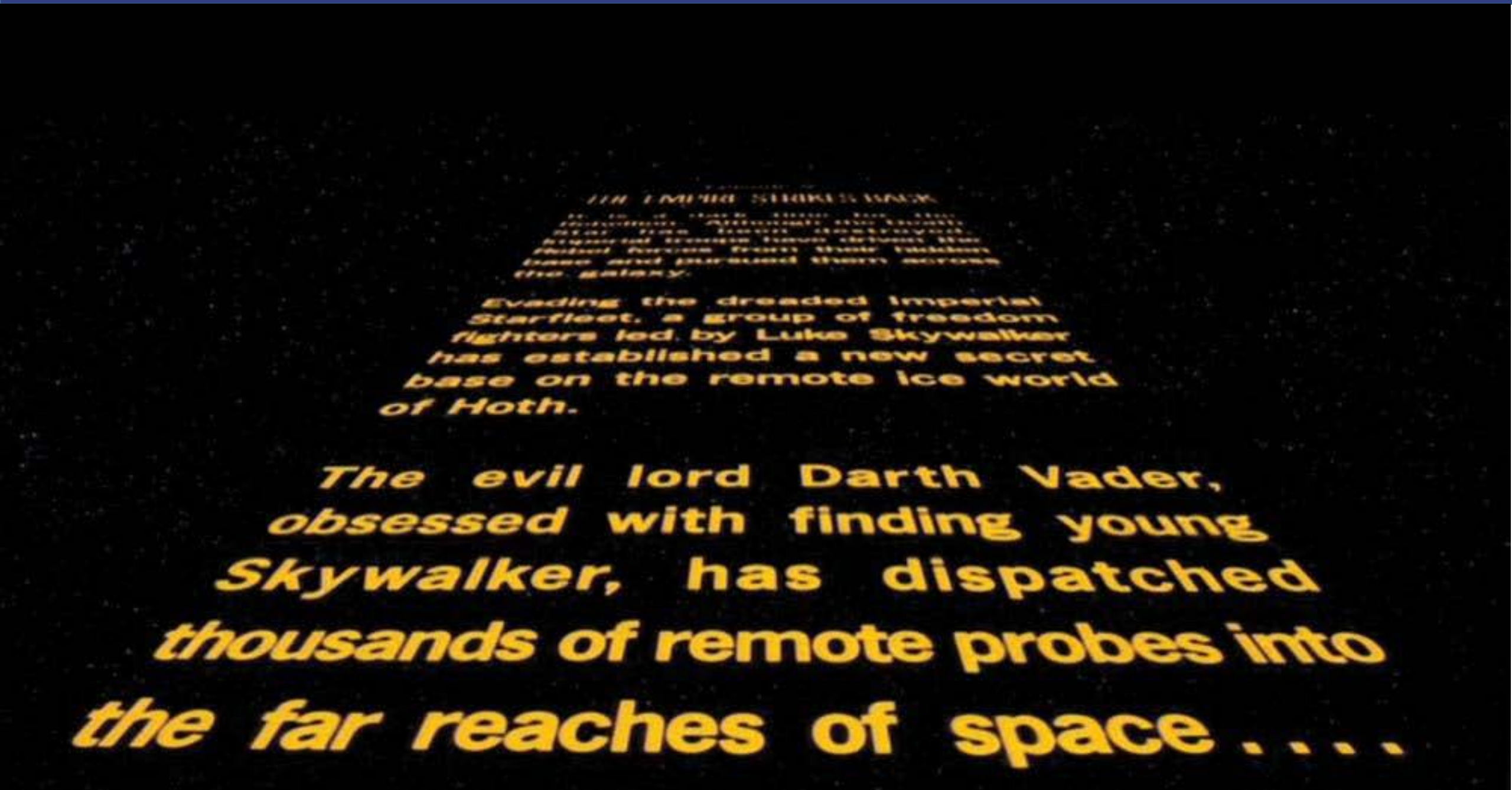
Индикаторы компрометации, доступные каждому

Эркин Рустамов
Директор Службы ИТ Безопасности

Eurasian Bank

Не так давно, в одной не очень далекой галактике...

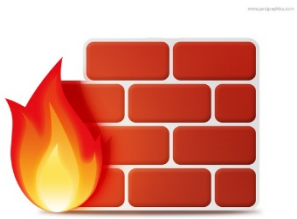
Eurasian Bank



Знание – самая надежная защита

Недостаточно технической информации

Медленная скорость обработки

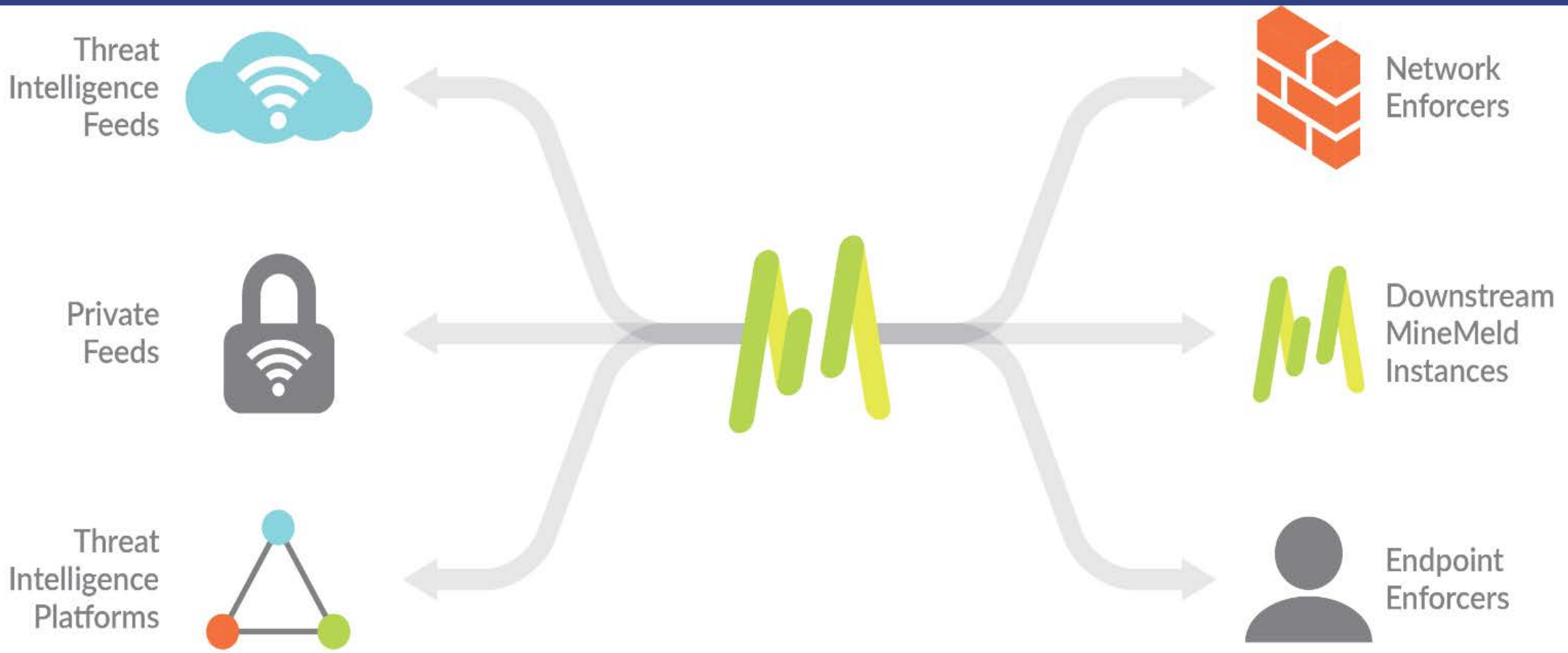


Несколько систем получателей IOC

Высокая стоимость услуг Threat Intelligence

Open Source спешит на помощь

Eurasian Bank



- Агрегация и корреляция IOC
- Интеграция с SIEM, IPS, Web и Mail gateway, Antivirus
- Классификация источников IOC
- Возможность создания своих источников и получателей IOC
- Поддержка различных форматов данных (STiX, TAXII, XML, CSV и т.д.)

Результат

Eurasian Bank

NODES

64	4	11
MINERS	PROCS	OUTPUTS

MINERS

196.2K
OF INDICATORS

12
ADDED

0
AGED OUT

OUTPUTS

124.5K
OF INDICATORS

24
ADDED

0
REMOVED

- IP и DNS адреса
- URL
- Email адреса
- Хеши файлов

367 000 IOC

SPAMHAUS

БАНК РОССИИ ФИНЦЕРТ

TALOS

www.blocklist.de fail2ban reporting service

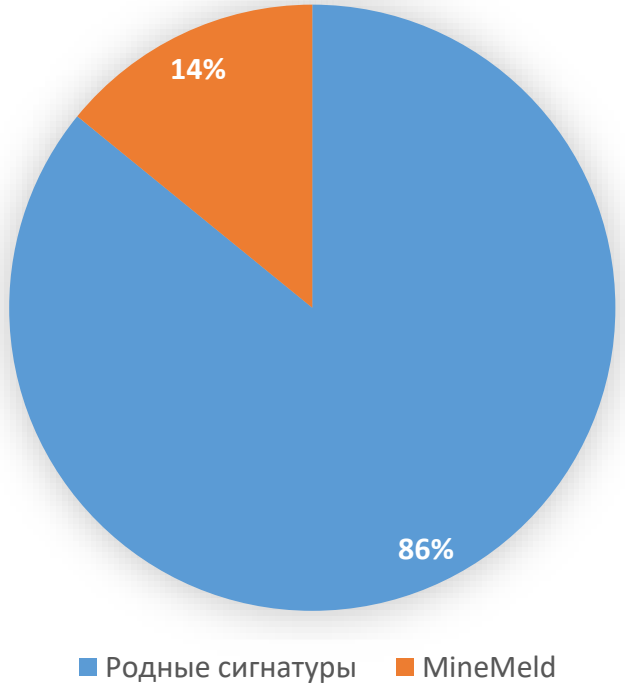
ZEUS TRACKER

Ransomware Tracker

ALIEN VAULT

CERT - PA

Блокировка соединений



Вместе весело шагать

Eurasian Bank

erkin.rustamov@eubank.kz

Спасибо за внимание!
Вопросы?