Kaspersky
Security Day
2021

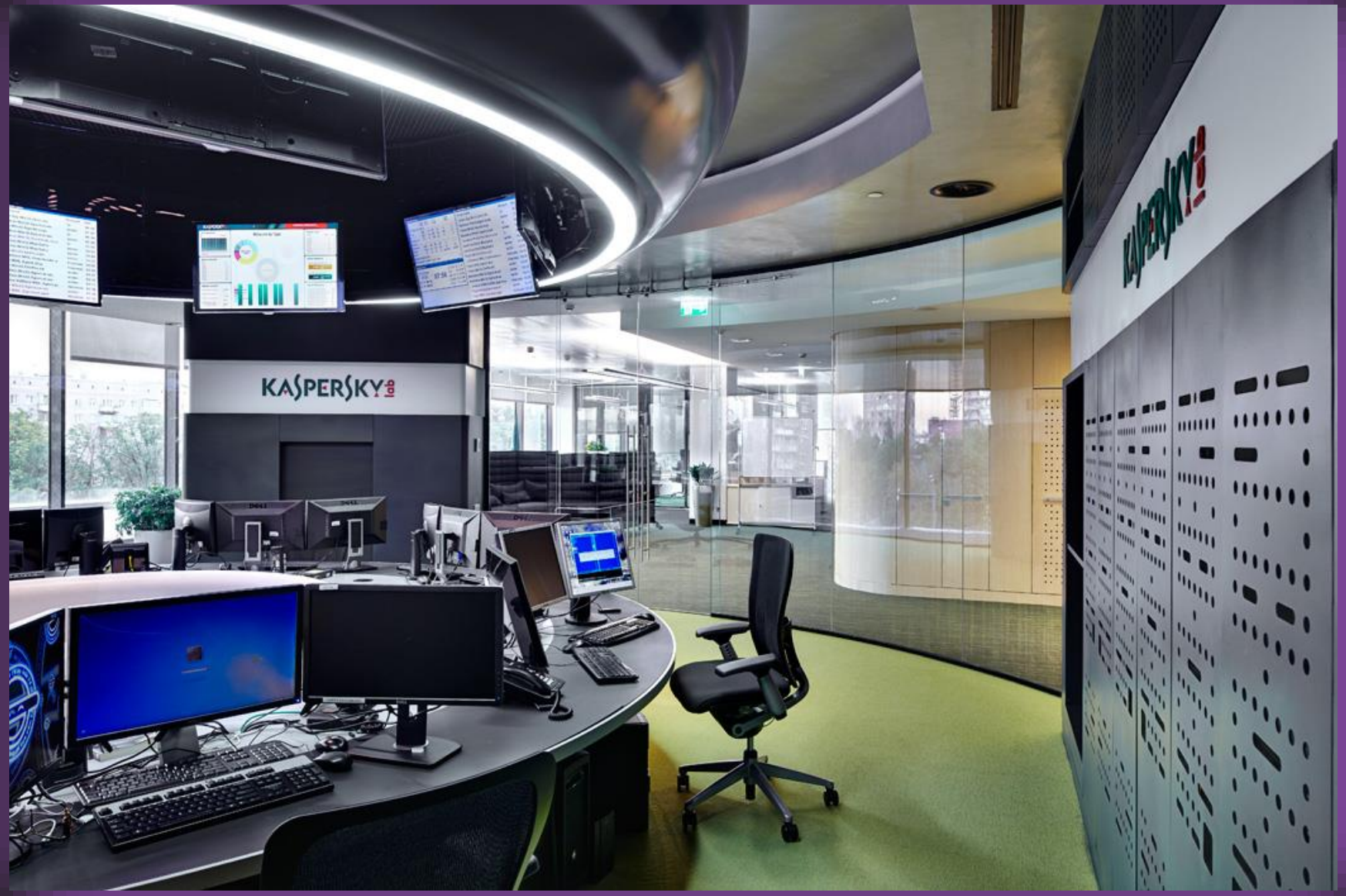
# 2 года с KUMA

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

kaspersky

# Kaspersky Infosecurity Team





splunk>

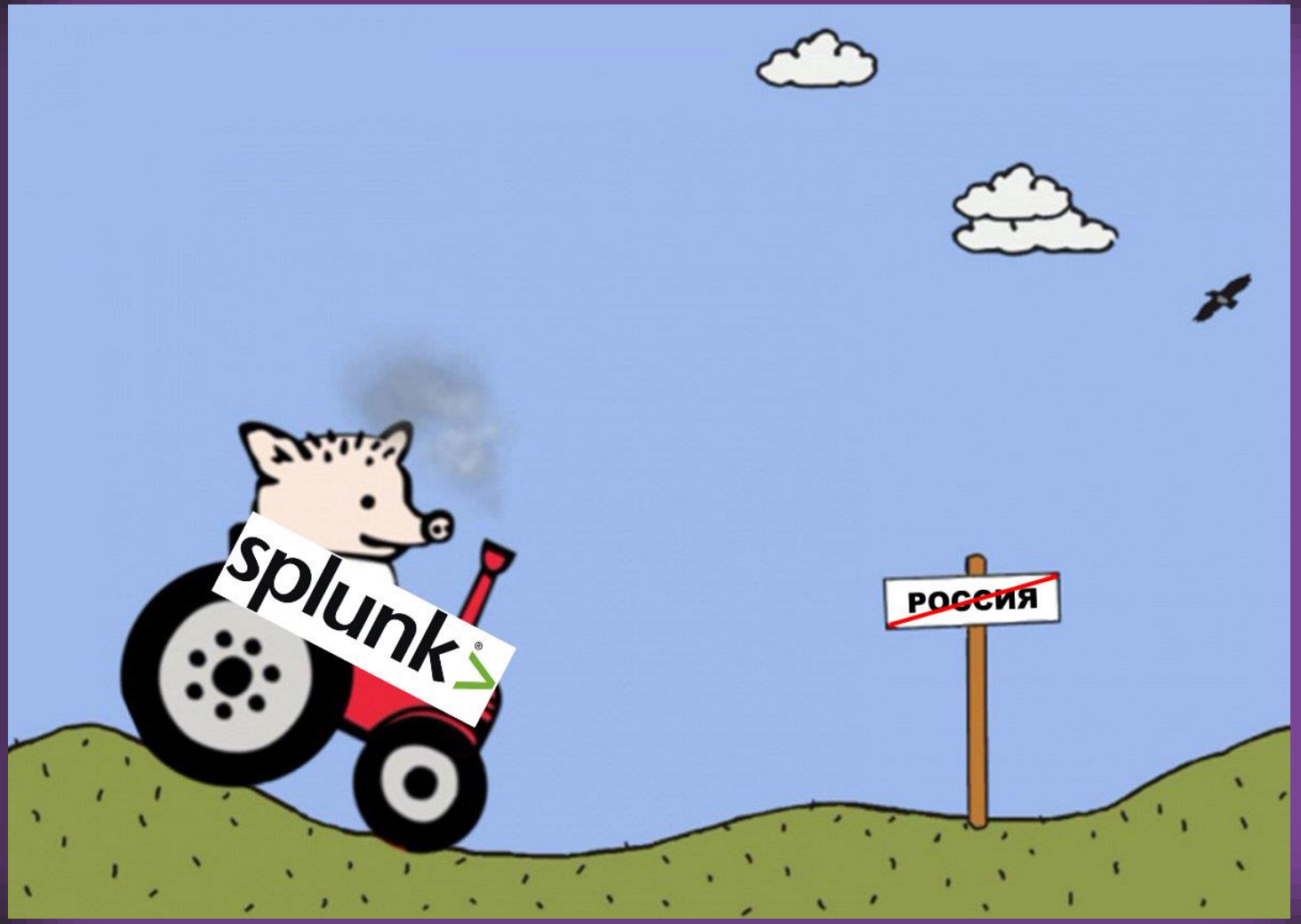
Elasticsearch Logstach Kibana

# Выбор SIEM: Опции.



# Выбор SIEM: Опции.





# Выбор SIEM: Опции.



Elasticsearch Logstach Kibana

# Выбор SIEM: Опции.




ArcSight™

IBM

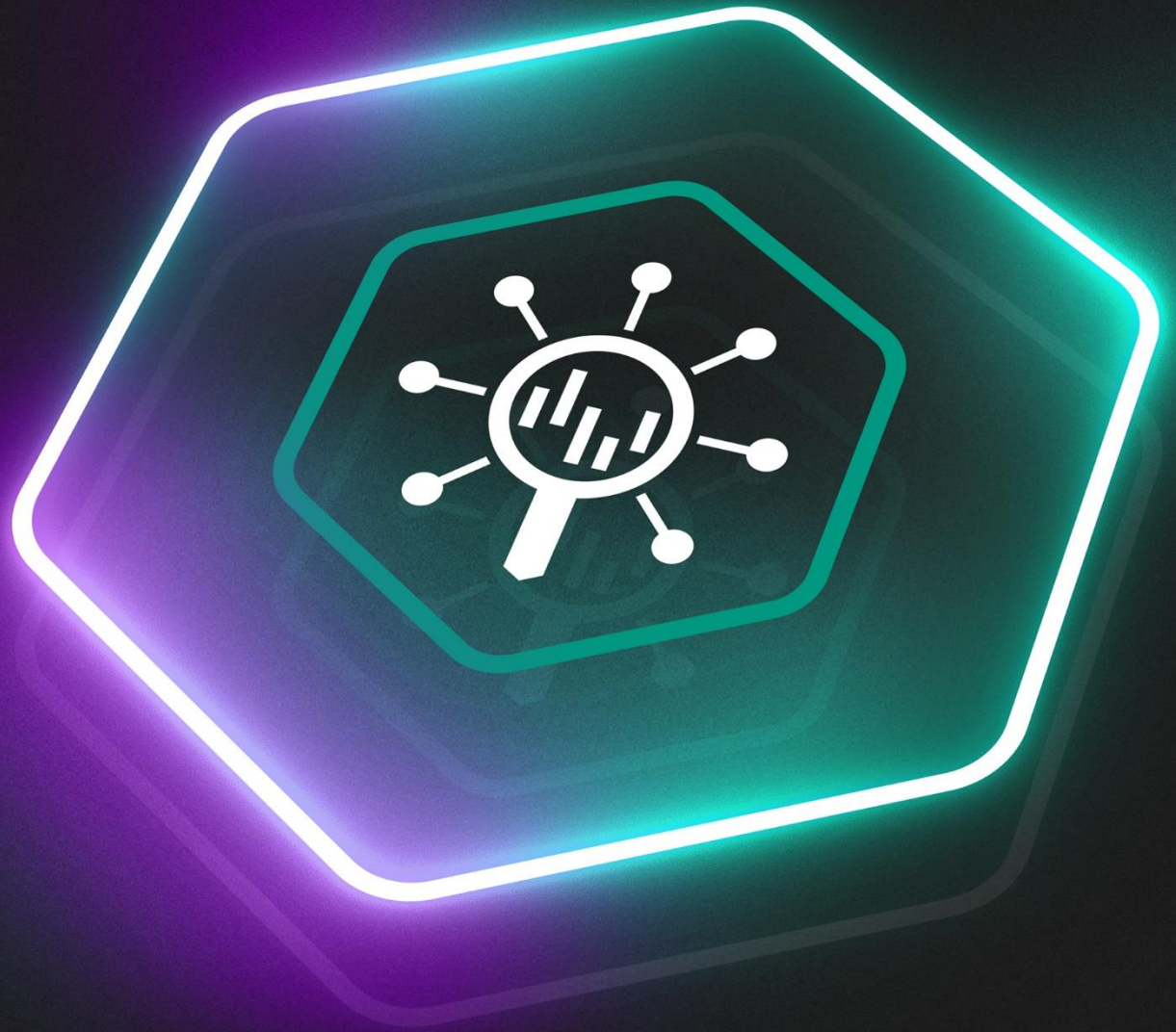
Radar


# MaxPatrol SIEM

PT POSITIVE TECHNOLOGIES

Наш выбор

# Kaspersky Unified Monitoring and Analysis Platform



# Проблемы и недостатки KUMA



# Плюсы KUMA



## Работа с большими объемами

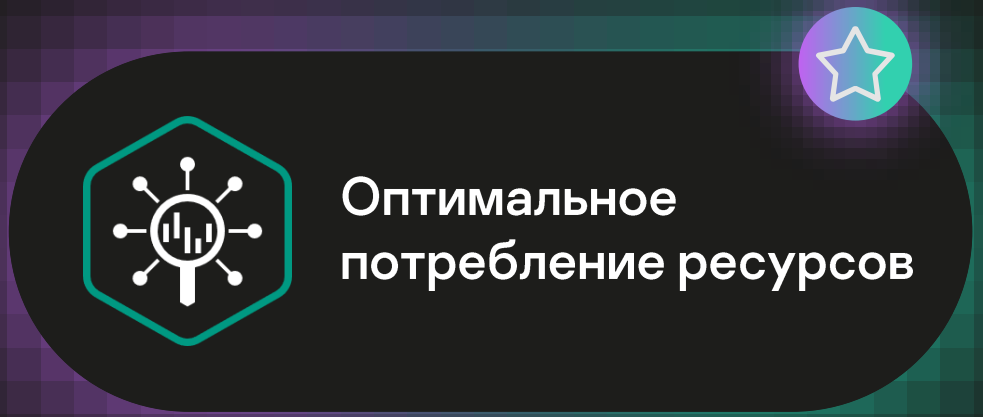
- В среднем 25 000 событий в секунду, в пиках до 55 000
- Около 400 Гб данных в день
- 30 различных источников, сотни серверов

## Совместимость с любыми источниками

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

# Плюсы KUMA





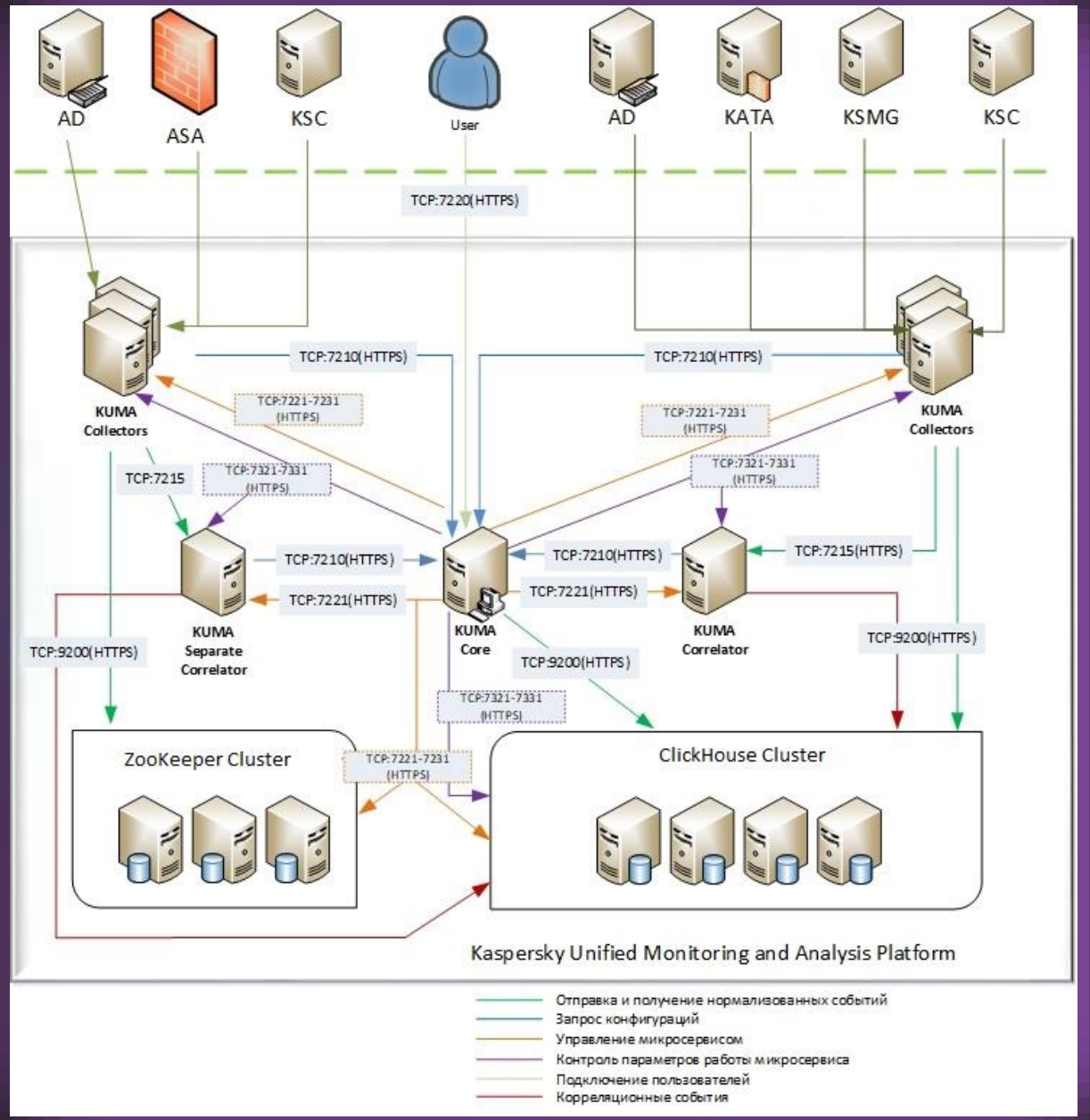

Пример – для 3K EPS

| KUMA | ELK-based SIEM |
|---|---|
| 12vCPU/12RAM/1TB | 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

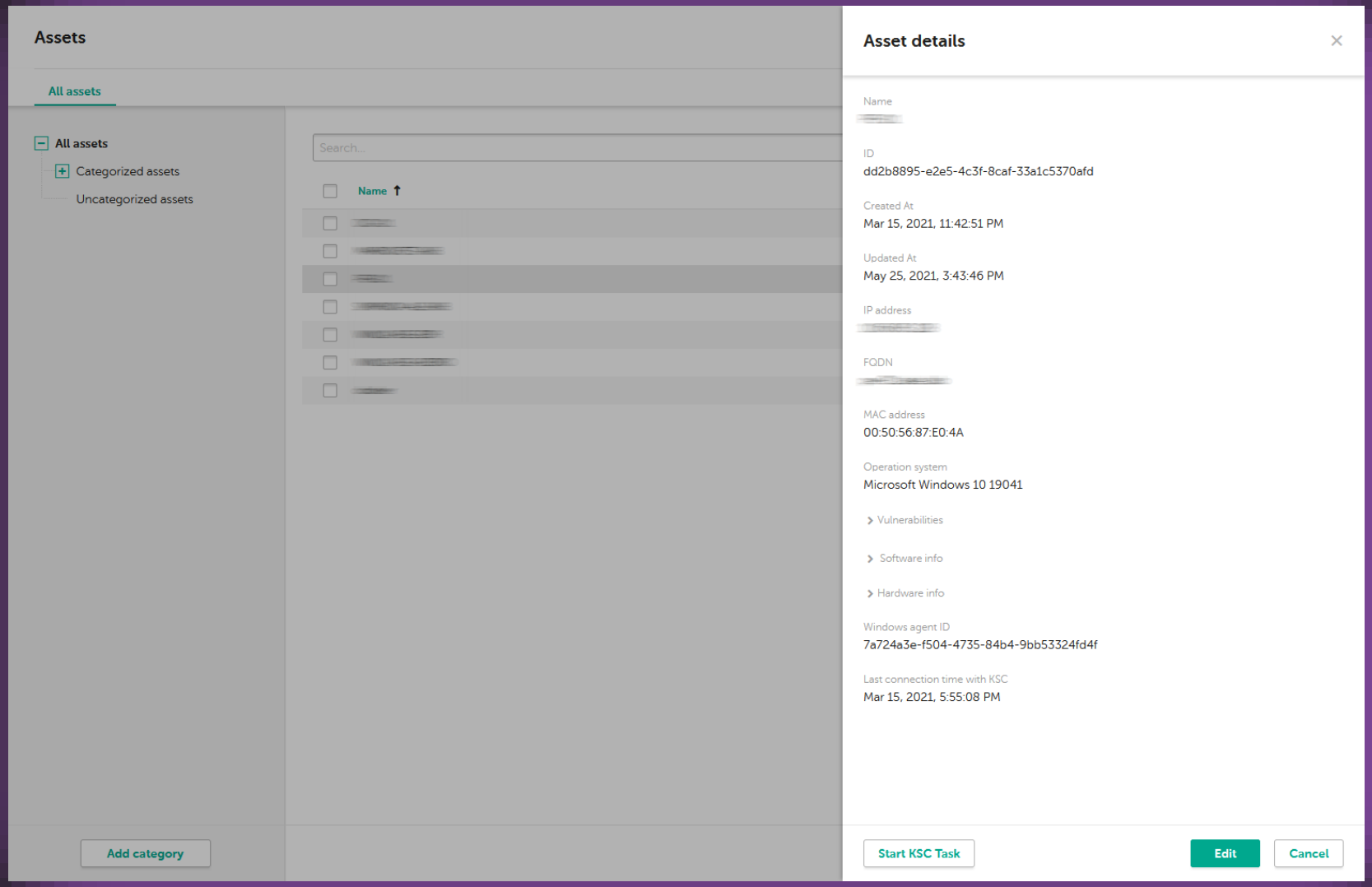


# Плюсы KUMA



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



Kaspersky
Unified Monitoring and
Analysis Platform

# Решение KUMA сделано и развивается ИБ-шниками для ИБ-шников

# Спасибо!

kaspersky