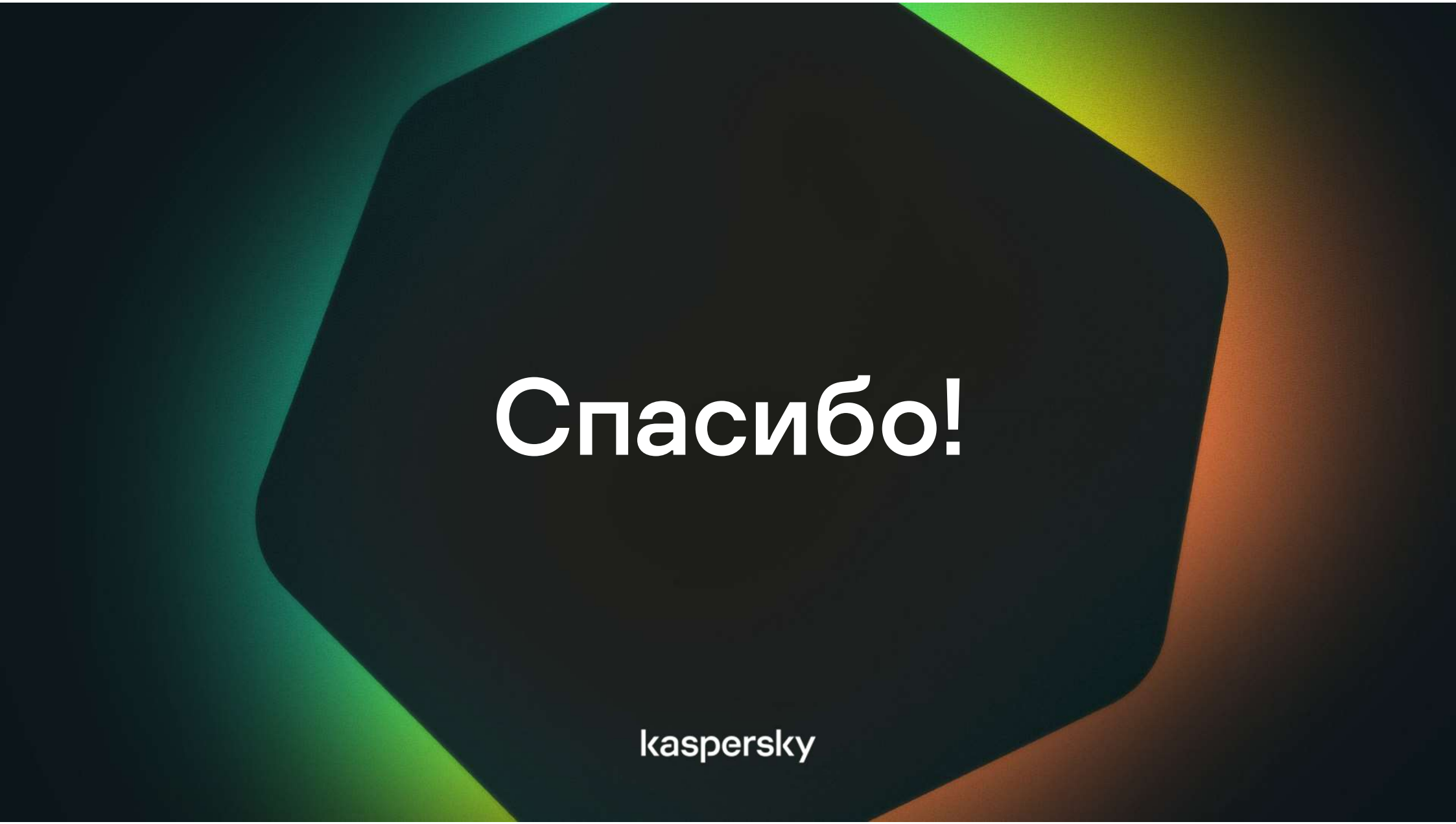
Гибкость создания распределенной инфраструктуры информационной безопасности

Установка портативной SD-WAN CPE для систем, где нет возможности установки полноценного сенсора

Разделение каналов передачи данных внутри канала SD-WAN / поддержка независимых сценариев, не влияющих друг на друга

Сеть в рамках завода: KICS + SD-WAN




Спасибо!
kaspersky

Kaspersky Anti Targeted Attack & Kaspersky EDR Expert

Презентация по продукту

kaspersky

Современные реалии ИБ

Расширяется и / или изменяется IT-инфраструктура, которая требует защиты

Усложняется ландшафт угроз и расширяется поверхность атаки, добавляется целевая киберагрессия и необходимость ИБ-замещения

Усиливаются требования регуляторов, особенно в отношении обеспечения защиты КИИ

Увеличиваются средние потери в результате одного киберинцидента

Процесс работы с инцидентами становится более сложным и ресурсозатратным

Присутствует глобальный дефицит ИБ-экспертов на рынке труда и неоптимальное использование их времени и таланта

Современные кибервызовы

Средний ущерб от успешной кибератаки

SMB: 105k$ **Enterprise:** от 1M$

38%

атак с высоким приоритетом, обнаруженных MDR-сервисом, связаны с APT-угрозами

>40%

случаев реагирования связаны с атаками шифровальщиков

Самые распространенные векторы атаки – эксплуатация уязвимостей, вредоносные письма и компрометация учетных записей

Самым пострадавшим регионом в 2023 году стала Россия и страны СНГ

В 2023 году атакам чаще всего подвергались промышленные предприятия, предприятия розничной торговли и госучреждения

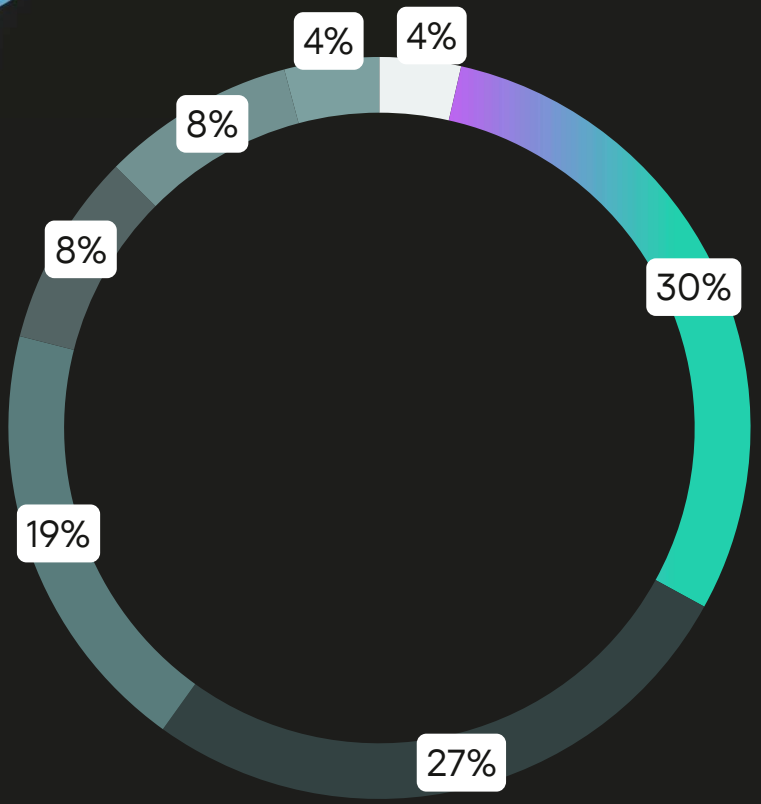
Защита рабочих мест остается критически важной задачей

Атаки длятся от 1–2 дней до нескольких месяцев

Источники данных: Cybersecurity Ventures, Kaspersky
Статистика подготовлена на основе уведомлений об обнаружениях, полученных от пользователей продуктов «Лаборатории Касперского», давших согласие на предоставление статистических данных.

Первопричины опасных инцидентов

- APT-атаки
- Следы APT-атак
- Инсайдер
- Вредоносное ПО
- Критические уязвимости
- Red team
- Социальная инженерия



Статистика подготовлена на основе уведомлений об обнаружениях, полученных от пользователей продуктов «Лаборатории Касперского», давших согласие на предоставление статистических данных.

Предложение для ИБ-команд с высоким уровнем экспертизы

Kaspersky
EDR Expert

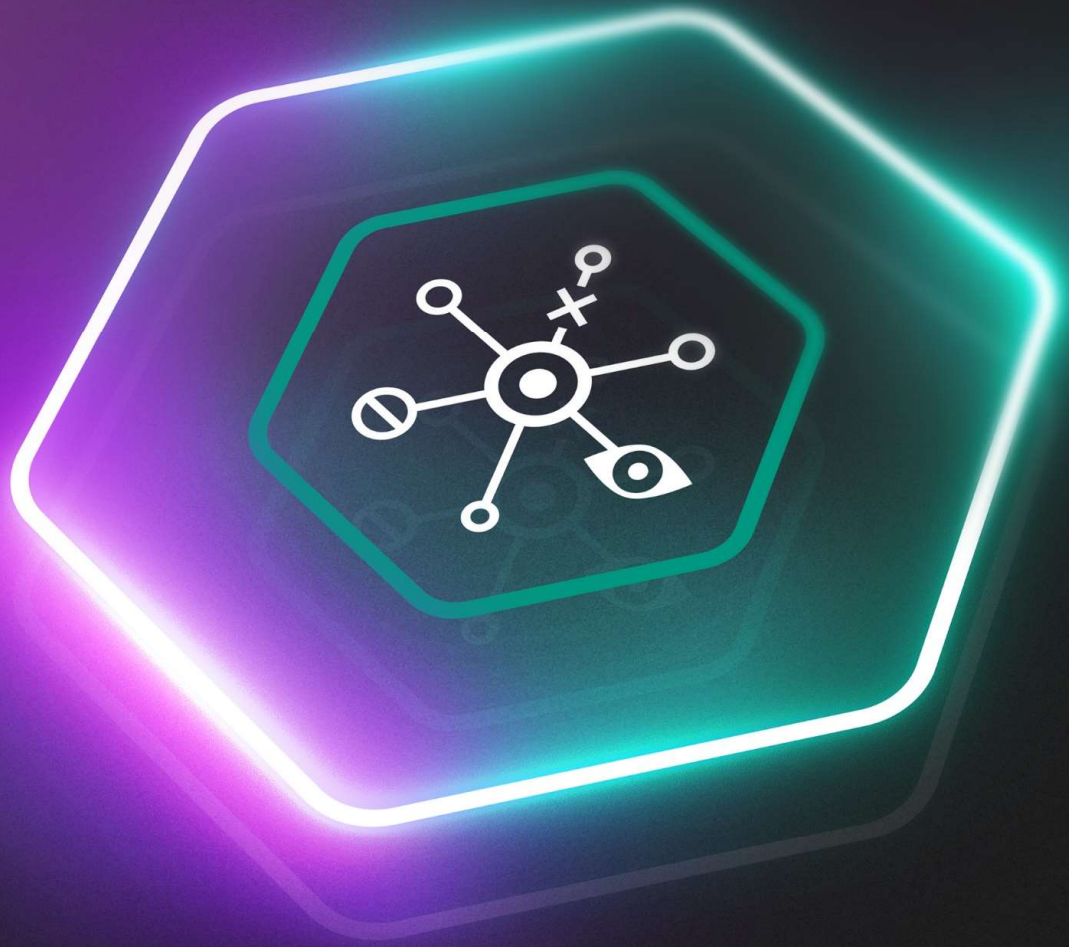
**Защита конечных точек
от сложных и APT-подобных атак**

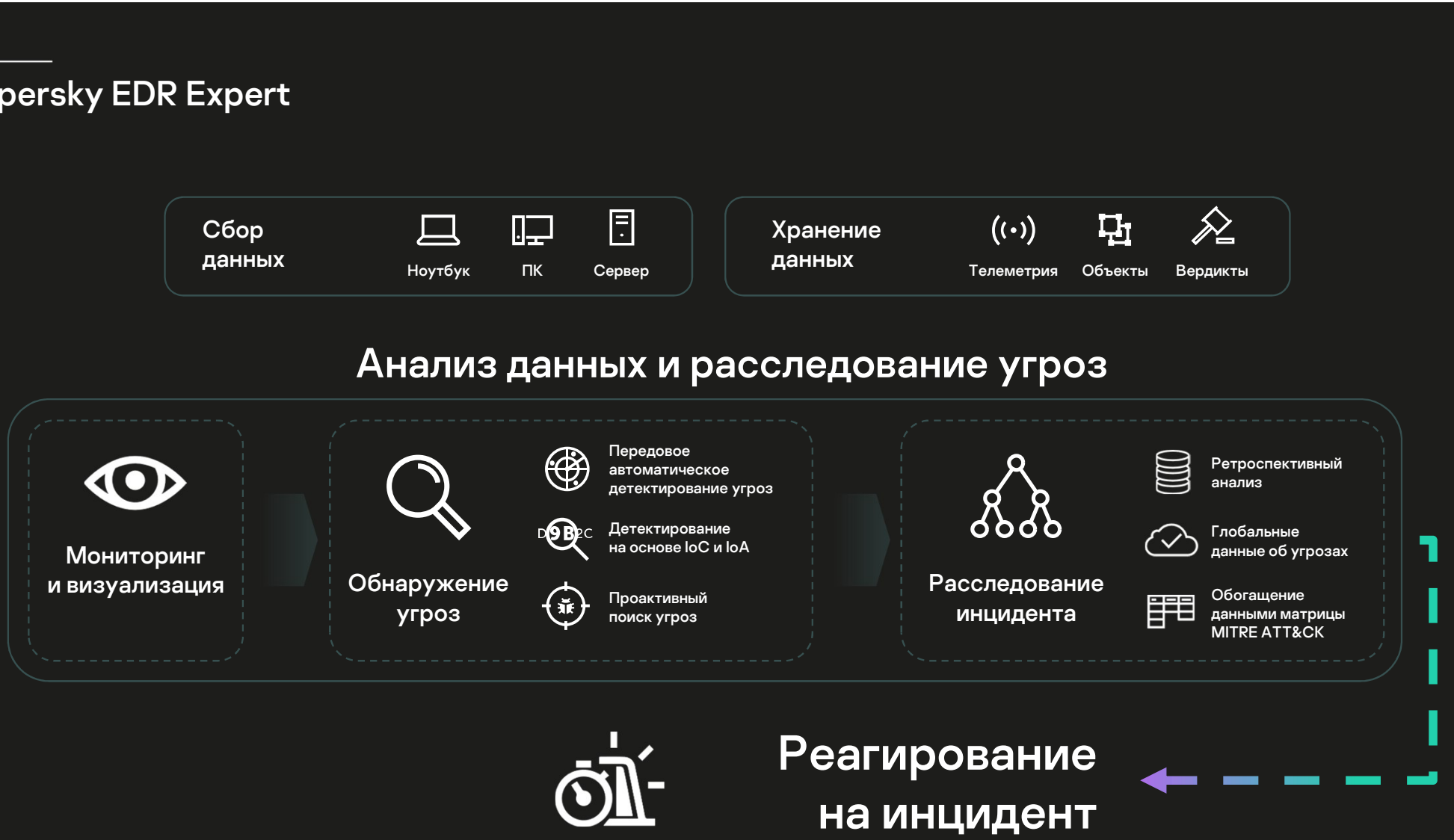
Kaspersky
Anti Targeted
Attack

**Защита сети и конечных точек
от целевых и APT-подобных атак**

Kaspersky EDR Expert

Мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутого обнаружения, эффективного расследования, проактивного поиска угроз и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств




Сбор данных
Ноутбук
ПК
Сервер
Хранение данных
Телеметрия
Объекты
Вердикты
Анализ данных и расследование угроз
Мониторинг и визуализация
Обнаружение угроз
Передовое автоматическое детектирование угроз
Детектирование на основе IoC и IoA
Проактивный поиск угроз
Расследование инцидента
Ретроспективный анализ
Глобальные данные об угрозах
Обогащение данными матрицы MITRE ATT&CK
Реагирование на инцидент

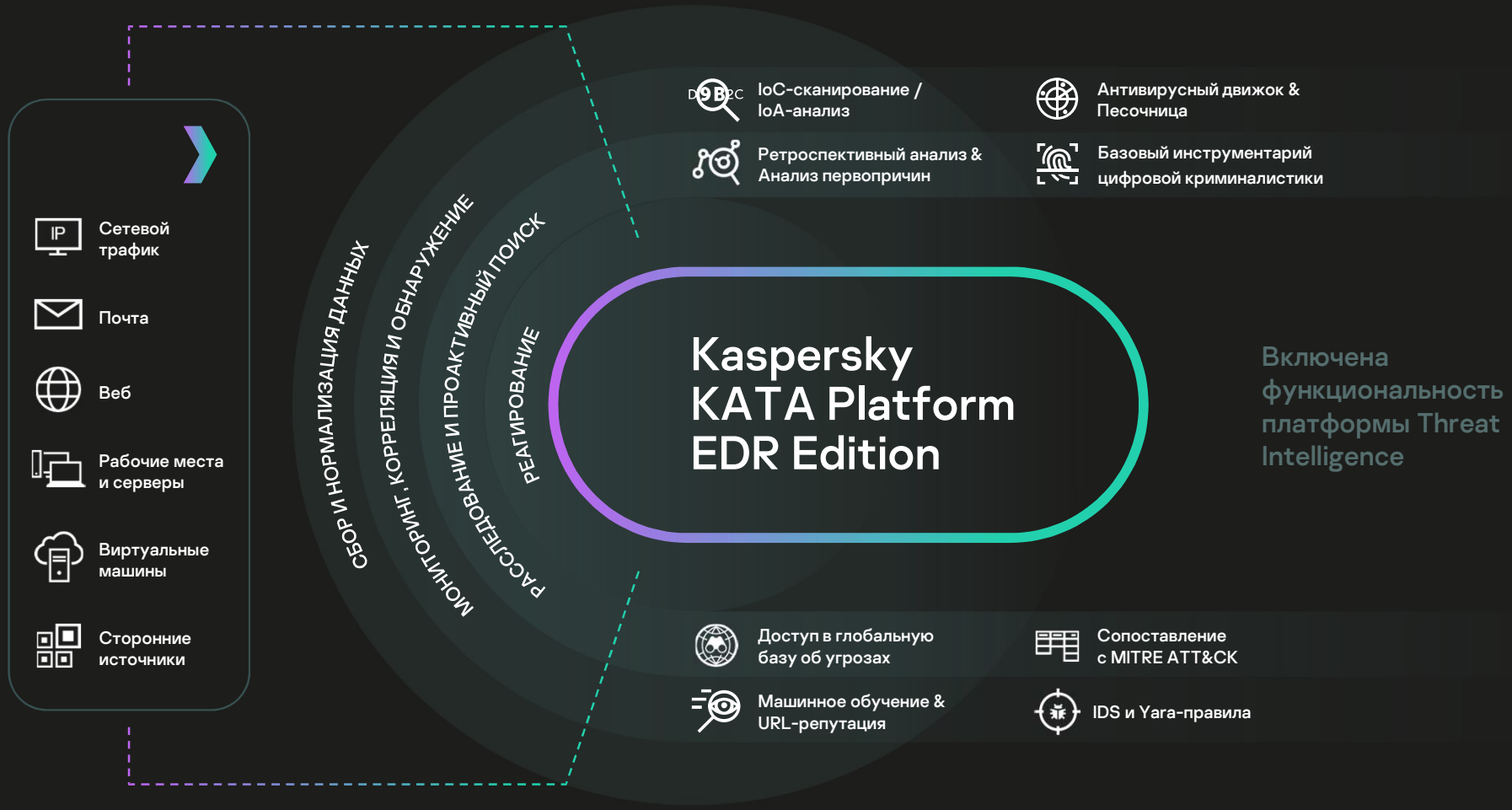
Сравнение EDR решений от «Лаборатории Касперского»

		Kaspersky EDR для бизнеса Оптимальный	Kaspersky Symphony EDR	Kaspersky EDR Expert
Общие сведения	Поддержка ОС Linux		•	•
	Совместная работа с EPP других вендоров			•
Этап: мониторинг / обнаружение угроз	Автоматическая защита конечных точек от массовых угроз	•	•	
	Обнаружение комплексных и целевых атак		•	•
	Глубокий анализ подозрительных файлов (Sandbox)			•
	Проактивный поиск угроз (Threat Hunting)		•	•
Этап: расследование инцидентов	Сопоставление с базой знаний тактик и техник злоумышленников MITRE ATT&CK		•	•
	Детальная информация по подозрительным файлам			•
	Ретроспективный анализ		•	•
	Базовый инструментарий цифровой криминалистики		•	•
Этап: реагирование	Действия по реагированию (запуск файла/скрипта, удаление файла, запрет запуска файла, сетевая изоляция)	•	•	•
	Возможность запуска проверки по YARA-правилам на конечных точках		•	•
	Сбор дополнительных данных для расследования инцидента		•	•
	Рекомендации по расследованию и реагированию		•	•

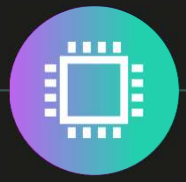
Kaspersky Anti Targeted Attack

Комплексное решение для защиты
от сложных угроз и APT-атак
с расширенным функционалом
обнаружения и реагирования
на уровне сети и конечных устройств
(при взаимодействии с Kaspersky EDR
Expert)

Ключевые возможности



Преимущества



Уникальный стек технологий

Собственный Antimalware Engine

Глобальная репутационная база KSN

Интеграция с Threat Lookup

Встроенный инструментарий для написания YARA правил

Targeted Attack Analyzer

CloudML для проверки APK файлов

Низкие системные требования

Требует на 30% меньше серверных ресурсов чем аналогичные отечественные решения

Масштабируемость

Отказоустойчивость всех компонентов системы

Легкое горизонтальное и вертикальное масштабирование

Развертывание неограниченного количества песочниц в рамках одной лицензии KATA и KEDR Expert

Преимущества

Автоматические и ручные сценарии реагирования

Автоматическое реагирование на почтовом и веб-трафике

Корреляция событий на сети и хостах

Создание правил автоматического запрета запуска исполняемых файлов по вердикту песочницы

Отправка объектов на исследование в песочницу в ручном режиме или по API

Взаимодействие с SIEM

Возможность отправки сырых событий с защищаемых хостов и готовых обнаружений в SIEM по API и Kafka

Автоматическое реагирование на инциденты с помощью EDR через API – изоляция хоста, создание правил запрета запуска файлов и процессов, а также запуск программ

Признание

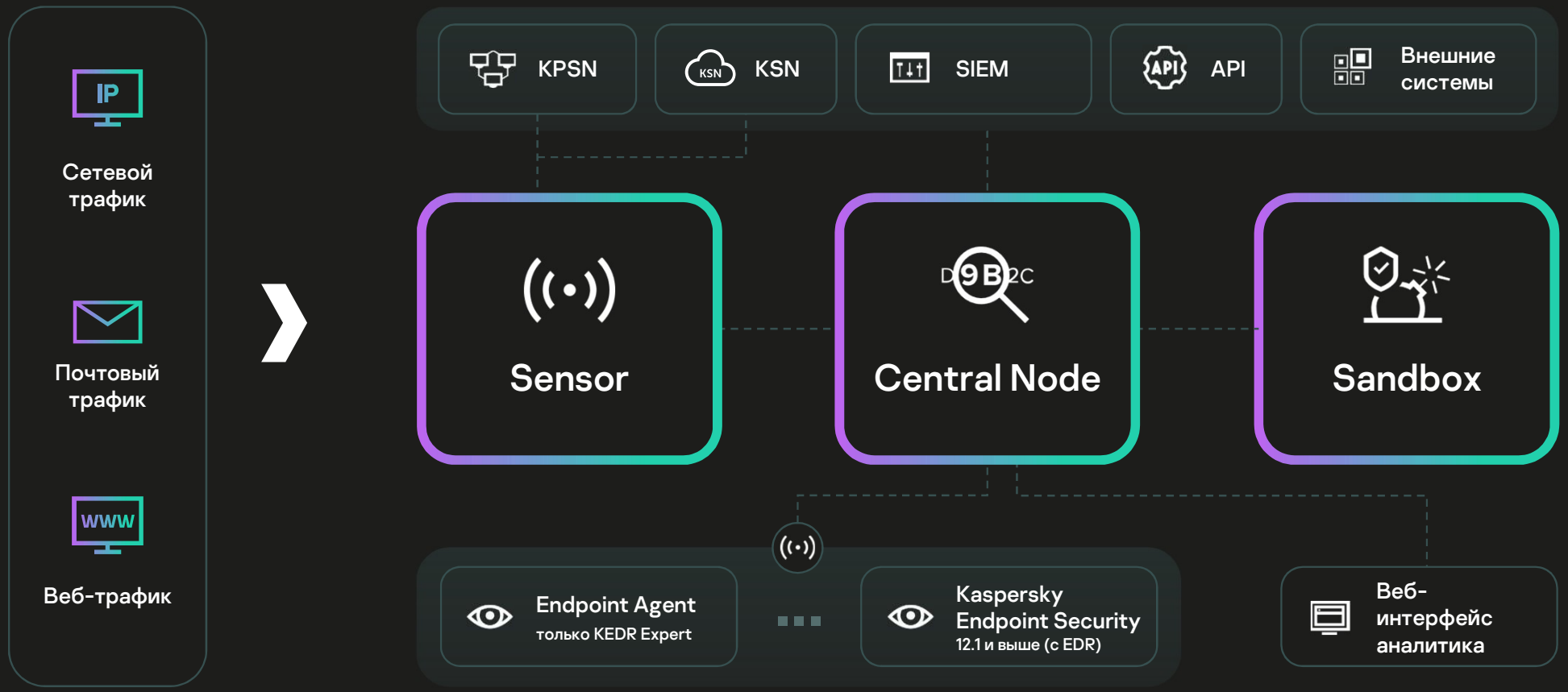
Высокие рейтинги международных агентств

Соответствие требованиям регуляторов

Доверие крупных клиентов

Архитектура
KATA & KEDR Expert

Типовое развертывание на 3 сервера



Платформа KATA и KEDR Expert построены на единой технологической платформе, которая включает:

Central Node (Центр анализа)

Основной серверный компонент платформы. Выполняет проверку данных, их анализ, а также публикацию результатов исследования в веб-интерфейс программы

Sandbox (Песочница)

Запускает виртуальные образы операционных систем и отслеживает поведение файлов в них с целью обнаружения вредоносной активности и признаков целевых атак на IT-инфраструктуру организации

Для автоматического сбора и последующей передачи информации для анализа, KATA и KEDR Expert используют:

Sensor (Сетевой сенсор)

Выполняет прием данных из сетевого, веб-трафика и почтового трафика, а также данных с хостов, защищаемых компонентом Endpoint Agent или Kaspersky Endpoint Security для передачи их на сервер с компонентом Central Node

Endpoint Agent (Агенты на конечных точках)

Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем семейств Microsoft Windows, GNU/Linux. Осуществляет постоянное наблюдение
за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами

На каждом сервере с компонентомCentral Node работают следующие модули и технологии KATA:

Anti-Malware Engine

Выполняет проверку файлов и объектов на вирусы и другого вредоносного ПО, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

Targeted Attack Analyzer

Обнаруживает индикаторы атак (Indicators of attack, IOA) по обновляемым и пользовательским правилам в событиях телеметрии, поступающих от компьютеров.

Mobile Attack Analyzer

Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

YARA

Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями KATA.

Kaspersky (Private) Security Network

Выполняет для KATA проверку репутации файлов и URL-адресов в базе знаний Kaspersky (Private) Security Network и предоставляет сведения о категориях веб-сайтов.

Intrusion Detection System

Технология позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки.

На каждом сервере с компонентомSensor работают следующие модули KATA:

Sensor

Выполняет прием данных из сетевого и почтового трафика и передает их на обработку на сервер с компонентом Central Node. Выполняет проверку поступающего трафика при помощи IDS-правил и репутации KSN.

Intrusion Detection System

Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.

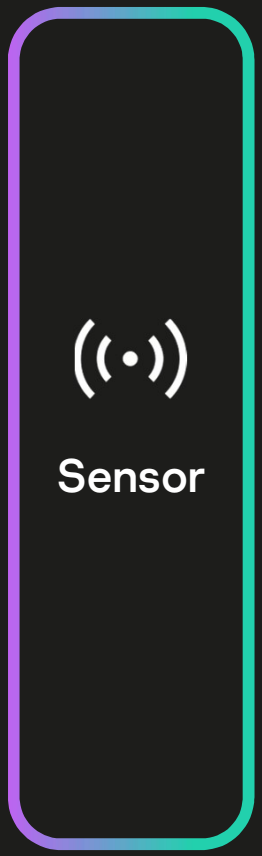
Kaspersky (Private) Security Network

Выполняет для KATA проверку репутации файлов и URL-адресов в базе знаний Kaspersky (Private) Security Network и предоставляет сведения о категориях веб-сайтов.

URL Reputation

Обнаруживает вредоносные, фишинговые, а также связанные с APT URL-адреса, которые ранее использовались злоумышленниками для целевых атак и вторжений
в IT-инфраструктуру организаций.

Шлюзы в роли компонента Sensor



Kaspersky Security для почтовых серверов

В качестве компонента Sensor может использоваться почтовый шлюз – Kaspersky Security для почтовых серверов, отправляющий сообщения электронной почты на обработку в KATA. По результатам обработки в решении KATA продукт может блокировать пересылку сообщений конечным пользователям.

Kaspersky Endpoint Agent

Компонент Sensor может выступать в качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent.

Kaspersky Security для интернет-шлюзов

В качестве компонента Sensor может использоваться веб-шлюз Kaspersky Security для интернет-шлюзов, отправляющий веб-ссылки и файлы на обработку в KATA Platform.
По результатам обработки в решении KATA, веб-шлюз будет блокировать корпоративным пользователям доступ к ссылкам и файлам для скачивания.

Компонент Sandbox запускает объекты в шаблонах операционных систем и анализирует их поведение для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Проверке подлежат не только запускаемые объекты, но и дочерние (например, скачиваемые из Интернета в процессе запуска исходного файла):

≈ 200

Несколько тысяч детектов с конкретными вердиктами (основаны на вредоносном и аномальном поведении). Из них около 200 правил с детектированием подозрительного поведения (suspicious activity)

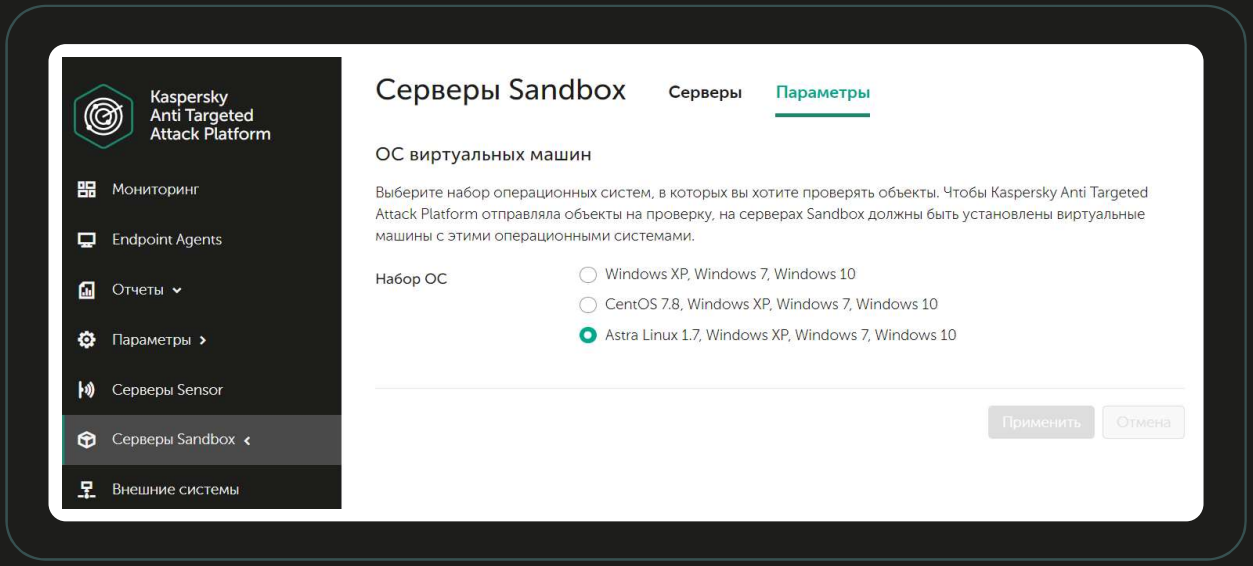
≈ 30 000

Вызовов API находятся под наблюдением

≈ 15 000

Правил для сетевого трафика (генерируемого исследуемым объектом внутри Sandbox)

Для компонента Sandbox имеется возможность установки пользовательских образов операционных систем Windows.



Возможен выбор набора операционных систем, на основе которого будут формироваться задачи на проверку объектов в компоненте Sandbox

- Windows XP, Windows 7, Windows 10
- Windows XP, Windows 7, Windows 10, CentOS 7.8
- Windows XP, Windows 7, Windows 10, Astra Linux 1.7

Агенты на уровне конечных точек собирают все необходимые данные с конечных устройств в инфраструктуре организации

Установленный на рабочем месте агент выполняет непрерывный мониторинг процессов, обмена данными, открытых сетевых подключений, состояния операционной системы, изменений
в файлах и т. п. Собранные данные и информацию, связанную с обнаружением подозрительных событий, агент отправляет в KATA для дополнительного исследования, анализа и сравнения с событиями, обнаруженными в других информационных потоках.

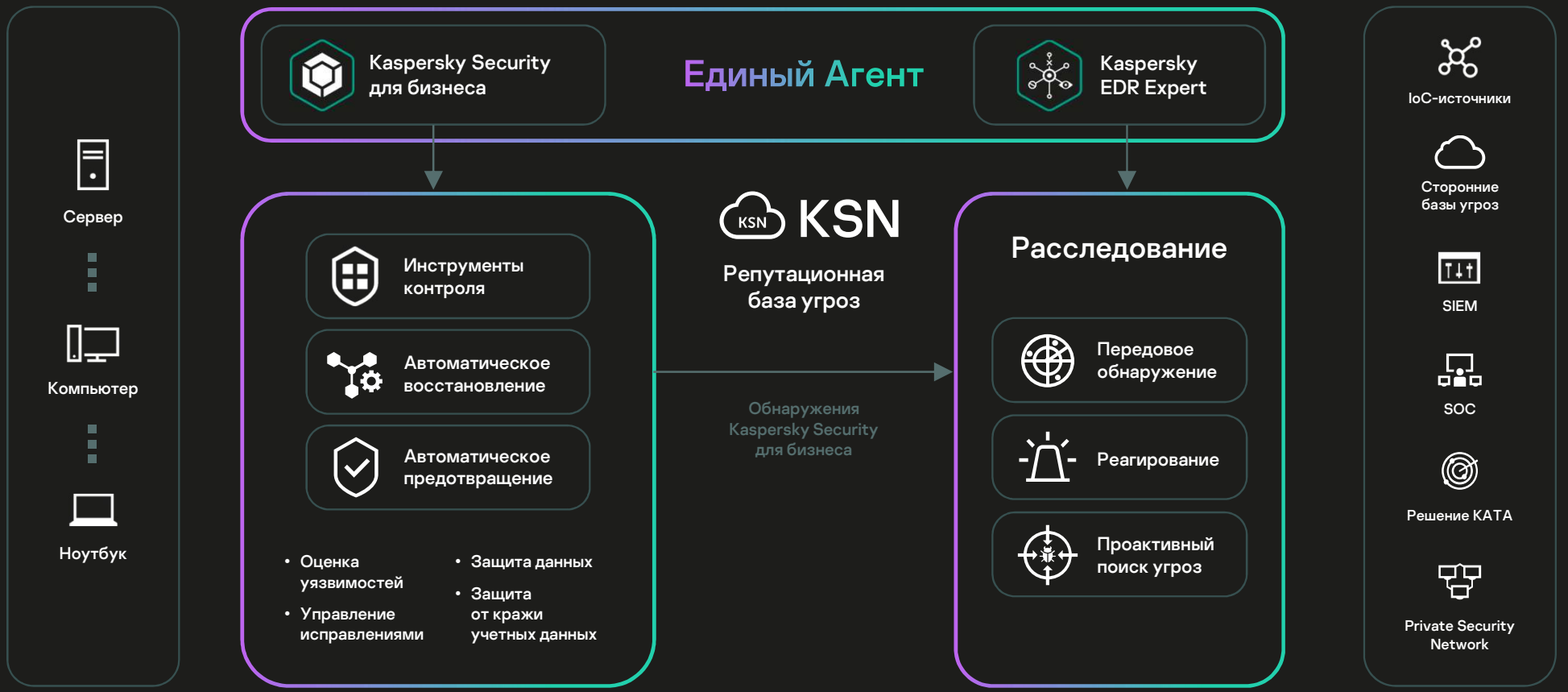
Компонент Endpoint Agent может работать следующими способами:

Компонент Endpoint Agent устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации и работающих под управлением операционных систем семейств Microsoft Windows и GNU / Linux

Endpoint Agent может использоваться совместно в составе продукта Kaspersky Endpoint Security for Business, а также совместно с Endpoint-решениями других производителей

На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node либо на Sensor, выступающий промежуточным звеном между Endpoint Agent и Central Node

Компонент Endpoint Agent



Кросс продуктовое взаимодействие

KATA с KEDR Expert. Этапы взаимодействия с системой

1. Детектирование угроз
2. Визуализация атак
3. Расследование инцидентов
4. Реагирование на угрозы
5. Администрирование и интеграция

Детектирование угроз

Основные возможности антивирусного модуля:

1

Автоматическое сканирование объектов из трафика

2

Использование встроенного и пользовательского списка паролей для проверки шифрованных файлов

3

Сканирование файла, отправленного с хоста через задачу компонента Endpoint Agent

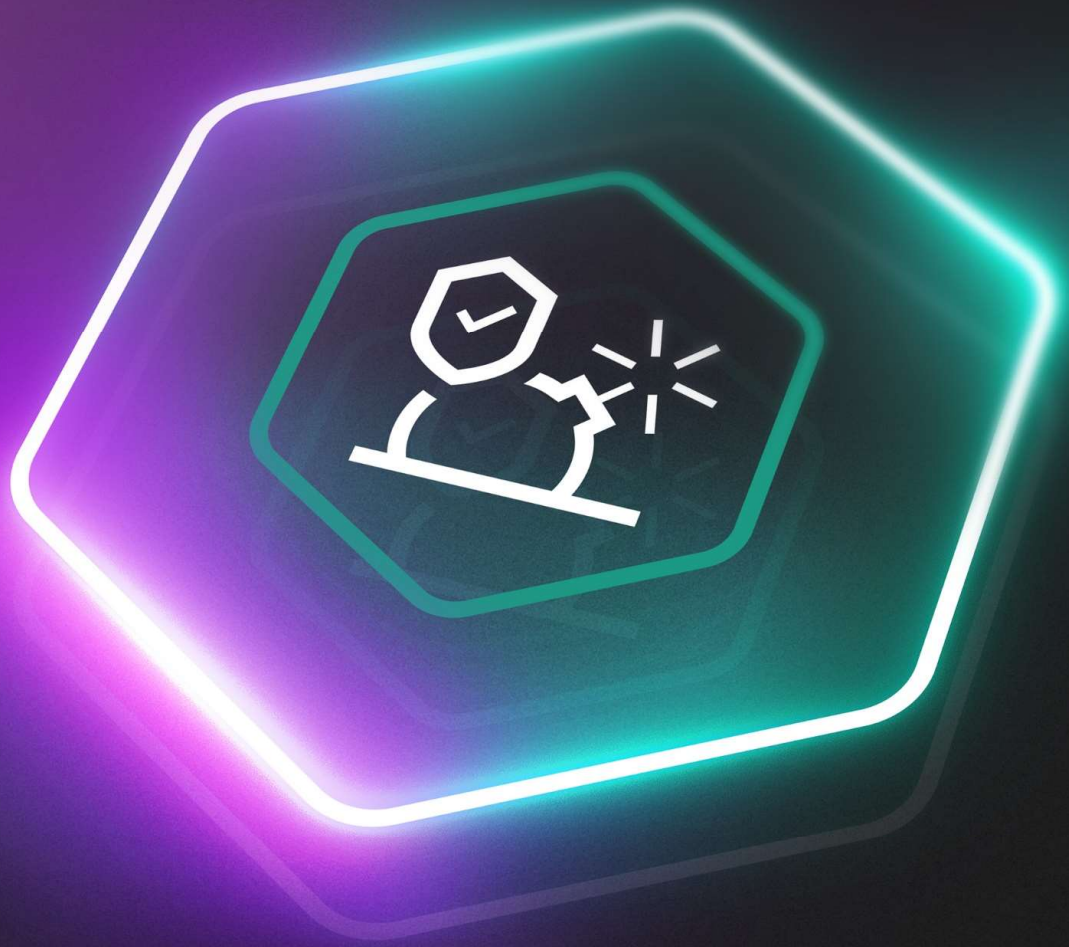
4

Возможность ручной загрузки файла на анализ через веб-интерфейс

AM engine анализирует объекты на наличие вредоносного или потенциально опасного кода, при необходимости отправляя их в Sandbox для последующей проверки. Благодаря такому подходу достигается высокая точность обнаружений и оптимизация нагрузки при потоковой проверке файлов.

KATA Sandbox

Использует ряд запатентованных технологий для качественной детонации получаемых на анализ объектов, противодействуя различным техникам обхода. Работает в автоматическом (объекты из трафика) и ручном режиме (загрузка объектов с хоста или через веб-интерфейс). Также, поддерживает различные кросс-сценарии для интеграции с сторонними системами и возможностью блокировки файлов на защищаемых хостах при использовании Endpoint agent.



Этапы работы

Этап 1

Для обнаружения активности вредоносных программ песочница запускает подозрительные объекты на собственных виртуальных машинах

Этап 2

Песочница получает задания для выполнения образцов с параметрами виртуализации, подобранными в зависимости от источника оцениваемого объекта и цели оценки (например, тип ОС, конфигурация ОС, среда, параметры запуска образца, продолжительность выполнения)

Этап 3

При выполнении образца песочница собирает:

- Журналы поведения образца (включая список вызовов системных функций, взаимодействие с другими процессами и файлами, сетевую активность, URL-адреса)
- Дампы памяти
- Загруженные объекты
- Генерируемый образцом трафик

Этап 4

После выполнения полученные артефакты сохраняются и затем обрабатываются специальным сканером. Если образец признается вредоносным, ему присваивается вердикт, а результаты сопоставляются с базой знаний MITRE ATT&CK. Все собранные данные сохраняются внутри системы, оставаясь доступными для дальнейшего анализа тактики и приемов злоумышленников. Это позволяет обойтись без дополнительных запросов к песочнице и сэкономить серверные ресурсы

Алгоритм работы Sandbox в платформе KATA

Комплексный набор возможностей помогает обеспечить высокоэффективное обнаружение угроз на основе поведенческого анализа:

Сопоставление поведения объекта
с базой знаний MITRE ATT&CK

Ускорение системного времени
на виртуальных машинах

Проверка трафика
движком IDS на виртуальных машинах при запуске файла

Моделирование
активности пользователя

Рандомизация
среды ОС

И другое

Intrusion Detection System (IDS)

Технология обнаружения вторжений включает в себя как традиционные средства обнаружения угроз в сетевом трафике посредством сигнатурного анализа, так и расширенную экспертизу базы Kaspersky Security Network и Threat Intelligence для оперативного реагирования на меняющийся ландшафт киберугроз.

В основе движка IDS — уникальный набор правил для анализа сетевого трафика, который позволяет распознать и обнаружить сетевую активность в более чем 80 протоколах. В число поддерживаемых протоколов входят: TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.

Сканирование трафика на предмет наличия признаков сетевых атак (IDS-правила) включает:

1. IDS-сигнатуры от экспертов Kaspersky
2. Возможность загрузки собственных правил в формате Snort или Suricata

Взаимодействие с глобальной базой знаний об угрозах (в автоматическом режиме):

Оперативное получение данных о новых угрозах и актуальных трендах в сфере киберпреступности

Сопоставление результатов внутренних расследований с глобальными репутационными данными

Ускорение процесса расследования инцидентов

Своевременное принятие необходимых мер для успешного отражения атак

Kaspersky Security Network (KSN)

Глобальная облачная инфраструктура, в которой хранятся репутационные вердикты и информация об объектах, обрабатываемых решением KATA (файлы, домены, URL, IP-адреса и многое другое)

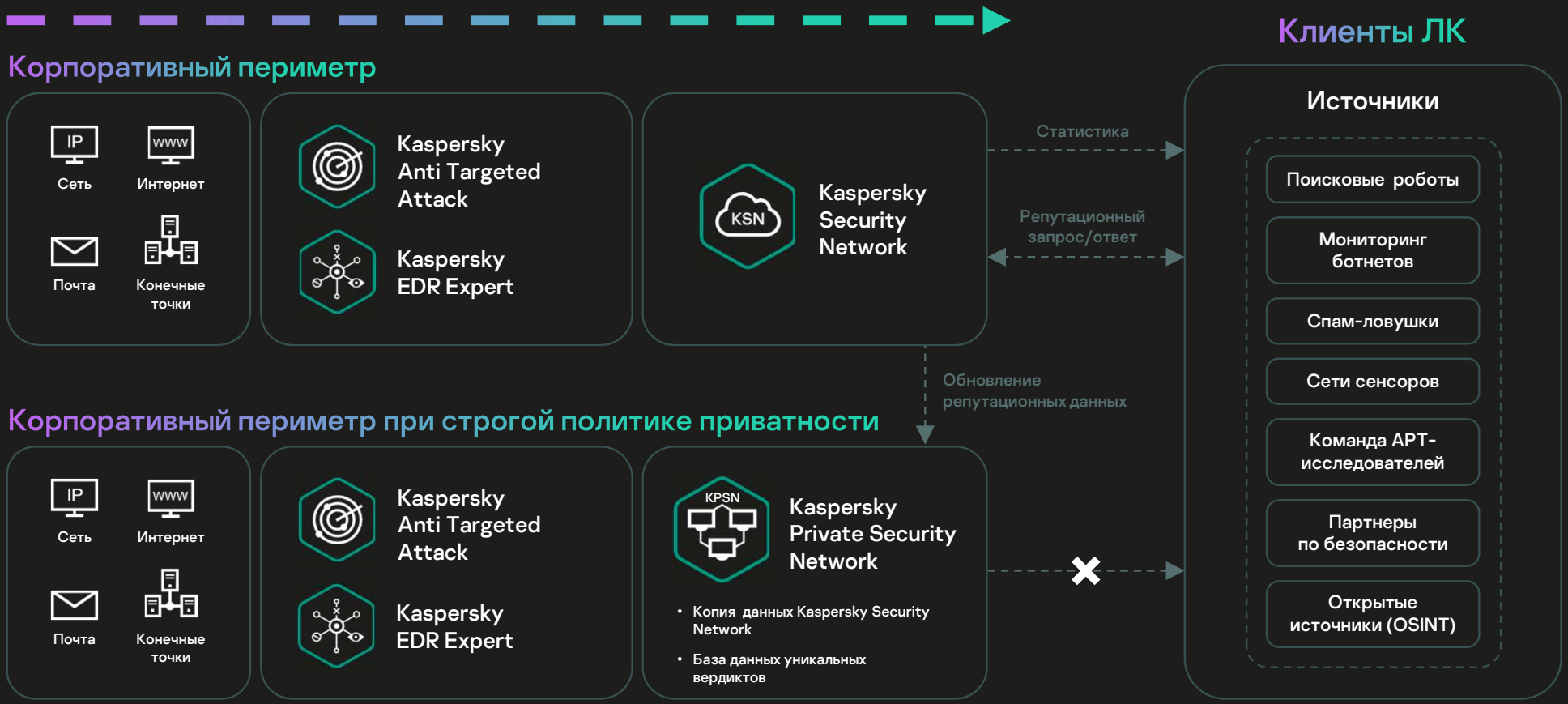
Также KSN использует облачные модели машинного обучения, например Cloud ML for Android (Mobile Attack Analyzer) для обнаружения угроз в APK-файлах.

Kaspersky Private Security Network (KPSN)

Ориентирован на организации, которые не имеют возможности отправлять свои данные в облако, но хотят пользоваться глобальной репутационной базой данных «Лаборатории Касперского»

Помимо частного доступа к нашей глобальной базе аналитических данных об угрозах, вердикты решения KATA сохраняются в локальной базе данных KPSN и предоставляются другим продуктам «Лаборатории Касперского», развернутым в рамках инфраструктуры организации, обеспечивая автоматическое реагирование. Используя KPSN, компании могут получать сведения о репутации из внешних сторонних систем без промежуточных шагов, напрямую через API.

Схема взаимодействия с глобальной аналитикой киберугроз



Обнаружение индикаторов компрометации (IoC)

Решение KATA позволяет централизованно загружать индикаторы компрометации из потоков данных об угрозах и поддерживает возможность создания запланированных задач сканирования IoC, повышая эффективность работы аналитиков

Ретроспективное сканирование базы данных позволяет повысить качество информации о ранее замеченных событиях и инцидентах безопасности

Сканирование защищаемых хостов на предмет наличия индикаторов компрометации (IoC):

1. Возможность импорта/экспорта собственных IoC-правил в формате OpenIOC
2. Возможность поиска IoC по действию пользователя в ретроспективных данных (в событиях с хостов)
3. Возможность проверки хостов на наличие IoC по расписанию

Анализатор целевых атак

Анализатор целевых атак (Targeted Attack Analyzer, TAA) обнаруживает подозрительную активность, используя расширенный эвристический анализ аномалий для автоматического поиска угроз в реальном времени

Поддерживает автоматический анализ событий и их сопоставление с уникальным набором индикаторов атак (IoA), поставляемых специалистами «Лаборатории Касперского».

Каждый раз, когда TAA обнаруживает аномалию в телеметрии с хостов, специалист по ИБ получает полную информацию о возможном инциденте: описание, рекомендации (например, по снижению риска повторного появления события), данные о степени уверенности в вердикте и серьезности события – для удобства классификации и ускорения реагирования.

Поиск индикаторов атаки (IoA) в событиях на защищаемых хостах с помощью Targeted Attack Analyzer:

Поиск индикаторов атак

в событиях, собираемых с защищаемых хостов в режиме реального времени

Возможность создания

и импорта собственных IoA-правил

Встроенные IoA-правила

от экспертов «Лаборатории Касперского»

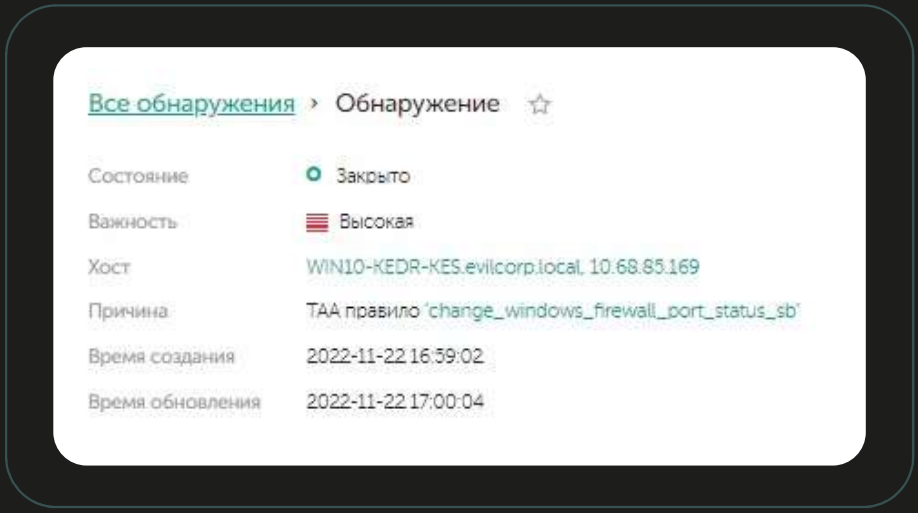
Автоматизация

Обнаруженные инциденты автоматически сопоставляются с базой знаний MITRE ATT&CK

Автоматическая отправка и блокировка файлов на защищаемых хостах по обнаружению Sandbox

1

Компонент Endpoint Agent в режиме реального времени направляет все события с защищаемых хостов на сервер для анализа по IoA-правилам



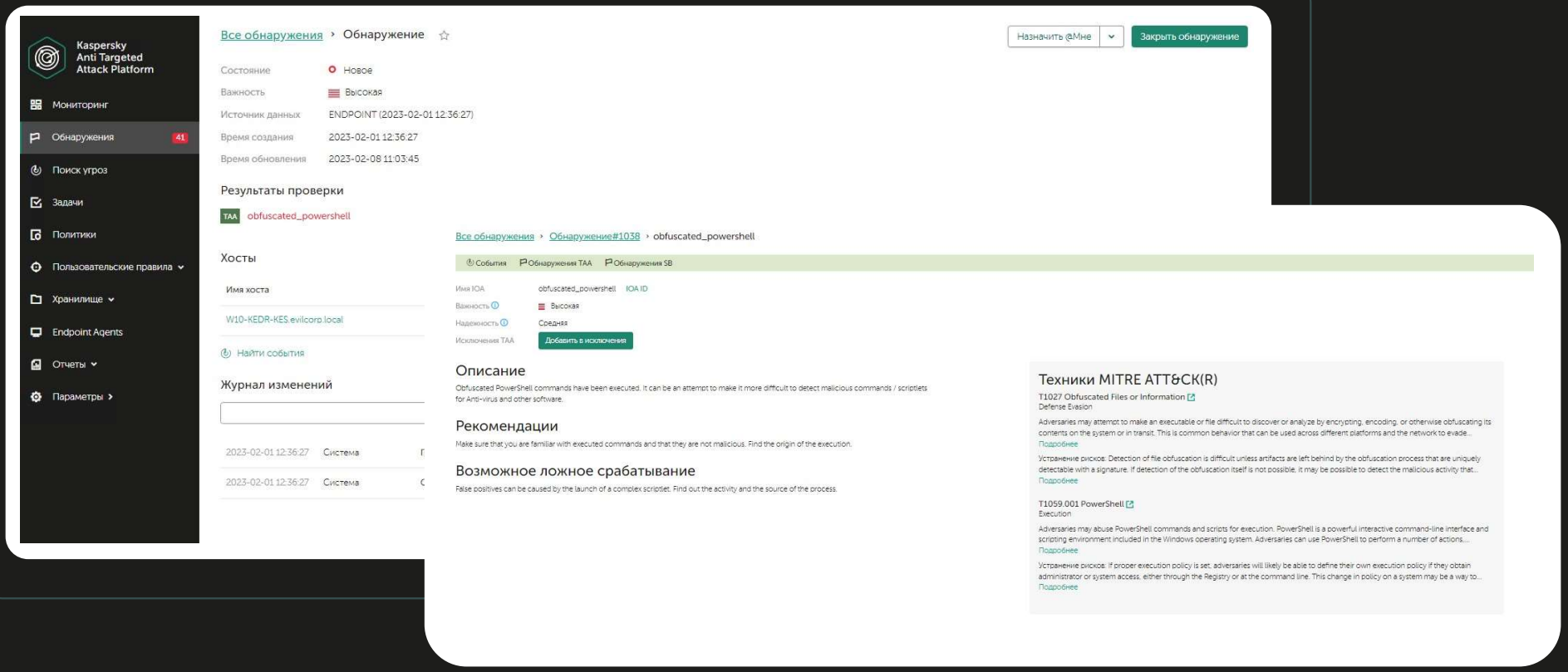
2

При срабатывании определенных IoA-правил, поставляемых в рамках экспертизы «Лаборатории Касперского», сервер можетинициировать запрос на получение файла-инициатора вредоносных событий у Endpoint Agent для получения детальной информации по инциденту

3

Если полученный файл при проверке в Sandbox получает статус средней или высокой степени важности, то сервер автоматически создаст правило запрета на запуск данного файла на всех защищаемых хостах с компонентом Endpoint Agent

Пример карточки обнаружения индикаторов атак (IoA) на хостах



Обнаружение с помощью правил для YARA

YARA – один из самых часто используемых инструментов поиска новых вариантов вредоносных программ

Он поддерживает сложные правила корреляции для поиска файлов с определенными характеристиками и метаданными, например содержащих строки, характерные для кода конкретного программиста. Возможность создания и загрузки пользовательских правил для YARA позволяет проверять объекты на наличие угроз с учетом специфики организации.

Сканирование объектов с помощью YARA-правил:

1

Автоматическая проверка всех объектов YARA-правилами

2

Возможность импорта/экспорта собственных правил

3

Проверка объектов с защищаемых хостов YARA-правилами по действию пользователя

4

Возможность проверки точек автозапуска на рабочих станциях с помощью YARA-правил

Визуализация атак

Для улучшения видимости происходящего в защищаемой инфраструктуре используются:

Настраиваемые дашборды с виджетами (возможность экспорта данных в PDF)

Отображение обнаружений в трафике и на хостах с указанием важности обнаружения, источника, используемой технологии детектирования

Визуализация поведения эмулируемого объекта в Sandbox

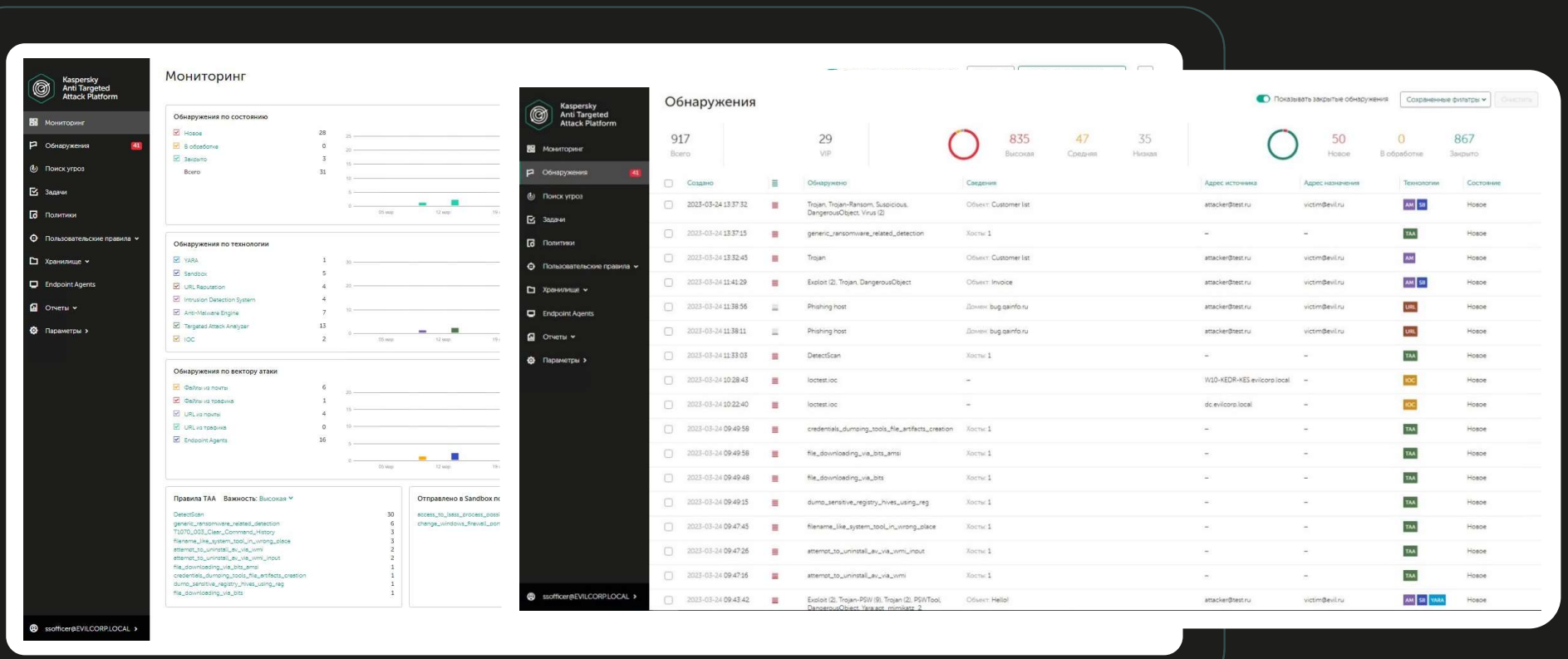
Визуализация дерева процессов, запускаемых на защищаемых хостах

Настройка нотификации об инцидентах на электронную почту

Создание и загрузка отчетов (HTML- и PDF- формат)

Гибкий механизм создания шаблонов отчетов

Визуализация атак



Расследование инцидентов

Для проведения расследования инцидентов у специалиста существуют следующие возможности:

Рекомендательная система для оперативного реагирования

Автоматическая приоритизация обнаружений

Создание базового workflow-реагирования на инциденты

Сбор дополнительной информации с защищаемых хостов с целью форензики

Поиск неизвестных угроз (Threat Hunting):

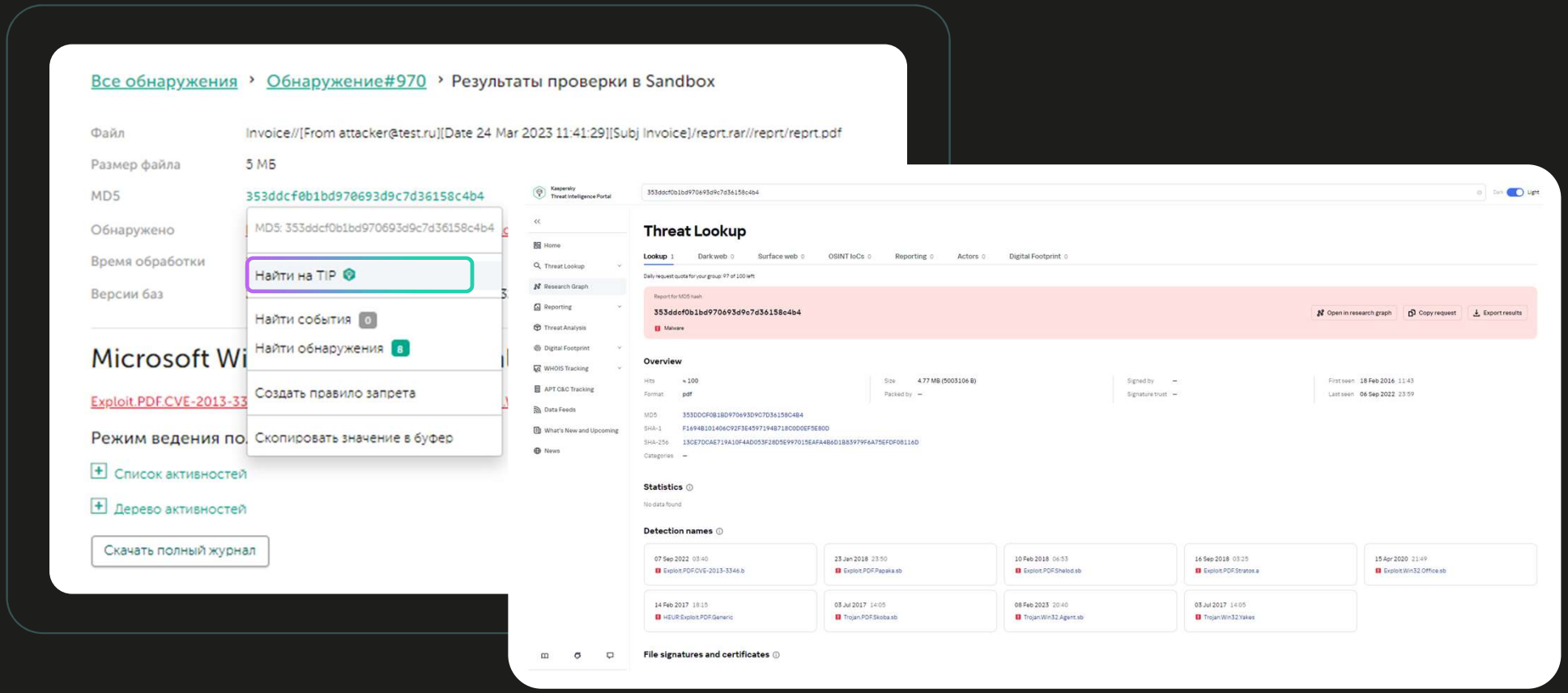
- Ретроспективный анализ по событиям, ранее собранным с защищаемых хостов
- Гибкий инструмент написания запросов поиска

Детализированные описания угроз на портале threats.kaspersky.com

Интеграция с Threat intelligence для обогащения знаний по обнаруженным IoC

Сопоставление событий с техниками матрицы MITRE ATT&CK

Интеграция с Threat Intelligence (tip.kaspersky.com) для обогащения знаний по обнаруженным IoC



Реагирование на угрозы

В решении KATA в рамках реагирования на инциденты доступны следующие возможности:

Изоляция скомпрометированного хоста от корпоративной сети

Завершение подозрительного процесса

Удаление вредоносного объекта или перемещение его в карантин

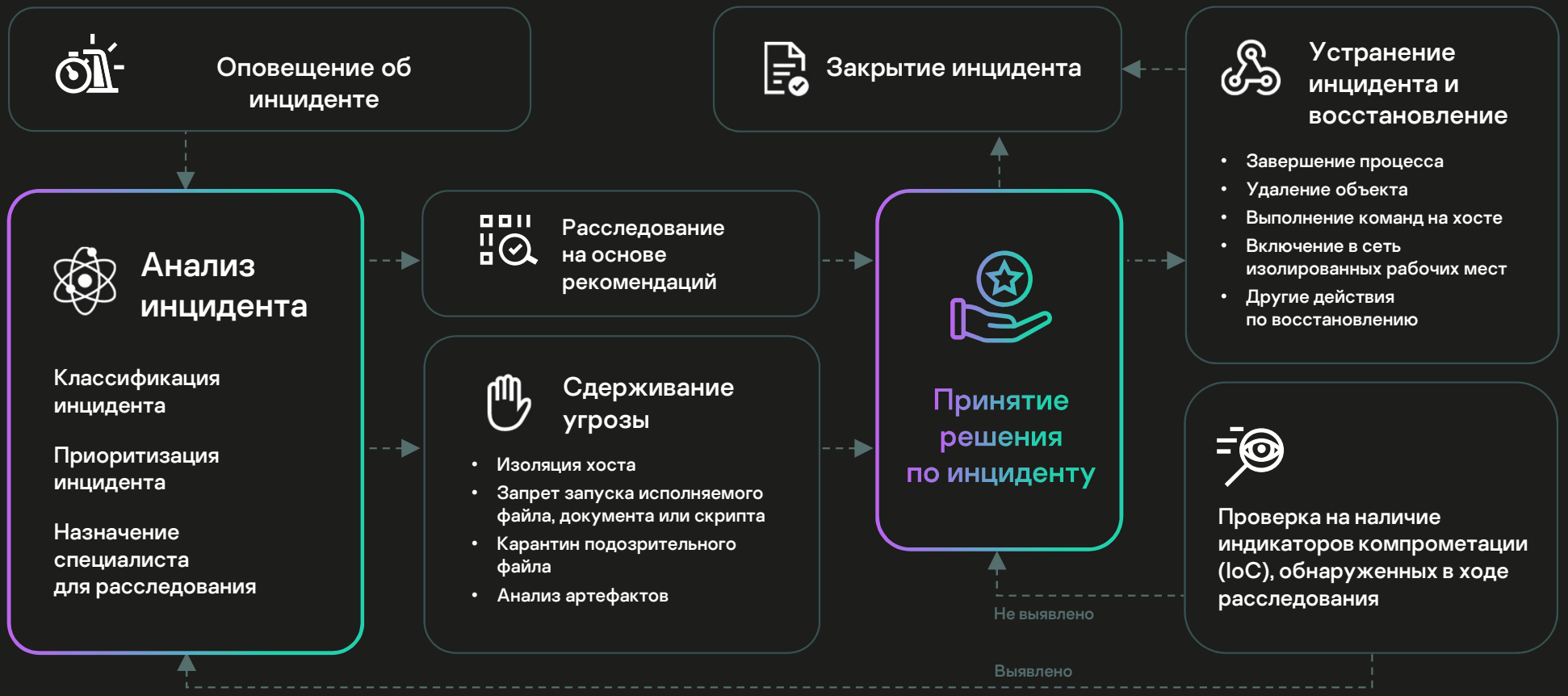
Автоматическое создание правил блокировки запуска подозрительных объектов в результате обнаружения Sandbox

Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

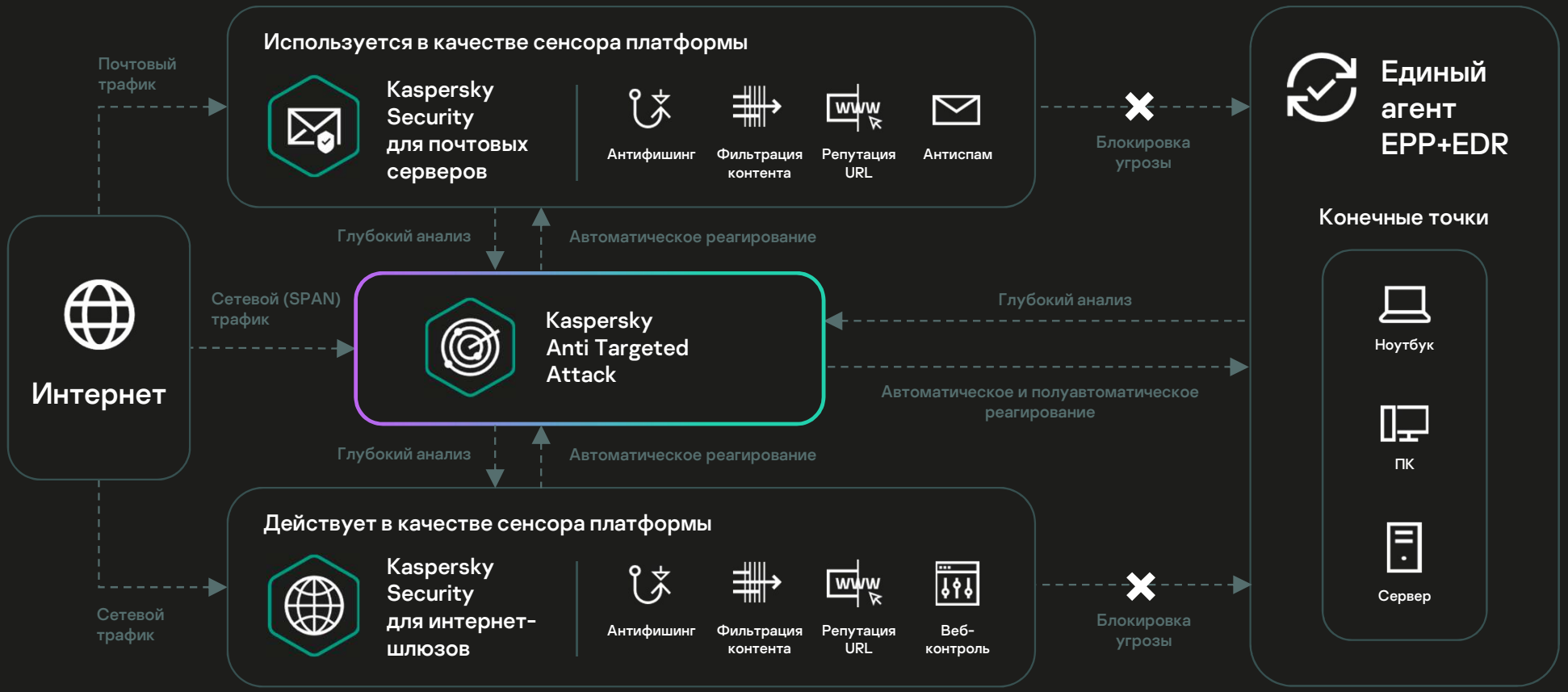
Выполнение команд и управление службами на защищаемом хосте

Запуск YARA-проверки

Схема централизованного реагирования на инциденты с помощью Kaspersky EDR Expert

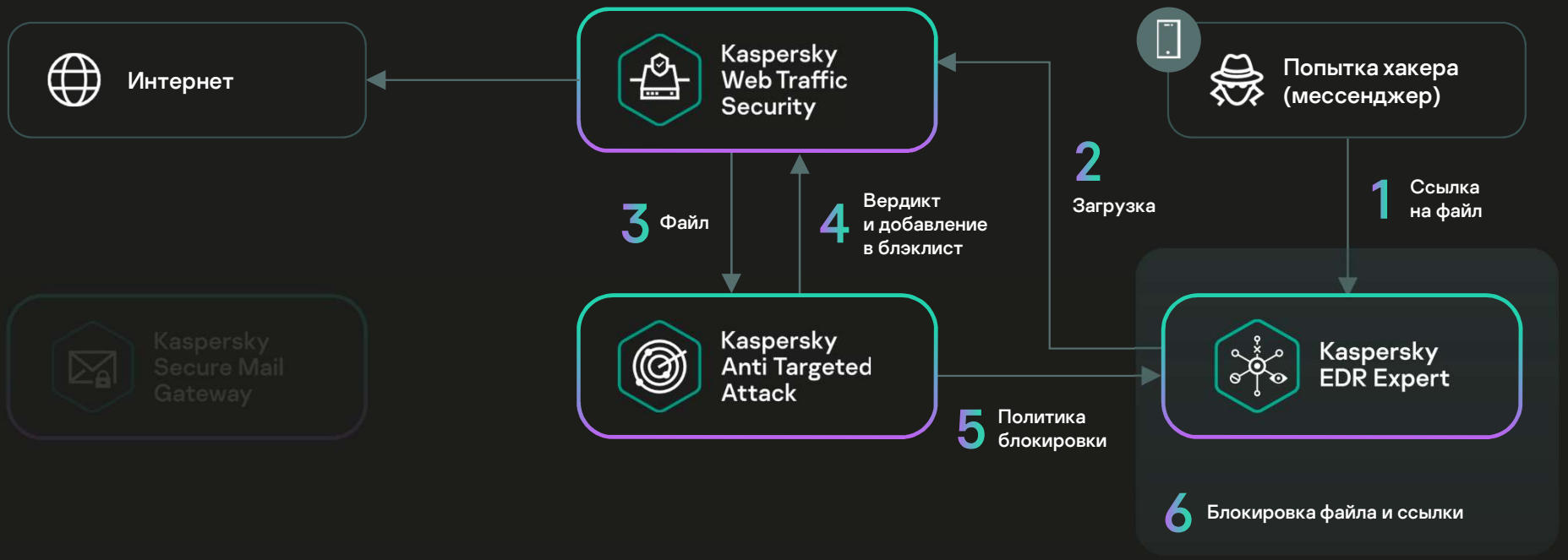


Автоматическое реагирование с помощью шлюзов

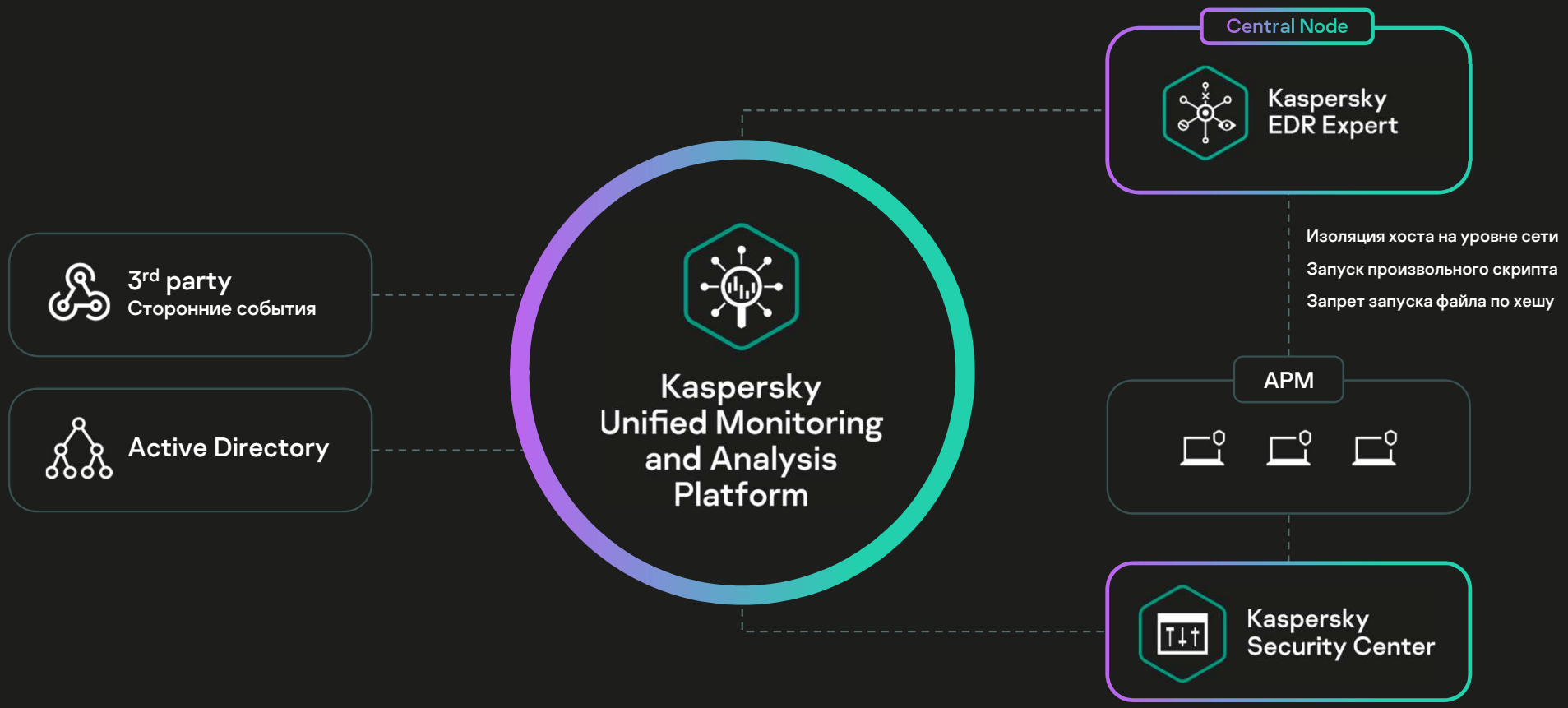


Демонстрация интеграции с KSMG и KWTS. Сценарий 1

Демонстрация интеграции с KSMG и KWTS. Сценарий 2



Автоматизированное реагирование на инциденты KES/KEDR Expert



Администрирование и интеграция

В рамках управления системой доступны следующие возможности:

1. Поддержка режима multitenancy (возможность создания иерархической структуры серверов)
2. Ролевая модель доступа (Администратор, Старший офицер безопасности, Офицер безопасности, Аудитор)
3. Аудит действий пользователей
4. Мониторинг работоспособности системы (виджеты, SNMP, syslog, почтовые уведомления)
5. Поддержка отказоустойчивого режима работы системы за счет развертывания кластера серверов

В решениях KATA & KEDR Expert доступны следующие возможности:

Интеграция с SIEM

Отправка данных об обнаружениях по протоколу Syslog и телеметрии с Endpoint Agent по API

Интеграция с локальной базой знаний

Kaspersky (Private) Security Network

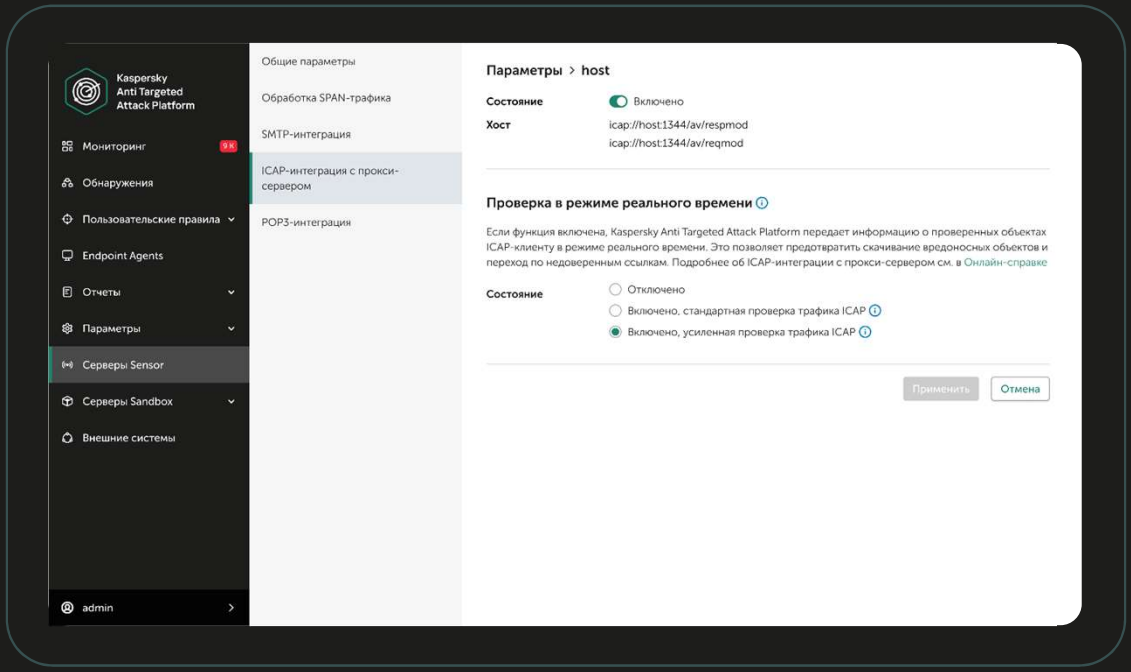
API для отправки сведений

об обнаружениях во внешнюю систему

API для проверки объектов

в KATA Platform с возвратом результатов сканирования

ICAP-клиент использует вердикт для регистрации информации, блокировки или одобрения контента без дальнейшего анализа.



3 типа интеграции ICAP с режимом блокировки:

- Отключено – вердикт не передается ICAP-клиенту.
- Стандартный (быстрый режим) – вердикт отправляется ICAP-клиенту. Используются антивирус, YARA, KSN и кэш Sandbox.
- Расширенный – вердикт отправляется ICAP-клиенту. Используются антивирус, YARA, KSN и полная эмуляция Sandbox.

Лицензирование

Kaspersky Anti Targeted Attack

Лицензируется по объему анализируемого трафика, количеству пользователей и числу проверяемых файлов API в секунду

Kaspersky EDR Expert

Лицензируется по количеству узлов, на которые устанавливается KEDR Expert

KEDR Expert может быть продан как самостоятельное решение (Stand-alone, без KATA) или в дополнение к используемой у заказчика KATA

Техническая поддержка

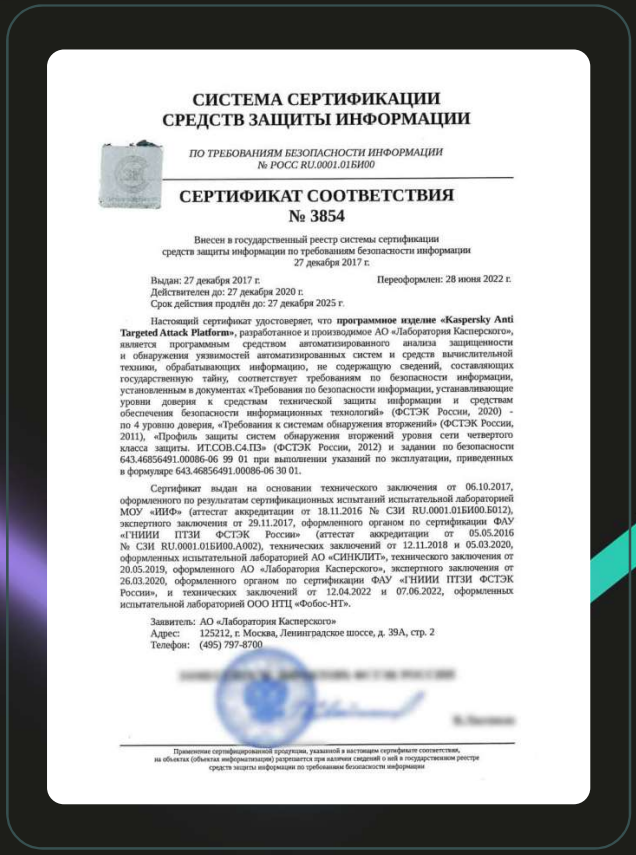
		Premium	Premium Plus
Каналы связи	Company account (веб-портал, уведомления через почту)	●	●
	Телефон	●	●
Время реакции в зависимости от уровня критичности	Критический (24/7)	2 часа	0,5 часа
	Высокий (в рабочие часы)	6 часов	4 часа
	Средний (в рабочие часы)	8 часов	6 часов
	Низкий (в рабочие часы)	10 часов	8 часов
Доступные услуги	Программные исправления	●	●
	Удаленное подключение для диагностики проблем	●	●
	Постпроектная поддержка	●	●
	Частные исправления	●	●
	Рекомендации по оптимизации	●	●
	Персональный технический менеджер		●
	Регулярные статус-встречи с TAMом для ретроспективного анализа зарегистрированных инцидентов, связанных с ТП		Ежеквартальный отчет
	Парсеры логов под заказ	10	20
	Количество включенных часов Professional Services (не менее 2 часов на 1 сессию)	0	16 часов (2 дня)

ФСТЭК

СОВ уровня сети
4 класса защиты

ФСБ

СОА класса АП, САВЗ Д



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3854

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
27 декабря 2017 г.

Выдан: 27 декабря 2017 г. Переоформлен: 28 июня 2022 г.
Действителен до: 27 декабря 2020 г.
Срок действия продлён до: 27 декабря 2025 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Anti Targeted Attack Platform»**, разработанное и производимое АО «Лаборатория Касперского», является программным средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем и средств вычислительной техники, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 643.46856491.00086-06 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00086-06 30 01.

Сертификат выдан на основании технического заключения от 06.10.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), экспертного заключения от 29.11.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 12.11.2018 и 05.03.2020, оформленных испытательной лабораторией АО «СИНКЛИТ», технического заключения от 20.05.2019, оформленного АО «Лаборатория Касперского», экспертного заключения от 26.03.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России», и технических заключений от 12.04.2022 и 07.06.2022, оформленных испытательной лабораторией ООО НТЦ «Фобос-НТ».

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ФСТЭК

САВЗ Б4, В4, СОВ уровня узла 4 класса защиты

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4597

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
14 октября 2022 г.

Выдан: 14 октября 2022 г.
Действителен до: 14 октября 2027 г.

Настоящий сертификат удостоверяет, что **программное изделие Kaspersky Endpoint Detection and Response**, разработанное и производимое АО «Лаборатория Касперского», является программным средством, реализующим функции средства антивирусной защиты и средства обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 643.46856491.00120-01 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00120-01 30 01.

Сертификат выдан на основании технического заключения от 18.08.2022, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), и экспертного заключения от 02.09.2022, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Истории успеха

МАГНИТ

Крупнейшая розничная сеть по торговле продуктами питания на российском рынке

ФОСАГРО®

Крупнейший поставщик всех видов удобрений на российском рынке

НОВОСТАЛЬ-М

Металлургический холдинг, основными активами которого являются Абинский Электрометаллургический Завод и Металлургический Завод Балаково

МКБ

Один из крупнейших российских коммерческих банков

Крупнейший перевозчик среди пригородных пассажирских компаний России

Jet

Крупный ИТ интегратор

Banca Popolare di Sondrio

Один из крупнейших итальянских банков

ANSALDO ENERGIA

Крупнейшая итальянская энергетическая инжиниринговая компания

Независимые тесты и признание

SE Labs протестировала эффективность технологий EPP и EDR от Kaspersky против широкого спектра кибератак и присвоила решению рейтинг AAA

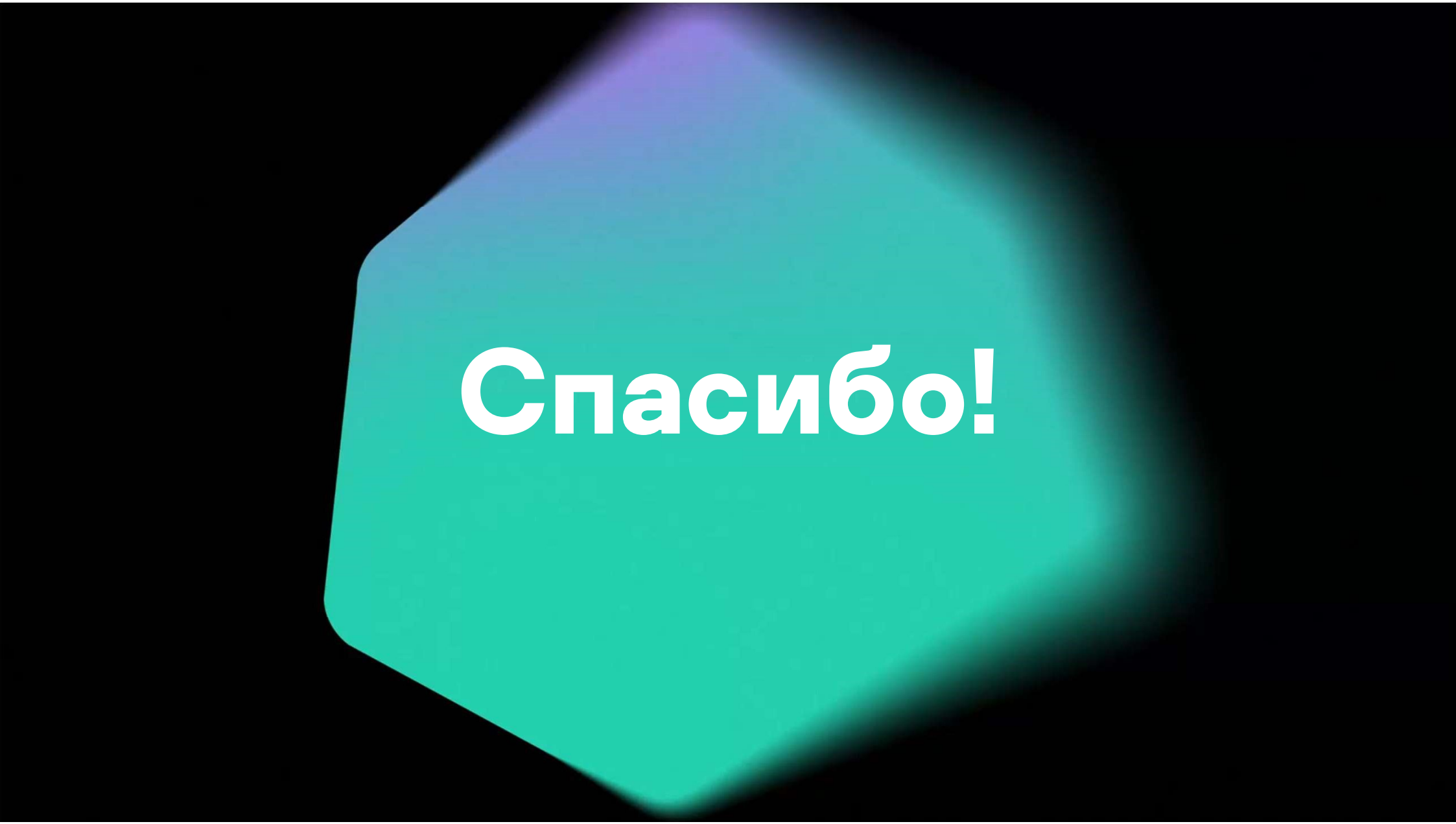
«Лаборатория Касперского» получила высокую награду Gartner Peer Insights Customers' Choice в категории EDR-решений. Покупатели высоко оценили платформу Kaspersky Anti Targeted Attack и Kaspersky EDR Expert

В независимом тесте ICSA Labs: Advanced Threat Defense платформа Kaspersky Anti Targeted Attack показала 100-процентный результат обнаружения угроз, не допустив ни одного ложного срабатывания

Исследовательская компания Radicati Group назвала Kaspersky ведущим игроком в отчете «Advanced Persistent Threat (APT) Protection – Market Quadrant, 2022»

Качество обнаружения подтверждено оценкой MITRE ATT&CK

Независимая лаборатория AV-Comparatives протестировала технологии EPP и EDR от Kaspersky и присвоила статус стратегического лидера


Спасибо!