Новые киберугрозы
Новая роль информационной безопасности в бизнесе в эпоху цифровой трансформации

Андрей Терехов

Системный инженер

22 Ноября, 2018

Мир сильно изменился…

Облачные вычисления

Облака, 1880-е, А.М. Васнецов

Виртуализация

«Thirty» 1937 г. В. Кандинский

Интернет вещей, IoT

«Личные ценности» 1937 г., Р. Магритт

…и продолжает меняться

Мир «Умных Вещей»

«Интернет вещей» будет генерировать 14,4 триллиона долларов в течение следующего десятилетия

Медицина

CREDIT SUISSE

Общий объем продаж одежды и аксессуаров, включающих компьютерные технологии, к 2019 году достигнет 42,5 млрд. Долл. США

Автомобильная промышленность

Совокупные расходы на IoT в 2020 году составят 2,9 триллиона долларов

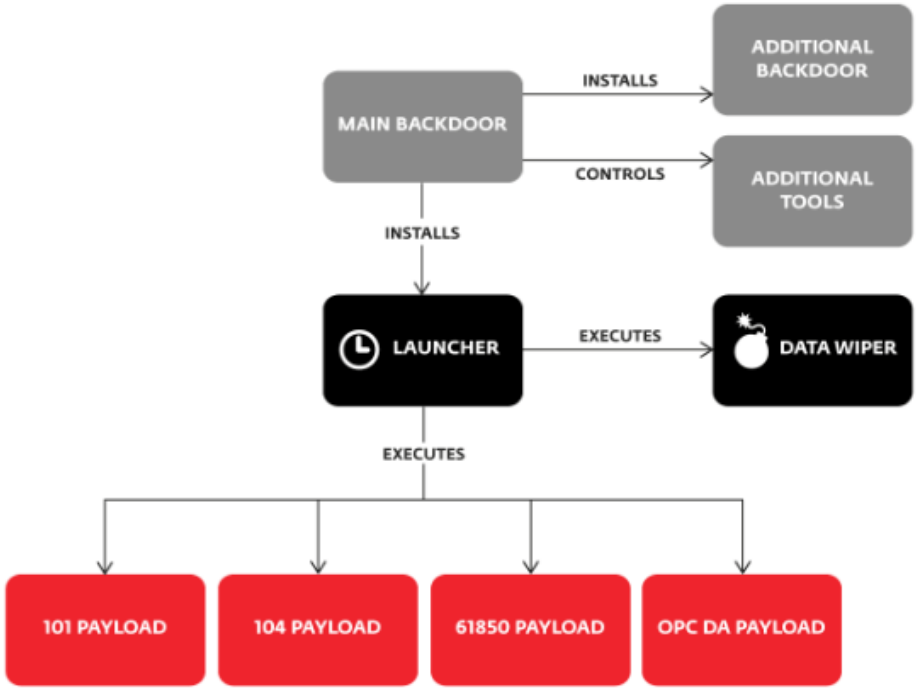
Сельское хозяйство

Gartner®

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЗНАЧИТЕЛЬНО РАСШИРЯЕТ ПОВЕРХНОСТЬ АТАКИ

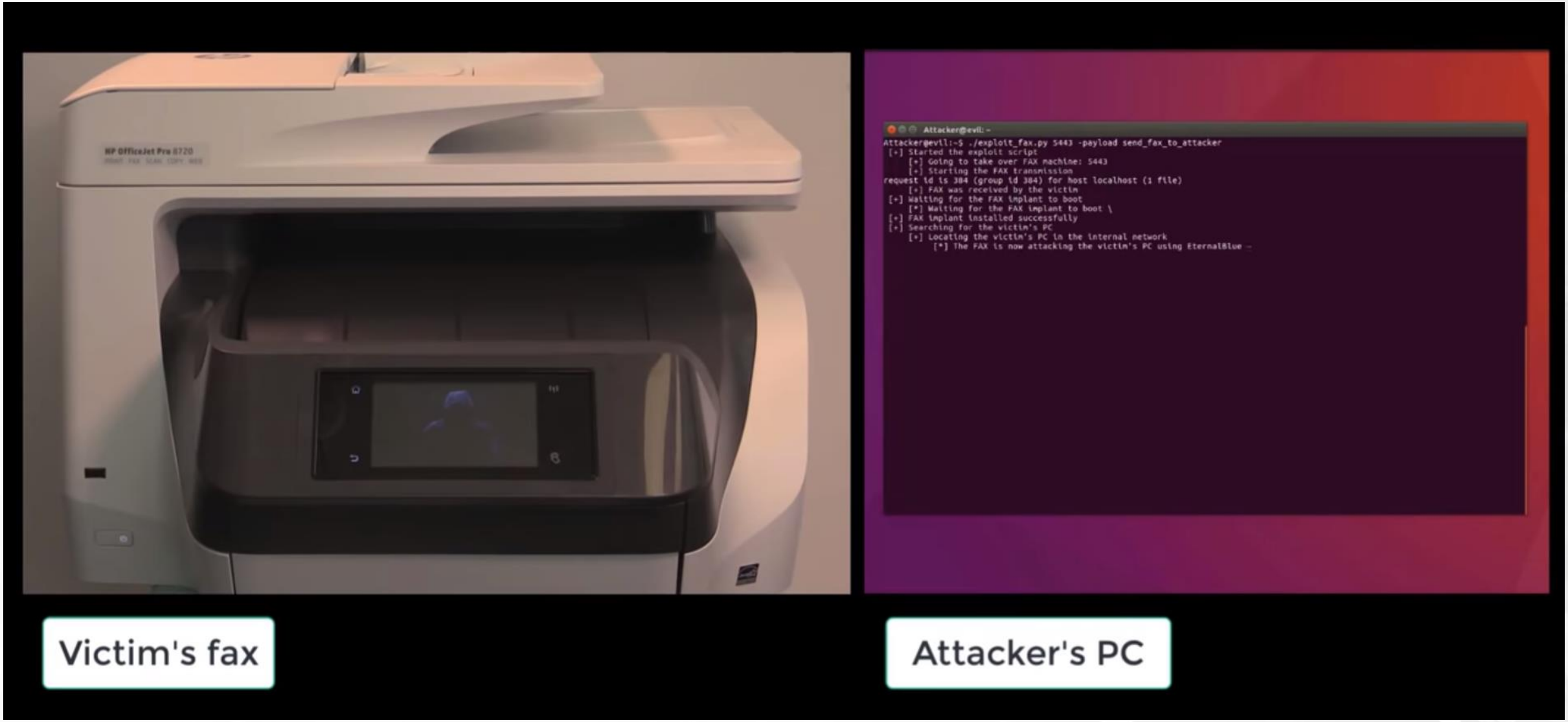
Несколько примеров

- Industroyer/CRASHOVERRIDE – вредоносное ПО, способное взаимодействовать с системами АСУТП
  - https://habr.com/company/eset/blog/330730/
  - Модули для IEC 101, IEC 104, IEC 61850, OPC DA
  - Широко распространенные промышленные протоколы, которые создавались десятилетия назад без учета вопросов безопасности
  - Главный компонент – бэкдор, используется атакующими д программы
  - Стоит упомянуть, что большинство C&C-серверов бэкдор
- Уязвимости в камерах Dahua и HikVision
  - https://www.csoonline.com/article/3269199/security/critical-hi cameras-dvrs-and-accounts.html
  - Удалённый доступ к видео, потенциальная компрометаци
  - Dahua, CVSS 10: 2017, 2013, 2013
  - HikVision, CVSS 10: 2017, 2013
  -



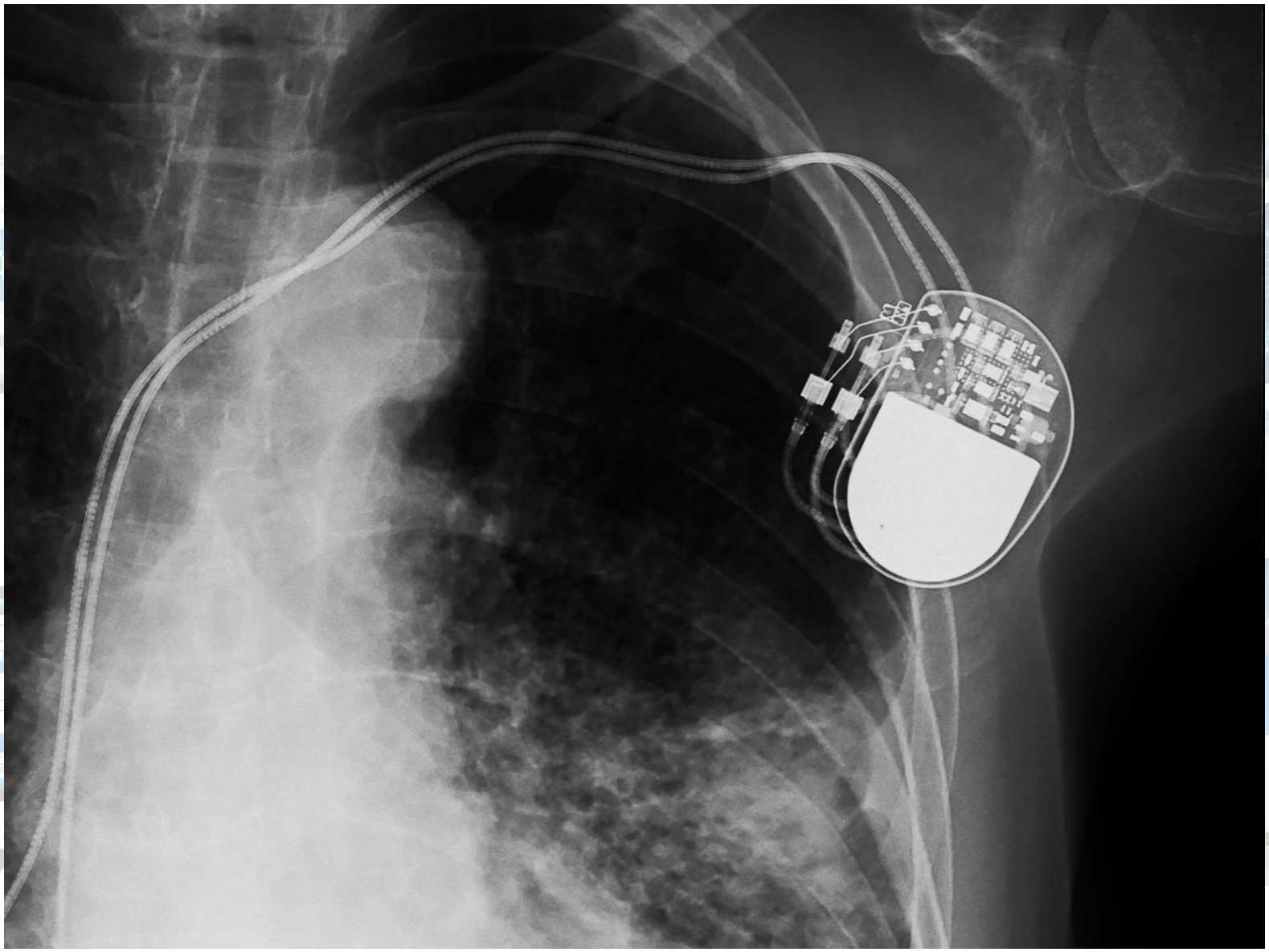
https://fortiguard.com/encyclopedia/virus/7412580
https://fortiguard.com/encyclopedia/ips/39673/hikvision-dvr-rtsp-request-remote-code-execution

IoT – «умные» устройства



IoT – промышленный уровень

Smart Metering

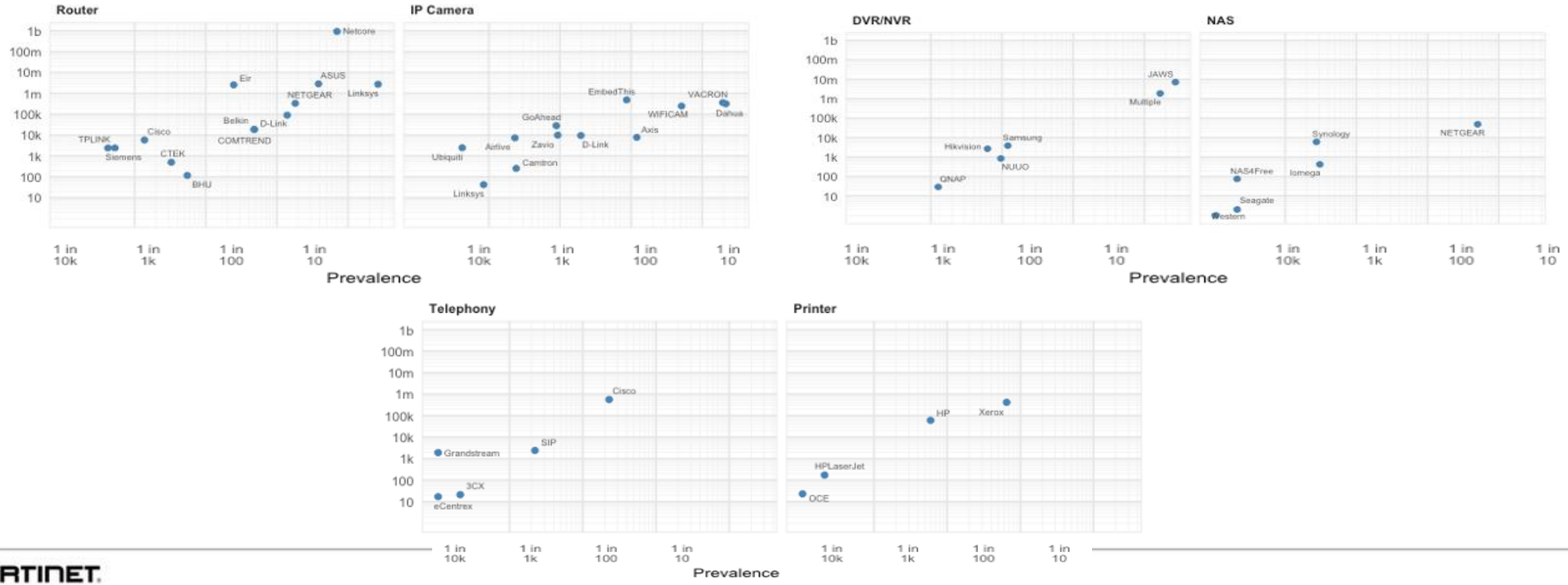


SCADA systems

Ландшафт угроз: динамика атак на IoT

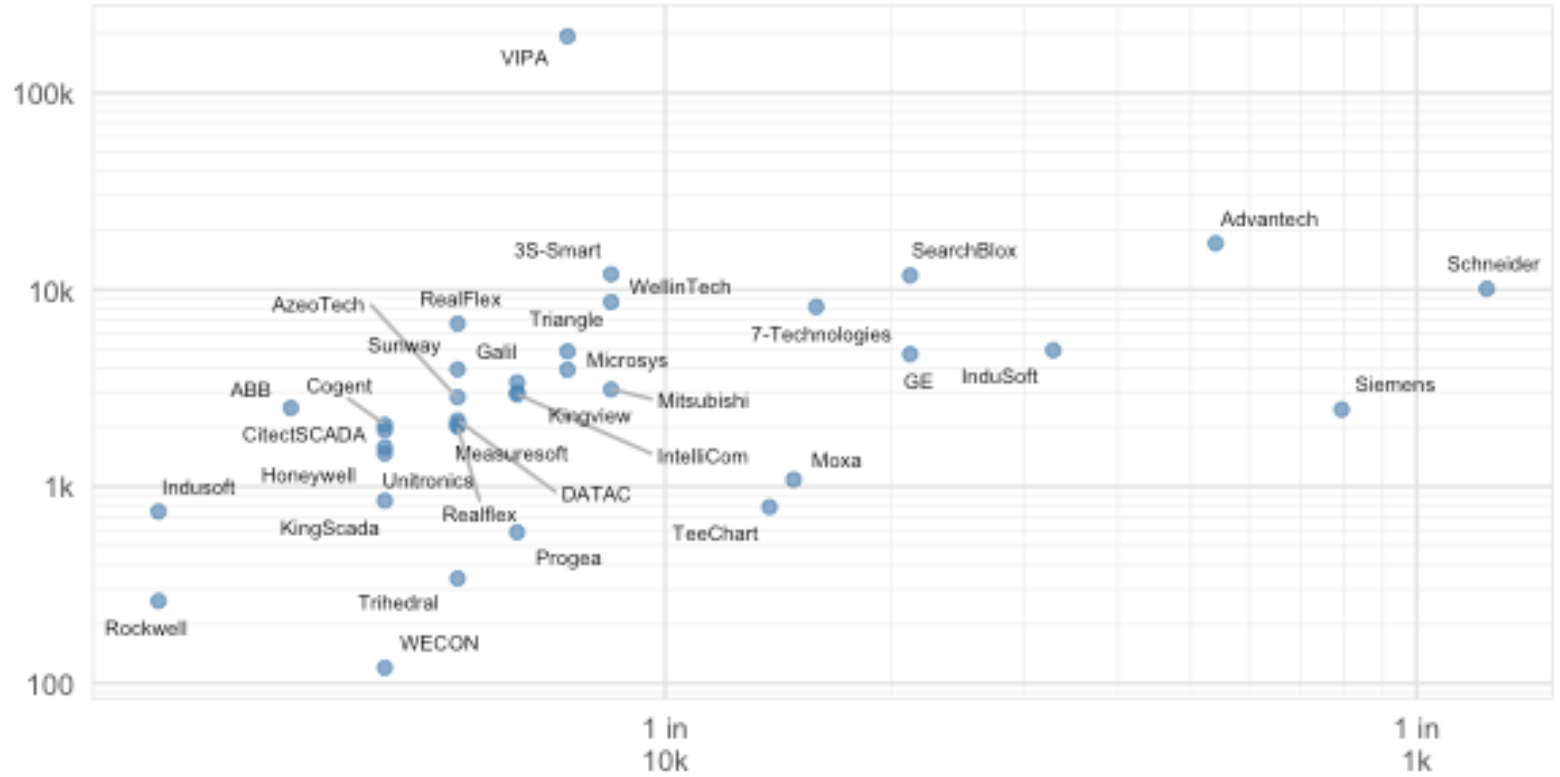
- IoT – привлекательная цель, рост ботнет-сетей IoT
- Цели – устройства 45 производителей
- Тактики: перебор паролей, эксплуатация уязвимостей, использование встроенных языков сценариев (Lua)
- Характерные примеры: VPNFilter, Mirai, NHS

Частота и объём атак на IoT по категориям



Ландшафт угроз: динамика атак на АСУ ТП

- Низкий объем атак (ожидаемо) – но ущерб от них существенно выше в сравнении с IoT
- Атаки останавливают работу систем, компрометируют критическую инфраструктуру и представляют угрозу жизни и здоровью людей
- Недавнее исследование Forrester – около 60% опрошенных промышленных компаний сталкивались с инцидентами ИБ в АСУ ТП в прошлом году



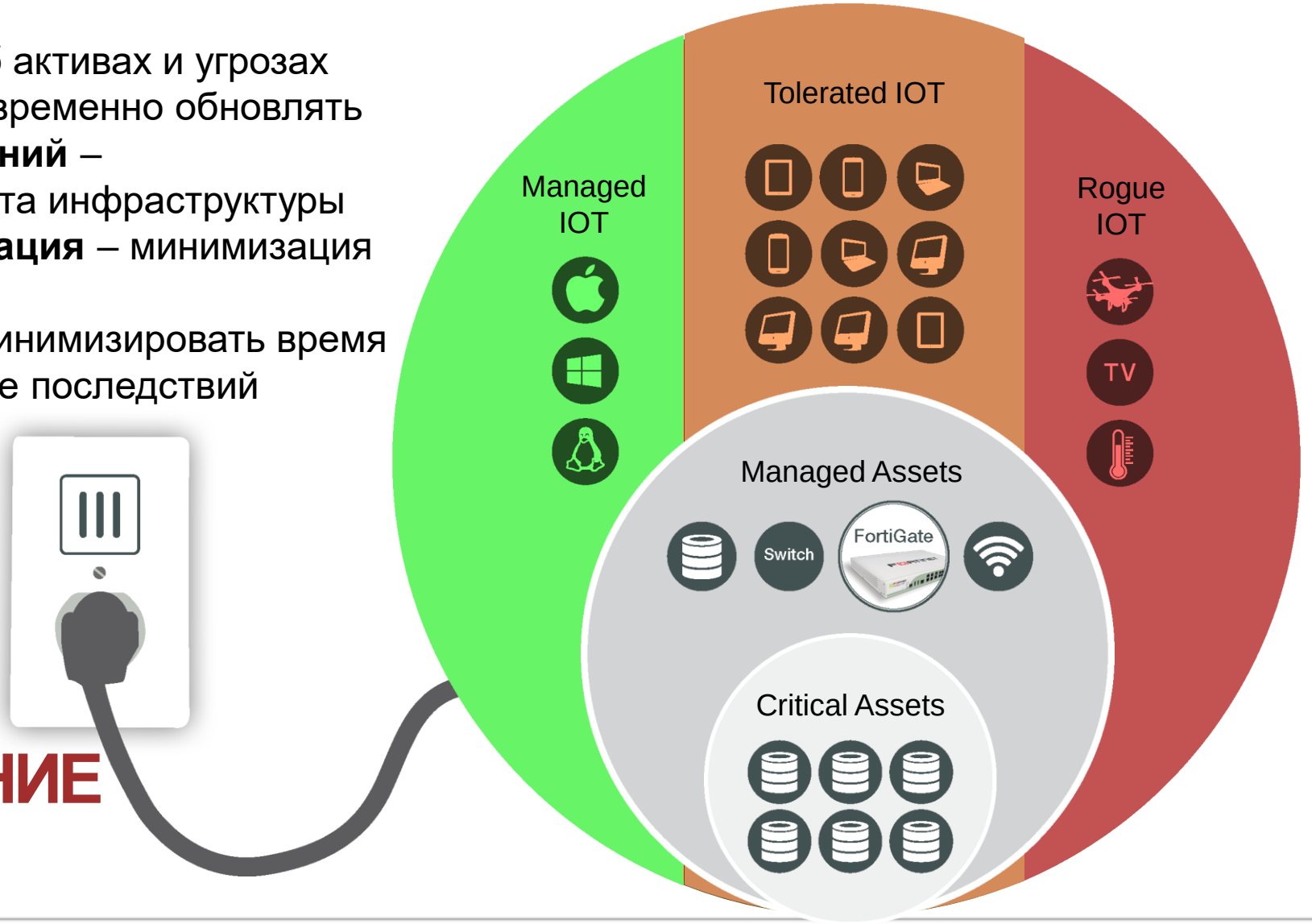
Частота и объём атак на IoT по категориям

Домен устройств – Где возникают уязвимости

БЕЗОПАСНОСТЬ ДОЛЖНА обеспечиваться на ВСЕХ доменах IoT инфраструктуры

Что делать – начать с простого

1. **Видимость** – знать всё об активах и угрозах
2. **Патч-менеджмент** – своевременно обновлять
3. **Предотвращение вторжений** – автоматизированная защита инфраструктуры
4. **Избыточность и сегментация** – минимизация ущерба от инцидентов
5. **Время реагирования** – минимизировать время на выявление и устранение последствий



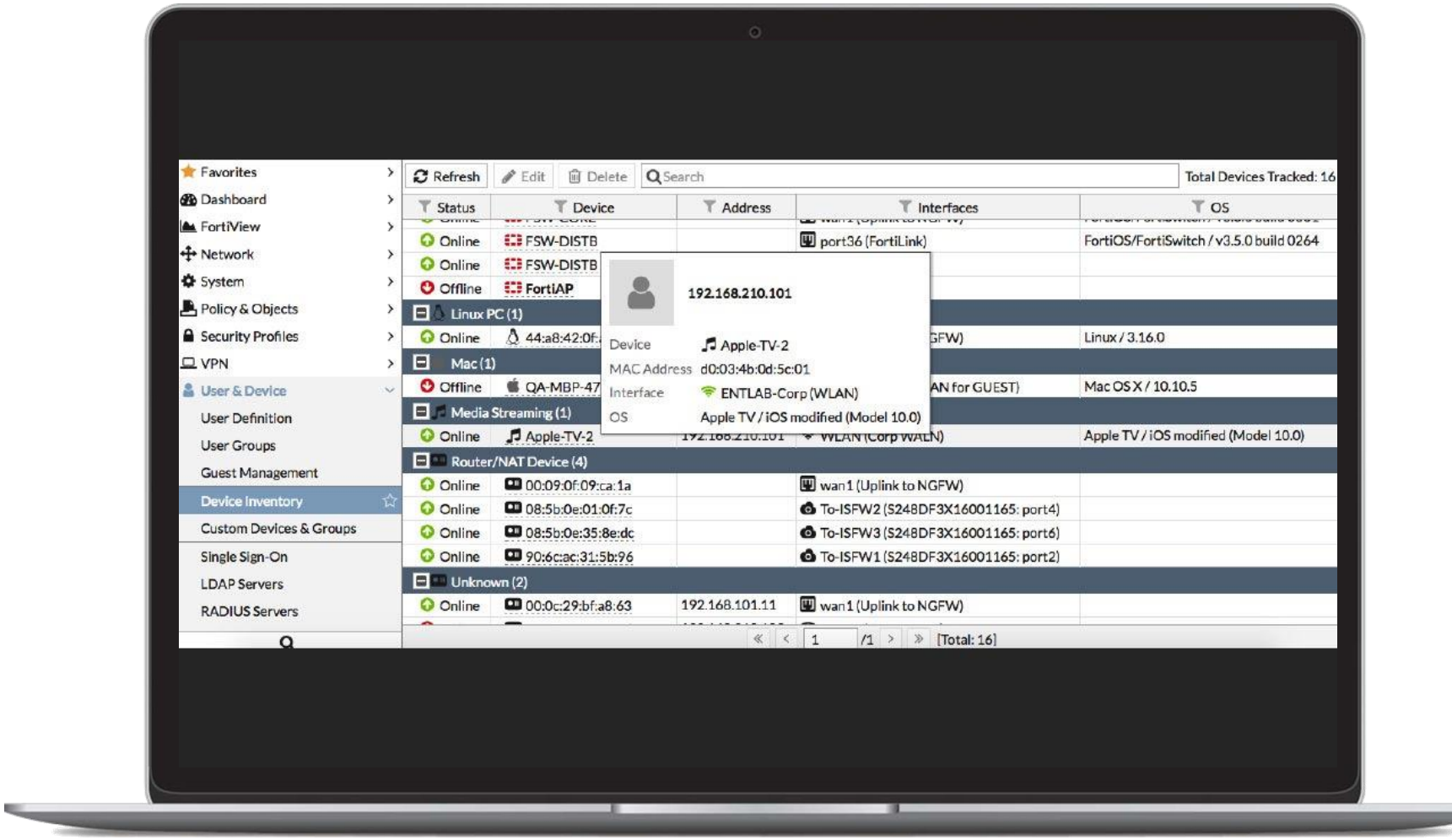
ИЗУЧЕНИЕ
СЕГМЕНТИРОВАНИЕ
ЗАЩИТА

Шаг 1 – Изучение и визуализация

Изучение и идентификация

Анализ устройств и авто-определение

- Профилирование устройств
- Тегирование устройств
- Типовая и расширенная классификация

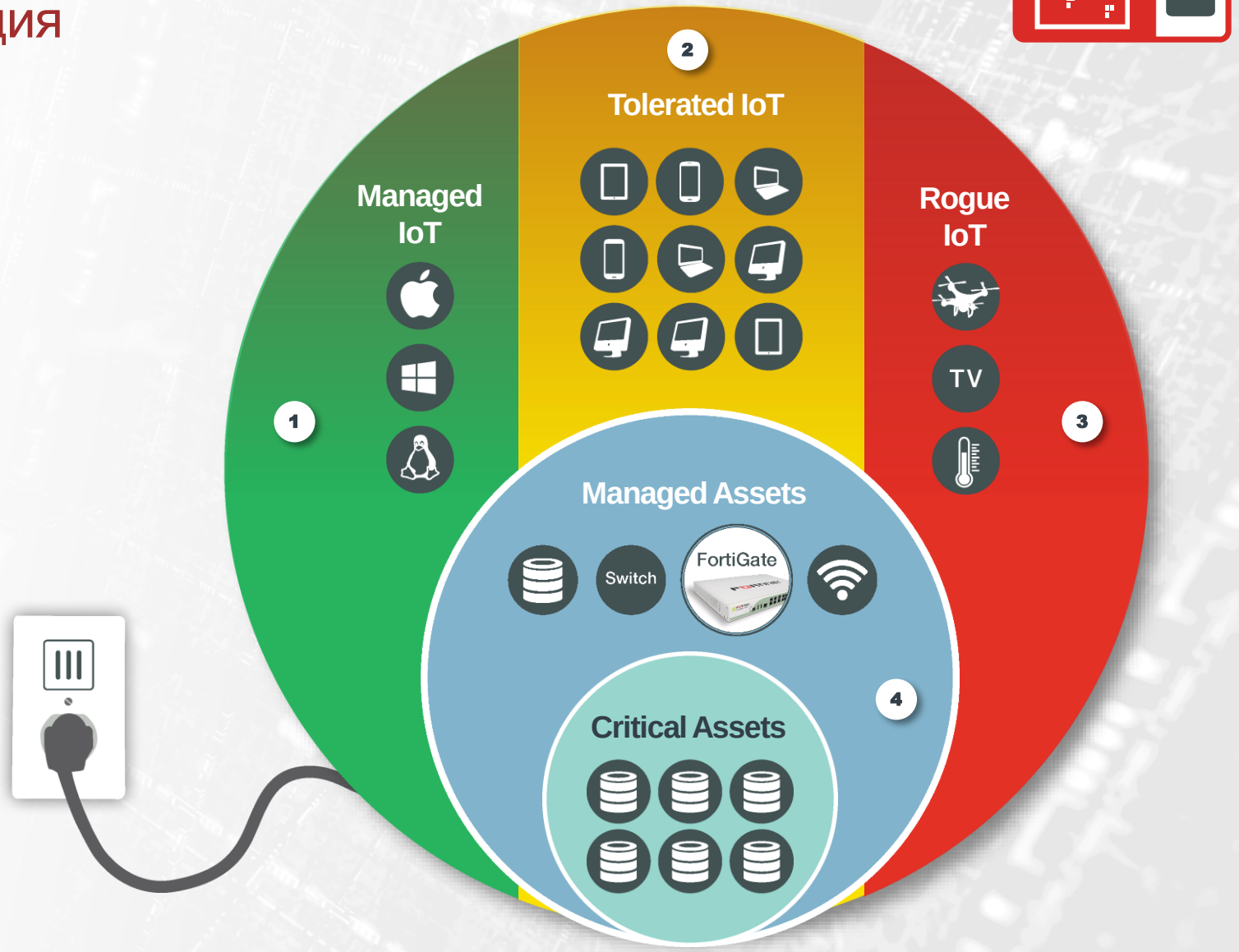


Шаг 2 - Сегментация

Security Fabric – Сегментация

Сегментирование IoT Сети

1. Централизованное управление
   - Полный доступ
2. Неуправляемые
   - Ограниченный доступ
3. Без доступа
4. 3rd Party DBs
   - Tivoli
   - AD
   - SIEM
   - VM Tools



Шаг 3 – Защита

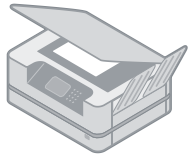
Шаблоны безопасности

Определение

- Адаптивные политики безопасности
- Предотвращение угроз
- Преднастроенные шаблоны
  - » порты, протоколы
  - » Сетевые устройства
  - » Идентификация IoT устройств

Как это работает – несколько примеров

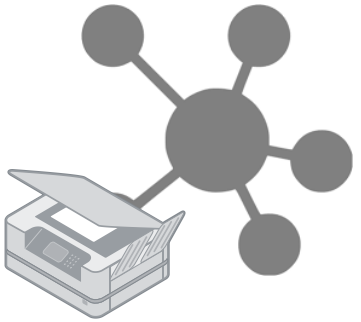
Динамическое профилирование устройств



1. Администратор подключает Принтер

2. Профилирование

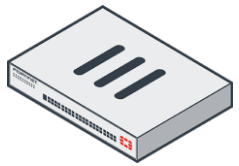
3. Результат - «принтер»



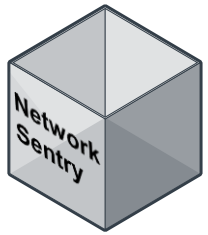
4. Предоставление доступа
Сегментация
Защита

Сдерживание угроз на границе сети

1. Пользователь подключает инфицированный ноутбук



2. Выявление заражения



3. Результат - карантин

4. Блокировка угрозы на уровне доступа


FORTINET