

Индикаторы компрометации, доступные каждому
Эркин Рустамов
Директор Службы ИТ Безопасности



Eurasian Bank

THE EMPIRE STRIKES BACK
In the year 4 ABY, the Galactic Empire, under the leadership of Emperor Palpatine, has established a new secret base on the remote ice world of Hoth.

Evading the dreaded Imperial Starfleet, a group of freedom fighters led by Luke Skywalker has established a new secret base on the remote ice world of Hoth.

The evil lord Darth Vader, obsessed with finding young Skywalker, has dispatched thousands of remote probes into the far reaches of space



МАЛОВАТО БУДЕТ!

Недостаточно технической информации



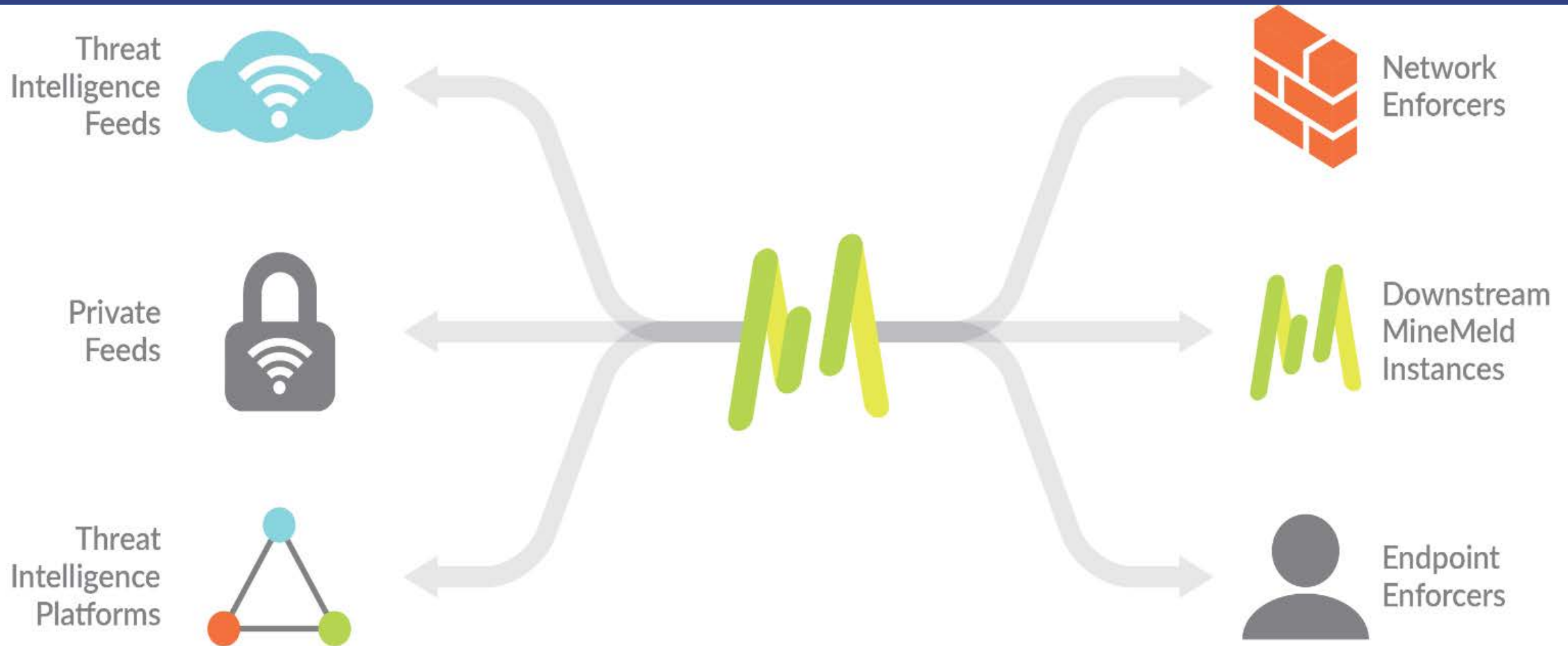
Медленная скорость обработки



Несколько систем получателей ИОС



Высокая стоимость услуг Threat Intelligence



- 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.)

NODES	64 MINERS	4 PROCS	11 OUTPUTS
MINERS	196.2K # OF INDICATORS	12 ADDED	0 AGED OUT
OUTPUTS	124.5K # OF INDICATORS	24 ADDED	0 REMOVED

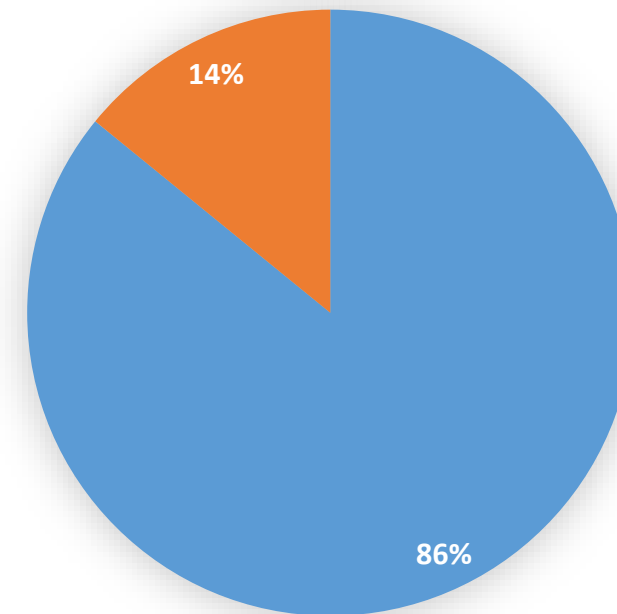
- IP и DNS адреса
- URL
- Email адреса
- Хеши файлов



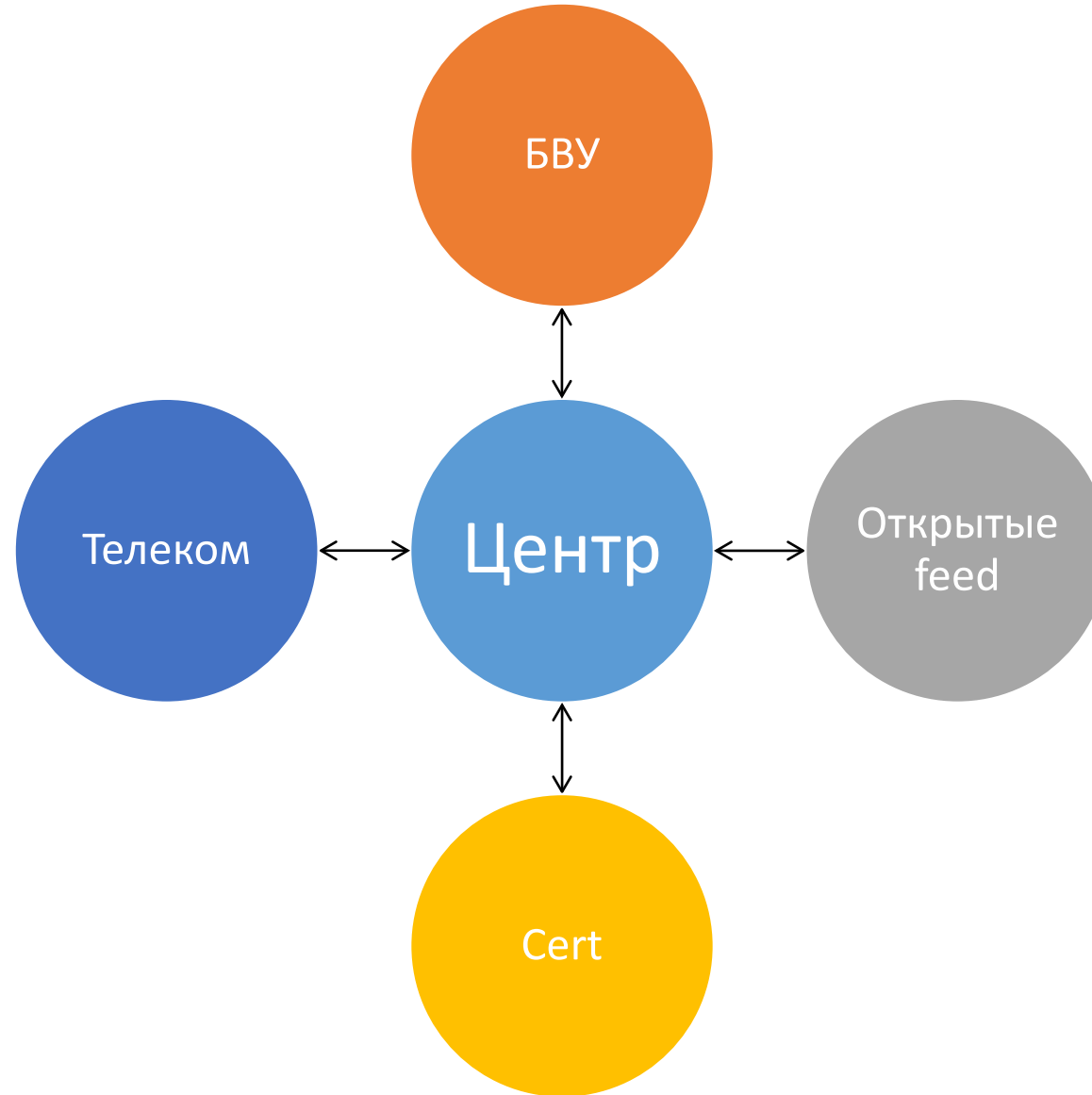
367 000 IOC



Блокировка соединений



■ Родные сигнатуры ■ MineMeld



Спасибо за внимание!
Вопросы?