Быть лучше каждый день

SOC МТС

Андрей Дугин
Начальник отдела обеспечения информационной безопасности

История SOC МТС

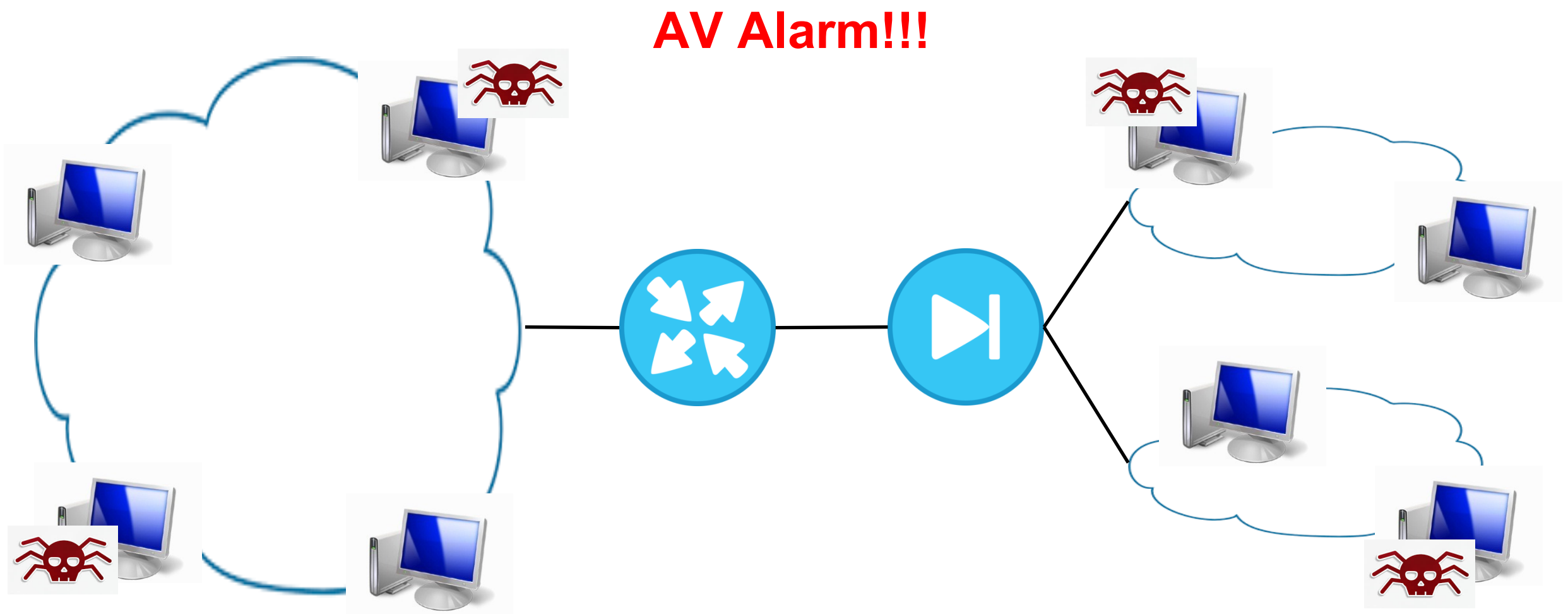
Коммерческий SOC

Корпоративный SOC

2005

2017

#1



#1

- Скрипт на удаление Punto Ыцшесрук
- Определение поведения как шифровальщика

#2

- Срабатывание множественных событий из одного региона
- Attacker Address = CONST, Attacker Hostname = “-”
- Target Address, user разные
- Нелегитимная перемаршрутизация?
- Царь-роутер?

#2

- Подключение маршрутизатора с hostname = “-”
- Отсутствие 802.1x на площадке
- DNS update на DHCP
- DNS resolving на коннекторах
- Регистрация системных событий Windows

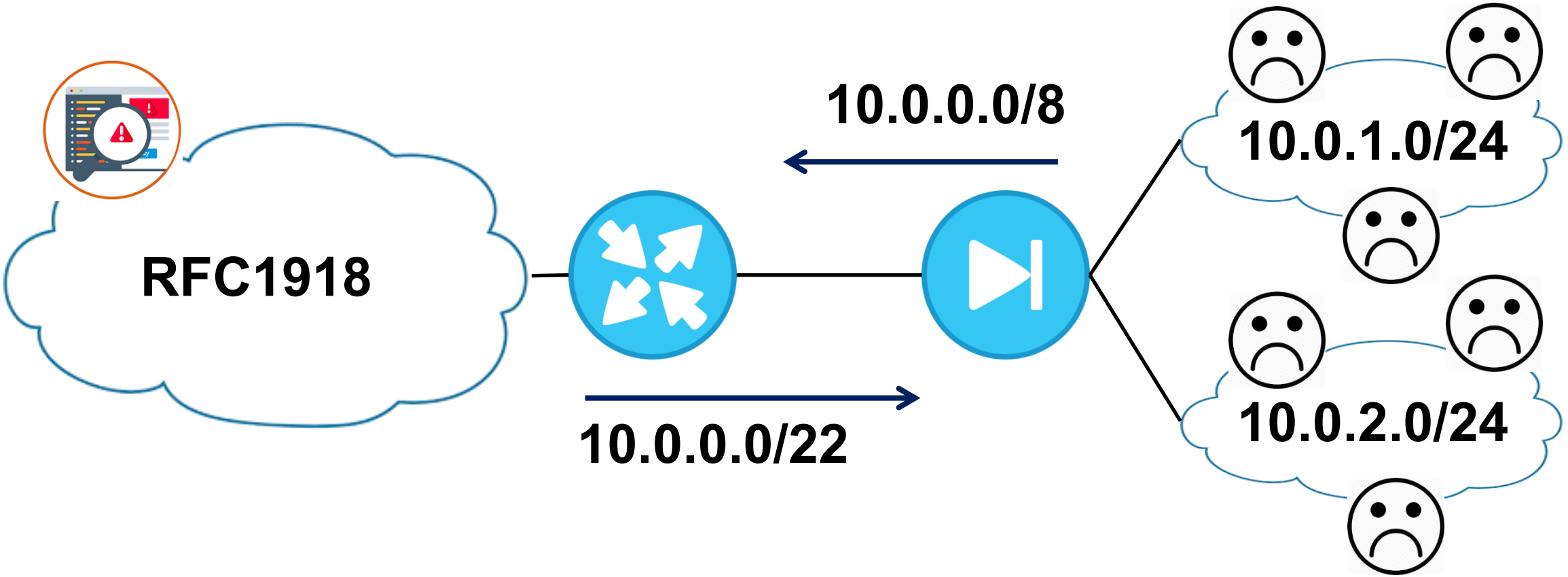
"SubjectUserName":"-", "SubjectDomainName":"-",

"SubjectLogonId":"0x0"

#2 ToDo

- DNS resolving на коннекторах SIEM – отключить
- 802.1x на площадке – включить

#3



#3 ToDo

- Проверка маршрутизации

```
# ping RFC1918nets
    TTL Expired in transit
```

- Проверка ICMP reply

```
# ping $HOST
  IF reply = TTL Expired in transit
    THEN STOP SCAN
```

- Быть лучше каждый день