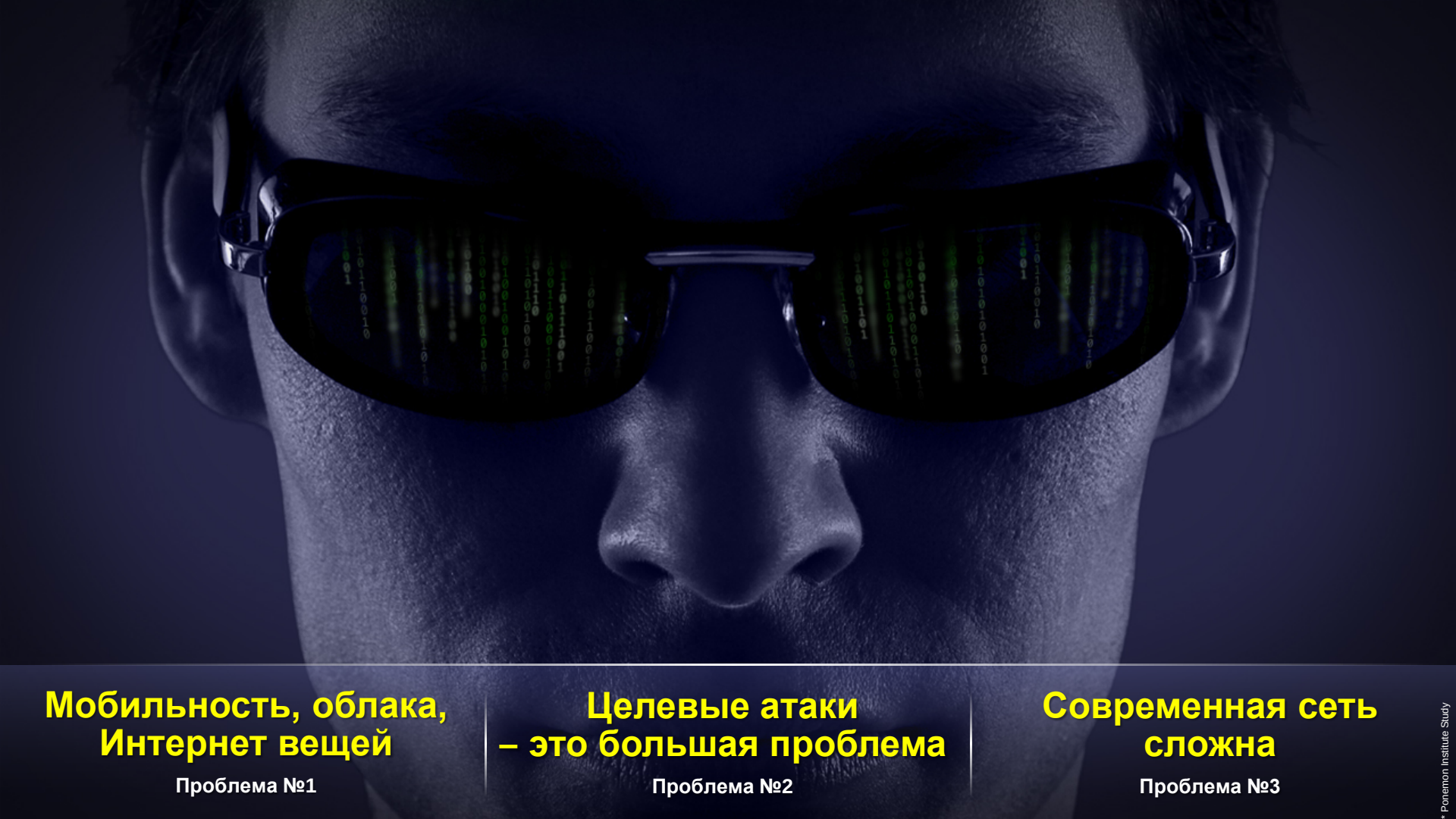
Как построить интегрированную систему борьбы с угрозами, охватывающую все предприятие, а не только периметр?

Назим Латыпаев
Системный инженер, Cisco



Мобильность, облака, Интернет вещей

Проблема №1

Целевые атаки – это большая проблема

Проблема №2

Современная сеть сложна

Проблема №3

* Ponemon Institute Study

С чем мы сталкиваемся?

Изменение бизнес-моделей

Динамичность угроз

Сложность и фрагментация

Как хакеры используют свои знания?!

ИНН / SSN:
от $1

Карта пациента:
>$50

Данные кредитной карты:
$0.25-$60

Банковская учетка
>$1000
зависит от типа учетки и баланса

DDOS
as a Service:
от $7/час

Глобальный рынок киберпреступности: $450млрд-$1трлн

Мобильное вредоносное ПО: $150

Спам:
$50 за 500K email

Разработка вредоноса:
$2500
(коммерческое ВПО)

Эксплойты
$1000-$300K

Учетка Facebook:
$1 за учетку с 15 друзьями

ДОБРО ПОЖАЛОВАТЬ В ЭКОНОМИКУ ХАКЕРОВ!

Проблемы с традиционной моделью «эшелонированной» безопасности на периметре

Точечные продукты

Высокая сложность, меньшая эффективность

Слабая прозрачность

Многовекторные и продвинутые угрозы остаются незамеченными

Ручные и статические механизмы

Медленный отклик, ручное управление, низкая результативность

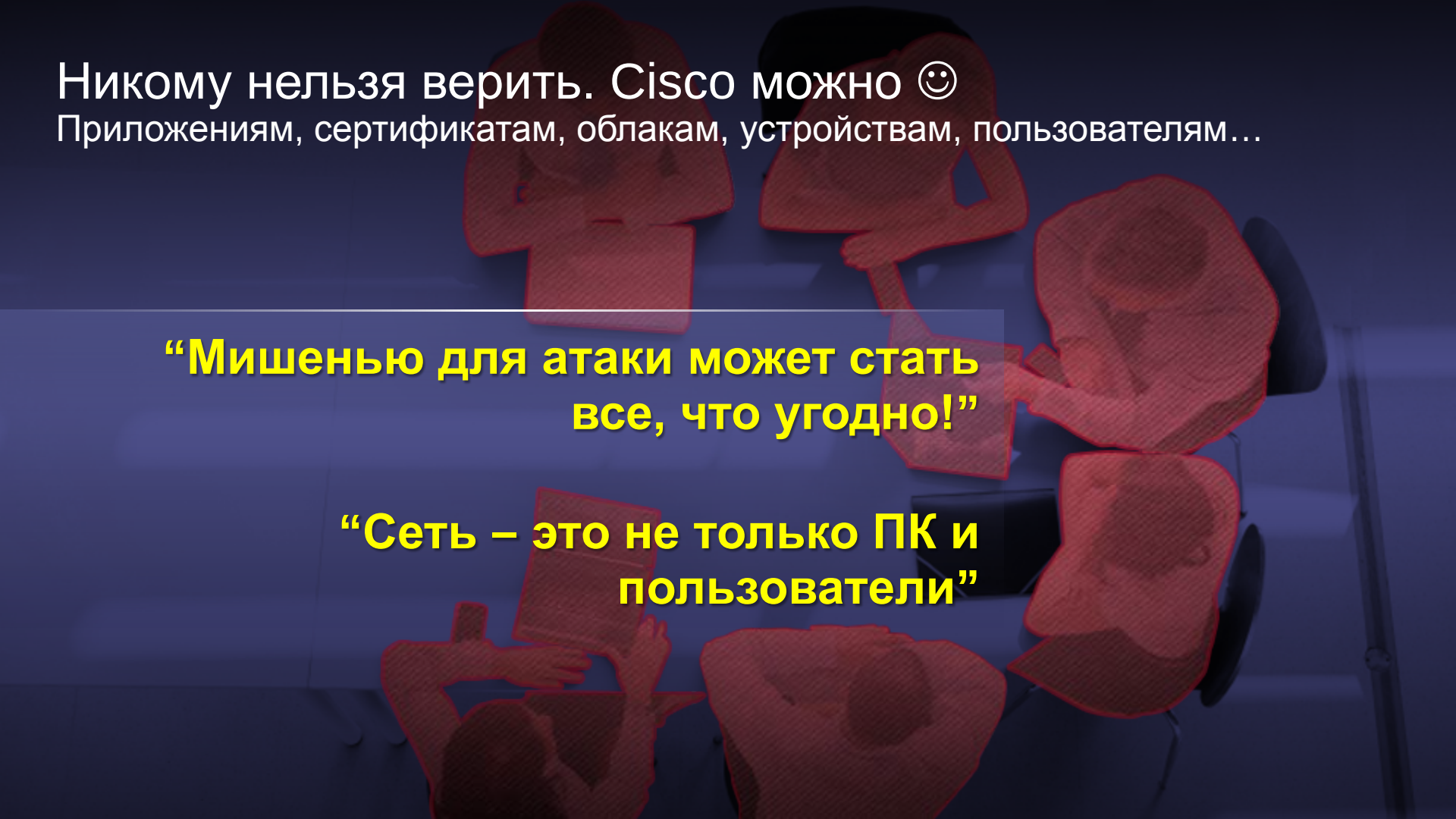
Наличие обходных каналов

Мобильные устройства, Wi-Fi, флешки, ActiveSync, CD/DVD и т.п.

← Как ваш NGFW защитит от этого?

Никому нельзя верить. Cisco можно ☺

Приложениям, сертификатам, облакам, устройствам, пользователям…



“Мишенью для атаки может стать все, что угодно!”

“Сеть – это не только ПК и пользователи”

100%-й безопасности нет – станьте как пионер, готовыми ко всему, включая заражение

Видимость и защита в течение всего жизненного цикла

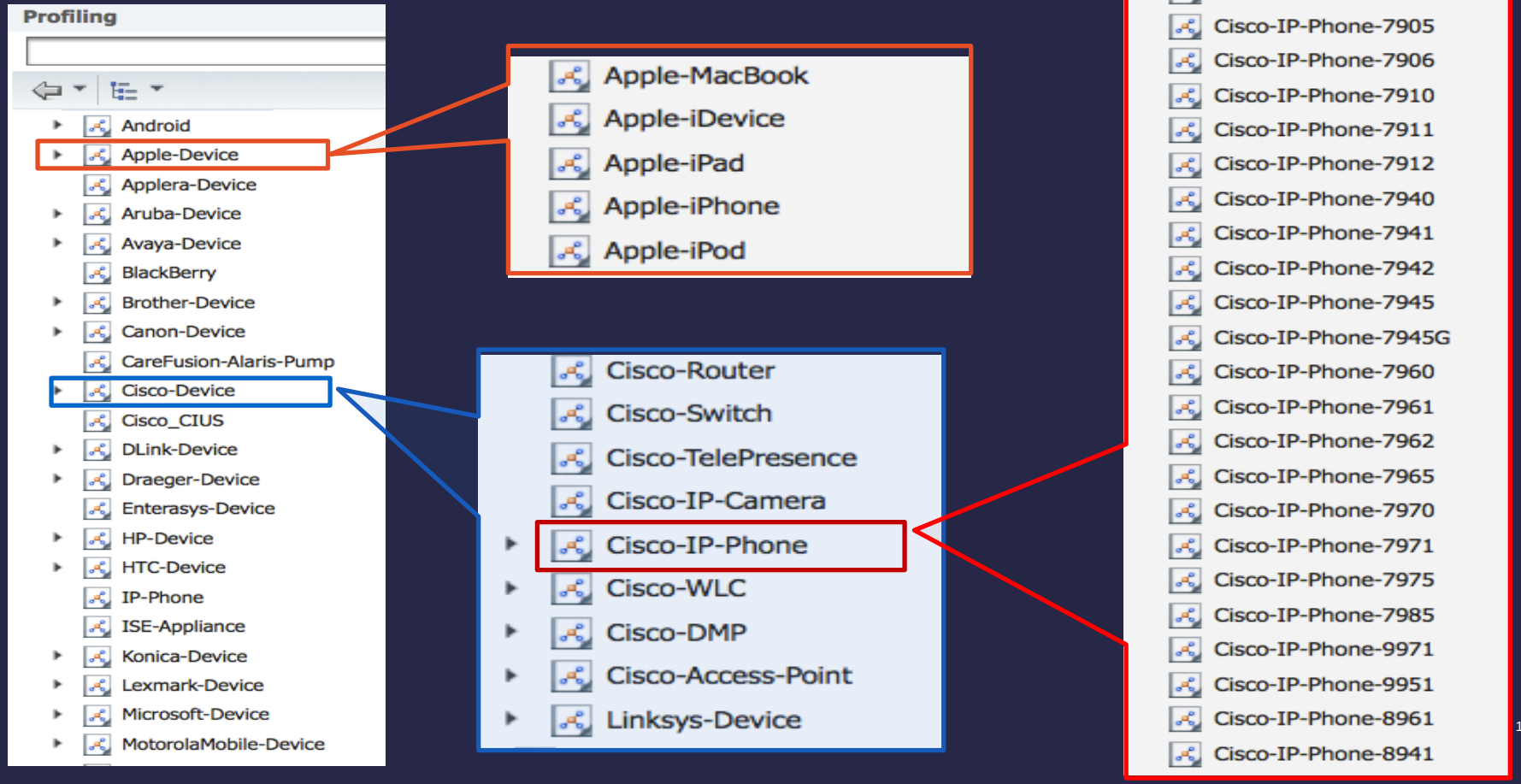
Вы не можете защитить то, чего не видите

На периметре вы видите только верхушку айсберга

Что сеть может сделать для вас?

Сеть как сенсор

Распознавание широкого спектра устройств



Опыт Cisco: идентификация и блокирование посторонних беспроводных устройств

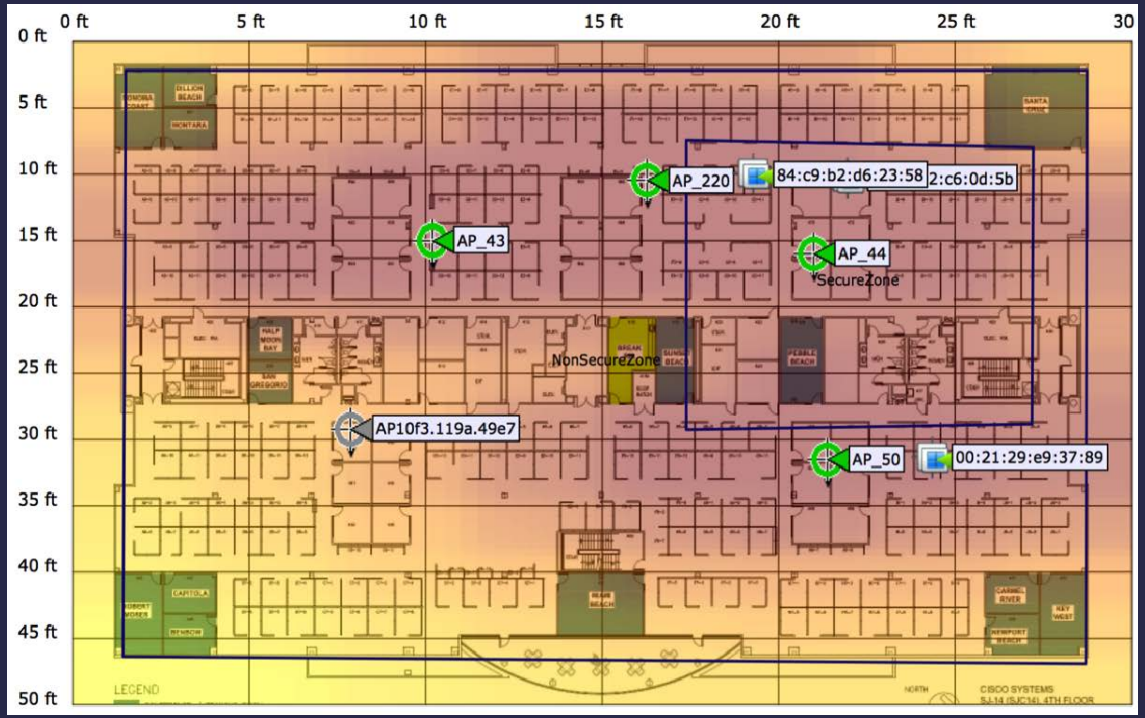
- Само мобильное устройство не может сказать, что оно «чужое»
  - Нужен внешний независимый контроль с помощью систем контроля доступа, в т.ч. и беспроводного
- Cisco Wireless Controller / Cisco Wireless Adaptive IPS / Cisco Wireless Location Services помогают контролировать беспроводной эфир
  - Все это часть функционала платформы Cisco Mobility Services Engine

Опыт Cisco: Интеграция информации о местоположении

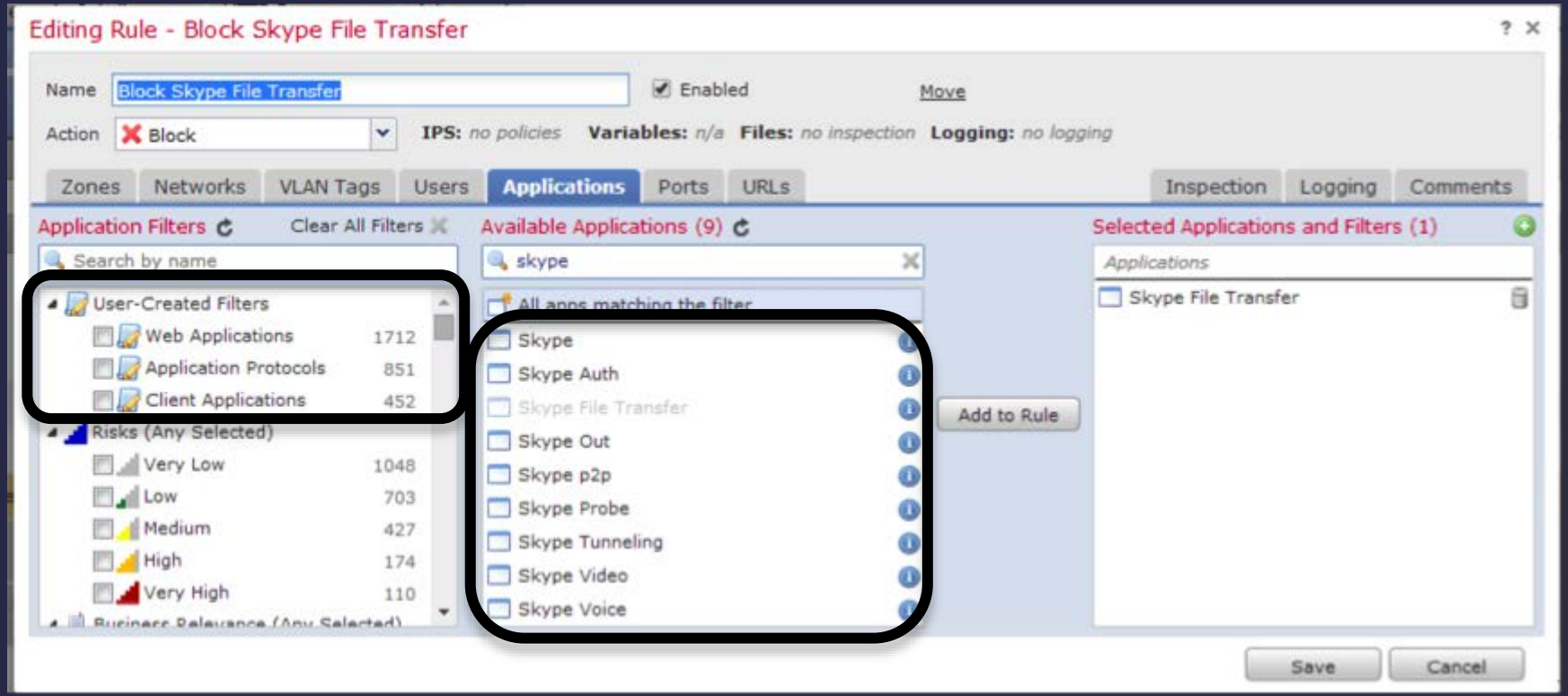
ISE получает **интеграцию с MSE 8.0/ CMX**

Это обеспечивает :

- Возможность использовать атрибуты местоположения в политике
- Определять **зоны безопасности**
- Периодически проверять местоположение в случае изменений
- Проводить повторную авторизацию в случае изменения локации

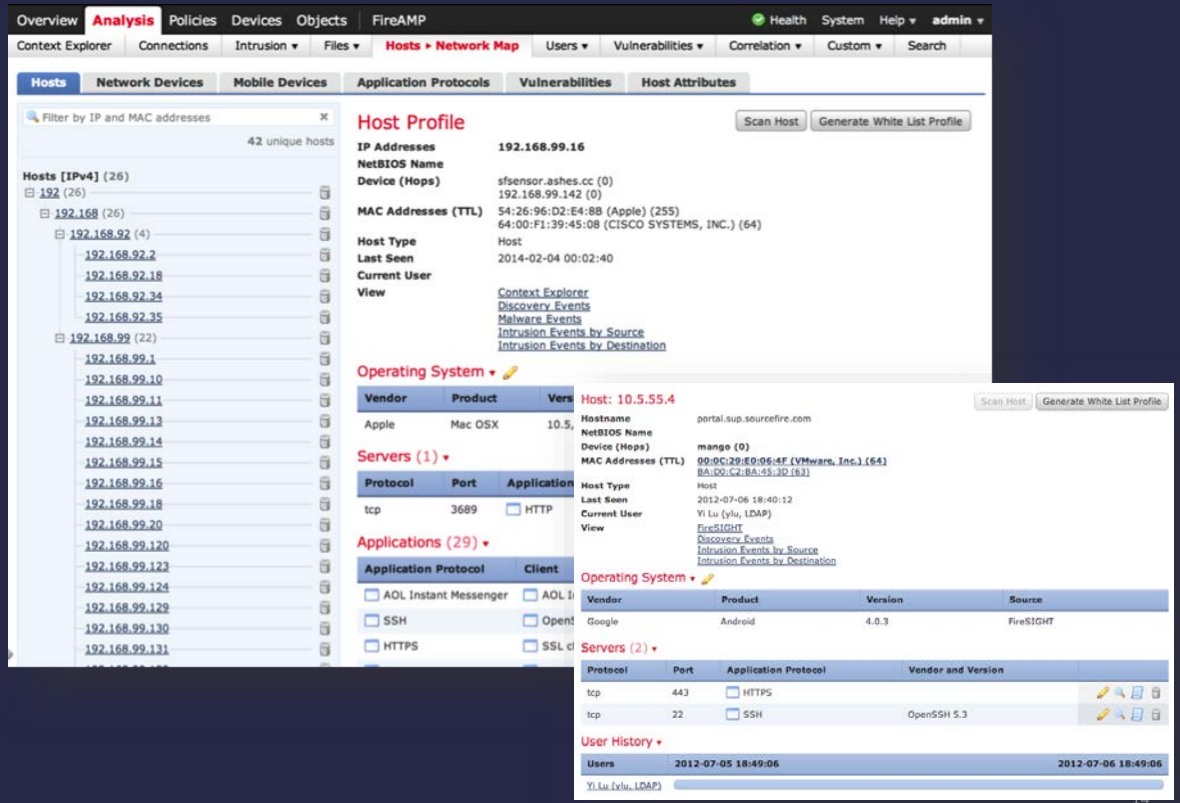


Распознавание приложений и их функций на примере Skype



Учет контекста: кто, что, где, когда и как

- Профиль хоста включает всю необходимую для анализа информацию
  - IP-, NetBIOS-, MAC-адреса
  - Операционная система
  - Используемые приложения
  - Зарегистрированные пользователи
  - Сетевой протокол
  - Транспортный протокол
  - Прикладной протокол
  - И т.д.
- Идентификация и профилирование мобильных устройств



NetFlow – сердце подхода «Сеть как сенсор»

Путь к самообучаемым сетям

Мощный источник информации

для каждого сетевого соединения

Каждое сетевое соединения
в течение длительного интервала времени

IP-адрес источника и назначения, IP-порты, время, дата передачи и другое

Сохранено для будущего анализа

Важный инструмент

для идентификации взломов

Идентификация аномальной активности

Реконструкция последовательности событий

Соответствие требованиям и сбор доказательств

NetFlow для полных деталей, NetFlow-Lite для 1/n семплов

Сетевые потоки как шаблоны вторжений

NetFlow – сердце подхода «Сеть как сенсор»

Пример: NetFlow Alerts с Lancope StealthWatch

Сканирование сети

Сканирование TCP, UDP, портов по множеству узлов

Обнаружение ботнетов

Когда внутренний узел общается с внешним сервером C&C в течение длительного периода времени

Отказ в обслуживании

SYN Half Open; ICMP/UDP/Port Flood

Фрагментированные атаки

Узел отправляет необычный фрагментированный трафик

Изменение репутации узла

Потенциально скомпрометированные внутренние узлы или получение ненормального скана или иные аномалии

Распространение червей

Инфицированный узел сканирует сеть и соединяется с узлами по сети; другие узлы начинают повторять эти действия

Утечки данных

Большой объем исходящего трафика VS. дневной квоты

У нас есть эмуляция атак и песочница, но не только

Репутационный анализ AMP

Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Поведенческий анализ AMP

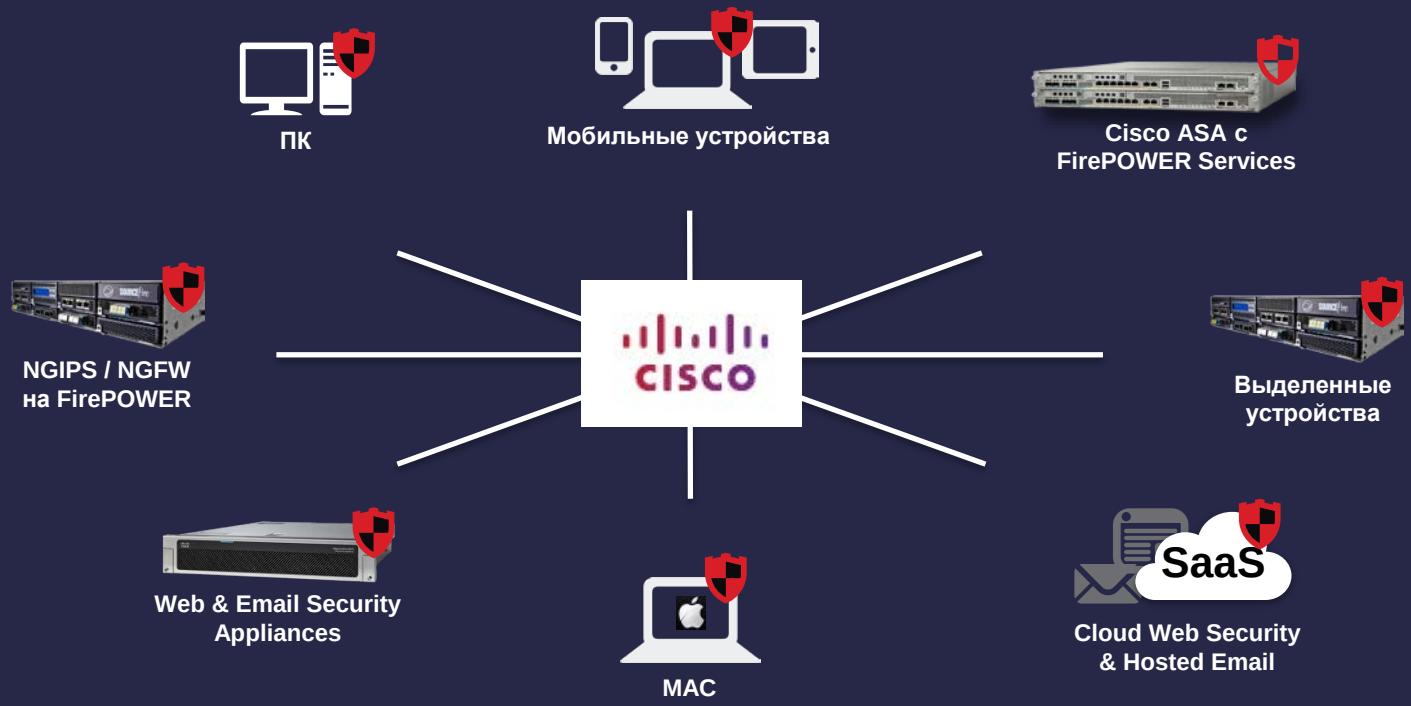
Признаки компрометации

Динамический анализ

Расширенная аналитика

Сопоставление потоков устройств

Платформа обнаружения вредоносного кода AMP
На маршрутизаторе, МСЭ, IPS, WSA/ESA, ПК, в облаке



Искусство сетевой безопасности
Важный совет

Разделяй и защищай

Сегментируйте сеть для локализации атак
TrustSec, ISE, VLAN/VRF/EVN, ACL

Сегментируйте сеть и контролируйте доступ для локализации атак

Сеть как защитная стена

ACI Vision: Policy Based, Automated Security at Scale

Сегментация сети

для локализации атак

Ролевой контроль доступа на базе топологии, способа доступа (TrustSec/SGT, ISE)

Сегментация сети (VLAN, TrustSec/SGT, VRF/EVN)

Контроль доступа

для выполнения политик

Контроль доступа пользователей на базе устройства, местоположения, типа сети, времени и других параметров (ISE)

Физические и виртуальные разрешения и запреты (Access Control Lists)

Единая политика для проводного/беспроводного/удаленного доступа (ISE, Unified Access Switches)

Cisco TrustSec

Сегментация на базе ролей и политик

Политика

- Кто может общаться и с кем
- Кто может получить доступ к активам
- Как система может общаться с другими системами

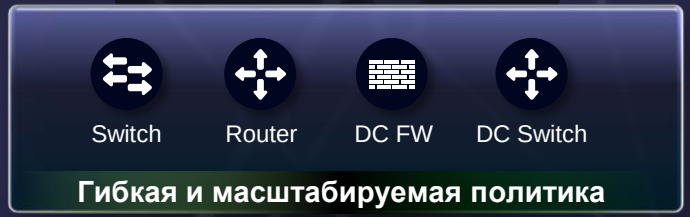
Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Простота управления доступом

Ускорение защитных операций

Единая политика везде



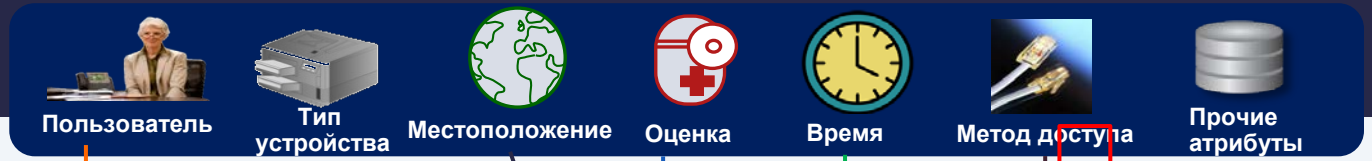
Реализация требований законодательства

Область действия аудита

Без сегментации

Упрощение выполнение требований и ускорение аудита при наличии сегментации

Опыт Cisco: контроль доступа внутри такой же, что и на периметре!



Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
Enabled	Game_Console	Game_Console-Registered		Game_Console
Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San_Jose AND CERTIFICATE:Subject Alternative Name MATCHES .*(demo.local)$ AND Radius:User-Name MATCHES ^(host/)	AD_Login
Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND LDAP1:badPwdCount MATCHES [0-5]	Employee_Wireless
Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry	Contrator_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
Disabled	Default-Posture	Any		CWA_Posture_Remediation
Enabled	Default	Any		Central_Web_Auth

Сеть как инструмент реагирования

Что сеть может сделать для вас?

Сеть как инструмент реагирования

Уменьшить время восстановления и ускорить реагирование

Например, анализ траектории вредоносного кода, интеграция с AD на уровне сети

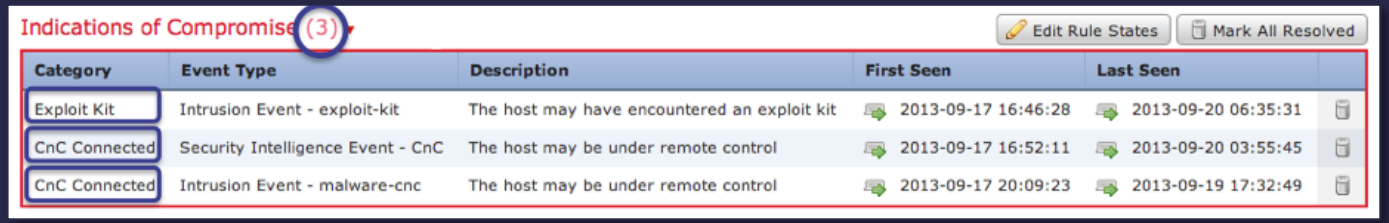
Автоматизировать настройку и динамически ее менять исходя из ситуации в сети

Например, ACL, QoS, динамические политики, корреляция событий

Интегрироваться с другими решениями для защиты инвестиций и роста качества защиты

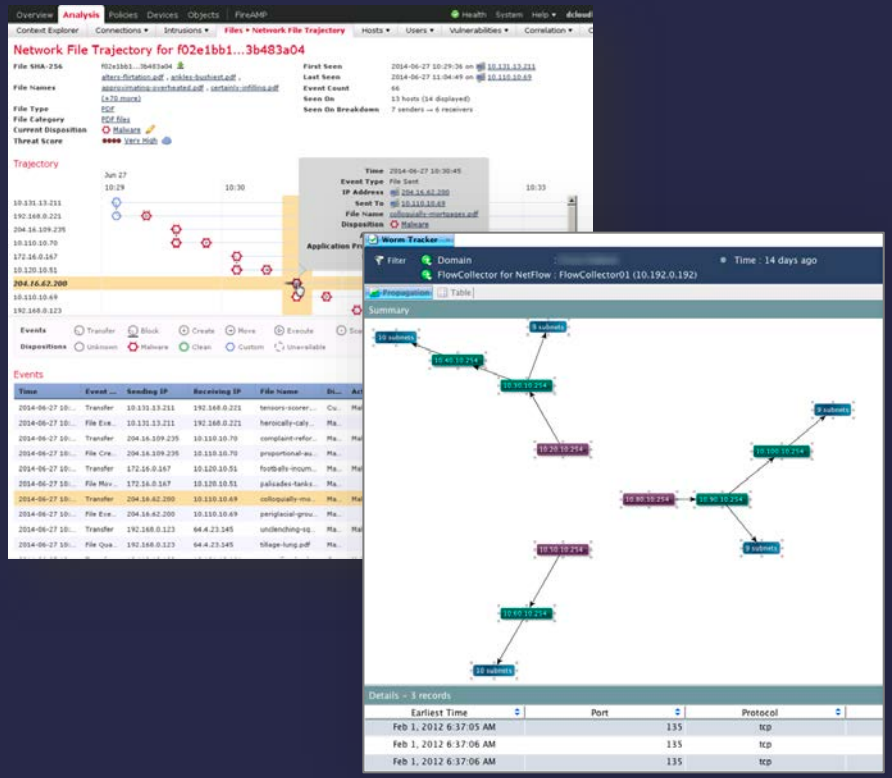
Например, RESTful API, eStreamer API и т.п.

Встроенная система корреляции событий FireSIGHT позволяет собирать данные по всей сети



Возможность отслеживать движение вредоносного ПО и злоумышленника по сети

- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс был отправной точкой?
- Почему это произошло?
- Что еще произошло?



Создание экосистемы по безопасности Cisco

Комплексное партнерское решение
Мобильность (MDM), Угрозы (SIEM), облако

Разработка экосистемы SSP
Архитектура открытой платформы

Встроенная безопасность в ИТ
ISE как “context directory service”

Использование значения Сети
Lancope, «Сеть как сенсор»

Текущая экосистема партнеров Cisco

CITRIX, MobileIron, SAP, Lancope, TIBCO, MaaS360 by Fiberlink, splunk>, Good, LogRhythm, QUALYS, Symantec, airwatch, RAPID7, IBM, hp, ArcSight, IBM Labs, NETSCOUT

Роль сетевой безопасности

Сеть как сенсор

Обнаружение аномального трафика
Обнаружение нарушений пользователями политик
Обнаружение чужих устройств, точек доступа & других

Сеть как защитная стена

Сегментация сети для локализации атак
Шифрование данных для защиты от человека посередине
Защита филиалов для Direct Internet Access

Сеть как инструмент реагирования

Автоматизированное, близкое к реальному времени отражение атак

Спасибо