Encrypted Traffic Analytics

Выявление угроз в зашифрованном трафике

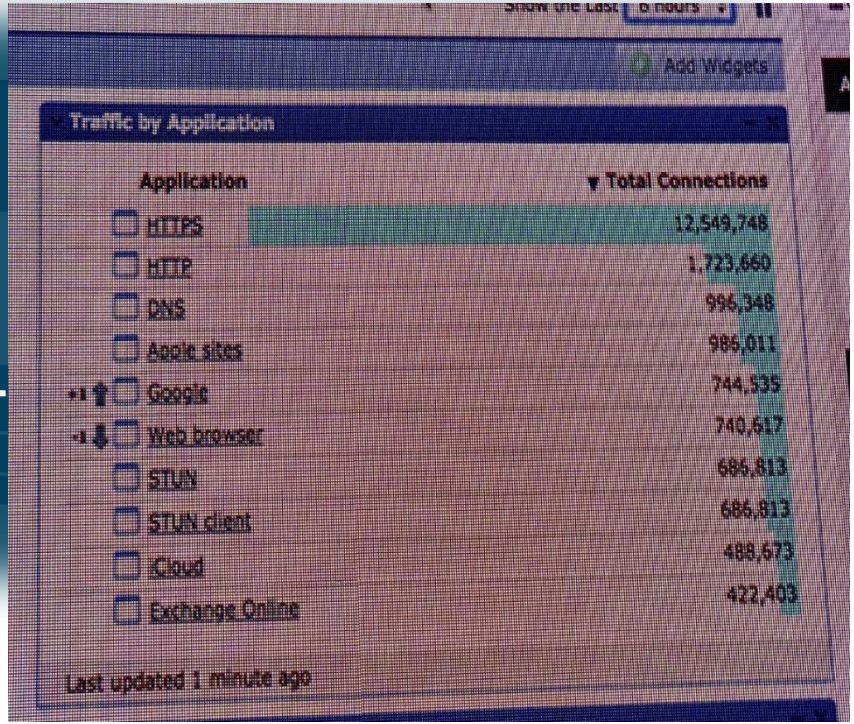
Владимир Илибман
Менеджер направления кибербезопасности

Павел Родионов
Инженер-консультант направления кибербезопасности

3 июля 2018

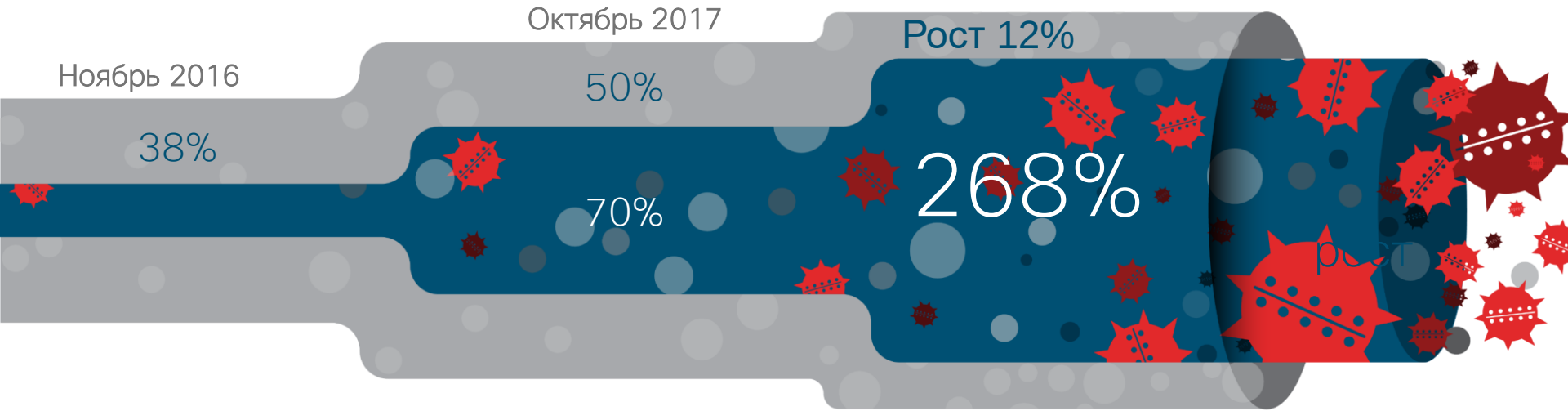
Сети становятся все более непрозрачными!

Google Chrome отметит все HTTP-сайты как ненадежные в июле 2018 года



Вредоносный код и шифрование

Атакующие используют шифрование, чтобы скрывать активность каналов C&C



Совокупный шифрованный веб-трафик

Вредоносные двоичные файлы с шифрованием

Новая реальность

81%

Организаций теряли деньги в результате атак

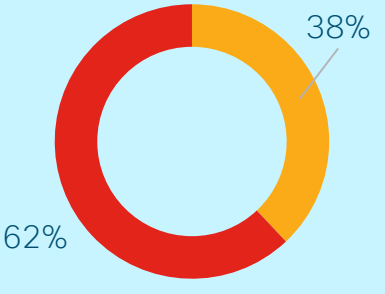
41%

Атакующих использует шифрование чтобы избежать обнаружения

64%

Не могут обнаружить вредоносное содержимое в зашифрованном трафике

Бизнес под угрозой

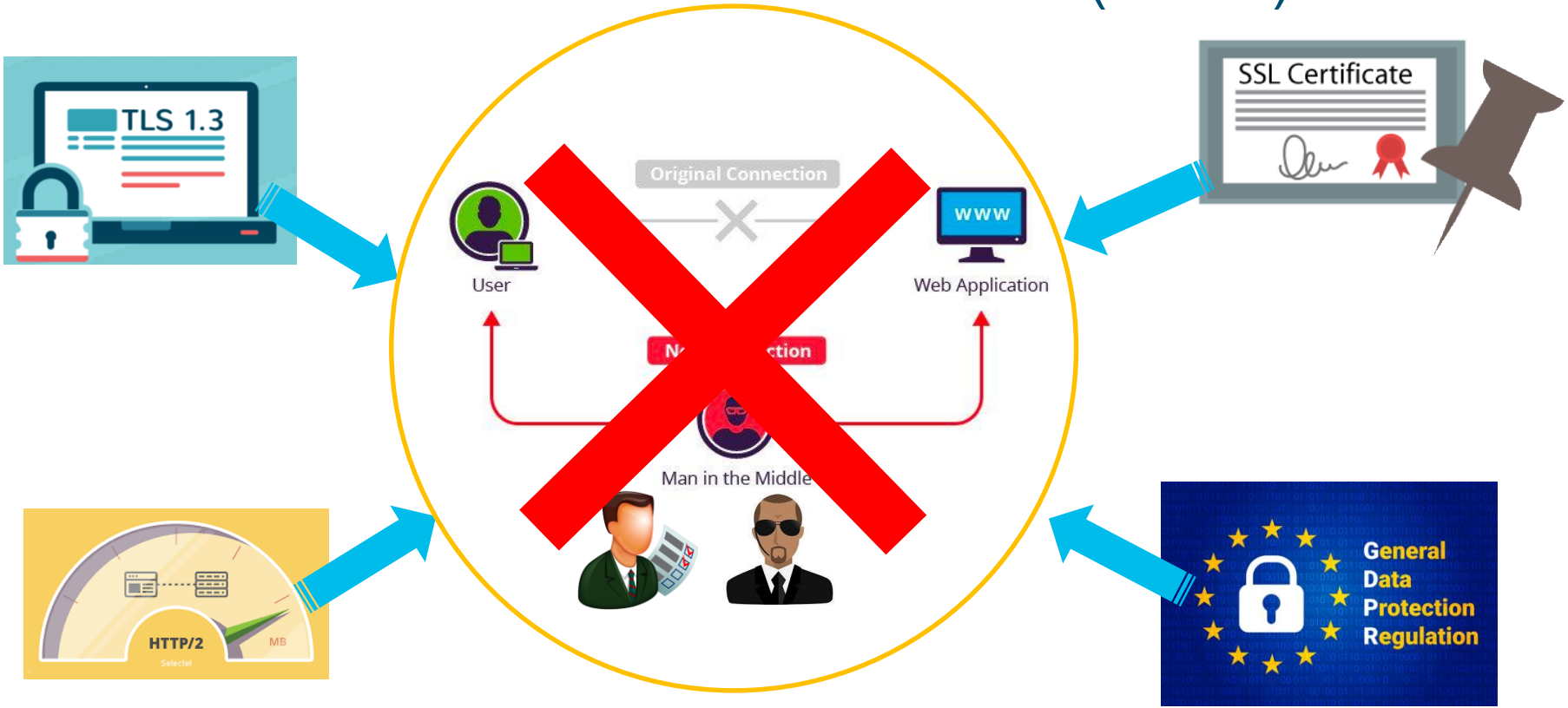


Новые векторы атаки

- Сотрудники активно используют HTTPS в Интернет: заражение вредоносами, скрытые каналы управления к командным серверам, кража данных
- Сотрудники из внутренней сети подключаются к DMZ-серверам: незаметное распространение по зашифрованным каналам

Источник: Ponemon Report, 2016

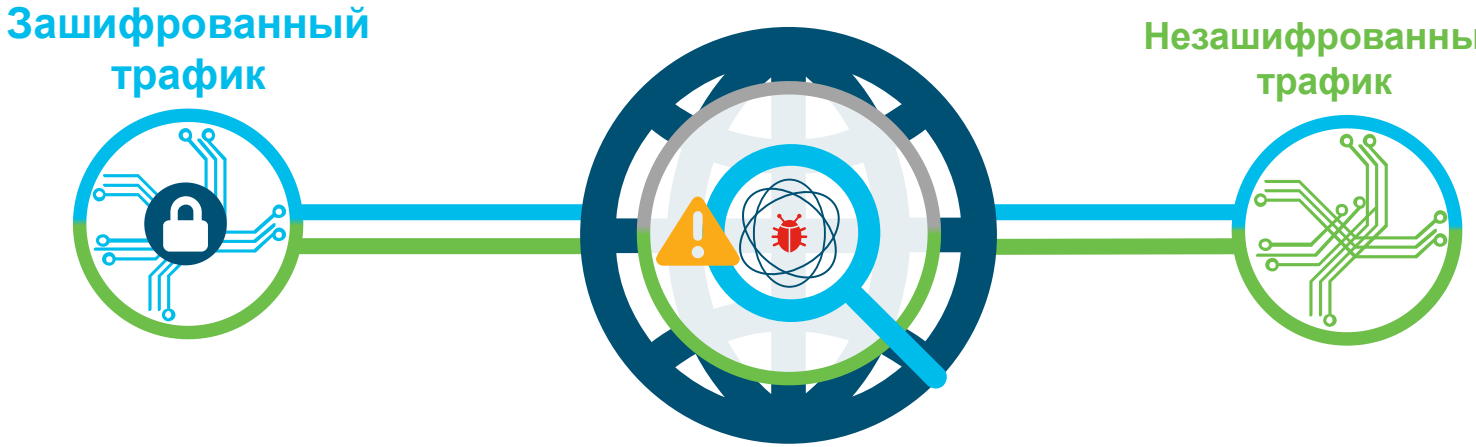
Традиционный подход предполагает использование Man-in-the-Middle (MITM)



Обнаружение угроз, использующих шифрование с помощью сетевой телеметрии

Новая технология: Cisco Encrypted Traffic Analytics

Первая в индустрии сеть с возможностью обнаруживать угрозы в зашифрованном трафике **без расшифровки**



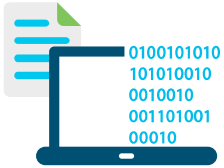
Защита сети в реальном времени, непрерывно, всюду

Encrypted Traffic Analytics (ETA)

Вредоносное ПО в зашифрованных соединениях

Является ли то, что передаётся внутри TLS вредоносным?

- Конфиденциальность сохраняется
- Обеспечивается целостность информации
- Адаптируется к новым стандартам шифрования



Соответствие требованиям с точки зрения регуляторики

Какие приложения используют сильное шифрование и как?

- Аудит нарушения политик использования TLS
- Пассивное обнаружение криптонаборов с известными уязвимостями
- Мониторинг использования шифрования в сети

Encrypted Traffic Analytics (ETA)

В основе – исследовательская работа специалистов Cisco

Известный вредоносный трафик

Известный «хороший» трафик

Выделение характерных признаков в сетевом трафике

Применение технологий машинного обучения для получения классификаторов

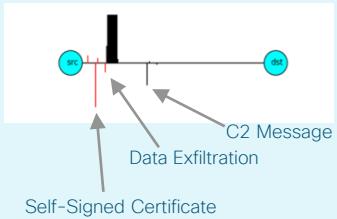
Сессии известного вредоносного ПО определяются в сетевом трафике с 99% аккуратностью и низким FDR

“Deciphering Malware's use of TLS (without Decryption)”

Blake Anderson, Subharthi Paul, David McGrew

https://arxiv.org/abs/1607.01639

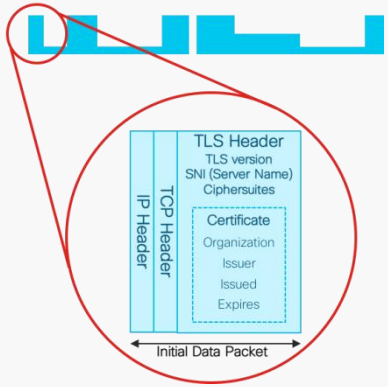
ETA – используемый набор данных

	TCP/IP	DNS	TLS	SPLT
Вредоносный трафик	Плохая репутация (или отсутствие)	c15c0.com afb32d75.com	Нетипичный fingerprint Необычный cert	 Bestafera
«Хороший» трафик	Часто используемый и известный адрес	cisco.com	Типовой fingerprint Типовой cert	 Google search

Что мы можем увидеть в зашифрованном трафике?

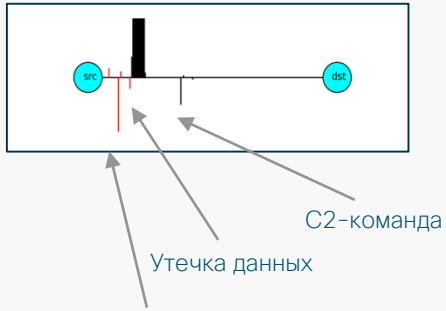
Initial data packet

Выжать максимум из доступных незашифрованных полей



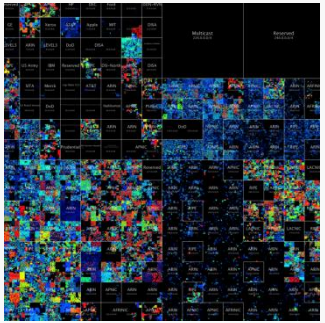
Частотно-временные характеристики размеров пакетов SPLT

Определение типа соединения по размерам и частотно-временным характеристикам пакетов



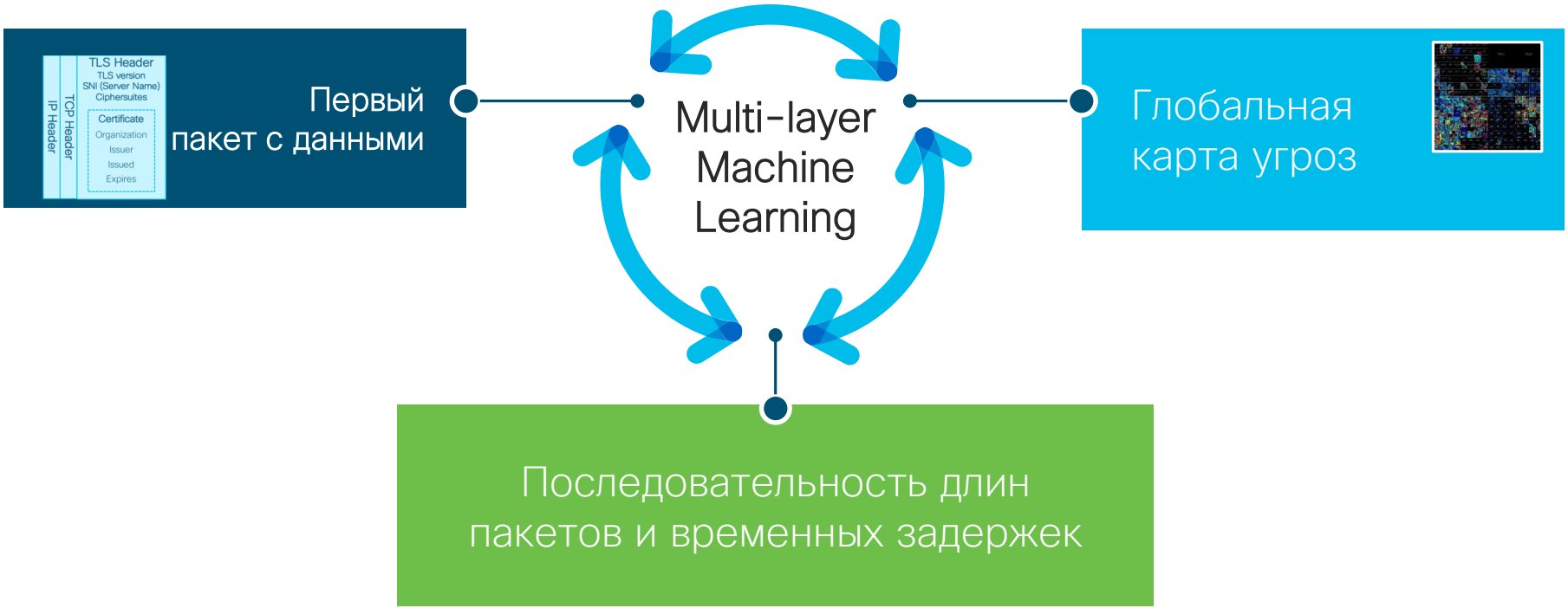
Глобальная карта рисков

Кто есть кто на тёмной стороне Internet



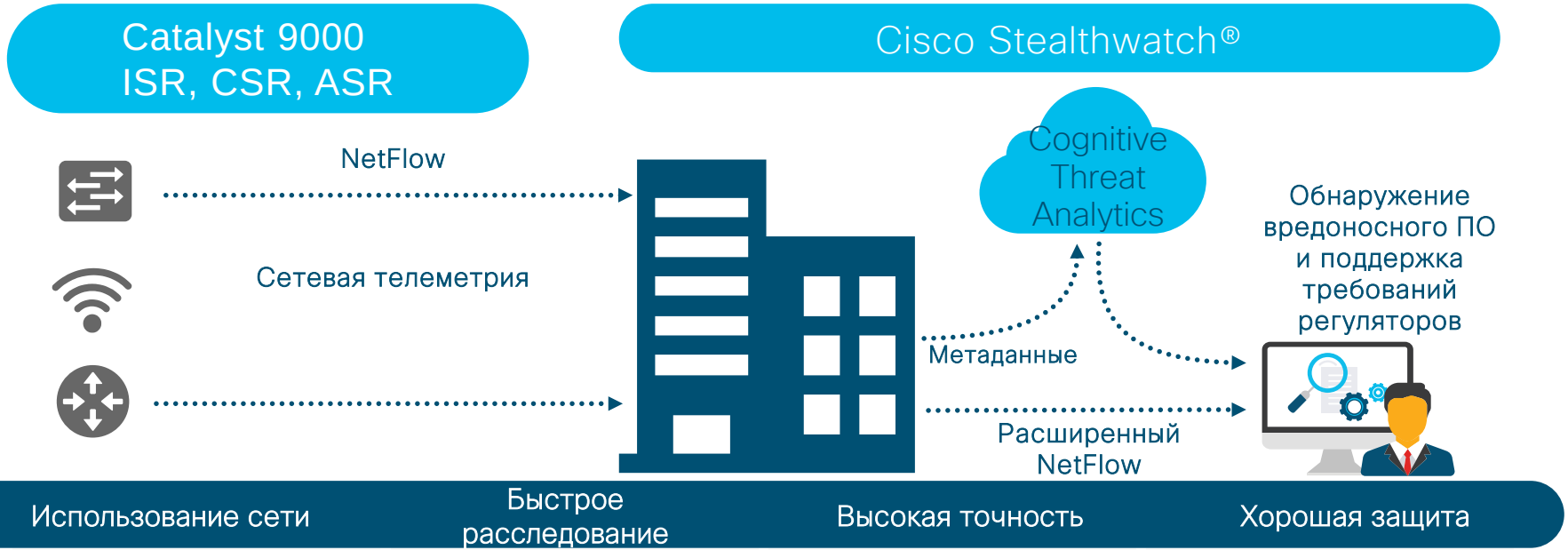
Репутационная и поведенческая информация о серверах в сети Internet

Многоуровневое машинное обучение



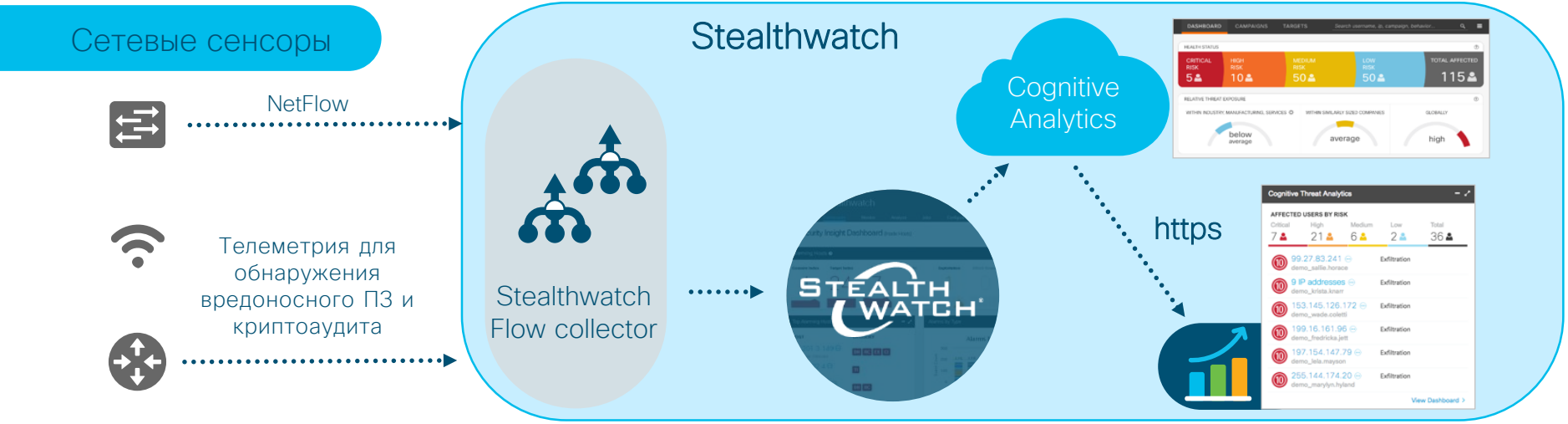
Элементы решения

Обнаружение вредоносной активности в зашифрованном трафике



Использование сети	Быстрое расследование	Высокая точность	Хорошая защита
Enhanced NetFlow от новых коммутаторов и маршрутизаторов Cisco	Продвинутая аналитика и машинное обучение	Корреляция глобальной и локальной информации	Постоянный контроль соответствия

Encrypted Traffic Analytics



Уникальная программно-аппаратная архитектура Cisco

Расширенный анализ NetFlow с Encrypted Traffic Analytics с современных устройств Cisco

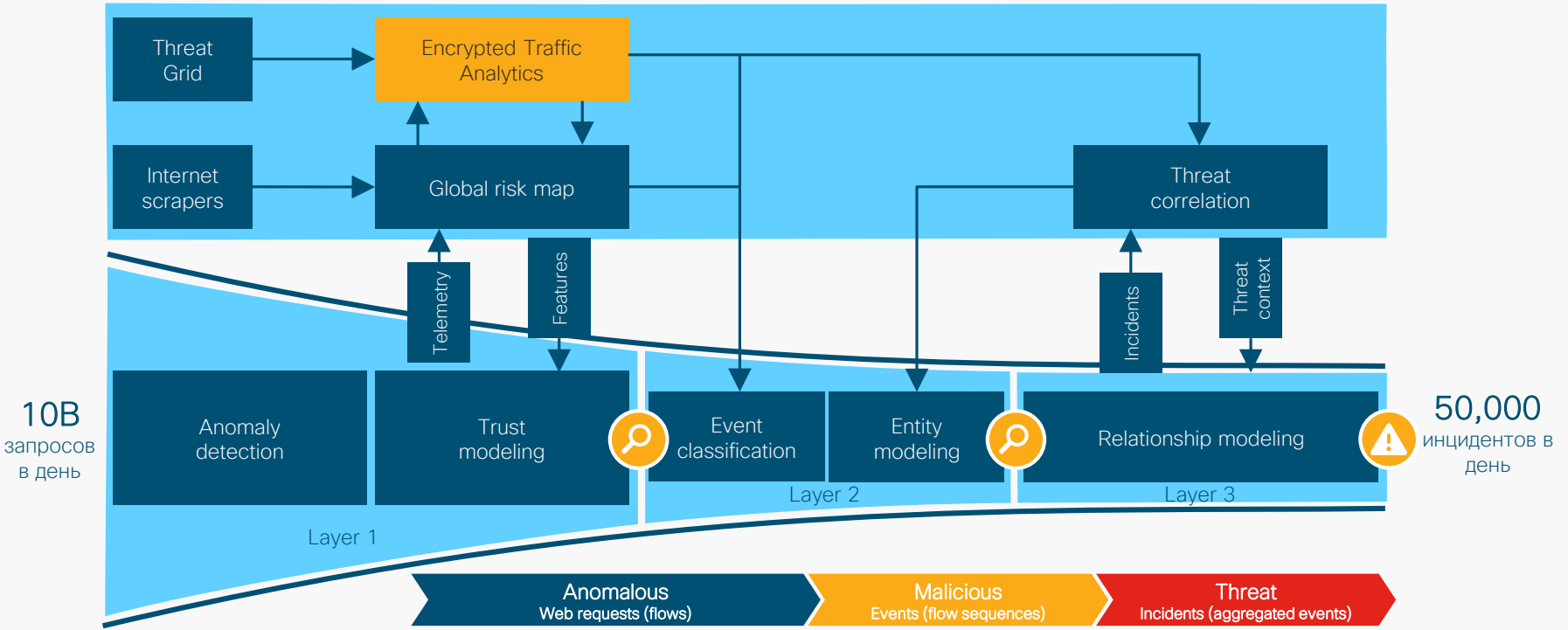
Возможности расширенного анализа и технологий машинного обучения снижают время расследования инцидентов

Глобальная и локальная корреляция знаний позволяет добиться высокой точности в обнаружении угроз

Какие метаданные отправляются в облако?

- Метаданные от Stealthwatch к Cognitive: Initial Data Packet (IDP), Sequence of Packet Lengths and Time (SPLT), прокси-логи (опционально).
- Метаданные отправляются только для трафика, пересекающего периметр (например, отправляемого в Интернет) и DNS-запросы.
- Канал между Stealthwatch Flow Collector и Cognitive защищён с помощью TLS.
- Большая часть трафика, отправленного в Cognitive удаляется через 2-4 часа после анализа.
- Cognitive Analytics обрабатывает ETA-данные (Enhanced NetFlow) в специализированном ЦОД, со всеми необходимыми настройками безопасности и приватности, с постоянным контролем.
- Разработка ведётся в соответствии с принципами безопасности и приватности в управлении данными.

Cognitive Analytics использует многослойное машинное обучение



Что нужно чтобы начать использовать ETA?
Лицензии, наборы, оборудование

Элемент решения	Версия ПО	Лицензия
Коммутаторы Cisco® Catalyst® 9000*	Cisco IOS® XE 16.6.1	Включена в Cisco DNA™ Advantage/ Cisco ONE™ Advanced
Маршрутизаторы ASR 1000, 4000 ISR, CSR, ISRv, 1100 ISR**	Cisco IOS XE 16.6.2	Включена в SEC/k9 license Cisco ONE foundation
Stealthwatch® с CA	v6.9.1	Management Console, Flow Collector, Flow Rate License
Stealthwatch с CA и ETA	v6.9.2 Cryptographic compliance (Q3CY17) Malware Detection (Q4CY17)	

*C9300 коммутаторы с ПО 16.6.1(июль 17), C9400 начиная с 16.6.2 (октябрь 17)

Доступно для тестов с 16.6.1, официальная поддержка с 16.6.2 (октябрь 17**)

Сеанс чёрной магии окончен, приступаем к разоблачению ;)

HTTP легко прочитать

http://nytimes.com/index.htm

http://salesforce.com/updateSalesTargets.js

http://api.gmail.com/newmail

http://dropbox.com/checkForUpdates

http://youtube.com/funnycatvideos

- Cognitive Analytics использует до 500 параметров из каждого запроса для анализа

Множество HTTP-запросов в одном потоке

http://nytimes.com/index.htm	(и 200 сопутствующих запросов)
http://salesforce.com/updateSalesTargets.js	(+20 запросов)
http://api.gmail.com/newmail	(1 запрос)
http://dropbox.com/checkForUpdates	(5 запросов)
http://youtube.com/funnycatvideos	(100+ запросов и потоковое видео)

- Cognitive Analytics использует до 500 параметров из каждого запроса для анализа
- Каждая загрузка страницы – от 50 до 200 HTTP запросов к тому же самому серверу

HTTPS запросы непрозрачны

https://1.2.3.4

https://123.123.123.123

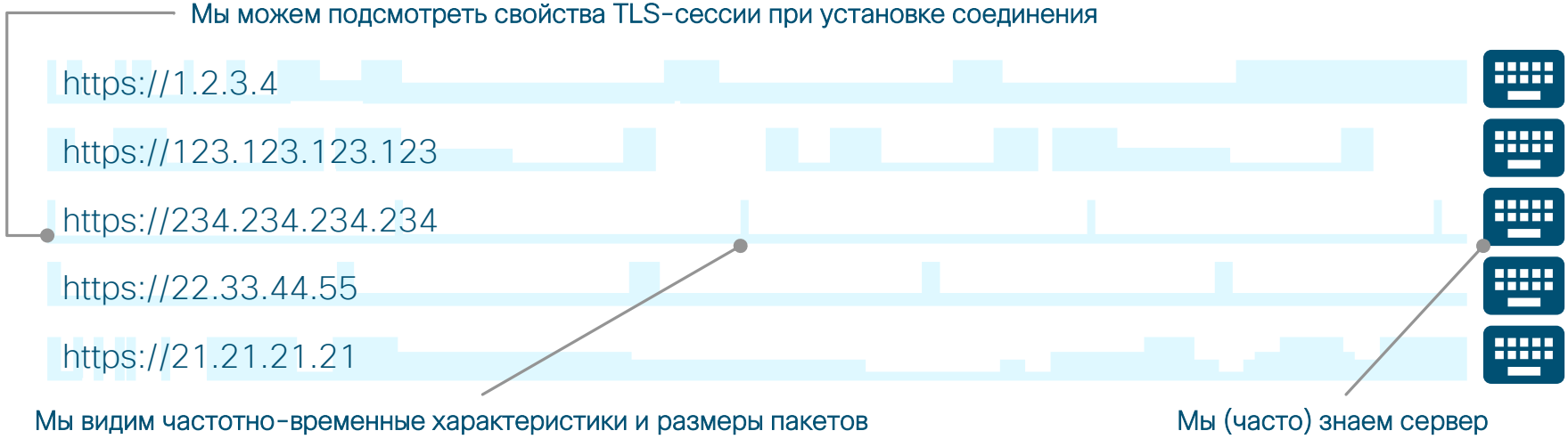
https://234.234.234.234

https://22.33.44.55

https://21.21.21.21

- Домены и сайты напрямую нам не видны

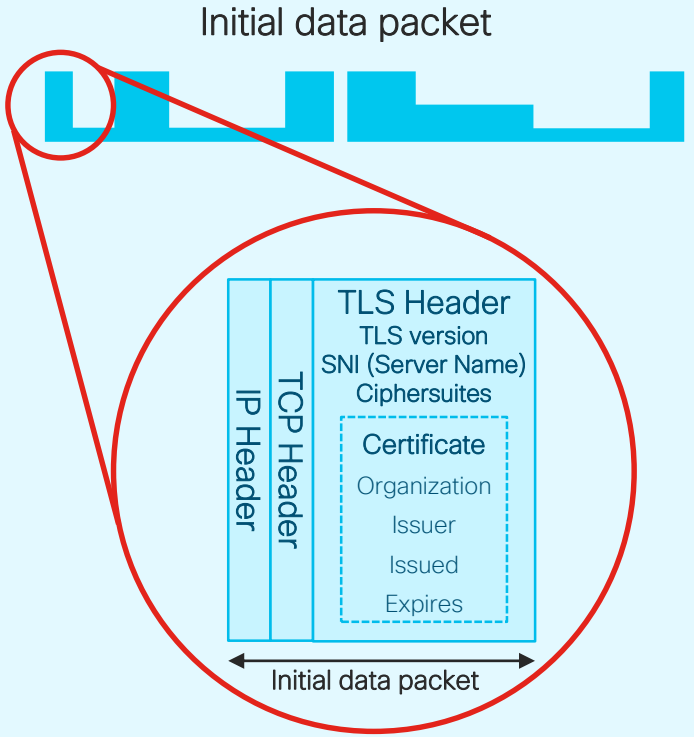
Но мы всё ещё можем получить КУЧУ информации ;)



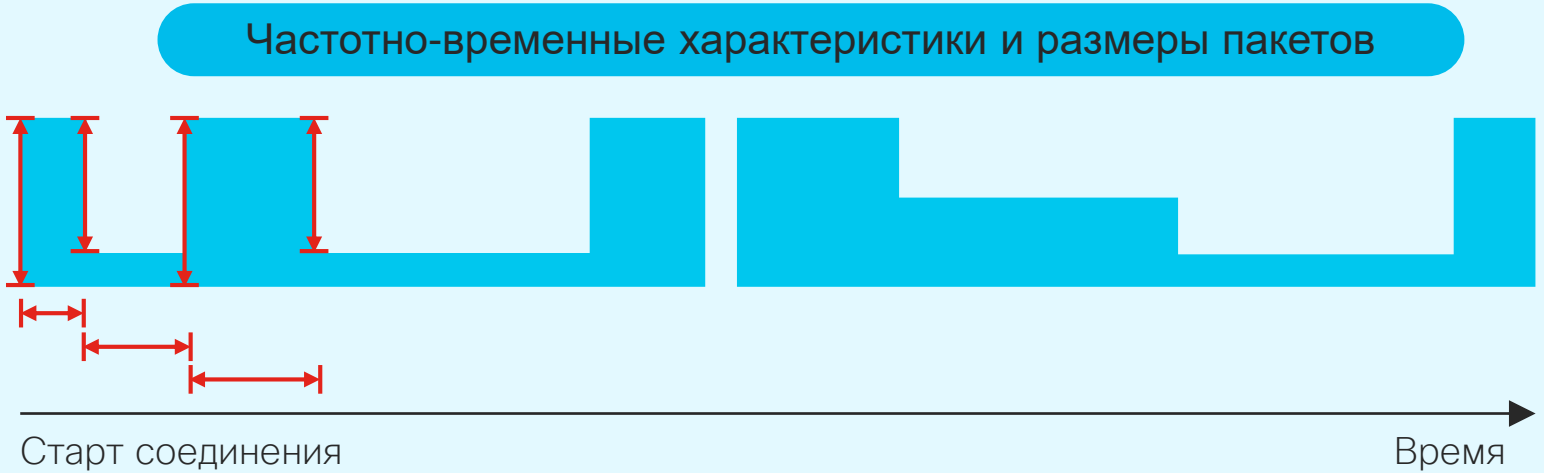
- Параметры установки TLS-сессии
- Частотно-временные характеристики и размеры пакетов
- Информация о домене (часто)

Initial data packet

- HTTPS-заголовок с несколькими интересными полями.
- Имена серверов из SNI-поля сертификатов.
- Информация из параметров установки TLS-сессии многое нам говорит об особенностях поведения сервера и клиента, иногда – о приложении.
- Информация из сертификата – всё равно, что информация о домене из whois.
- А также многое другое при использовании глобальной репутации и корреляции.



Sequence of packet lengths and times (SPLT)
Частотно-временные характеристики и размеры пакетов



- Размер и временные характеристики первых пакетов позволяют нам сделать вывод о типе данных внутри зашифрованного соединения.
- Мы умеем различать видео, web, вызовы API, голосовые звонки, и множество других типов данных друг от друга, а также классифицировать их.

Глобальная карта угроз Cisco

Кто есть кто на тёмной стороне Internet

- Модели учитывают больше 20 параметров с каждого из 150 миллионов известных вредоносных, опасных, или иным способом влияющих на безопасность сайтов.
- Параметры включают информацию о характеристиках домена, информацию из whois, данные из TLS-сертификата, статистику использования, а также шаблоны поведения для каждого сервера.

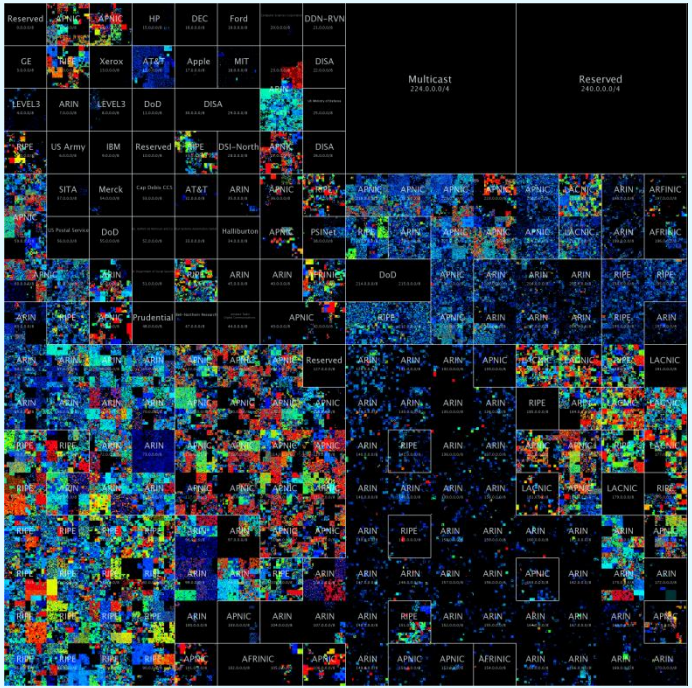


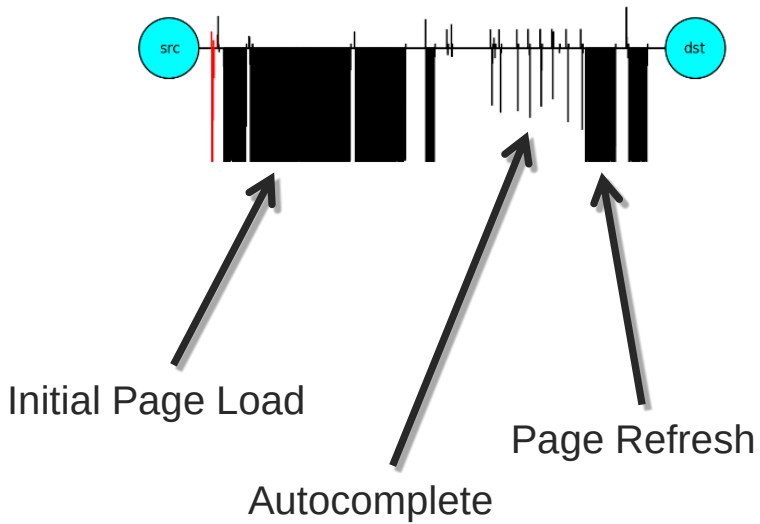
Image: http://census2012.sourceforge.net/images.html

Рассмотрим на примере: Bestafera

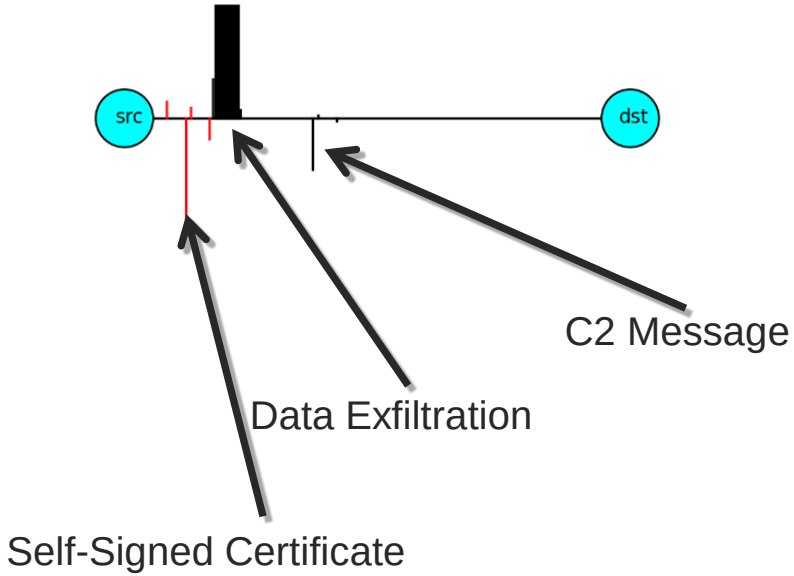
Пробует собрать пользовательские данные для онлайн банкинга и переслать их на сервер управления– производит запись вводимых символов и крадет конфиденциальные/персональные данные

Шаблоны поведения для длины пакетов/времени

Google Search



Bestafera



Цифровой отпечаток TLS (Bestafera)

TLS ClientHello

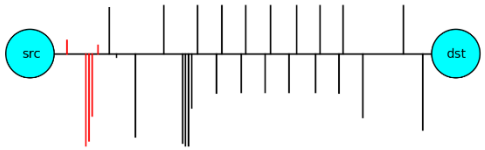
```
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 214
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 210
        Version: TLS 1.0 (0x0301)
      > Random
        Session ID Length: 0
        Cipher Suites Length: 120
      > Cipher Suites (60 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 49
      > Extension: ec_point_formats
      > Extension: elliptic_curves
      > Extension: SessionTicket TLS
      > Extension: Heartbeat
```

Возможные клиенты

Настоящий клиент

OpenSSL
(v: 1.0.1r)

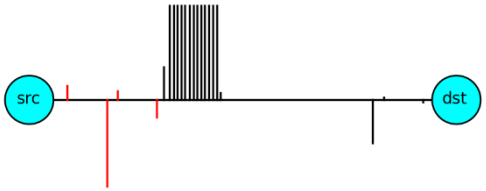
Как следствие



+

(v: 52.0)

=



+

OpenSSL

(v: 1.0.1r)

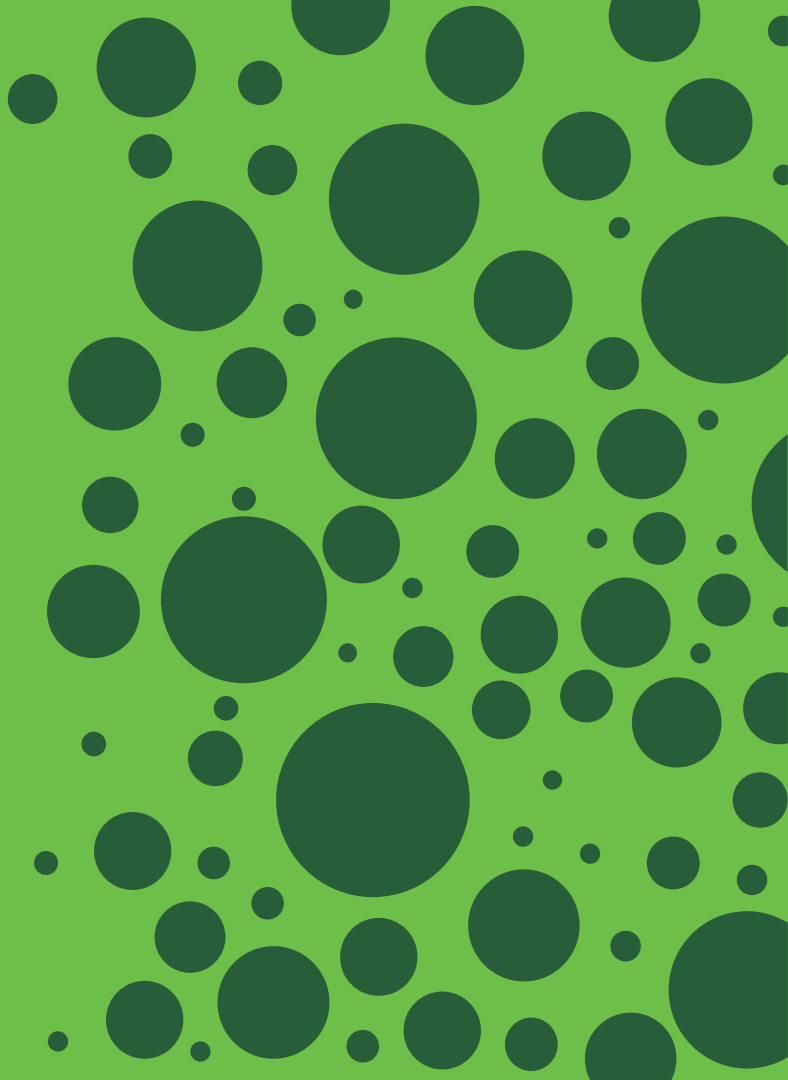
=

+

TALOS

cisco Cisco Umbrella

Практические результаты внедрений и тестирований



Публичные мероприятия:

- Mobile World Congress (MWC) 2018
- RSA Conference 2018
- Cisco Live, Orlando 2018

Проверки сторонними лабораториями

- Miercom Solution Validation

What is Mobile World Congress?

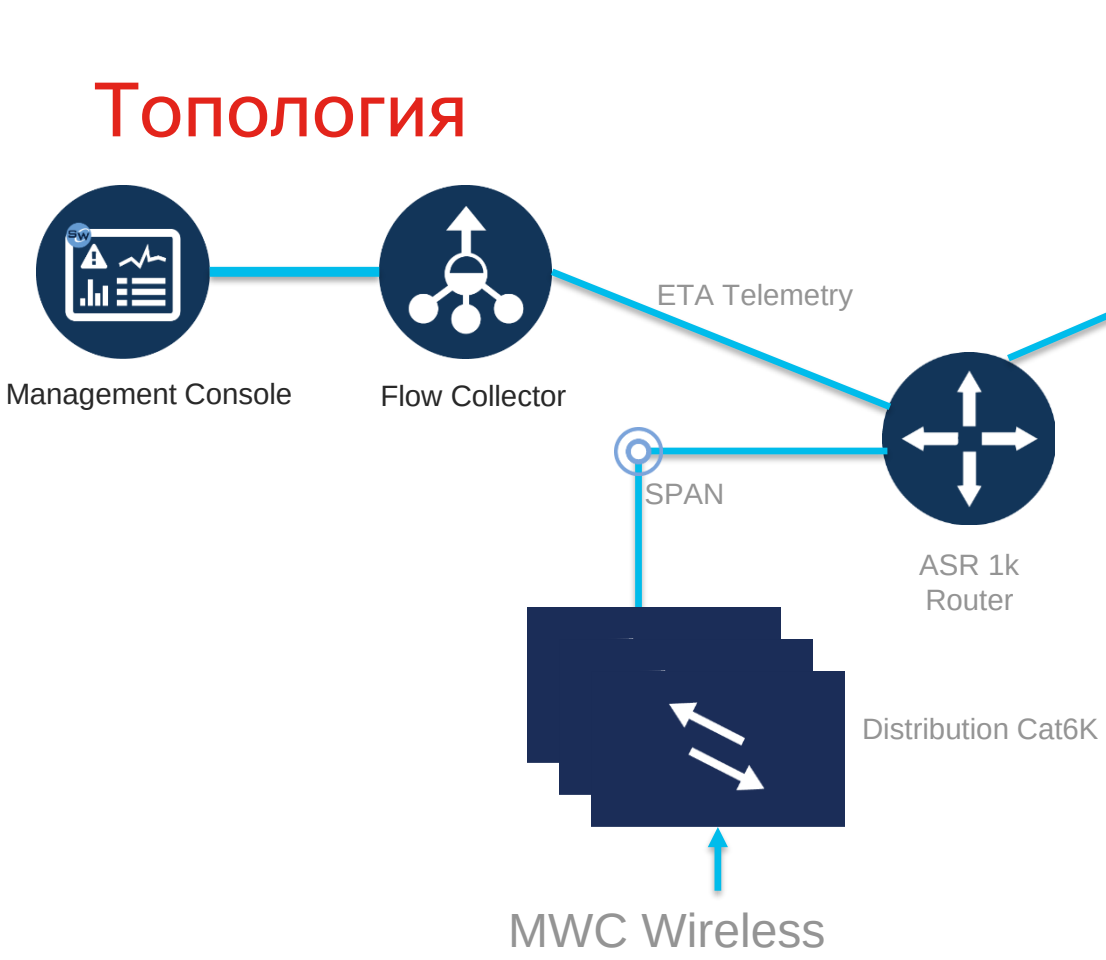
GSMA MOBILE WORLD CONGRESS

BARCELONA 26 FEB-1 MAR 2018

Более чем 107,000 посетителей из 205 стран и территорий
Около 55% посетителей имеют руководящие позиции, включая более чем 7,700 CEOs

Stealthwatch мониторил весь беспроводный трафик в/из Интернета с использованием Encrypted Traffic Analytics

Топология



We enabled ETA on an ASR1001-X with the MWC's Internet bound traffic SPAN'ed from a distribution Cat6K switch to the ASR1001-X on a GigE port

ETA на Mobile World Congress 2018

Массивный охват сети

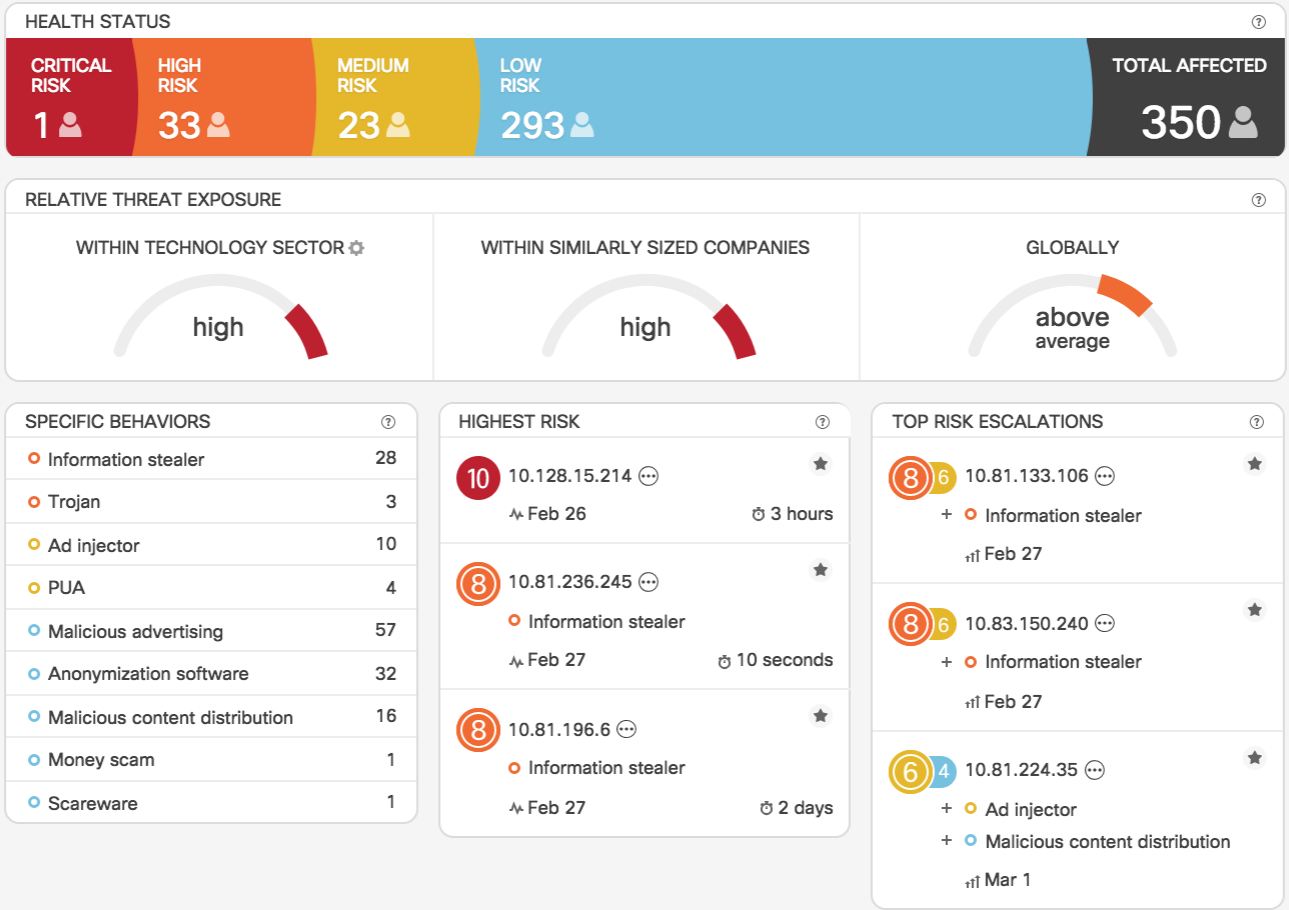
- 55+ миллионов потоков
- 82% HTTPS vs 18% HTTP
- В пиковые часы более 20 000 потоков/сек от беспроводных пользователей

Выявленные угрозы

- C&C и эксфильтрация данных (data exfiltration)
- 350 детектирований с использованием ETA
- Множество экземпляров вредоносного ПО включая мобильное malware
- Более 30 приложений с использованием TLS 1.0

Итоги детектирования

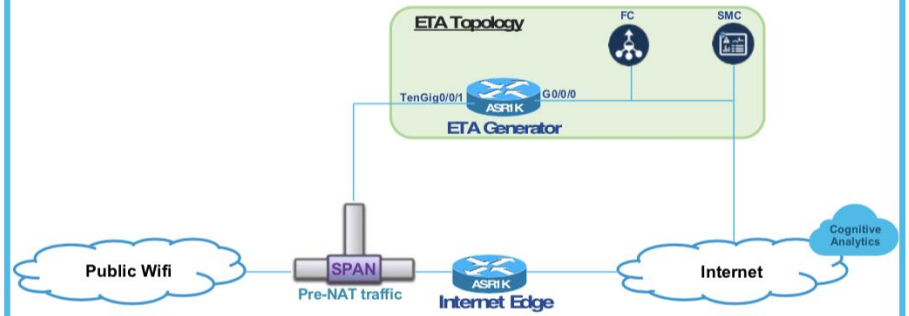
Android Malware	Android.spy, Boqx, infected firmware
Adware	OSX Malware Genieo, RevMob, AdInjector
Possibly unwanted applications	Tor, BitTorrent, phishing
Various	SALITY malware, SMB service discovery malware, Conficker, cryptomining



RSA Conference (RSAC) - 2018

- Monitored Public WiFi
- 45,000+ Attendees
- 42+ Million Flows Analyzed
- **82% HTTPS vs 18% HTTP**
- 10K+ fps from Wireless Users

ETA Topology



Threats Detected

- 300+ Stealthwatch Alarms, 180 Detections using ETA
- C&C and Data Exfiltration
- Multiple High- and Medium-risk Detections
- Numerous Malware Instances including Android Malware
- Several Applications using TLS 1.0 & SSL 3.0

Cisco Blog: https://blogs.cisco.com/security/cisco-catches-thousands-of-hidden-threats-on-a-massive-public-network

Тестирование Miercom в 2018

Test Setup

ASR1001-X router: IOS XE 16.6.2 release with an enterprise license

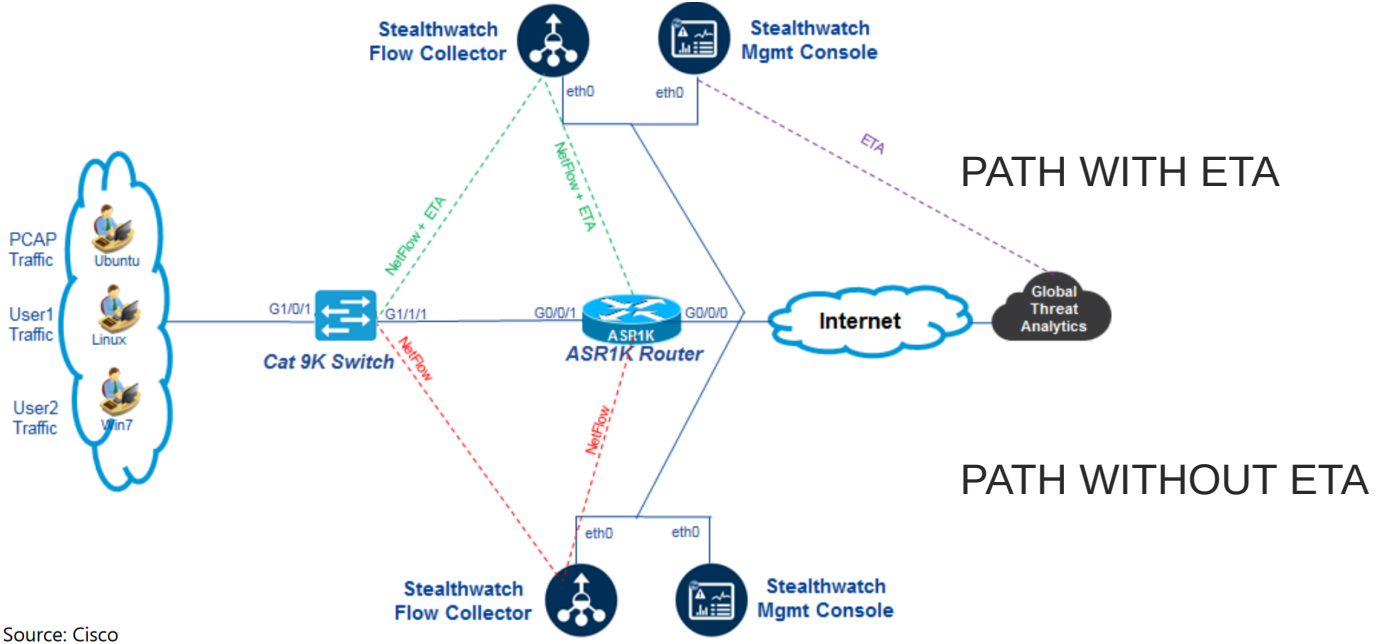
Cisco Catalyst 9300 switch (C9300-24P): IOSXE 16.6.2, Network Advantage & DNA Advantage licenses

Stealthwatch Enterprise (Flow Collector & Management Console) virtual appliances: release with 6.9.2-01 ROLLUP patch installed on a Cisco UCS C200 M2

PCAP PC: Ubuntu 16.04.3 LTS installed on a Cisco UCS C200 M2

Набор ноутбуков использовался для генерации различных типов вредоносного трафика

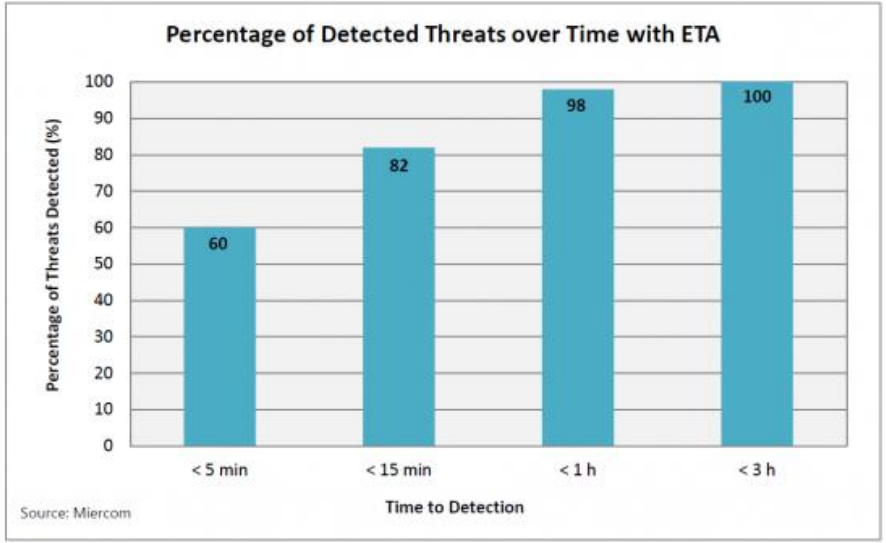
74 pcap семплов были запущены и 51 использовали шифрованный трафик



Source: Cisco

Результаты тестирования

Cisco ETA показала на 36% более высокую скорость детектирование в сравнении с системой без опции ETA system, находя 100% угроз в течении 3 часов.



https://blogs.cisco.com/security/encrypted-traffic-analytics-receives-miercom-performance-verified-certification
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/miercom-report-eta- perf.pdf

Выводы

- Большая часть сетевых коммуникаций сейчас зашифрованы.
- Прямая расшифровка трафика не является жизнеспособным вариантом.
- ETA это решение, а не точечный продукт, которое покрывает.
  - Branch, WAN и Cloud маршрутизаторы
  - Кампусные коммутаторы
  - Cisco Stealthwatch Enterprise
- ETA предоставляет :
  - Анализ криптографического соответствия.
  - Обнаружение вредоносной активности в зашифрованном трафике БЕЗ расшифровки.

www.cisco.com/go/eta

- ETA Overview
- ETA Deployment Guide
- Martin Rehak, Blake Anderson Securing Encrypted Traffic on a Global Scale; Cisco Blogs
- Blake Anderson, David McGrew; Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity; KDD, 2017
- Open source package for network data capture and analysis: https://github.com/cisco/joy


CISCO