

**Kaspersky
Security Day
2021**

2 года с KUMA

**Андрей Евдокимов,
руководитель отдела ИБ
Лаборатории Касперского**

kaspersky

Kaspersky Infosecurity Team

2



splunk >

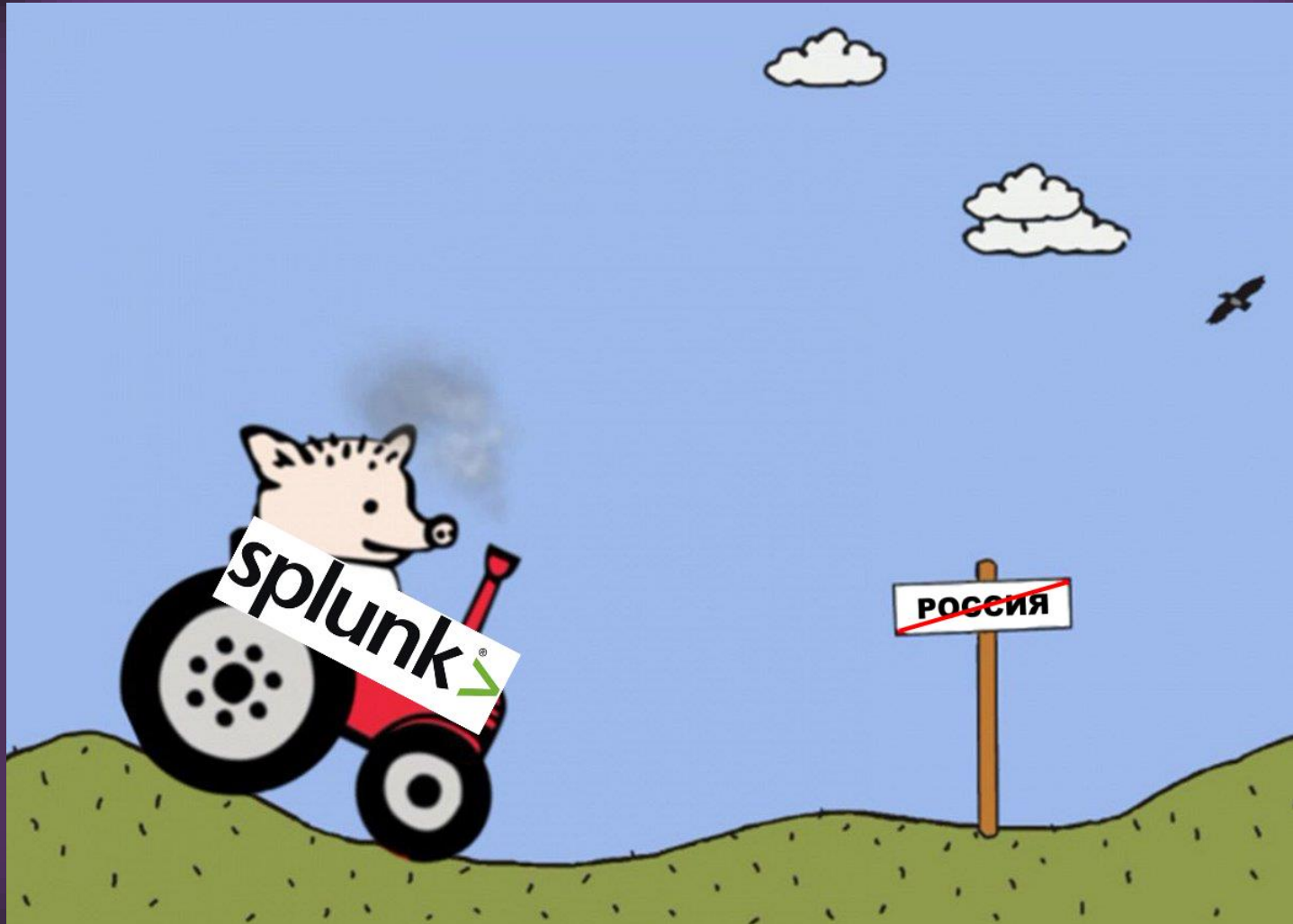


Elasticsearch

Logstash

Kibana







Elasticsearch



Logstash



Kibana



ArcSight™

IBM Q Radar



?

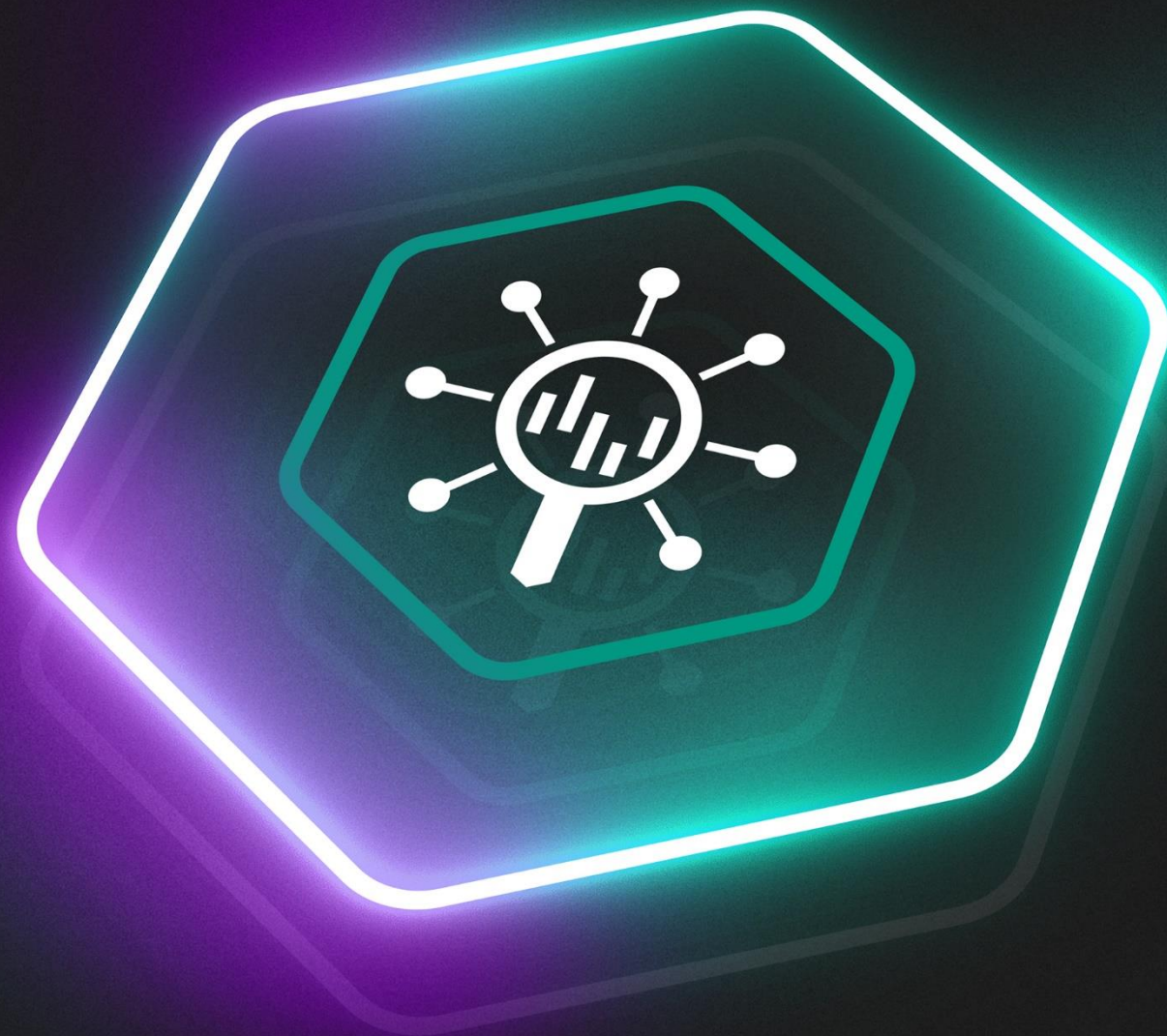
MaxPatrol SIEM



POSITIVE
TECHNOLOGIES

Наш выбор

**Kaspersky
Unified
Monitoring and
Analysis Platform**



Проблемы и недостатки KUMA

10





Работа с большими объемами

- В среднем 25 000 событий в секунду, в пиках до 55 000
- Около 400 Гб данных в день
- 30 различных источников, сотни серверов



Совместимость с любыми источниками

- Чтение файлов из сетевых папок
- Listener TCP/UDP (syslog, kafka, http...)
- Прямые запросы в SQL базы
- Netflow



Оптимальное
потребление ресурсов



Пример – для 3K EPS

KUMA

12vCPU/12RAM/1TB

ELK-based SIEM

56vCPU/128RAM/26,4TB

KUMA:

1 x Core = 4 CPU 12GB RAM; 2 x Collector = 8 CPU 48Gb RAM

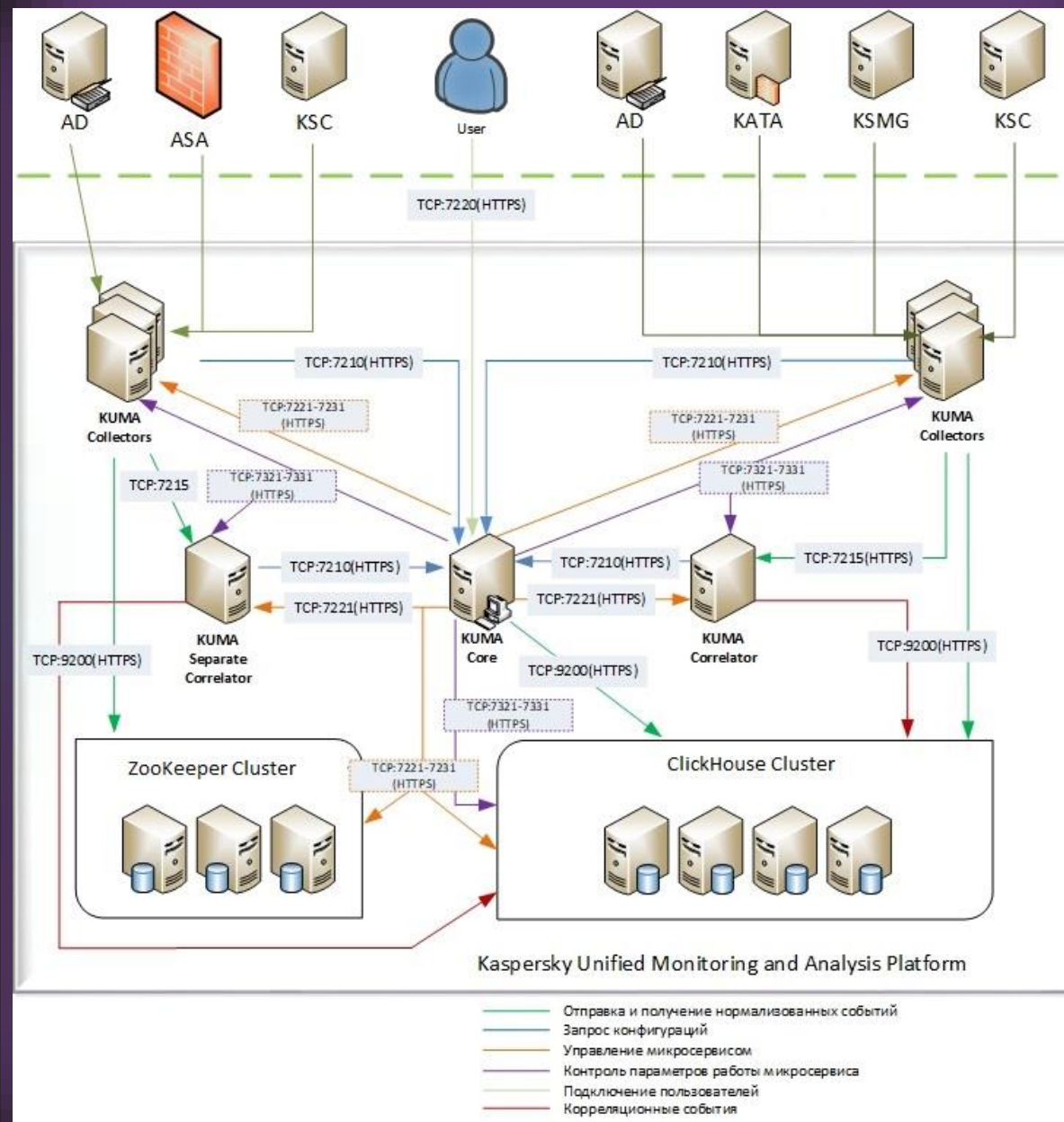
2 x Correlator = 16 CPU 32GB RAM; 3 x ZooKeeper 2 CPU 6GB RAM

4 x ClickHouse = 32CPU 64GB RAM

Плюсы KUMA



Легкая
масштабируемость



Плюсы KUMA

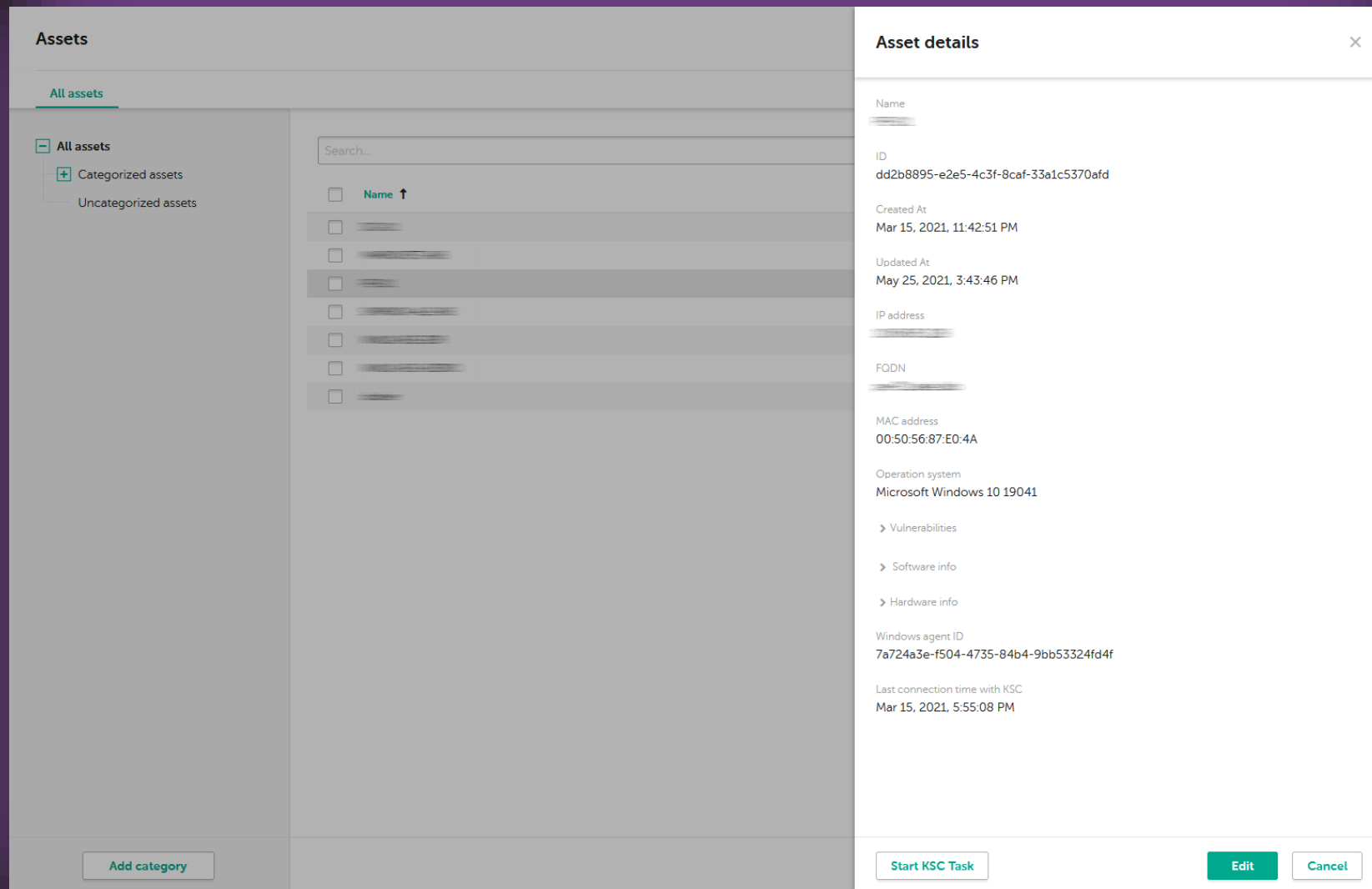


KUMA: несколько кликов —
и у нас полная информация
о хосте (ОС, уязвимости,
установленное ПО и
многое другое)



Splunk: тяжеловесный
запрос с join'ами,
нагружающий searchhead

14

A screenshot of the KUMA web interface. The main panel is titled 'Assets' and shows a list of assets under the 'All assets' tab. A search bar is at the top of the list. The left sidebar has a tree view with 'All assets' expanded, showing 'Categorized assets' and 'Uncategorized assets'. At the bottom of the sidebar is an 'Add category' button. The right panel is titled 'Asset details' and shows information for a specific asset. The details include Name, ID, Created At, Updated At, IP address, FQDN, MAC address, Operation system, Vulnerabilities, Software info, Hardware info, Windows agent ID, and Last connection time with KSC. At the bottom of the details panel are buttons for 'Start KSC Task', 'Edit', and 'Cancel'.

Assets

All assets

All assets

Categorized assets

Uncategorized assets

Search...

Name ↑

Asset details

Name

ID

dd2b8895-e2e5-4c3f-8caf-33a1c5370afd

Created At

Mar 15, 2021, 11:42:51 PM

Updated At

May 25, 2021, 3:43:46 PM

IP address

FQDN

MAC address

00:50:56:87:E0:4A

Operation system

Microsoft Windows 10 19041

Vulnerabilities

Software info

Hardware info

Windows agent ID

7a724a3e-f504-4735-84b4-9bb53324fd4f

Last connection time with KSC

Mar 15, 2021, 5:55:08 PM

Add category

Start KSC Task

Edit

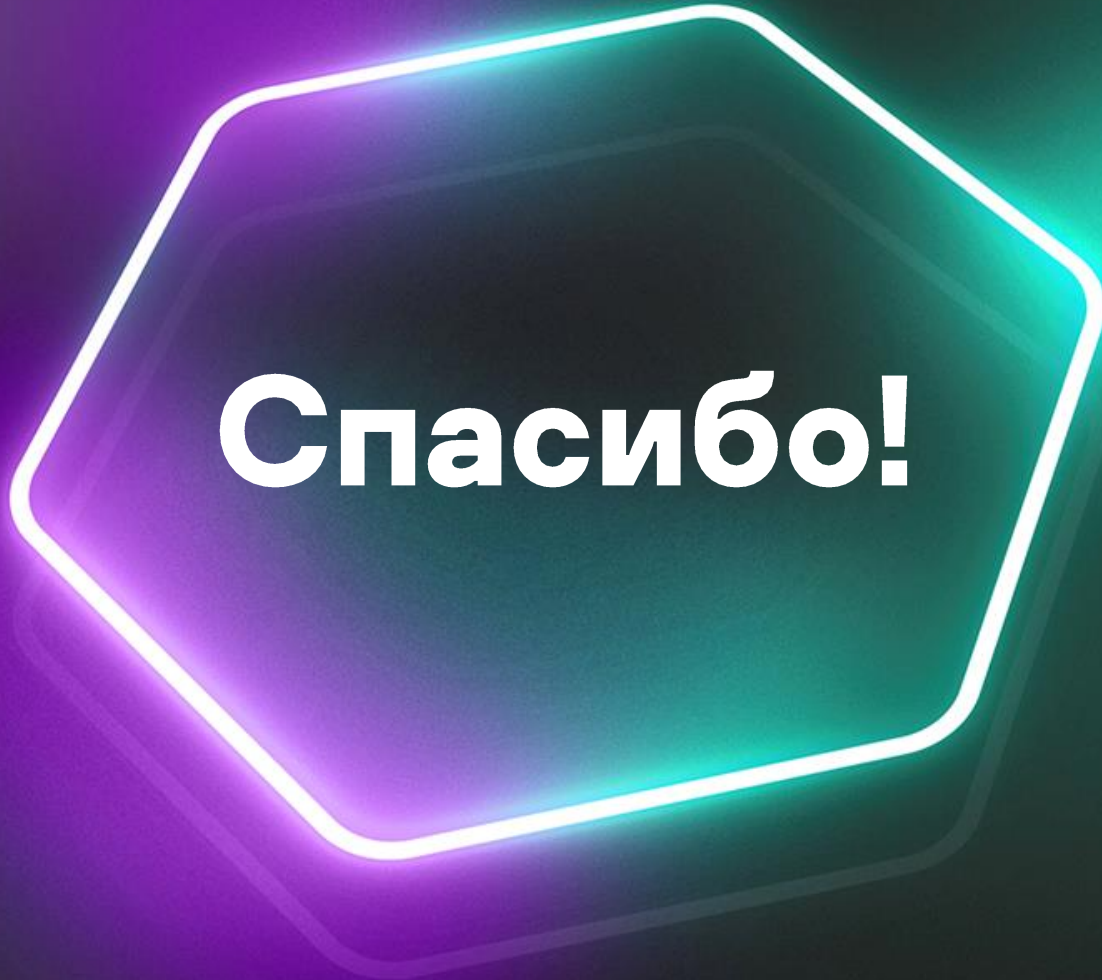
Cancel



Kaspersky
Unified Monitoring and
Analysis Platform

Решение KUMA

сделано и
развивается
ИБ-шниками
для ИБ-шников



Спасибо!

kaspersky