

Центральный элемент единой платформы безопасности

kaspersky



**Борис Осепов, инженер
предпродажной поддержки**

Есть два вида компаний:
те, что были взломаны, и те,
что пока еще не знают, что были взломаны.

Спарк Флоу
(Sparc Flow)
How to
Investigate
Like a Rockstar

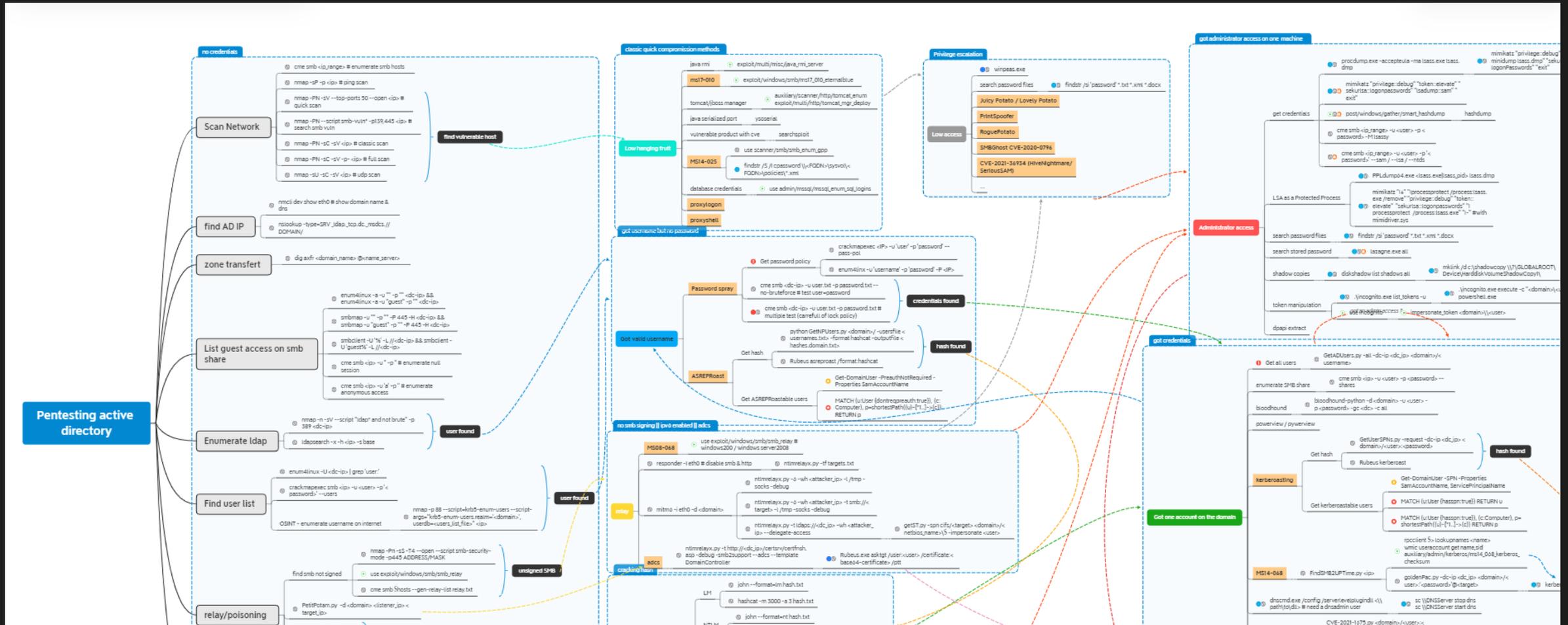
A *step by step* process for
BREAKING into a **BANK**
(or any company really...)

How to...

HACK LIKE
A PORNSTAR

Sparc FLOW

Подготовка злоумышленников



Подготовка злоумышленников бывает и такая 😊



А насколько подготовлены вы?



- Процедура управления инцидентами?
- Выстроенный процесс реагирования на инциденты?
- Регламент резервного копирования?
- А может RDP наружу? 😊

Масштаб угроз

1994

1

новый вирус
каждый час

2006

1

новый
вирус
каждую
минуту

2011

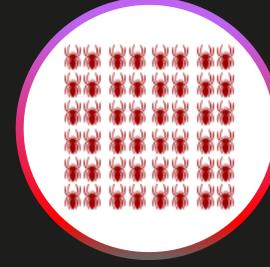
1

новый вирус
каждую
секунду

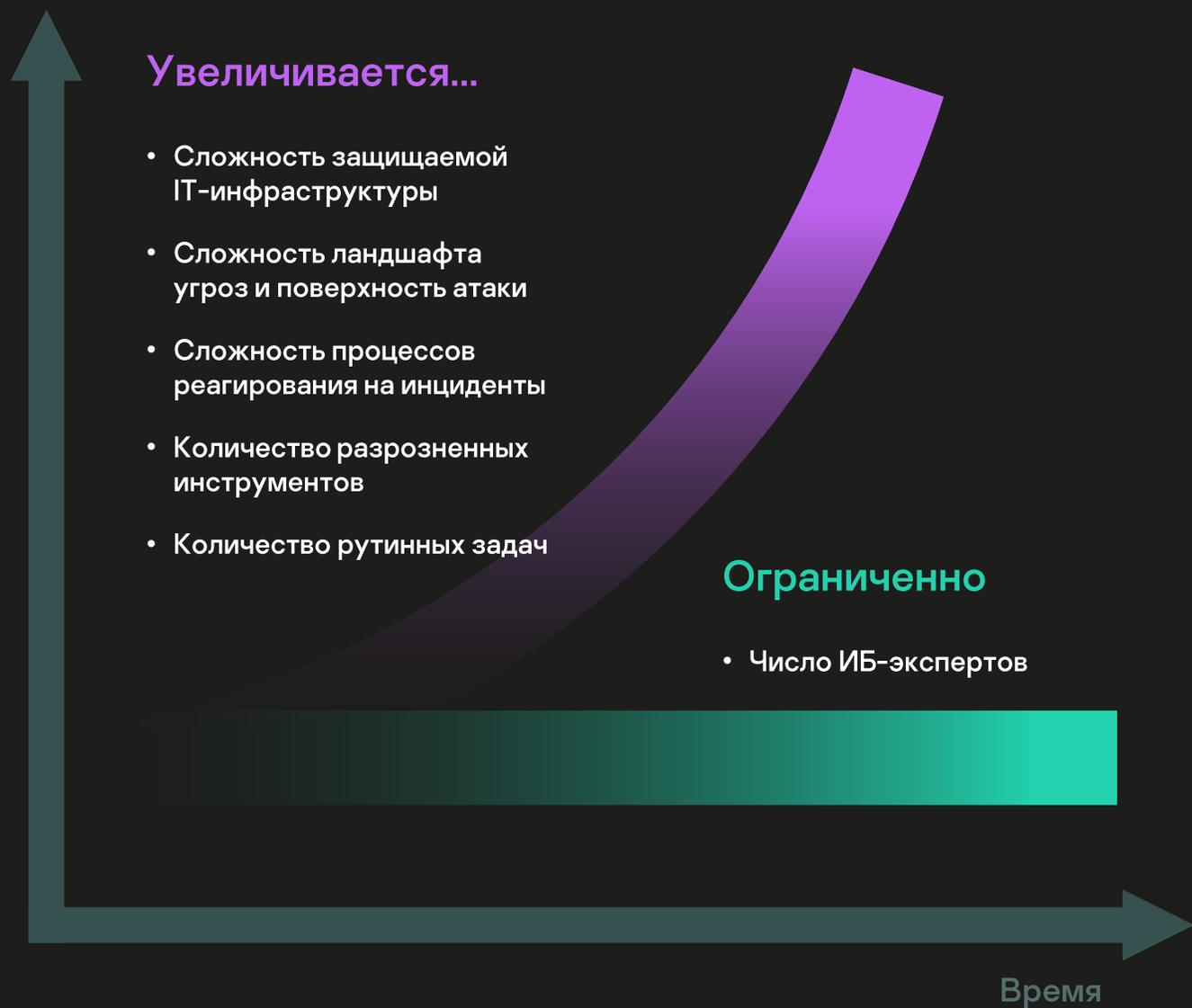
2021

370 000

новых
вредоносных
образцов в
день



IT-безопасность: современные реалии



Общий дефицит ИБ-экспертов на рынке труда



Неоптимальное использование времени и таланта экспертов

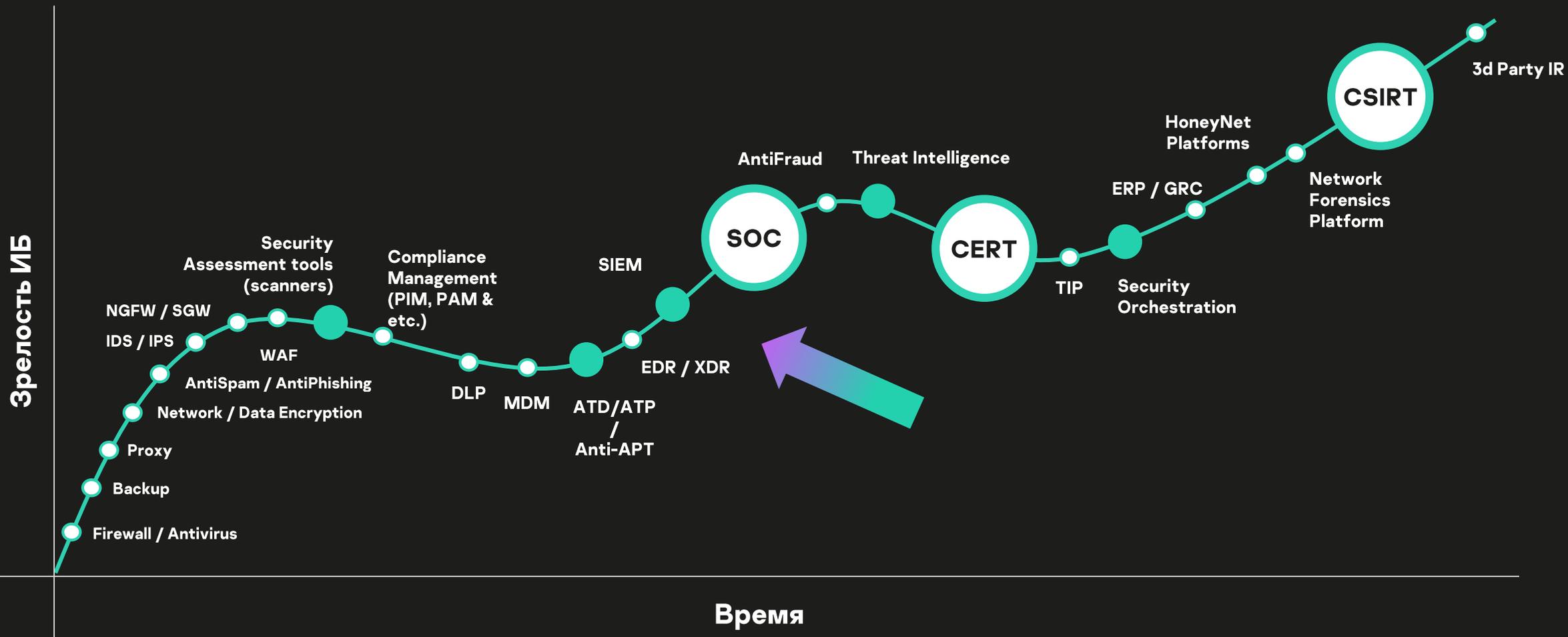


Недостаточная поддержка ИБ-сотрудников



Отсутствие программ подготовки собственных специалистов

Зрелость систем защиты компании



Инцидент – до и после

Известные угрозы

- Блокировка или автоматическое обнаружение угроз

Продукты, оповещения

До компрометации

КОМПРОМЕТАЦИЯ

Неизвестные угрозы

- Выявление сложных угроз
- Расследование

Поиск киберугроз

После компрометации

Сдерживание угроз

- Реагирование и пошаговые рекомендации

Реагирование на инциденты

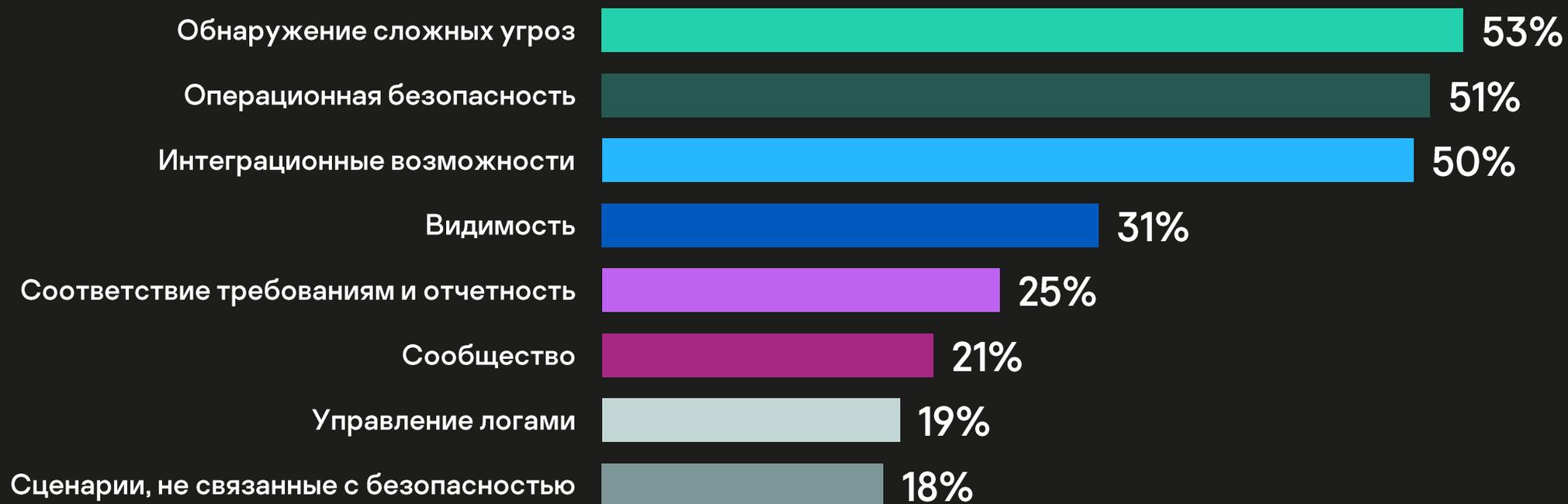
Время

Современный эталон реагирования

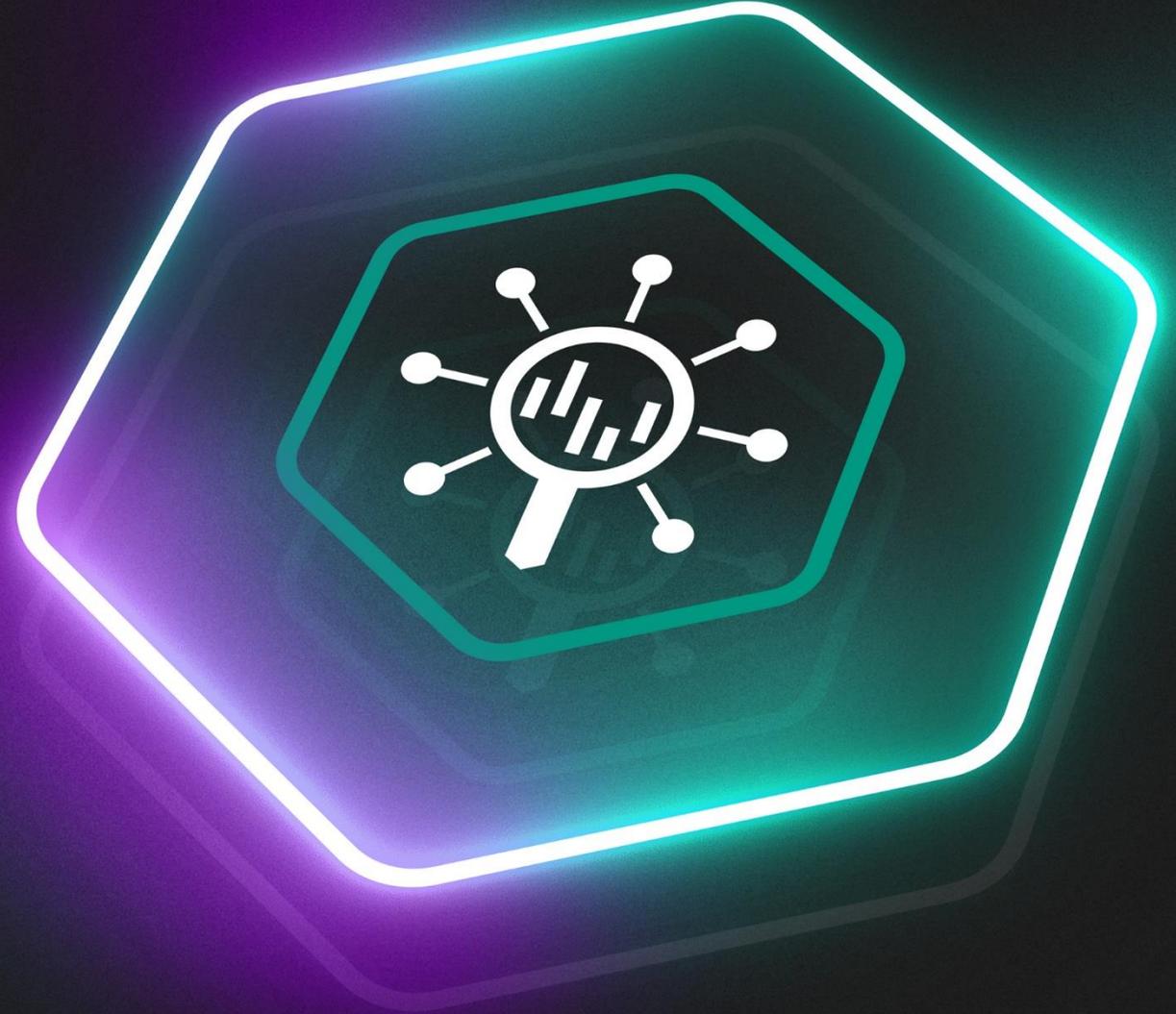


SIEM — основная платформа SOC сегодня

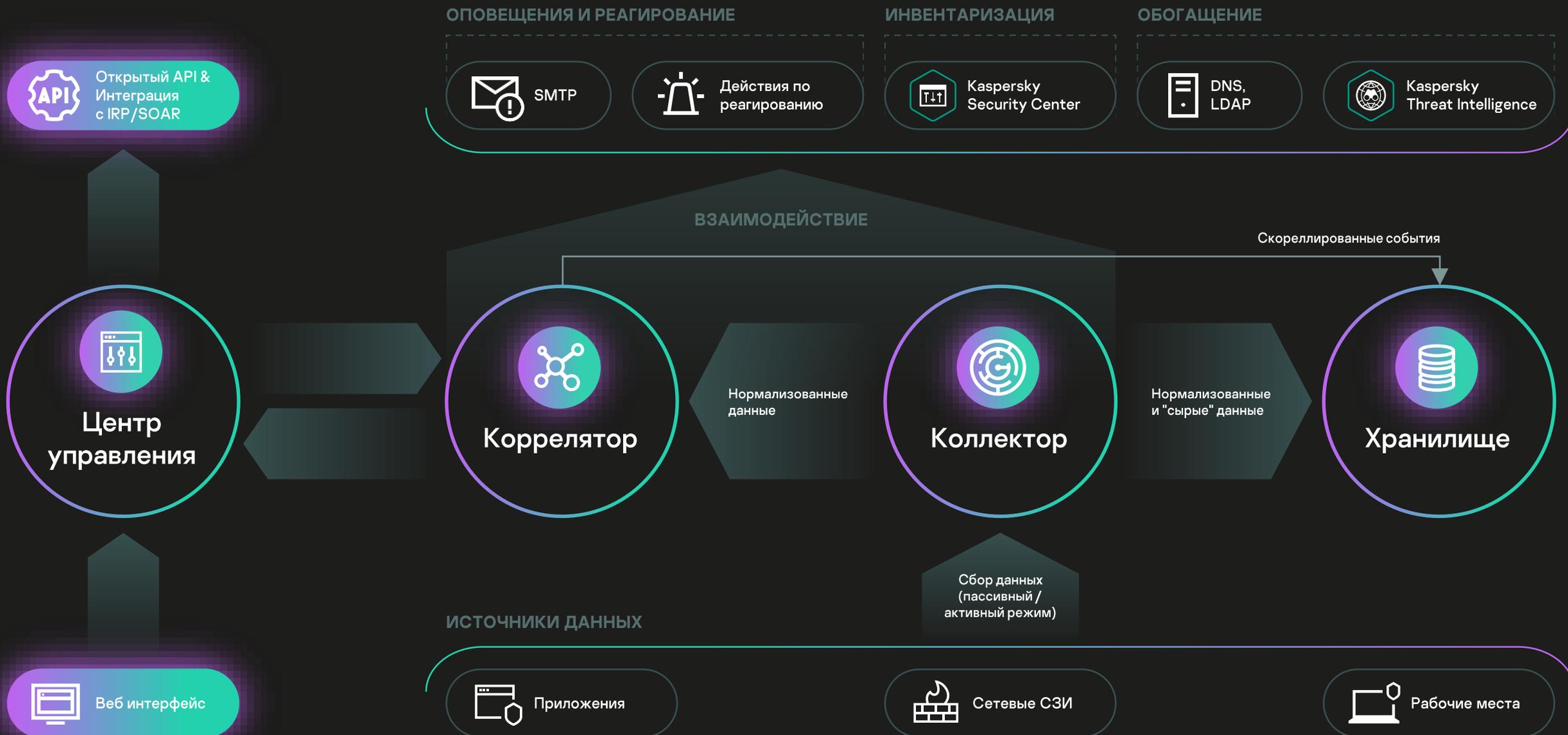
Ценность SIEM

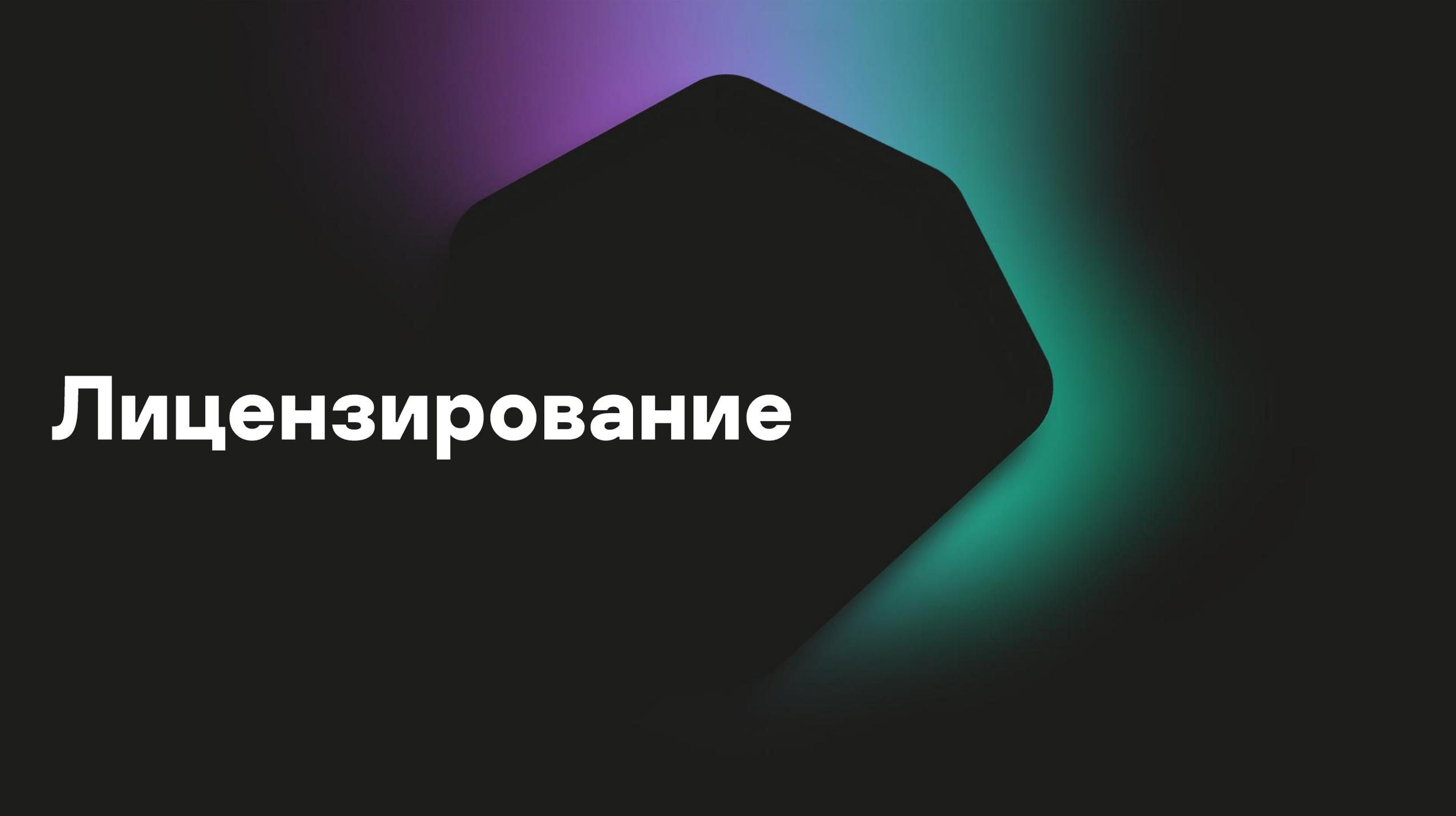


Kaspersky Unified Monitoring and Analysis Platform



Архитектура КУМА





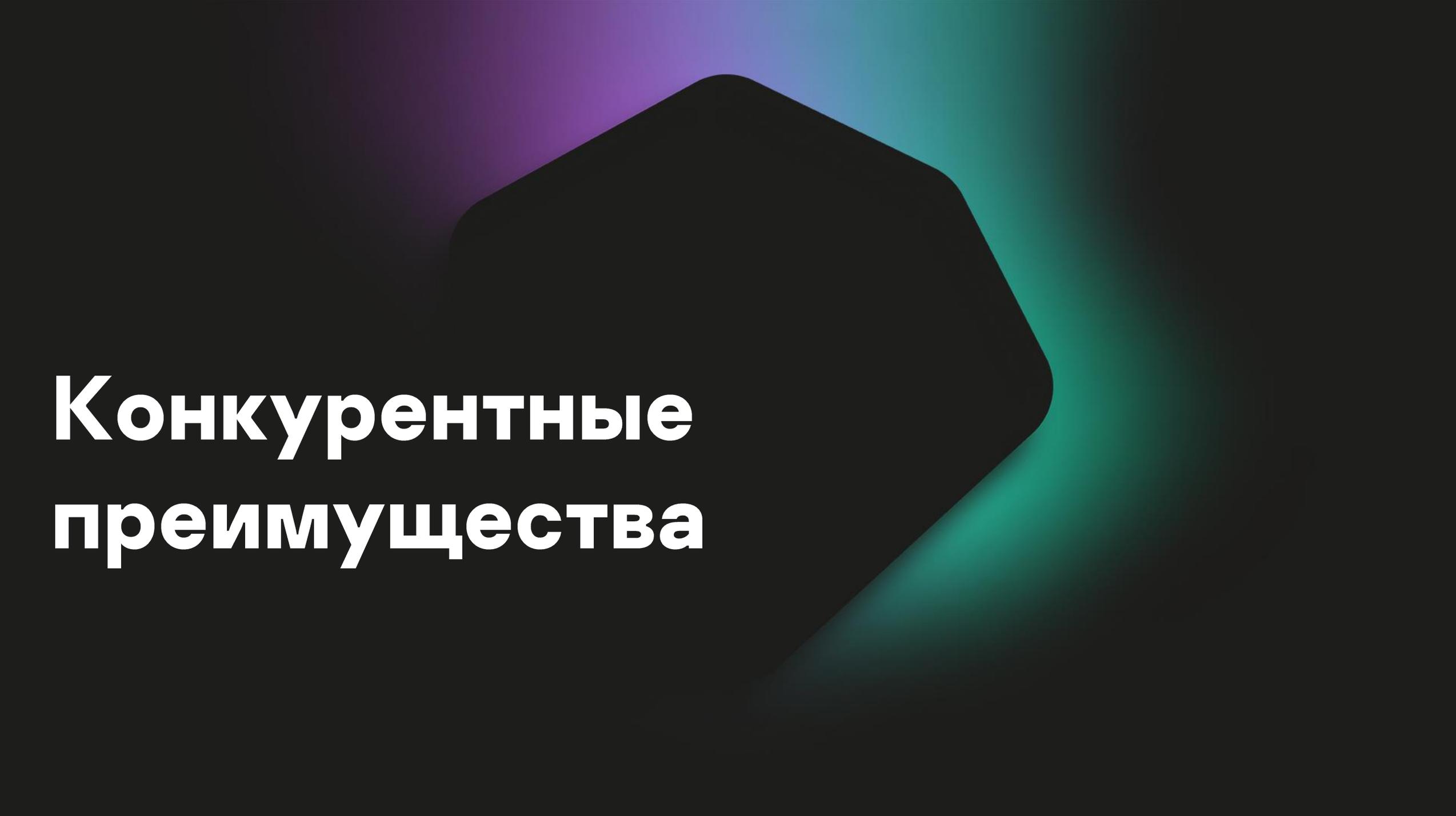
Лицензирование

- Учет по количеству «чистых» EPS (шаг по 100 EPS)
- min лицензия от 500 EPS
- По используемым модулям:
 - ГосСОПКА
 - Netflow
 - High Availability
- Срок действия 1 и 2 года



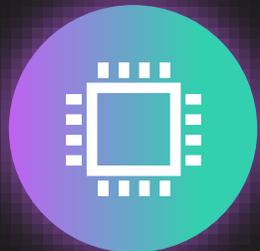
Техническая поддержка

	Стандартная поддержка Premium	Расширенная поддержка Premium+
Режим работы, SLA	1 приоритет - 2 часа, 24*7 2 - 6 часов, 5*8 3 - 8 часов, 5*8 4 - 10 часов, 5*8	1 приоритет - 30 мин, 24*7 2 - 4 часа, 24*7 3 - 6 часов, 5*8 4 - 8 часов, 5*8
Консультации по настройке	Да	Да
Исправления ошибок (в том числе private fix)	Да	Да
Количество пользовательских коннекторов	10 <small>*по мере развития продукта цифра будет уменьшена</small>	20
Выделенный аккаунт менеджер, мониторинг качества	Нет	Да
Включено часов Professional services <small>*для разработки дополнительных коннекторов, ревью архитектуры и схемы развёртывания итд</small>	0	16 часов <small>*не менее 2 часов одна сессия</small>



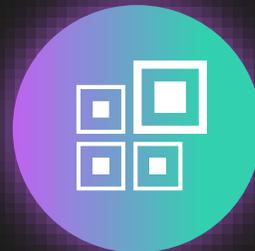
Конкурентные преимущества

Ключевые преимущества



**Высокая
производительность**

300k+ EPS на один узел



Масштабируемость

Гибкая микросервисная
архитектура



**Низкие системные
требования**



Интеграция «из коробки»

С продуктами сторонних поставщиков
и решениями «Лаборатории Касперского»

Kaspersky Unified Monitoring and Analysis Platform (SIEM)



Преимущества Сертификат ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

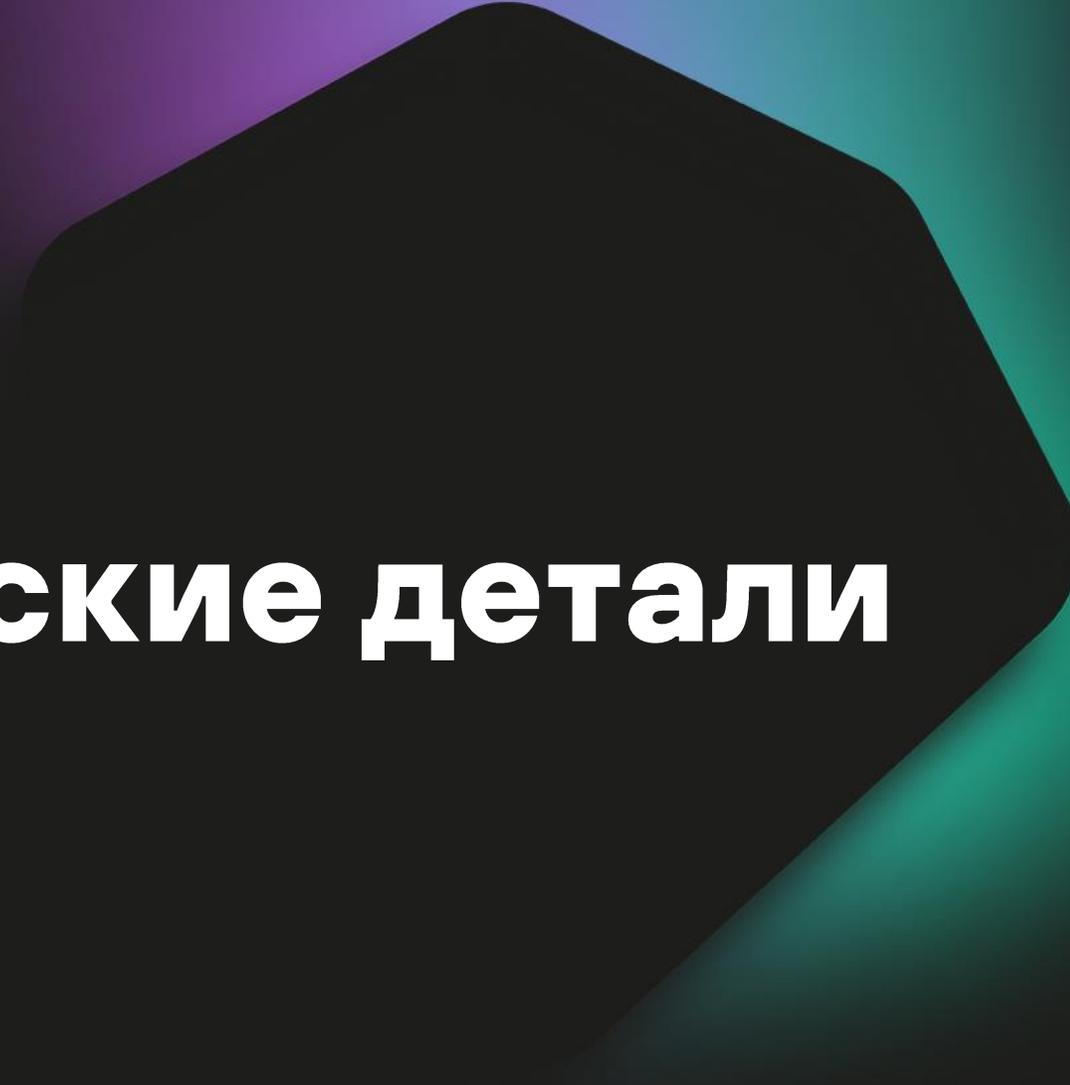
СЕРТИФИКАТ СООТВЕТСТВИЯ № 4455

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

Выдан: 28 сентября 2021 г.
Действителен до: 28 сентября 2026 г.

Переоформлен: 26 октября 2021 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Unified Monitoring and Analysis Platform (версия 1.5)»**, 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 техническим условиям ТУ 643.46856491.00116-02 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00116-02 30 01.



Технические детали

Примерный сайзинг

< 5k EPS, 90 дней хранения

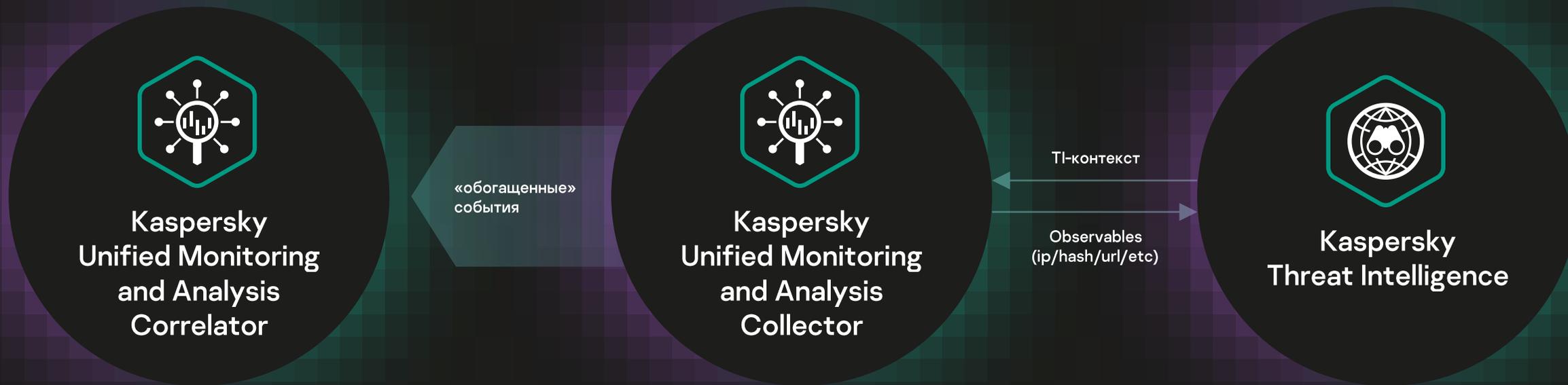
All-in-one

- CPU – 16 CPU
- RAM – 32 ГБ
- Storage – 6* ТБ

Инвентаризация информационных активов



Потоковое «обогащение» событий



«сырые» события

Источники данных



Приложения



Сетевые СЗИ



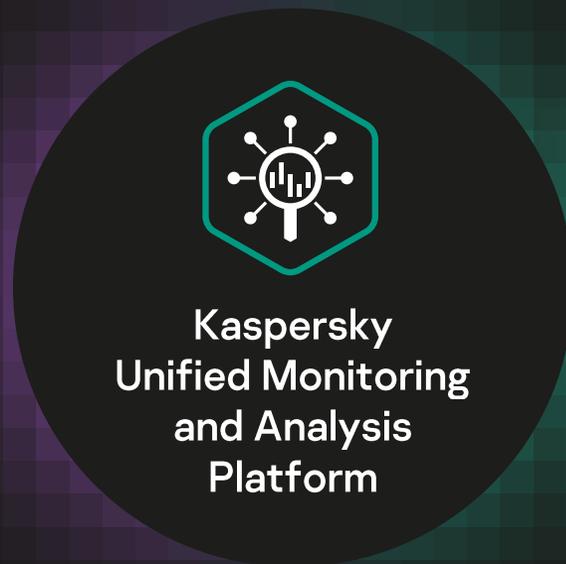
APM

«Обогащение» событий по запросу



Запрос по индикатору
(вручную/авто)

Пример -URL:
"example.com")



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



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,

Обогащение с помощью KTL

DeviceCustomString2	KES
DeviceCustomString2Label	ProductName
DeviceCustomString3	11.0.0.0
DeviceCustomString3Label	ProductVersion
DeviceCustomString5	{'engine':3,'method':5}
DeviceCustomString6	71
DeviceCustomString6Label	DetectionType
Service	[Example] KSC
FilePath	http://guestt03.top/favicon
FlexString1	Показать информ
FlexString1Label	Добавить в Cyber
FlexString2	Web Threat Protection
FlexString2Label	TaskName
Severity	
Type	
Raw	

Обогащение KTL

Веб-адрес
http://guestt03.top/favicon.ico

Группы данных для запроса

- Зона
- Общая информация о веб-адресе
- Доступ к файлу осуществлялся пользователем

Диспетчер задач

Статус	Задача	Создан	Время создания
✔ Завершено	KTL	osepov	6 авг. 2021 г. 09:00:00

10

Информация о веб-адресе

Зона
Red

Общая информация о веб-адресе

Категории
CATEGORY_BOTNET_CNC, CATEGORY_MALWARE

Количество файлов
0

Связь с APT
false

Адрес сервера
guestt03.top

Количество IPv4
83

Веб-адрес
guestt03.top/favicon.ico

Поддержка Multitenancy

Тенанты

Показать отключенных

<input type="checkbox"/>	Название	Ограничение EPS	Описание	Выключено	Создан
<input type="checkbox"/>	test	0			1 сент. 2021 г. 13:07:25
<input type="checkbox"/>	Main	0			27 авг. 2021 г. 15:45:41

Добавить тенанта

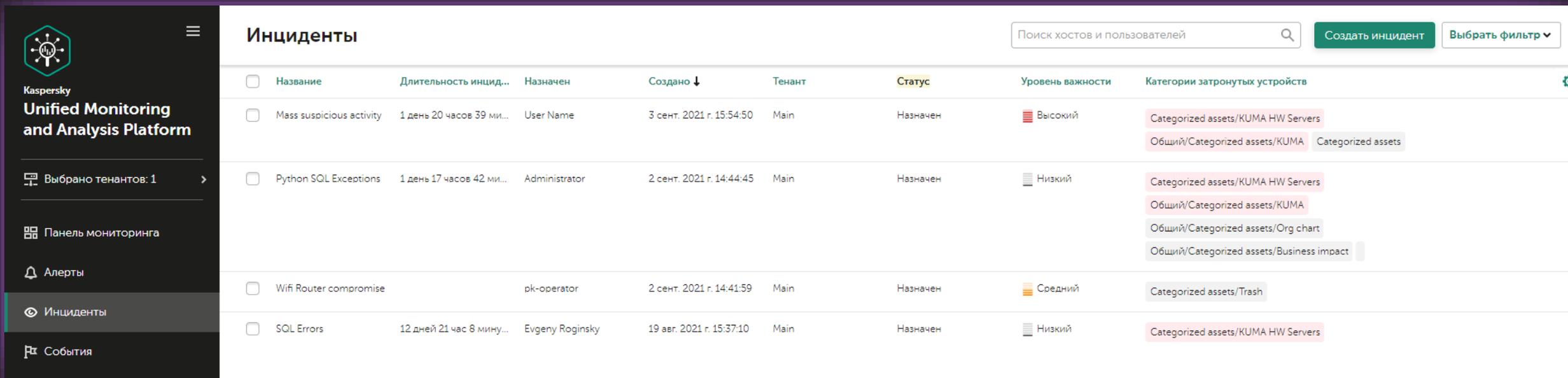
Название

Ограничение EPS

Описание

- **Разделение данных, конфигурации и прав доступа**
- **Возможность ограничения EPS для каждого тенанта отдельно**
- **Целевой сценарий для MSSP и центров Госсопка**

Новые функции по управлению инцидентами



The screenshot displays the 'Инциденты' (Incidents) section of the Kaspersky Unified Monitoring and Analysis Platform. The interface includes a search bar, a 'Создать инцидент' (Create Incident) button, and a 'Выбрать фильтр' (Select Filter) dropdown. The main content is a table with columns for Name, Duration, Assignee, Created, Tenant, Status, Priority, and Affected Asset Categories. The table lists five incidents with various details such as 'Mass suspicious activity', 'Python SQL Exceptions', 'Wifi Router compromise', and 'SQL Errors'.

<input type="checkbox"/>	Название	Длительность инцид...	Назначен	Создано ↓	Тенант	Статус	Уровень важности	Категории затронутых устройств
<input type="checkbox"/>	Mass suspicious activity	1 день 20 часов 39 ми...	User Name	3 сент. 2021 г. 15:54:50	Main	Назначен	Высокий	Categorized assets/KUMA HW Servers Общий/Categorized assets/KUMA Categorized assets
<input type="checkbox"/>	Python SQL Exceptions	1 день 17 часов 42 ми...	Administrator	2 сент. 2021 г. 14:44:45	Main	Назначен	Низкий	Categorized assets/KUMA HW Servers Общий/Categorized assets/KUMA Общий/Categorized assets/Org chart Общий/Categorized assets/Business impact
<input type="checkbox"/>	Wifi Router compromise		pk-operator	2 сент. 2021 г. 14:41:59	Main	Назначен	Средний	Categorized assets/Trash
<input type="checkbox"/>	SQL Errors	12 дней 21 час 8 мину...	Evgeny Roginsky	19 апр. 2021 г. 15:37:10	Main	Назначен	Низкий	Categorized assets/KUMA HW Servers

- Экспорт в НКЦКИ
- Создание инцидентов автоматически или вручную
- Управление инцидентами - назначение ответственного, изменение приоритета, эскалация, ведение истории, т. д.

Динамическая категоризация активов

Изменить категорию ×

*Название
Windows

*Родительская категория
Main/Categorized assets/OS 

*Тенант
Main ▾

*Способ категоризации
Активно ▾

*Уровень важности
Низкий ▾

Описание
Описание

Автоматическая категоризация выключена

*Регулярность категоризации
1ч ▾

*Условия
И + Добавить условие + Добавить группу

Если ОС ▾ like ▾ Windows ×

Проверить условия

- Динамическая категоризация по:
 - FQDN
 - IP
 - CVE
 - ОС
 - Версия билда ОС
- Логические операторы AND, OR, NOT и группировки
- Возможность проверки условий

Группировка алертов

The screenshot displays the 'Parameters' (Параметры) configuration page for alerts in the Kaspersky Unified Monitoring and Analysis Platform. The interface is divided into a left sidebar, a central navigation pane, and a main configuration area.

Left Sidebar: Contains the Kaspersky logo and the text 'Unified Monitoring and Analysis Platform'. Below this, it shows 'Выбрано тенантов: 1' and a list of navigation items: 'Панель мониторинга', 'Алерты', 'Инциденты', 'События', 'Устройства', 'Отчеты', 'Ресурсы', 'CyberTrace', 'Диспетчер задач', 'Параметры' (highlighted), 'Состояние источников', and 'Метрики'. At the bottom, it shows 'User Name'.

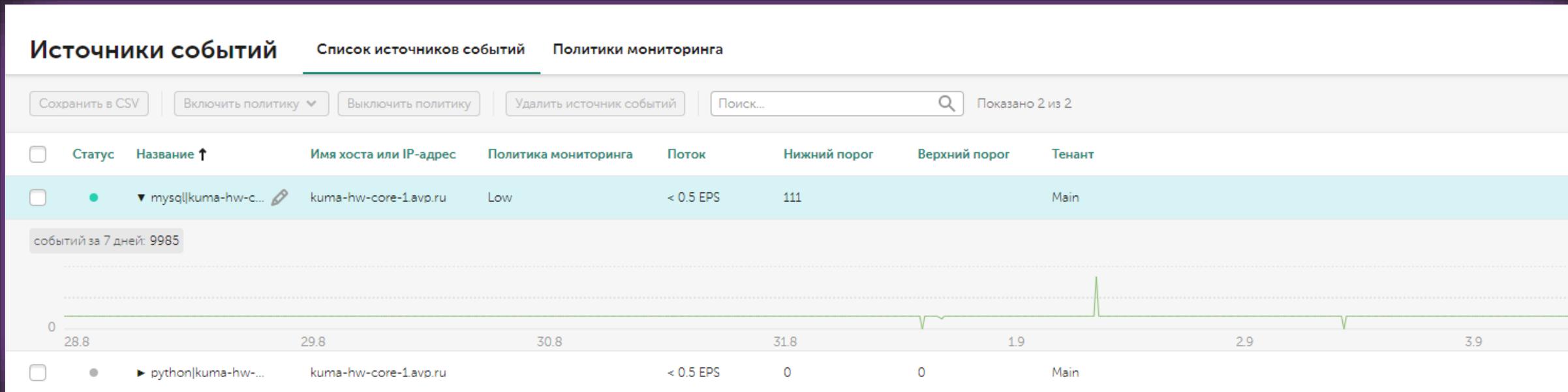
Central Navigation Pane: Lists various system components: 'Доступ', 'Пользователи', 'Тенанты', 'Active directory', 'Анализ угроз', 'KTL', 'CyberTrace', 'Интеграции', 'KSC', 'LDAP', 'R-Vision', 'НКЦКИ', 'Другое', 'Алерты' (highlighted), 'Лицензия', 'Уведомления', and 'Инциденты'.

Main Configuration Area: Titled 'Параметры', it is divided into two sections:

- Алерты:** Includes a 'Выключено' checkbox, a '*Тенант' dropdown menu set to 'Main', and a '+ Добавить' button.
- Правила сегментации:** Contains a list of rules. The first rule is visible with the following details:
 - *Название: Attack to 10.10.10.10
 - *Правило корреляции: R050_Windows event log cleared
 - *Селектор: 'И' (AND) with '+ Добавить условие' and '+ Добавить группу' buttons.
 - Condition: 'Если' (If) dropdown, 'поле события' (event field) dropdown, 'DestinationAddress' dropdown, '=', 'константа' (constant) dropdown, and the value '10.10.10.10' with a close button 'x'.

A green 'Сохранить' (Save) button is located at the bottom of the configuration area.

Мониторинг доступности источников



- **Мониторинг источников по минимальному кол-ву событий в период времени**
- **Уведомление по почте в случае недоступности**
- **Возможность задать разные политики**

Поддержка новых видов транспорта

The screenshot shows a configuration page for 'Транспорт' (Transport). The left sidebar contains a navigation menu with 8 items: 1. Подключение источников, 2. Транспорт, 3. Парсинг событий, 4. Фильтрация событий, 5. Агрегация событий, 6. Обогащение событий, 7. Маршрутизация, 8. Проверка настроек. The main content area is titled 'Транспорт' and includes a subtitle: 'Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#)'. Below this are two tabs: 'Основные параметры' (Active) and 'Дополнительные параметры'. The 'Основные параметры' section contains: '*Коннектор' (Create), '*Тип' (Dropdown menu with a list of transport types), '*URL', and 'Описание'. The dropdown menu for '*Тип' is open, showing a scrollable list of transport types: internal, tcp, udp, netflow, nats, kafka, http, sql, file, ftp, nfs, wmi, wec, and snmp.

- **Поддержка сбора событий через механизм Windows Management Instrumentation (WMI)**
- **FTP**
- **NFS**
- **SNMP v1/v2/v3**

Мастер добавления нового источника

1 Подключение источников
2 Транспорт
3 Парсинг событий
4 Фильтрация событий
5 Агрегация событий
6 Обогащение событий
7 Маршрутизация
8 Проверка параметров

Парсинг событий

Парсинг событий

*Хранить исходное событие: Не хранить

*Сохранить дополнительные поля: Да

Примеры событий: Загрузить из файла

```
Feb 2 11:57:59 192.168.33.131 fenotify-2.alert:  
CEF:0|FireEye|MPS|6.2.0.74484|WI|web-infection|5|rt=Feb 02 2014 16:57:47 Z  
src=169.250.0.1 dpt=20 shost=OC-testing.fe-notify-examples.com proto=tcp  
dst=127.0.0.20 dvchost=WebMPS cs3Label=osinfo cs3=FireEyeTestEvent OS Info  
filePath=comp1_0_2- someur1.x1y2z3.com spt=10 dvc=192.168.33.131  
smac=XX:XX:XX:XX:XX:XX cn1Label=vlan cn1=0 externalId=2 cs4Label=link  
cs4=https:// WebMPS.localdomain/event_stream/ events_for_bot?inc_id\=2  
dproc=IEx123 dmac=XX:XX:XX:XX:XX:XX cs2Label=anomaly cs2=anomaly-tag  
datatheft keylogger cs1Label=sname cs1=FireEye-TestEvent-SIG
```

Нормализация: Использовать синтаксис CEF при нормализации

```
{?P<date>\S+\s\d+\s\d+:\d+:\d+}\s(?:P<device>\d+\.\d+\.\d+\.\d+)\s.*WI\|(?  
P<name>[^\|]+\|)\d
```

Перенести названия полей в таблицу + Добавить регулярное выражение

Сопоставление

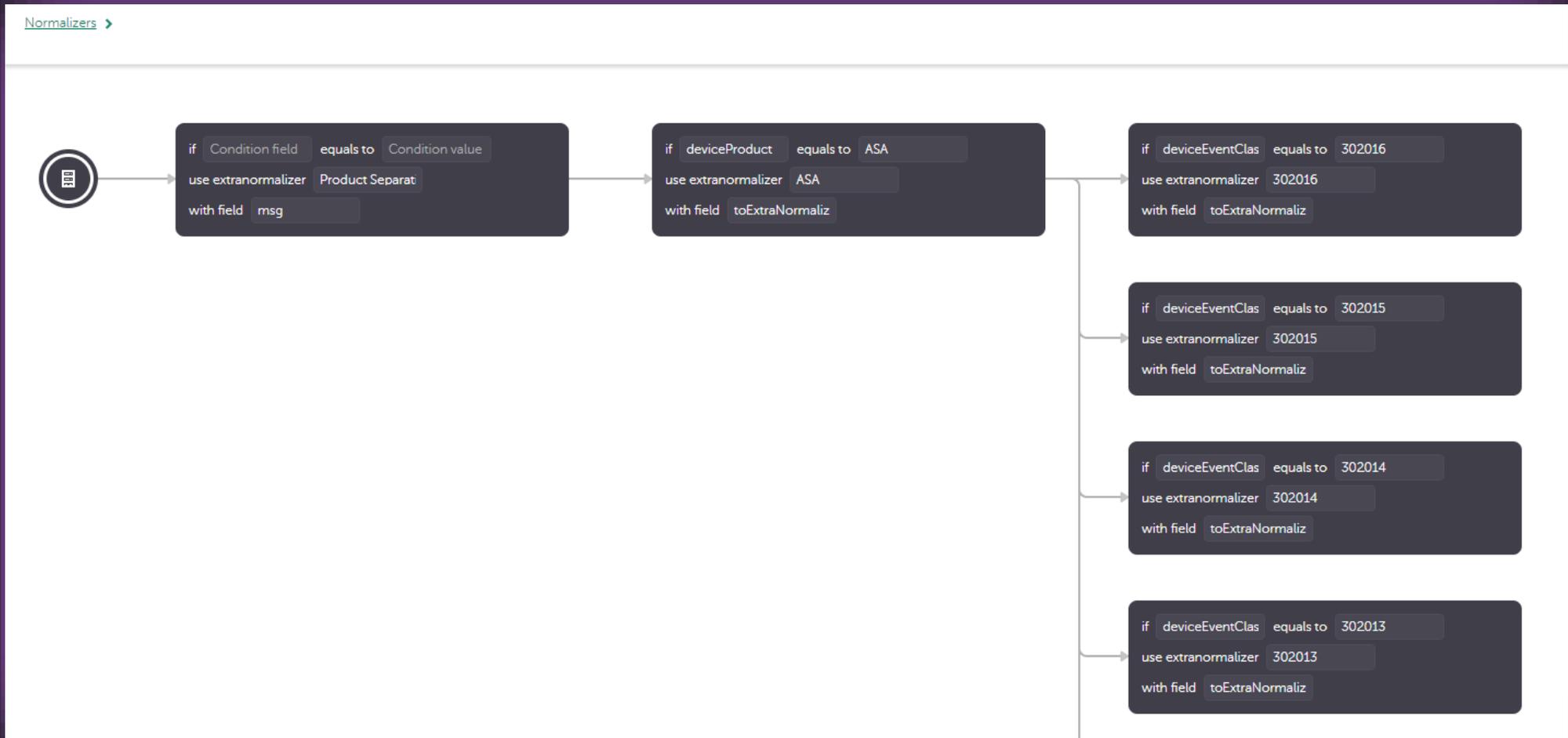
Исходные данные	Поле KUMA	Подпись	Примеры
date	DeviceReceiptTime		2 февр. 2021 г. 14:57:59
device	DeviceAddress		192.168.33.131
name	Name		web-infection

+ Добавить строку Очистить все

OK Отмена

- Пошаговый мастер для добавления нового источника
- Проверка правил нормализации на примерах событий
- Подсвечивание синтаксиса

Мастер добавления нового источника

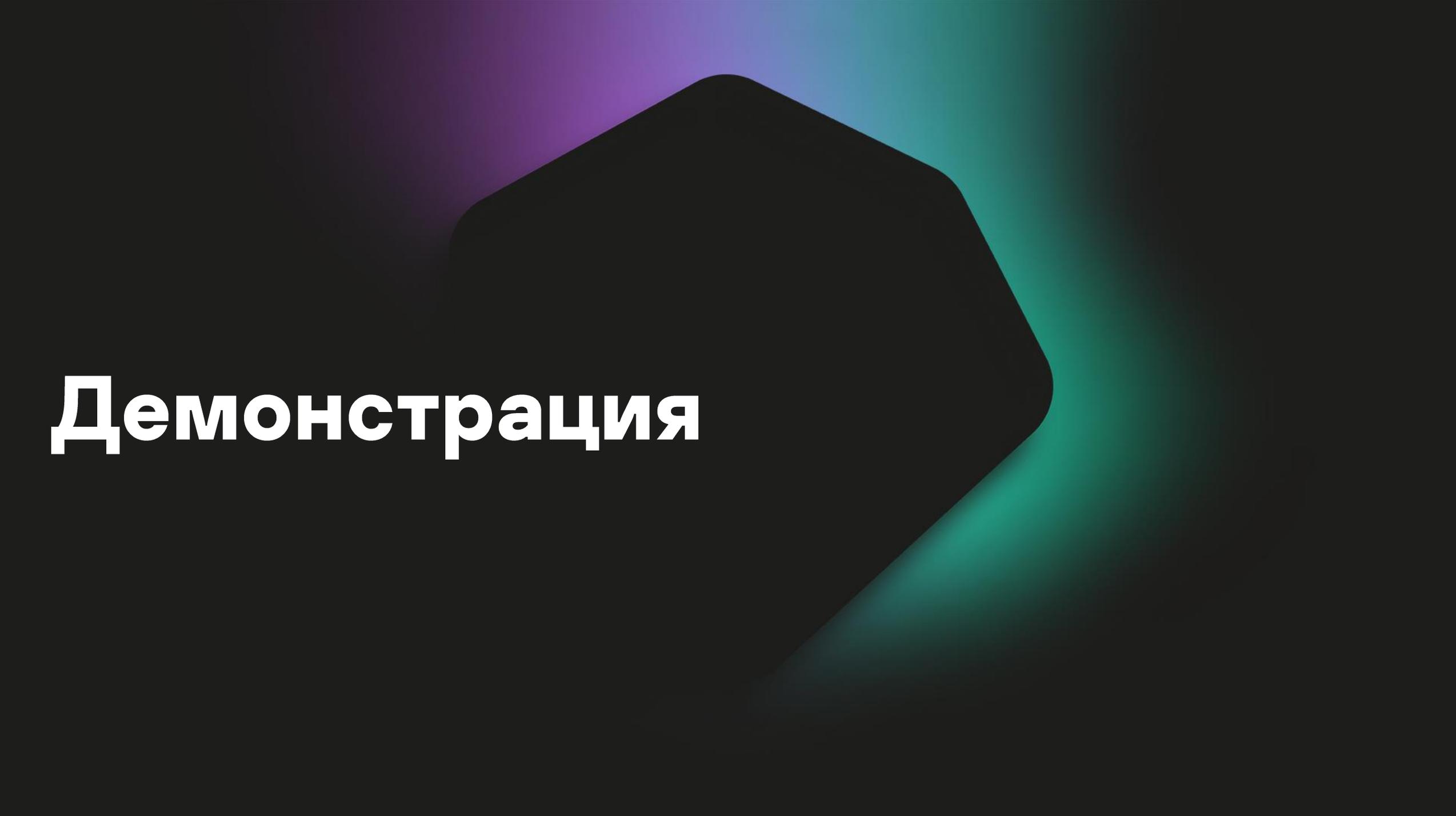


Другие новые функции

- **Переход на Oracle Linux 8**
- **Новый пакет правил корреляции (>50шт)**
- **Поддержка новых источников данных «из коробки»**
- **Поддержка сбора логов из SQL базы KSC**
- **Улучшения UI/UX**
- **Возможность бэкапа и восстановления полной конфигурации**
- **Авторизация пользователей через AD**
- **Настраиваемая агрегация алертов**
- **Расширение списка поддерживаемых источников данных**
- **Замена инсталлятора на Ansible (поддерживает и распределенную установку)**
- **RESTful API**
 - **Возможность работы с ассетами и активными списками**
 - **Поддержка multitenancy**
 - **Возможность работы с событиями, алертами**
- **и др.**

KUMA Релиз 1.6 (12.2021)

- **Поддержка сценариев иерархического развёртывания**
- **Поддержка Astra Linux («Смоленск»)**
- **Утилита для конвертации *sigma*-правил в ресурсы KUMA**
- **Расширение списка поддерживаемых источников логов**
- **Расширение набора правил корреляции.**



Демонстрация

Спасибо