Мониторинг угроз с использованием StealthWatch: Детальный обзор

Павел Родионов

CSE Security, Cisco

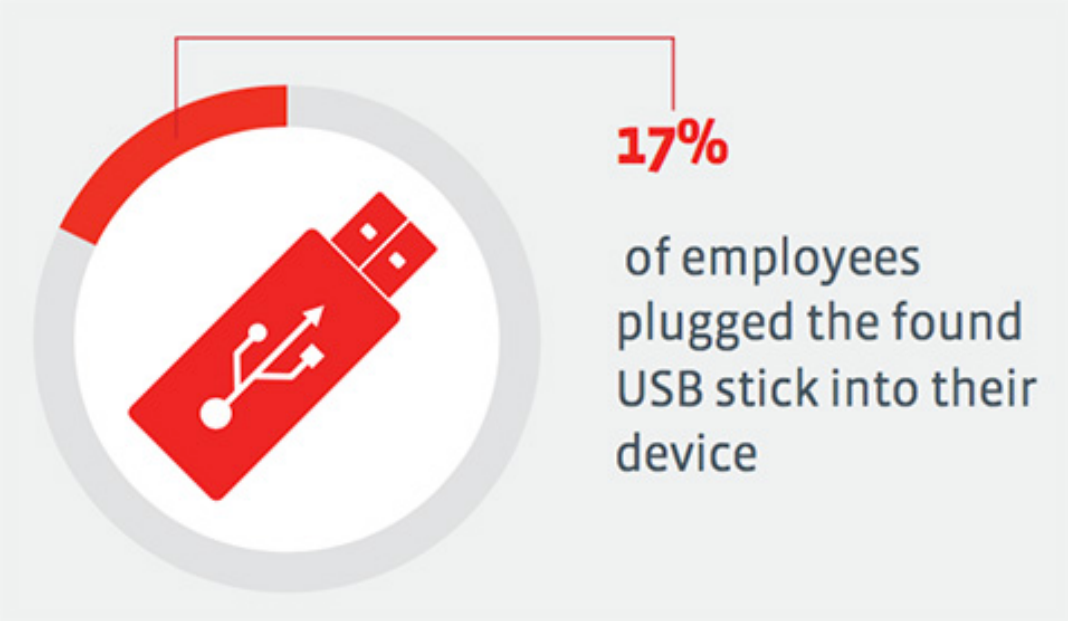
CCIE #11155, GREM

Программа

- Введение
- Использование сетевой телеметрии
- Организация данных
- Обнаружение Индикаторов Компрометации
- Расследование вторжения
- Итоги

“ Мир полон очевидных вещей, которых никто не замечает.”
Шерлок Холмс, *Собака Баскервилей*

Социальный эксперимент: 200 USB Flash оставили в публичных местах



http://www.net-security.org/secworld.php?id=19033

Программа

- Введение
- Использование сетевой телеметрии

Об этой сесии: Видимость через изучение данных

Возможность понять:

- Откуда данные пришли
- Как данные обрабатываются
- Как использовать эти данные

Что объединяет всех?

Сетевая телеметрия

Телеметрия: процесс автоматизированной коммуникации при котором измерения и другие данные собираются на удаленных или недоступных точках и передаются на оборудование получателя для анализа и мониторинга.
https://en.wikipedia.org/wiki/Telemetry

Аналитика данных с помощью телеметрии:

Обнаружение

- Идентификация бизнес-критичных приложений и сервисов в сети

Идентификация дополнительных Индикаторов Компрометации (IoC)

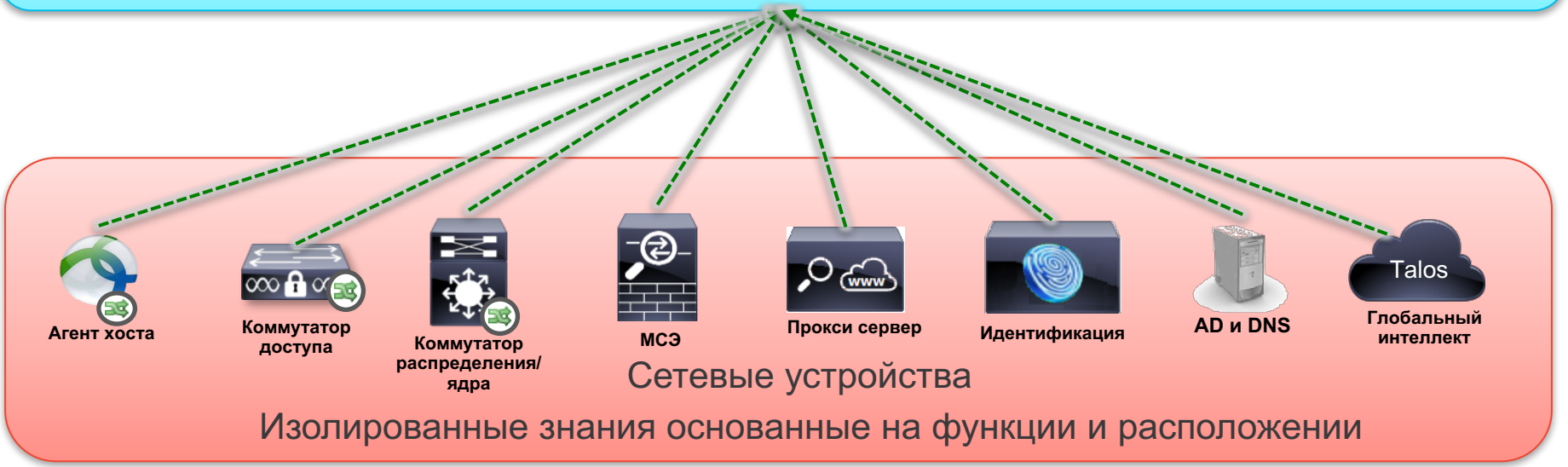
- Политики и Сегментация
- Сетевое поведение и Обнаружение Аномалий (NBAD)

Лучше понимать / реагировать на IOC:

- Аудит всех коммуникаций между хостами

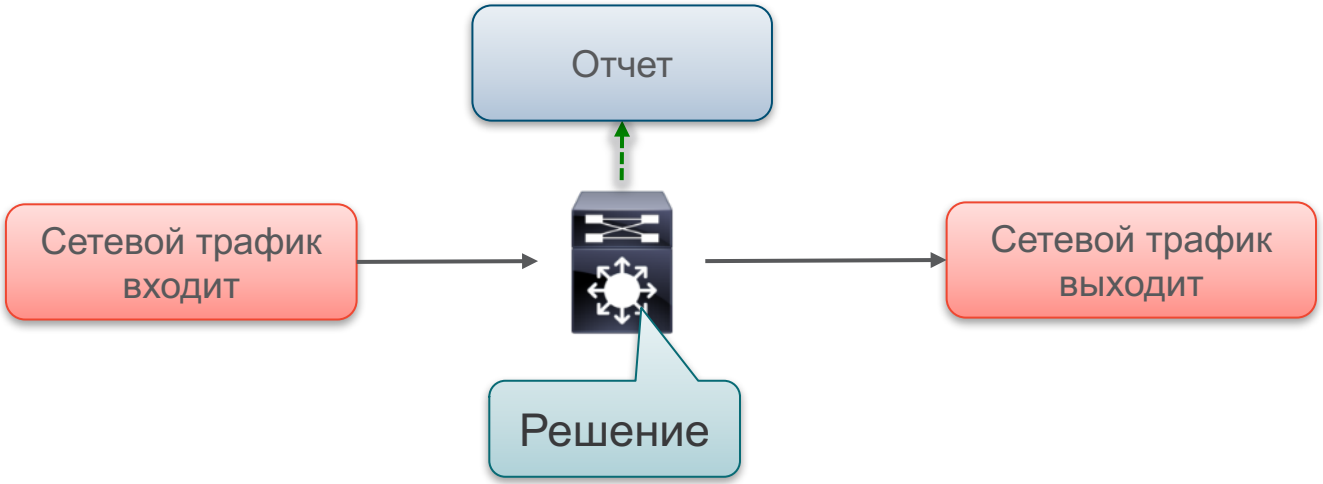
Cisco Stealthwatch

Cisco Stealthwatch: Это коллектор и аггрегатор сетевой телеметрии с целью аналитики безопасности и мониторинга



Понять сетевую телеметрию

“Информация! Мне нужна информация! Я не могу лепить кирпичи без глины!
Шерлок холмс, **Медные буки**



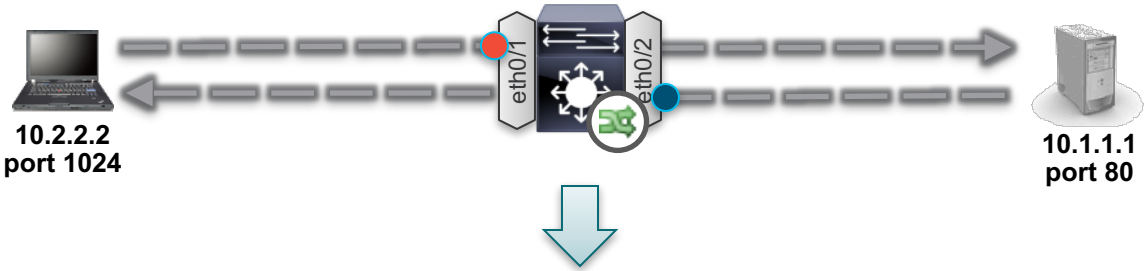
Версии NetFlow

Версия 5
Фиксированный формат
18 Заданных полей

Версия 9
Шаблонная
108 Заданных полей

IPFIX
Стандартизована
Шаблонная
Поля изменяемой длины
450+ Заданных полей

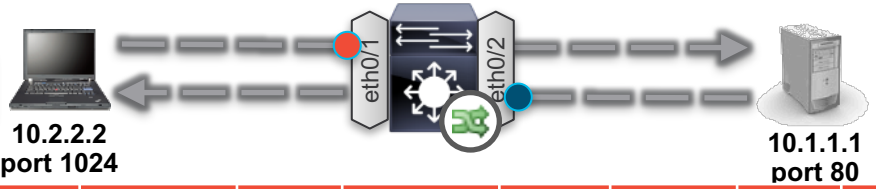
Транзакционная телеметрия с NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100	SYN,ACK,FIN

Обработка телеметрии: “Склеивание сессий”

Однонаправленные потоки

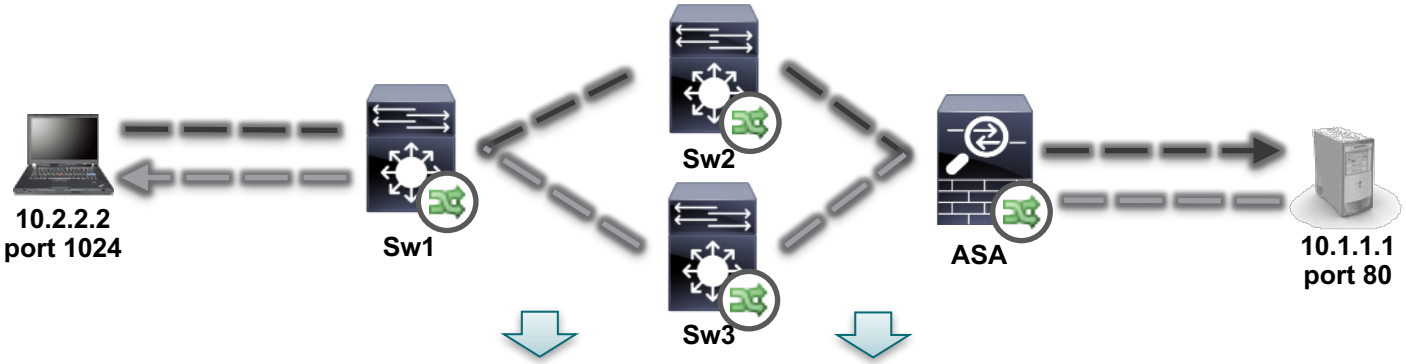


Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Client SGT	Server SGT	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	100	1010	eth0/1 eth0/2

Двунаправленные:
- Запись двусторонней сессии
- Позволяет легко визуализировать и анализировать

Обработка телеметрии: “Дедупликация”



Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	App	Client SGT	Server SGT	Exporter, Interface, Direction, Action
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	HTTP	100	1010	Sw1, eth0, in Sw1, eth1, out Sw2, eth0, in Sw2, eth1, out ASA, eth1, in ASA, eth0, out, Permitted ASA eth0, in, Permitted ASA, eth1, out Sw3, eth1, in Sw3, eth0, out Sw1, eth1, in Sw1, eth0, out

Stealthwatch Системные компоненты

Stealthwatch Management Console
- Управление и отчетность
- До 25 Flow Collectors
- До 6 миллионов fps глобально
- 2 физических и виртуальных модели
- Отказоустойчивость

Cisco Security Packet Analyzer
- Полный пакетный захват на сети
- 2 физические модели

Stealthwatch Flow Collector
- Сбор и анализ
- До 4000 экспортеров
- До одновременно 240,000 fps
- 4 физических и 3 виртуальных модели

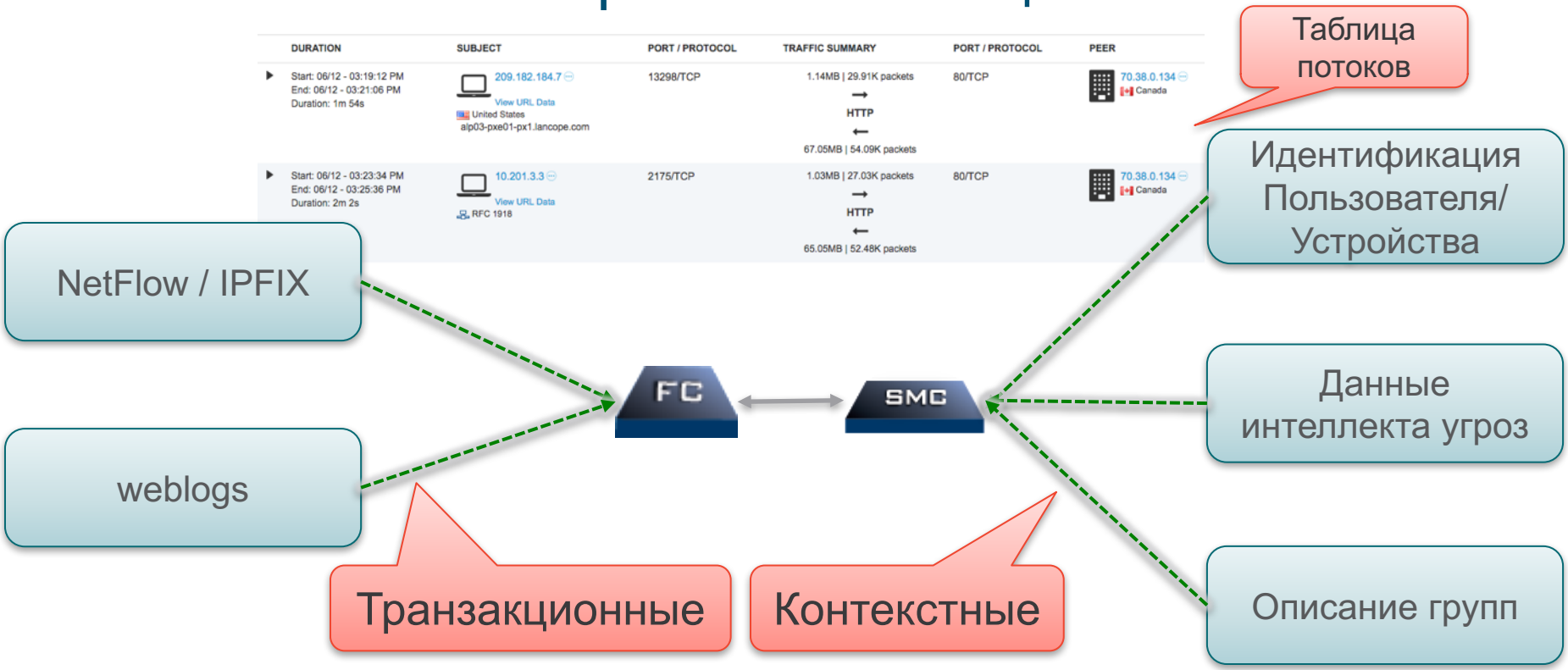
UDP Director
- UDP Копир пакетов
- Отправляет на разные узлы
- Отказоустойчивость
- 2 физических и виртуальных модели

Stealthwatch Flow Sensor
- Генерирует IPFIX из SPAN/TAP
- Контекстные поля (прим. App,URL,SRT,RTT)
- Физические и виртуальные модели

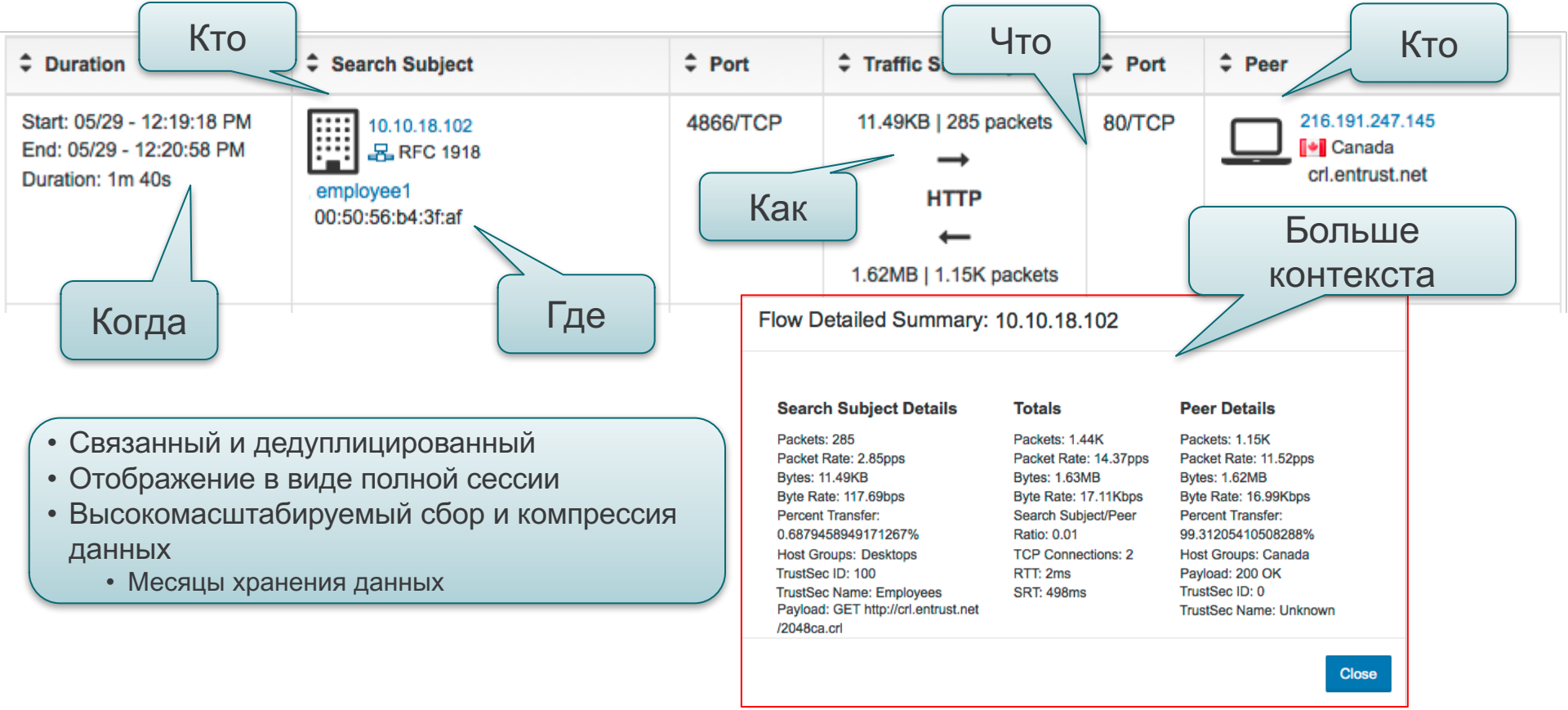
Endpoint License Concentrator
- Собирает AnyConect NVM потоки данных и отправляет на Flow Collector
- Виртуальный аплаенс

Cloud License Concentrator
- Собирает потоки с Cloud License Agents и отправляет их на FC

Stealthwatch: Построение таблицы потоков



Двусторонняя запись потока



- Связанный и дедуплицированный
- Отображение в виде полной сессии
- Высокомасштабируемый сбор и компрессия данных
  - Месяцы хранения данных

Контекстная телеметрия

“Это мелочи, но нет ничего важнее мелочей.
Шерлок Холмс, **Медные буки**

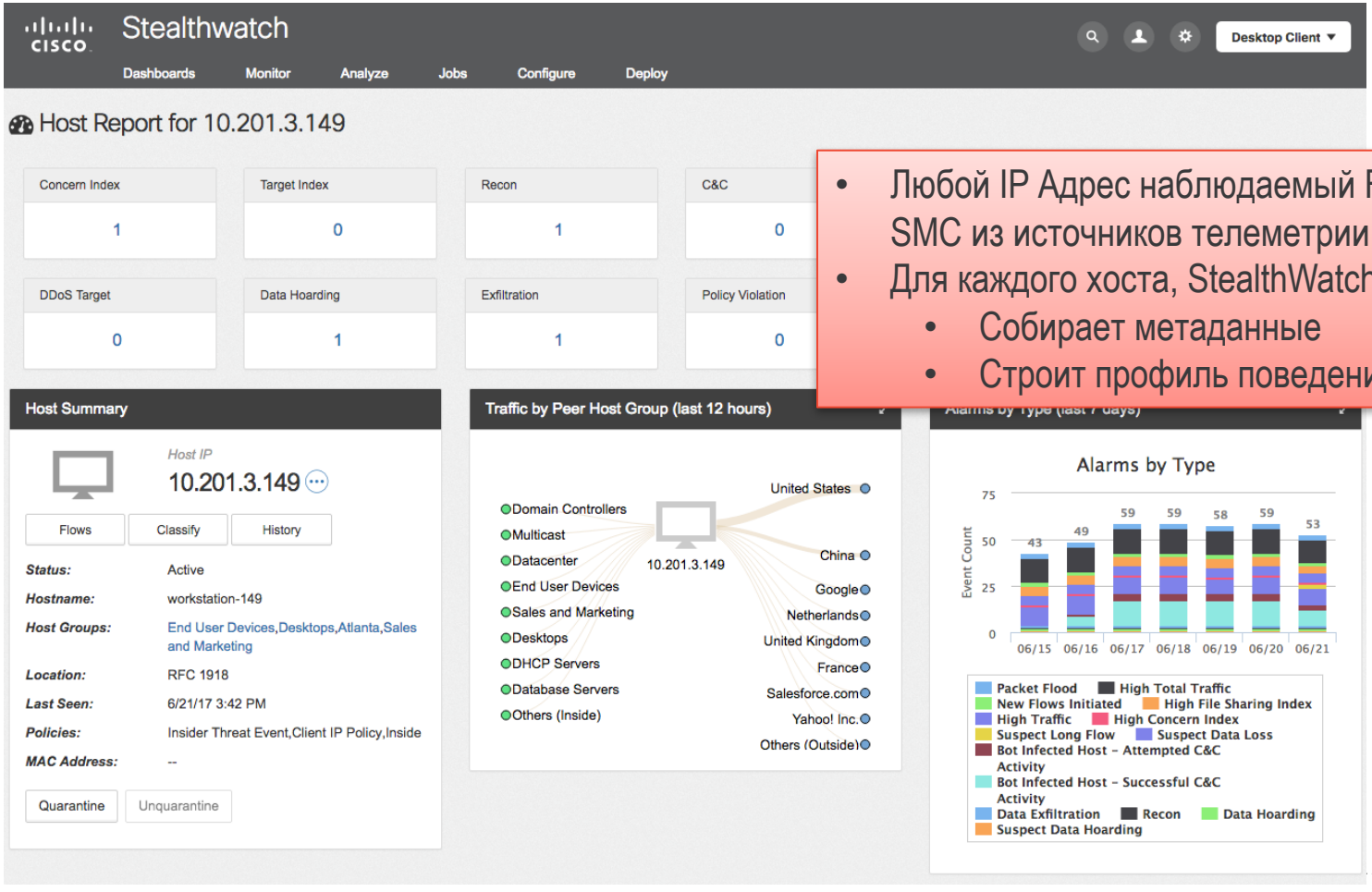
Кто?

IP Адрес: **10.10.10.10**

Что?

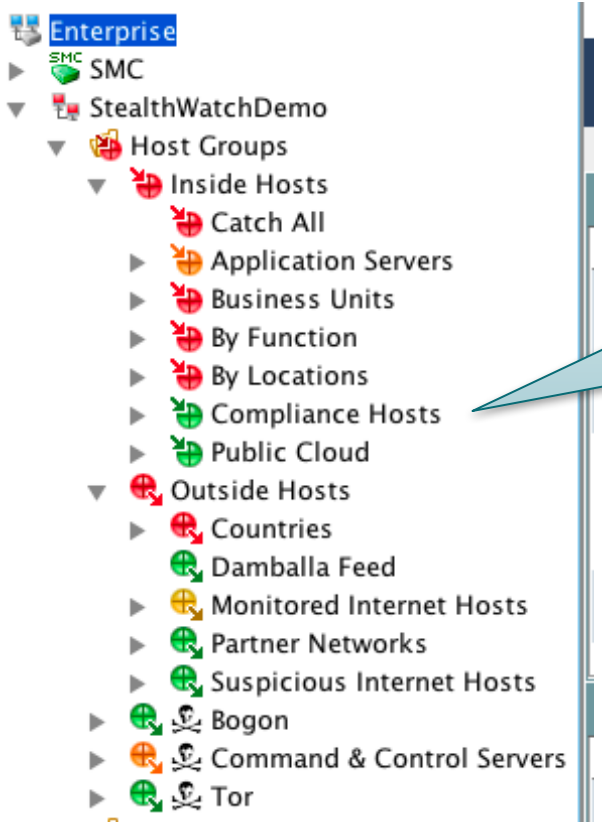
Где?

Концепция: Хост



- Любой IP Адрес наблюдаемый Flow Collector или SMC из источников телеметрии
- Для каждого хоста, StealthWatch
  - Собирает метаданные
  - Строит профиль поведения

Концепция: Группы хостов



Применяем знание окружения

- Виртуальный контейнер IP адресов
- Задается пользователем
- Схожие атрибуты
- Моделирование любого процесса/приложения

ISE как источник Телеметрии

- Аутентификация Пользователя / Устройства
- Профиль устройства
- Пассивная идентификация

Cisco ISE

pxGrid

Stealthwatch Management Console

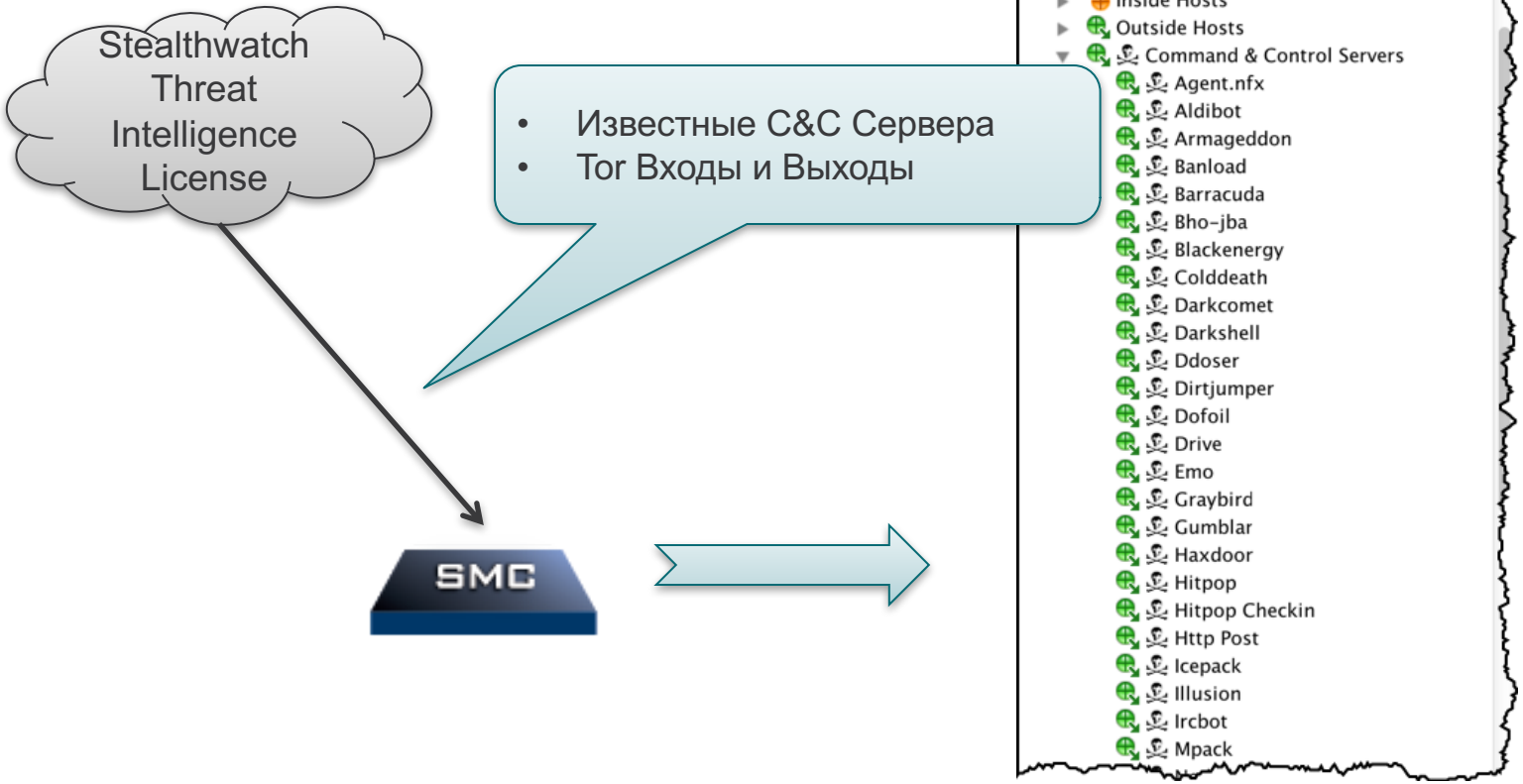
- Хранит историческую таблицу сессий
- Корреляция NetFlow с пользователем
- Построение отчетов на пользователя

Start Active Time	End Active Ti...	User Name	Host	Device Type	MAC Address
Apr 15, 2013 2:08:33 PM (17 minutes 6s ago)	Current	student01	192.168.103.101	VMWare-Device	00:50:56:85:5c:3d (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student04	192.168.104.100	WindowsXP-Workstation	00:50:56:85:13:c4 (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod08-mgmt.demo.local	192.168.108.100	WindowsXP-Workstation	00:50:56:85:13:cc (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod09-mgmt.demo.local	192.168.109.100	WindowsXP-Workstation	00:50:56:85:13:ce (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student05	192.168.105.100	WindowsXP-Workstation	00:50:56:85:13:c6 (VMware, Inc.)

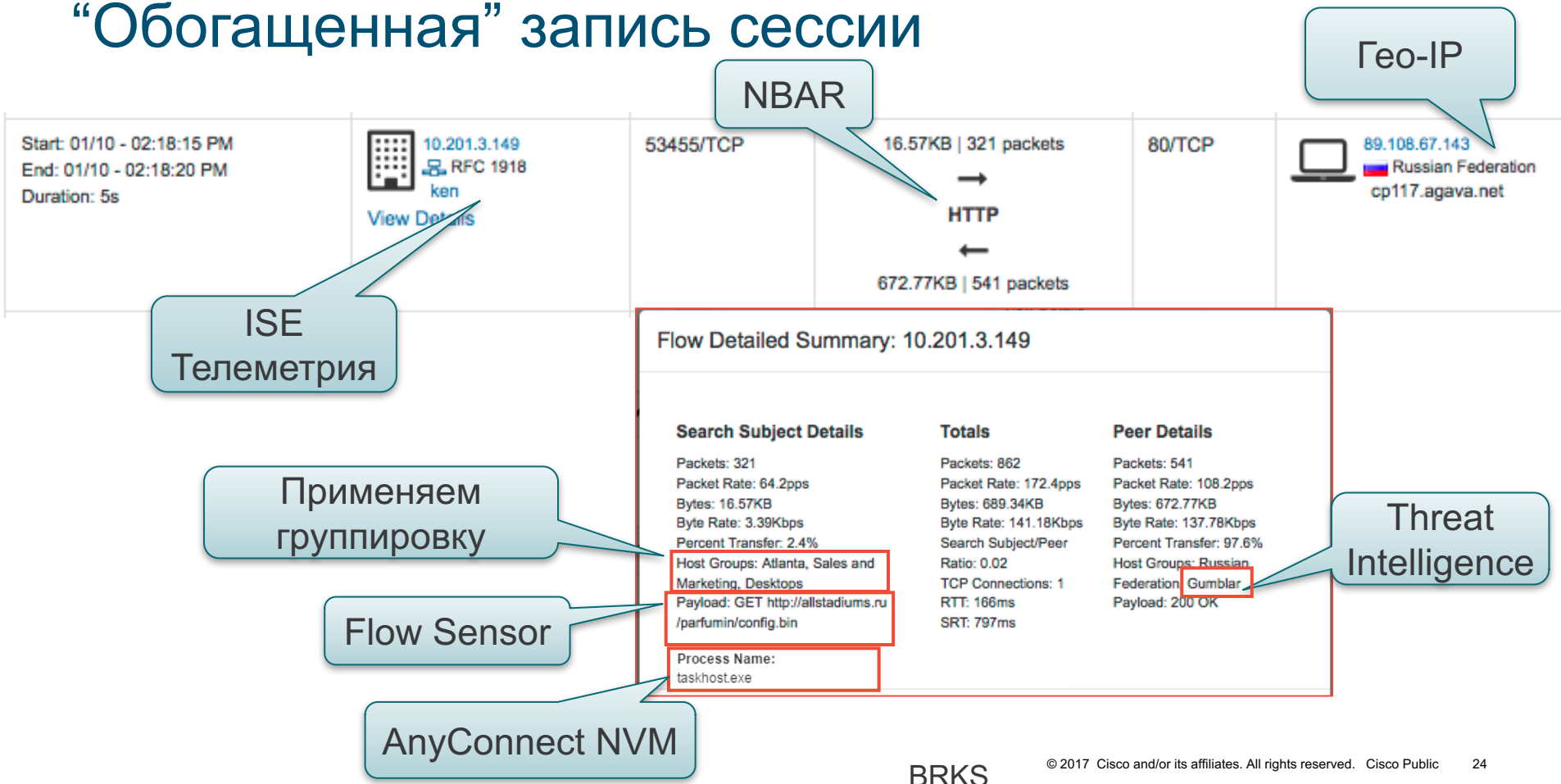
Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Apr 15,13 02:08:33.241 PM	✓		student01	00:50:56:85:5C:3D	192.168.103.1...	sw1	GigabitEthernet0/4	PermitAccess
Apr 15,13 02:08:21.241 PM	✓		DEMO\student04	00:50:56:85:13:C4	192.168.104.1...	sw1	GigabitEthernet0/5	PermitAccess
Apr 15,13 02:08:21.219 PM	✓		host/pod08-mgmt.demo.local	00:50:56:85:13:CC	192.168.108.1...	sw1	GigabitEthernet0/9	PermitAccess
Apr 15,13 02:08:21.192 PM	✓		host/pod09-mgmt.demo.local	00:50:56:85:13:CE	192.168.109.1...	sw1	GigabitEthernet0/10	PermitAccess
Apr 15,13 02:08:21.144 PM	✓		DEMO\student05	00:50:56:85:13:C6	192.168.105.1...	sw1	GigabitEthernet0/6	PermitAccess
Apr 15,13 02:08:21.082 PM	✓		DEMO\student07	00:50:56:85:13:CA	192.168.107.1...	sw1	GigabitEthernet0/8	PermitAccess

Таблица Аутентифицированных Сессий

Глобальный интеллект



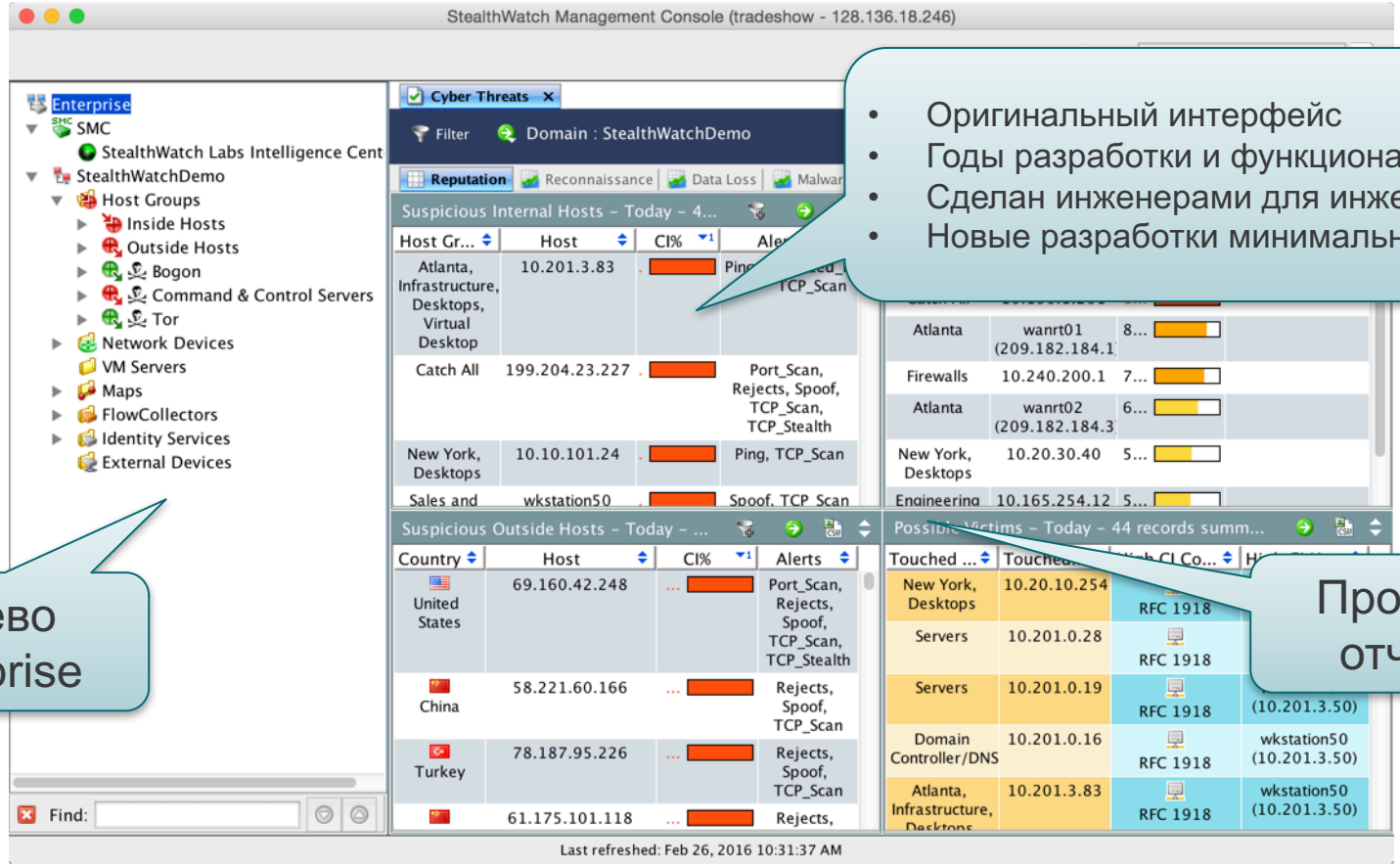
“Обогащенная” запись сессии



Программа

- Введение
- Использование сетевой телеметрии
- Организация данных

Со стороны: SMC Интерфейс 1: Java (Swing) Клиент



- Оригинальный интерфейс
- Годы разработки и функциональности
- Сделан инженерами для инженеров
- Новые разработки минимальны

Дерево Enterprise

Просмотр отчетов

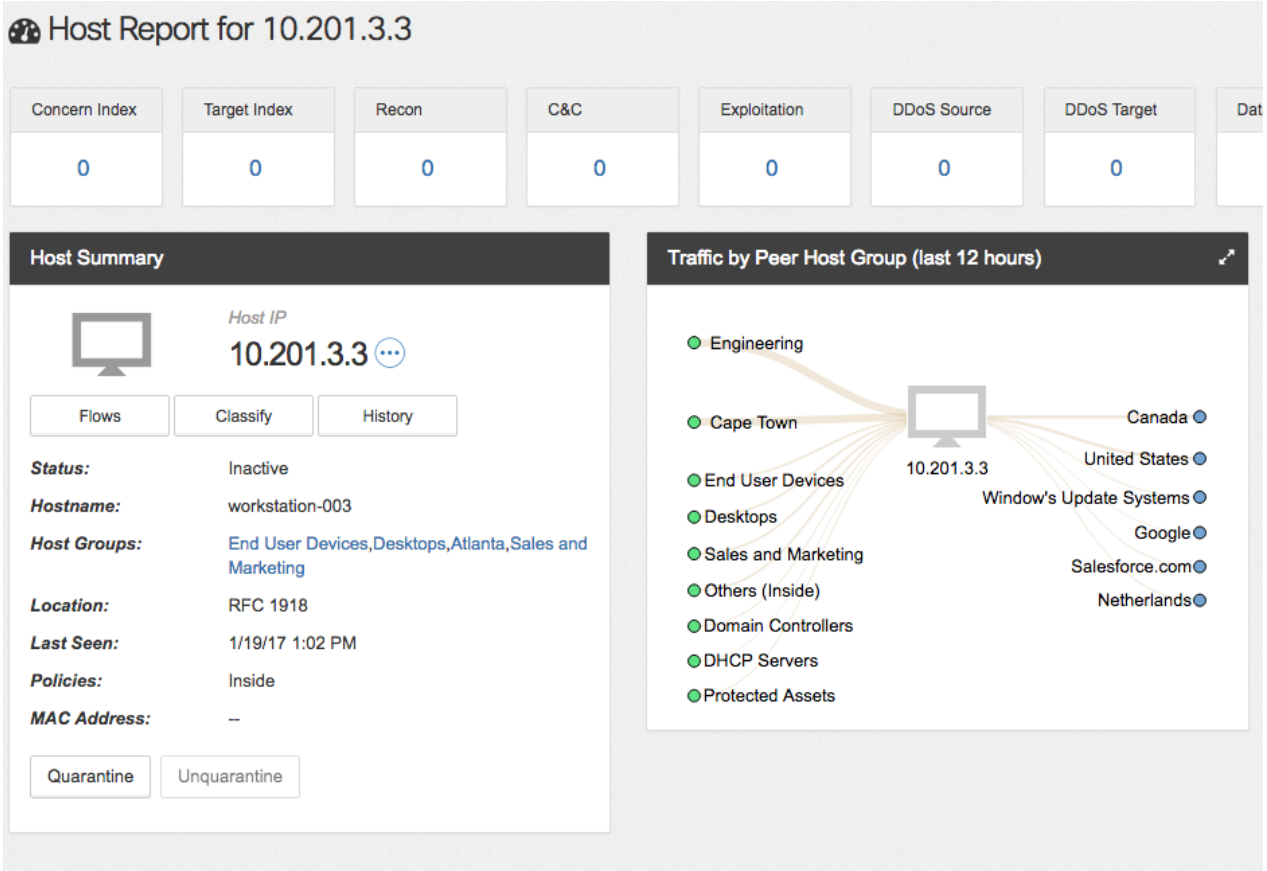
Со стороны: SMC Интерфейс 2: “Web” Интерфейс

- Представлен в Stealthwatch 6.5
- Новые функции добавляются сюда

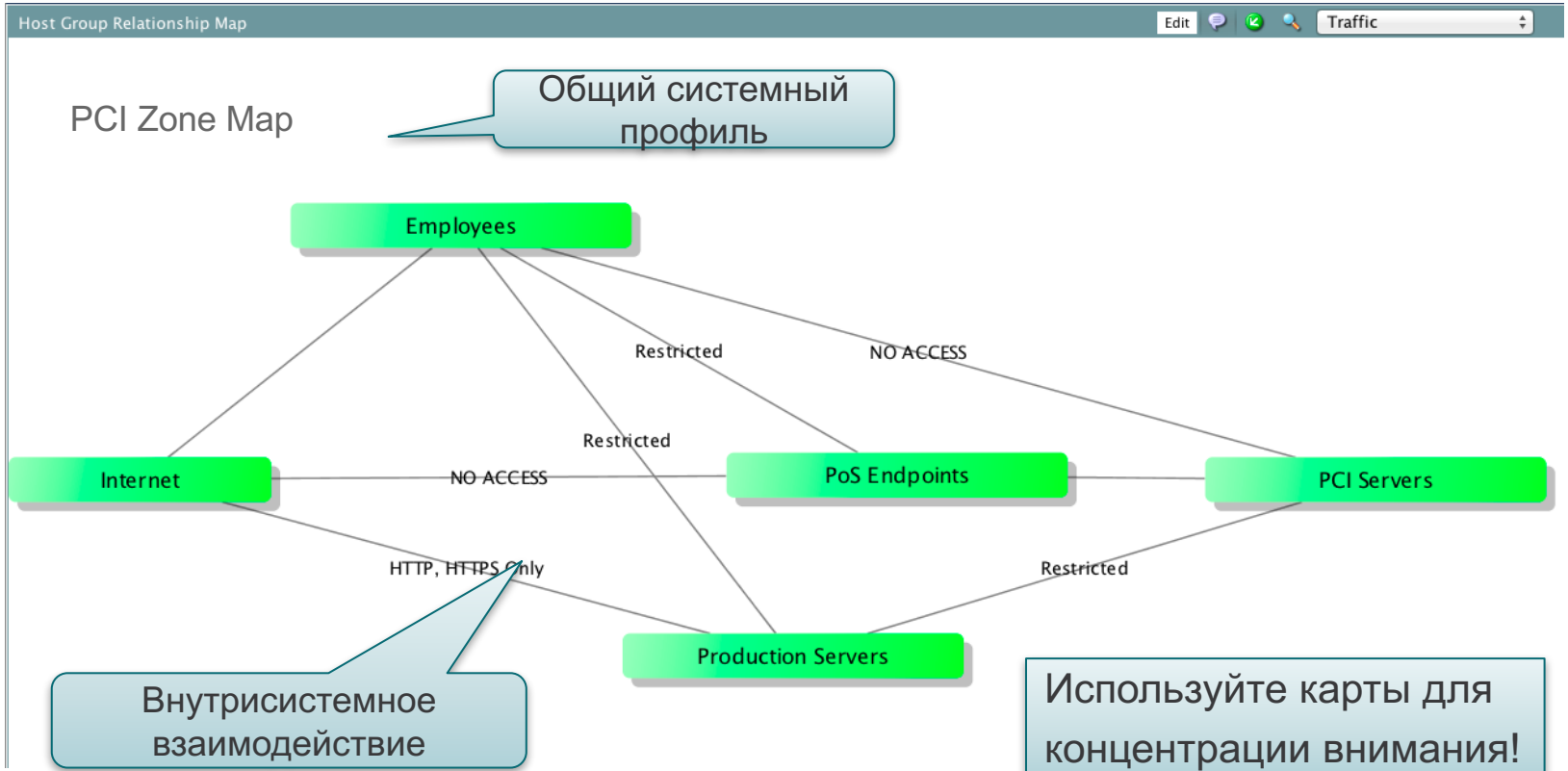
Функции уникальные для WEB интерфейса:

- ISE Remediation
- Собственные события
- SGT поля в Flow Record
- Web данные прокси
- Данные с Endpoint
- Настройка Active Directory
- Частные приложения
- Управление работами
- “First Seen”

Хостовый отчет о подозрительном хосте



Карта потоков данных



Программа

- Введение
- Использование сетевой телеметрии
- Организация данных
- Обнаружение Индикаторов Компрометации

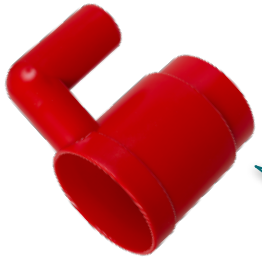
Концепция: Индикатор компрометации

Свидетельство, наблюдаемое в сети или операционной системе указывающее на высокую вероятность компроиметации

- http://en.wikipedia.org/wiki/Indicator_of_compromise

IoC из аналитики данных

Поведенческий анализ:
- Использует понимание не нормального поведения
- Политика и сегментация



Обнаружение аномалий:
- Идентификация отклонений от “нормы”

Обнаружение угроз с StealthWatch

Модель безопасности StealthWatch

События безопасности (“Алгоритмы”)

События безопасности (“Алгоритмы”)

Security Event

Security Event

Security Event

Security Event

Security Event

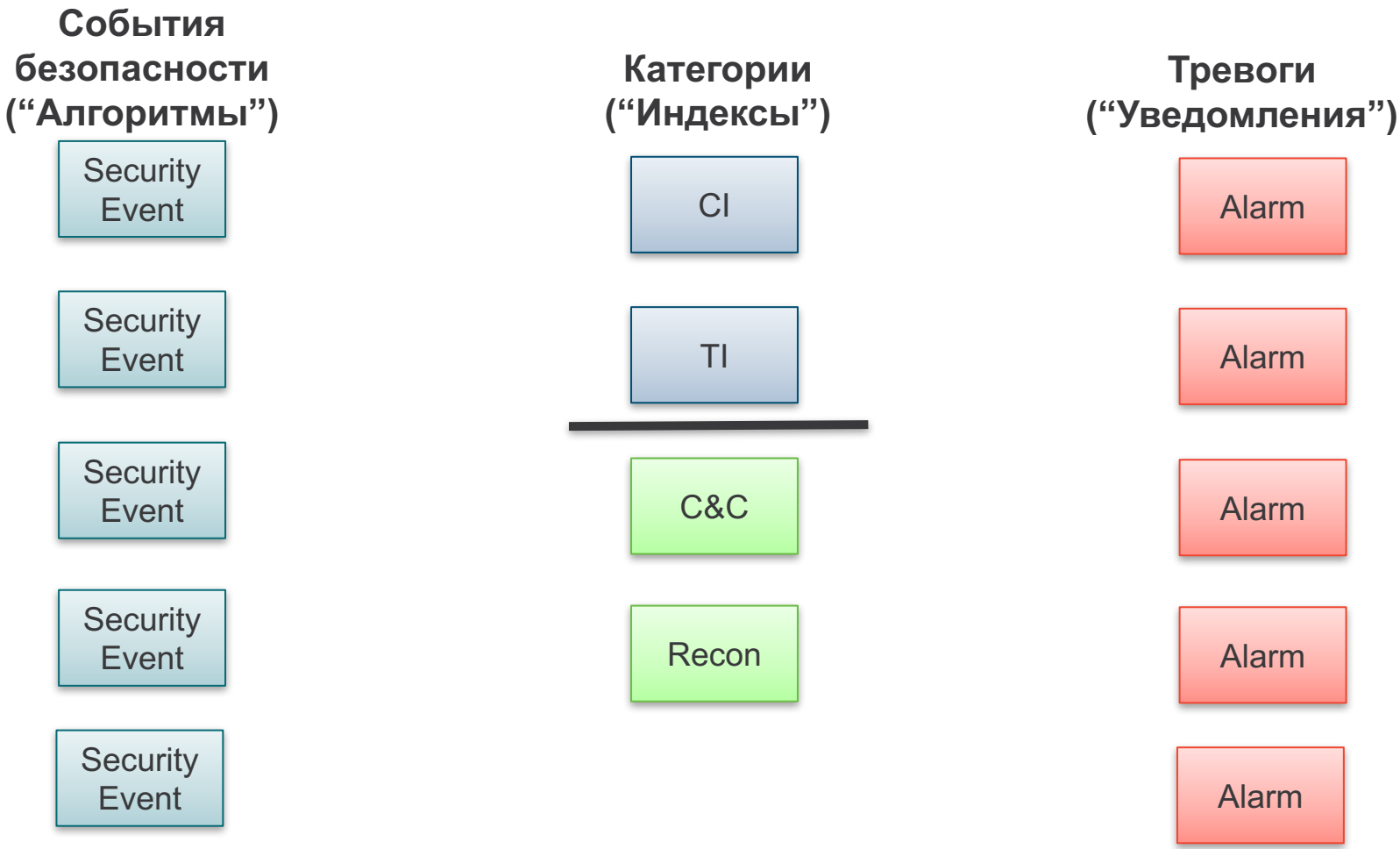
Категории (“Индексы”)

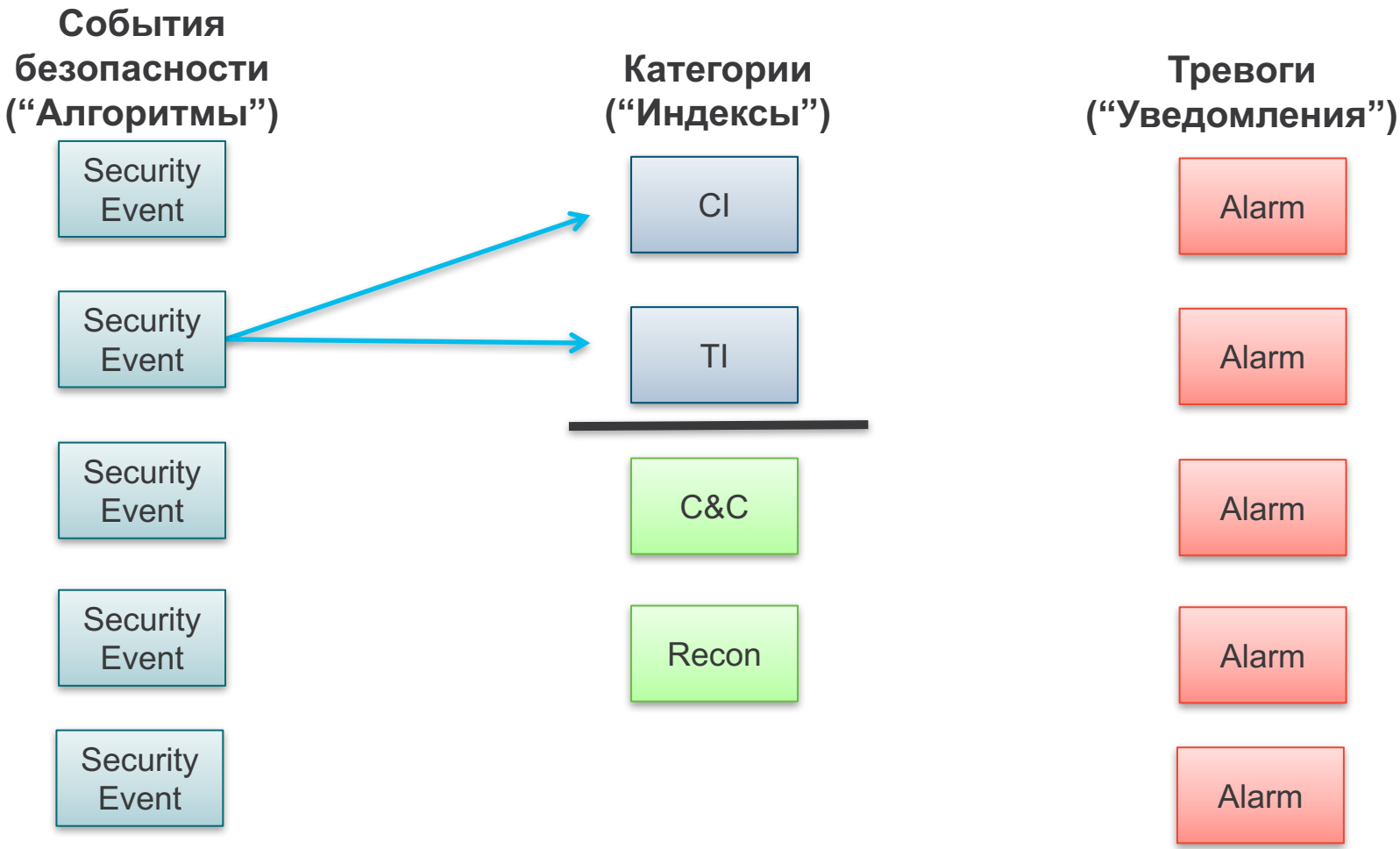
CI

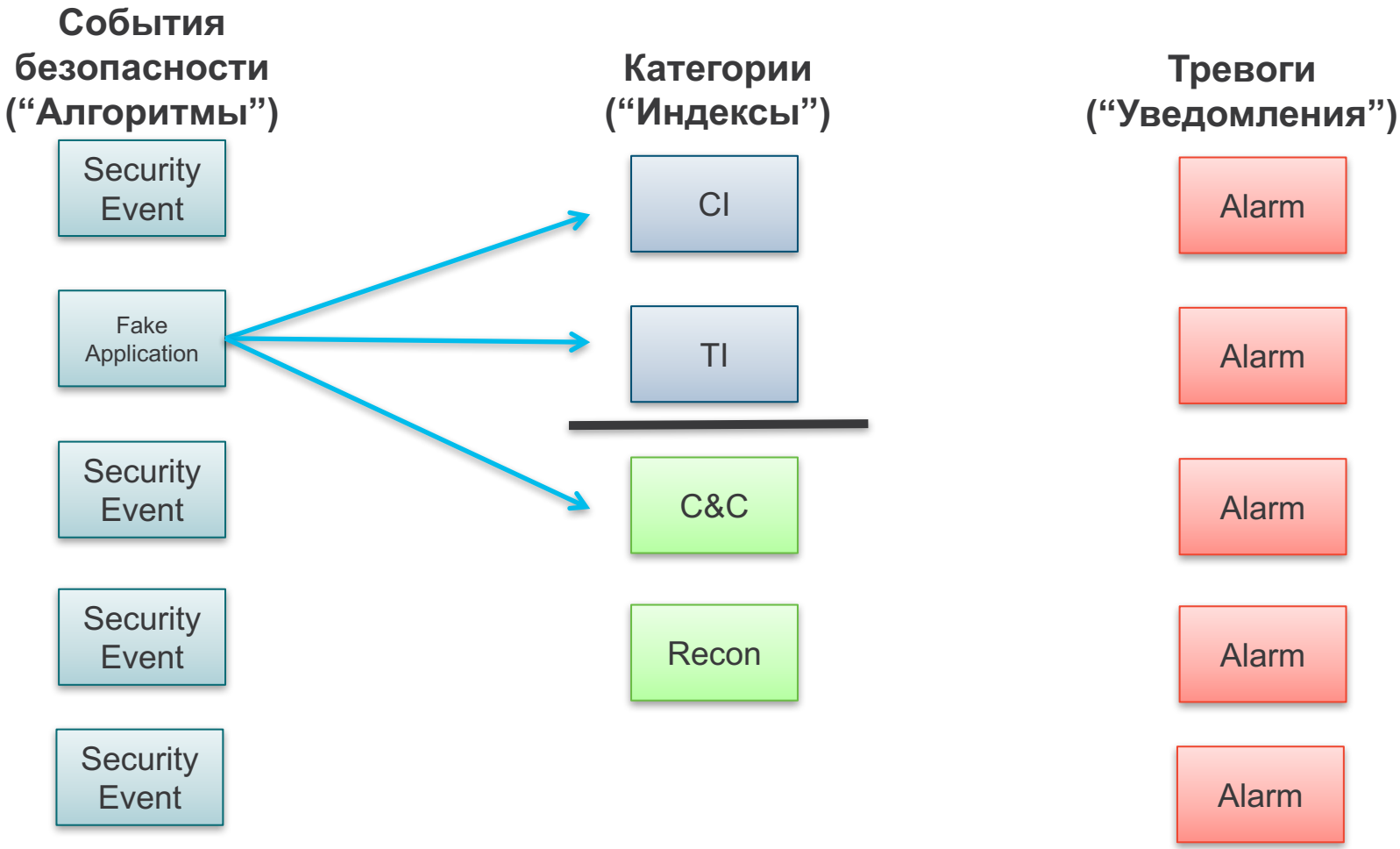
TI

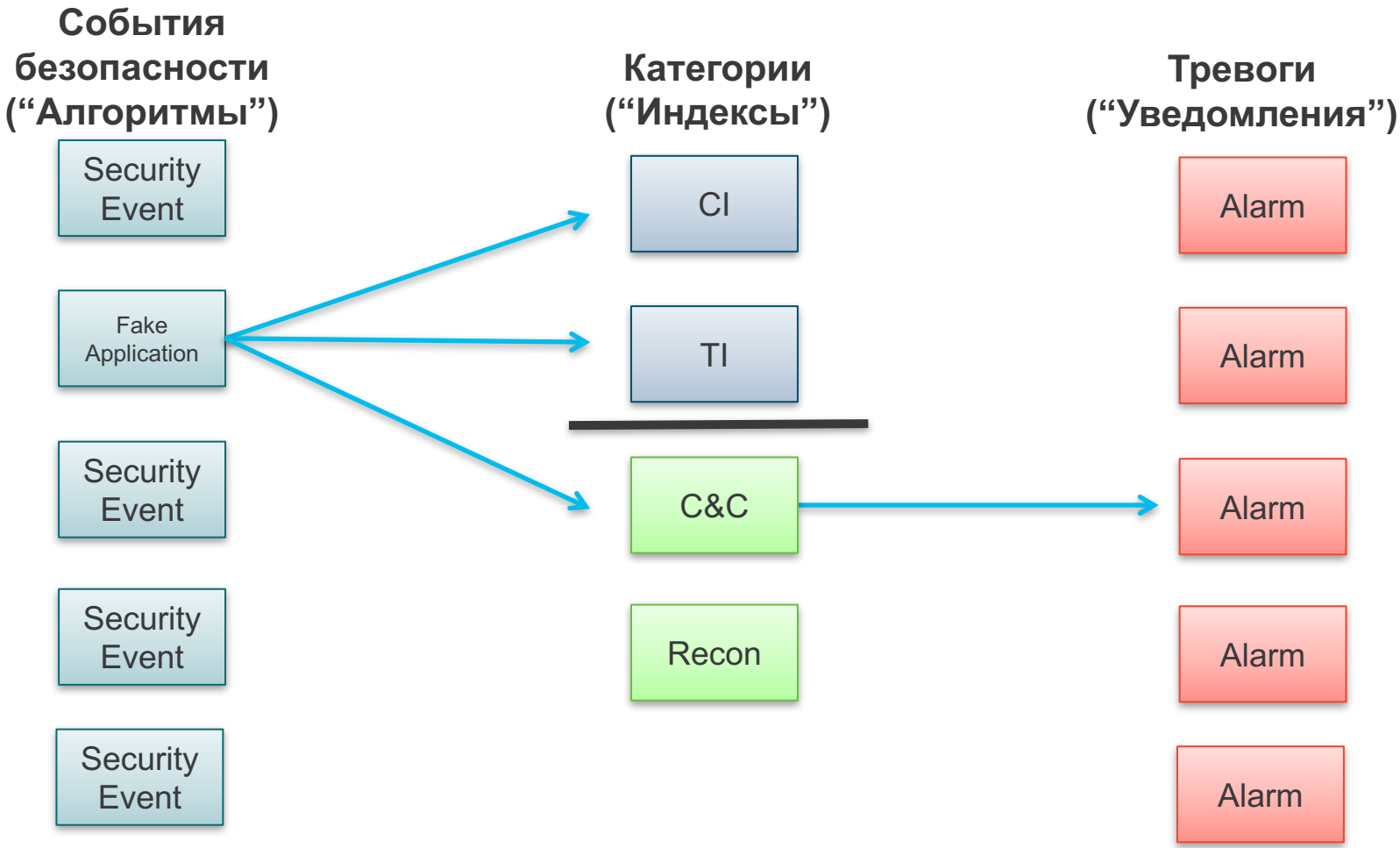
C&C

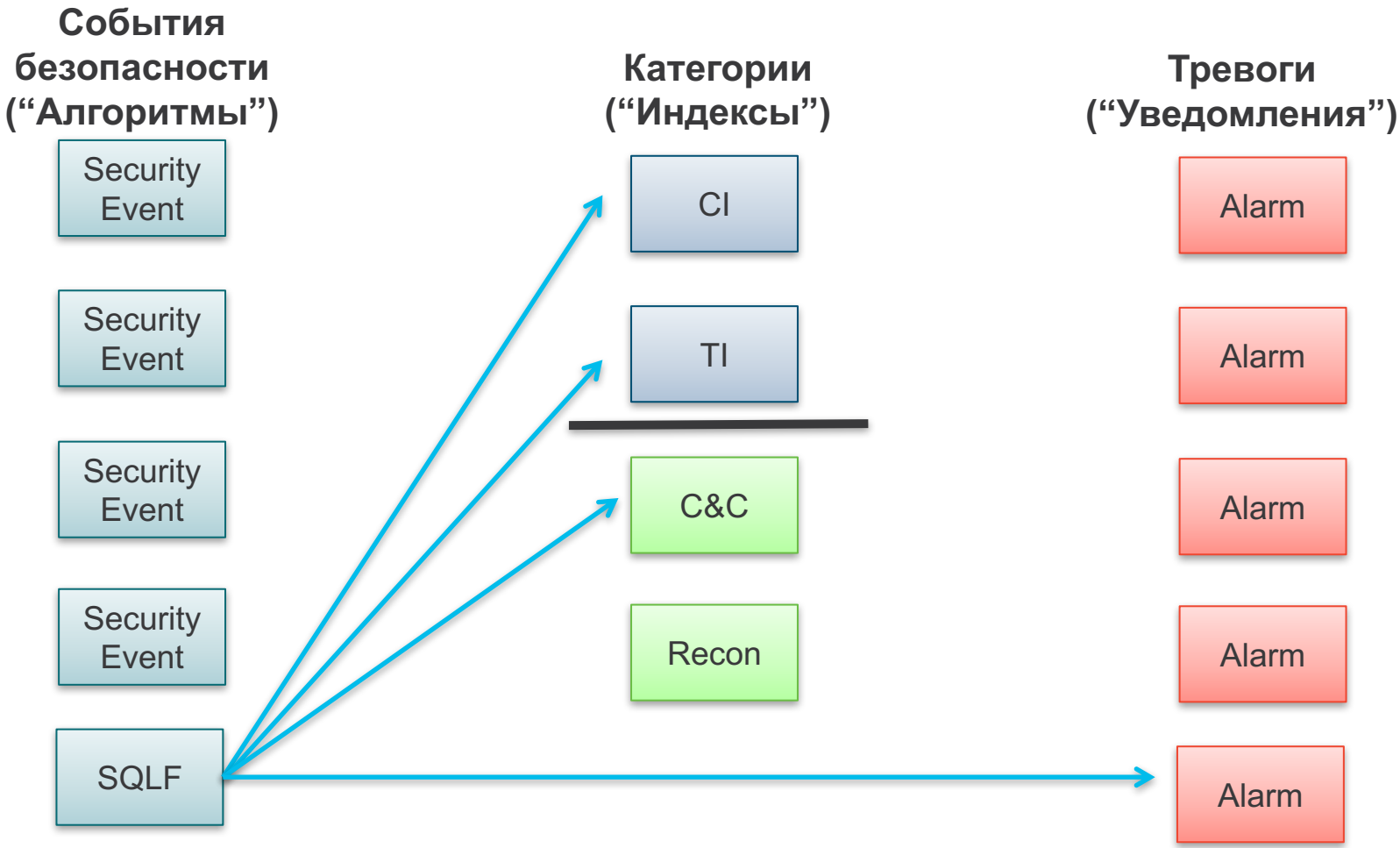
Recon



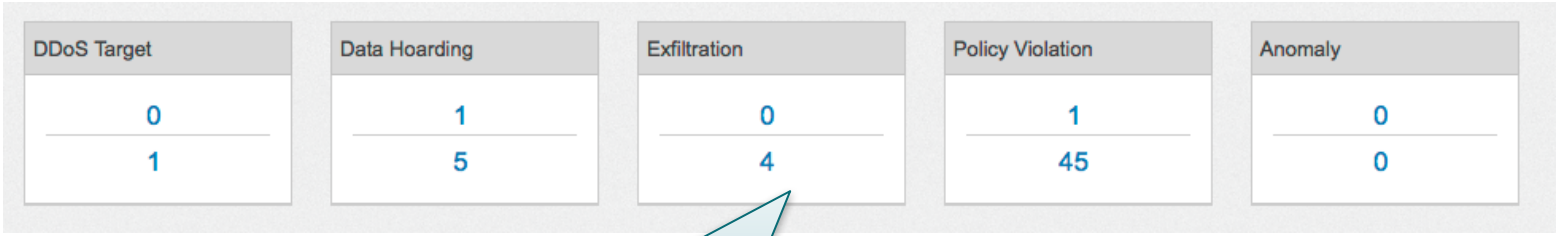








Категории тревог



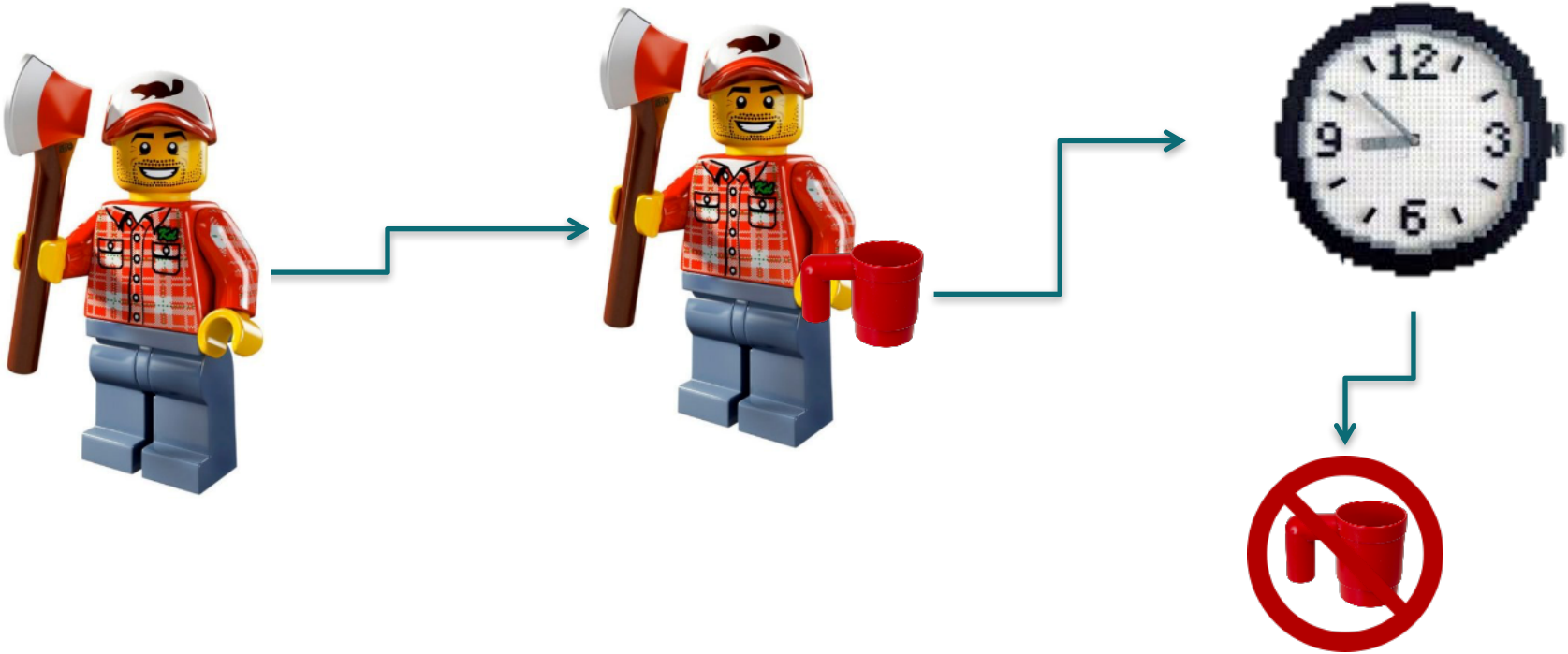
Каждая категория набирает очки

Stealthwatch: Тревоги

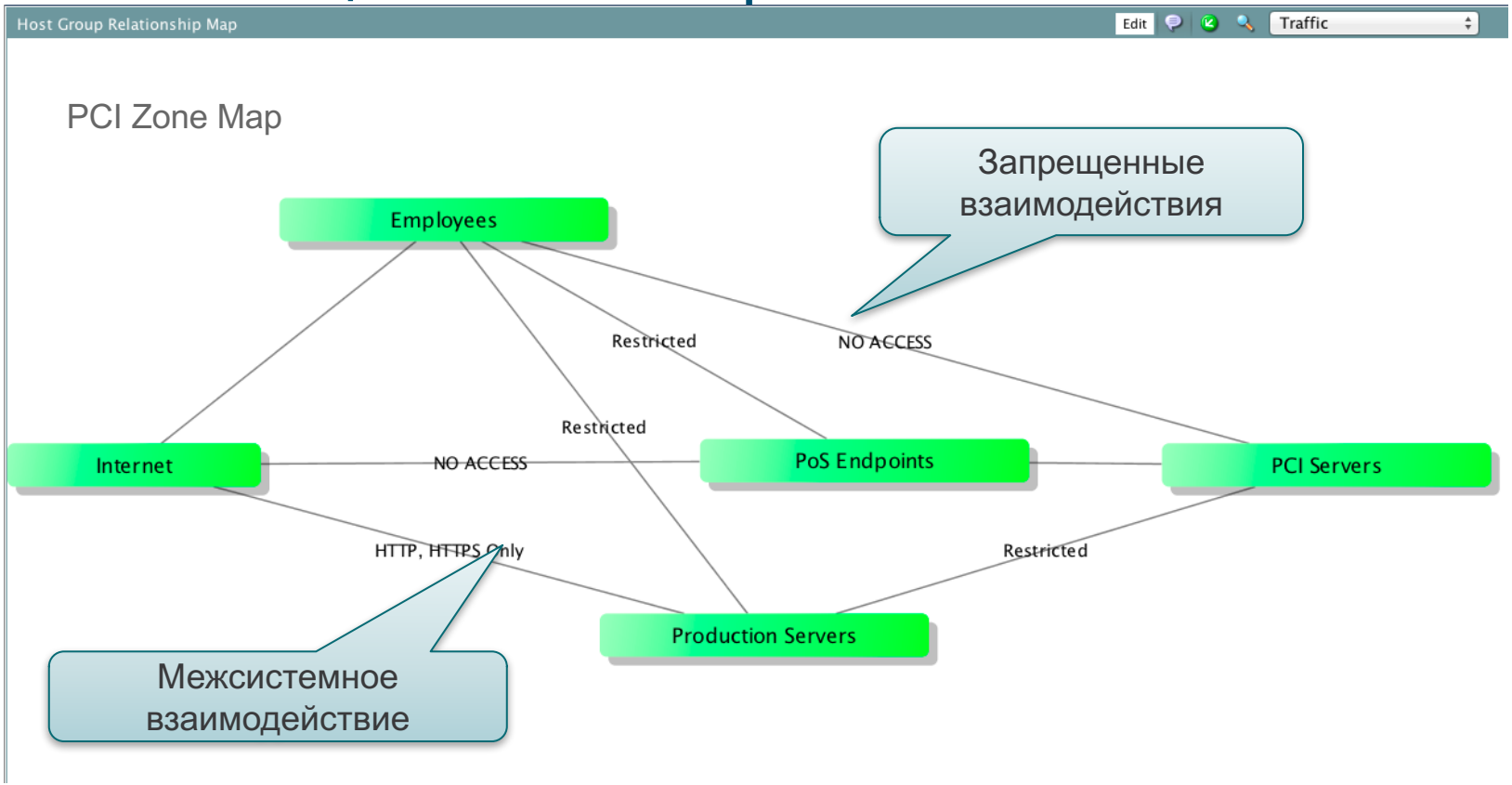
- Показывает серьезные отклонения в поведении и нарушение политики
- Известные и неизвестные атаки генерируют тревоги
- Активность выбивающаяся из нормы, разрешенного поведения или установленных политик

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details
1/19/17 2:15 PM	Datacenter,Atlanta,Terminal Servers	10.201.0.23	--	Multiple Hosts	Suspect Data Loss	10.201.0.23	--	edward	Observed 312.09M bytes. Un-baselined Host. Policy maximum allows up to 200M bytes.

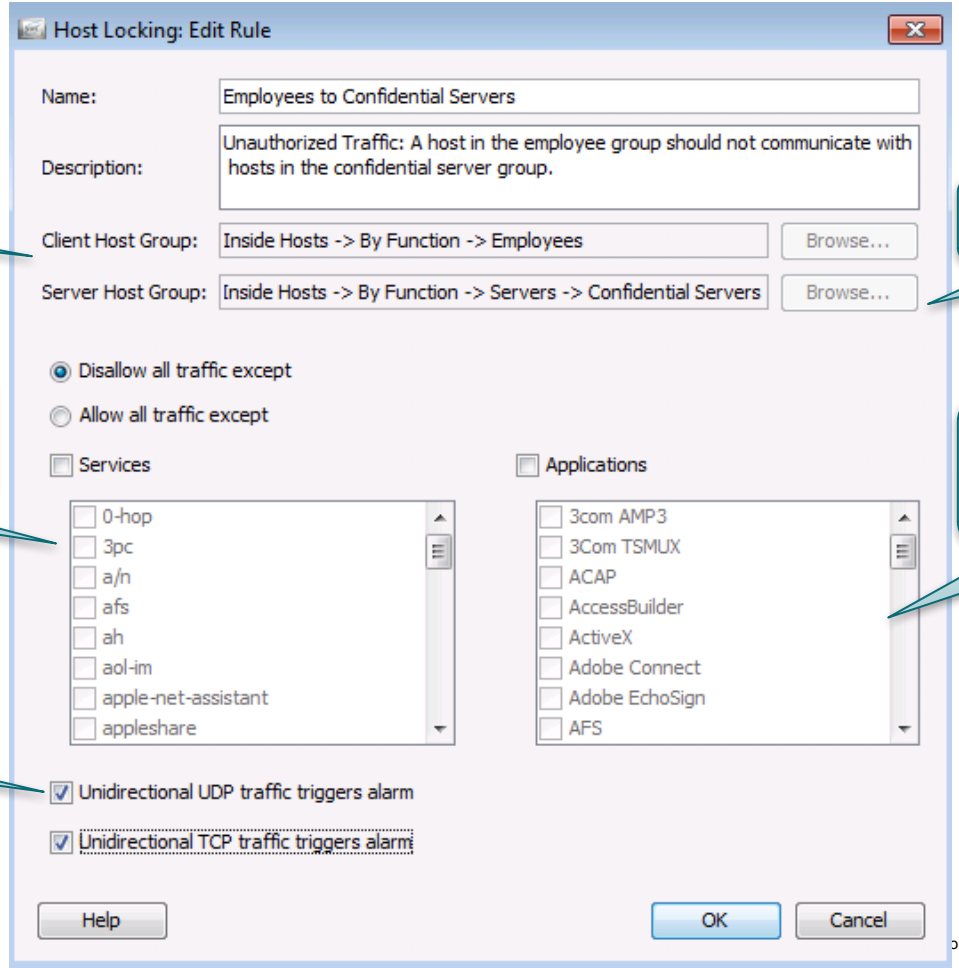
Анализ поведения: Известное плохое поведение



Сегментация и мониторинг



Нарушение политик: Политики хоста



Клиентская группа

Группа серверов

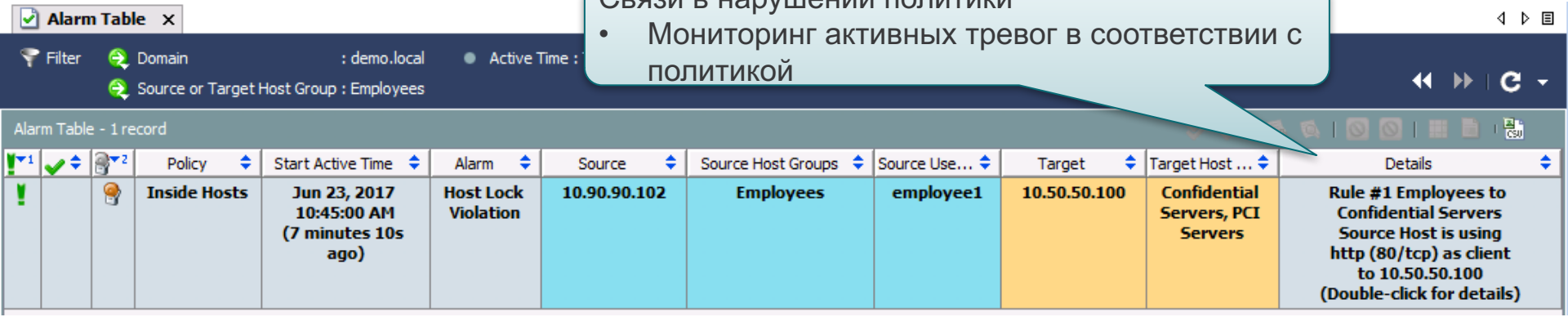
Условия клиентского трафика

Условия Серверного трафика

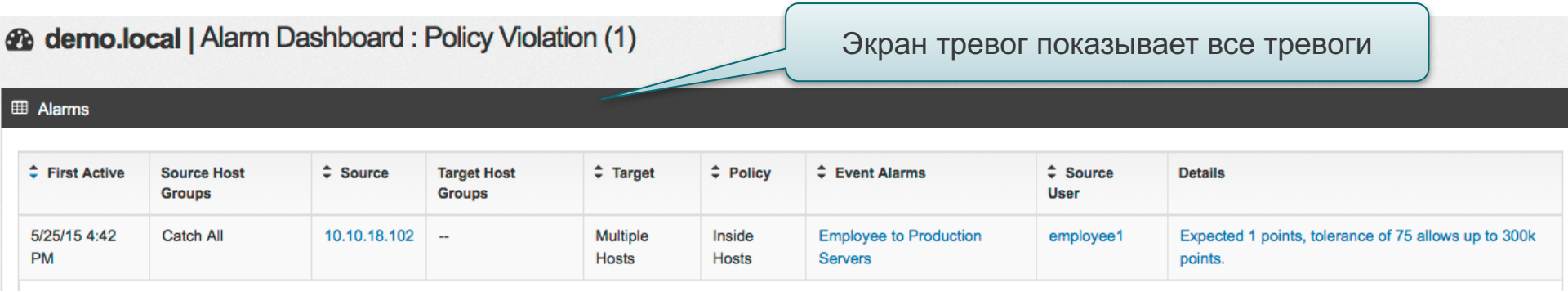
Удачное или неудачное соединение

Нарушение политик: Политики хоста

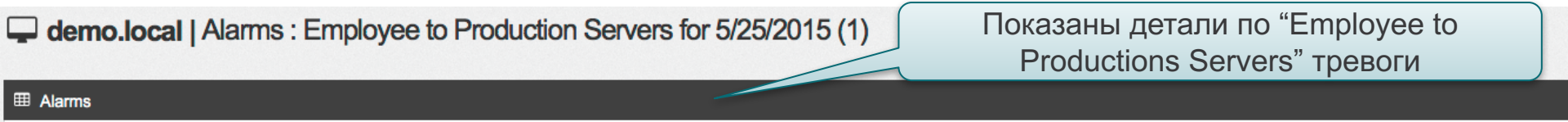
Связи в нарушении политики
- Мониторинг активных тревог в соответствии с политикой



Нарушение политик: Собственные события

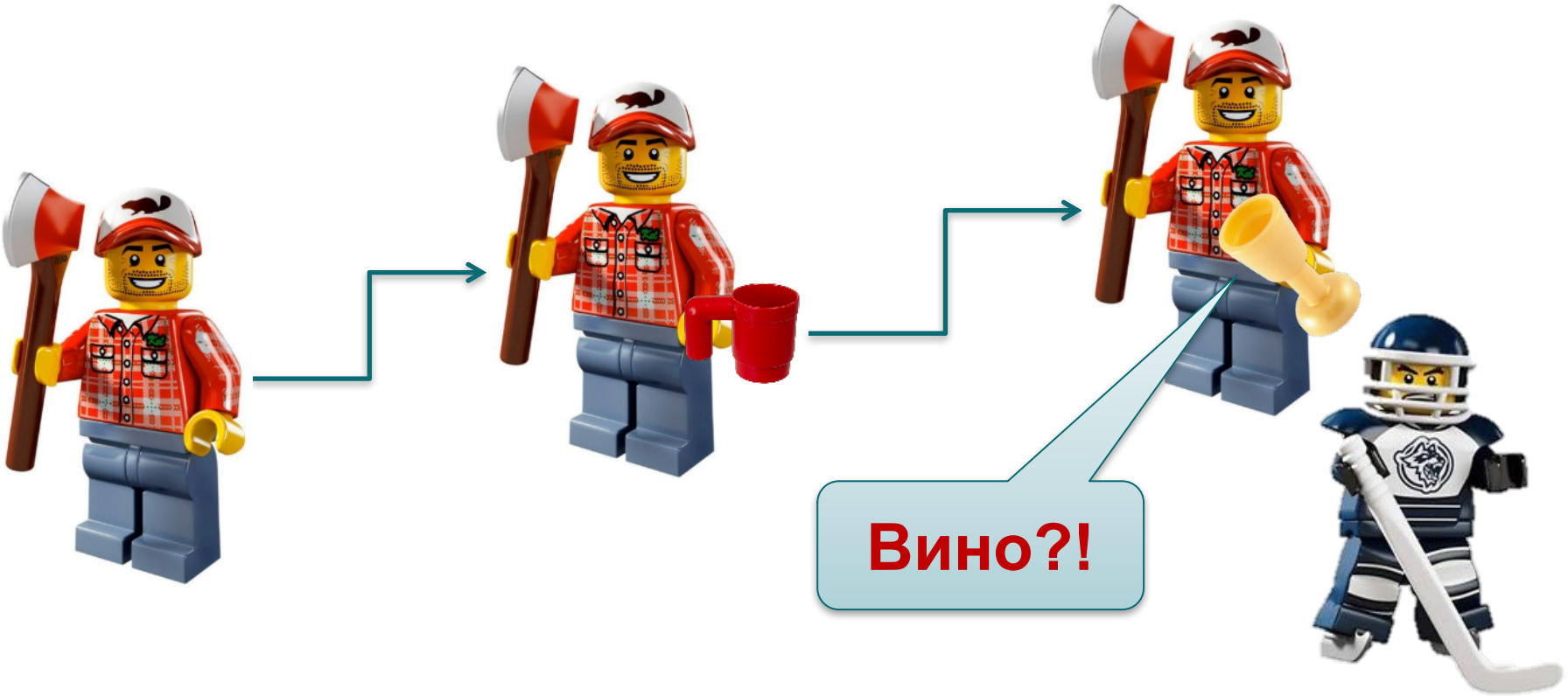


First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
5/25/15 4:42 PM	Catch All	10.10.18.102	--	Multiple Hosts	Inside Hosts	Employee to Production Servers	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.



First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active	Active	Acknowledged
5/25/15 4:42 PM	Catch All	10.10.18.102	Catch All	10.3.200.10	Employee to Production Servers	Inside Hosts	employee1	View Details	Current	Yes	No

Обнаружение аномалий: Отклонение от нормы



Пример категории тревог: Concern Index

Concern Index: Отслеживает хосты, нарушающие целостность сети

Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops, Atlanta	10.10.101.118	313,624,542	3,136%	High Concern Index	Ping, Ping_Scan, TCP_Scan
New York, Desktops	10.50.100.83	190,075,544	1,901%	High Concern Index, High File Sharing Index, High Total Traffic	Ping, Rejects, TCP_Scan

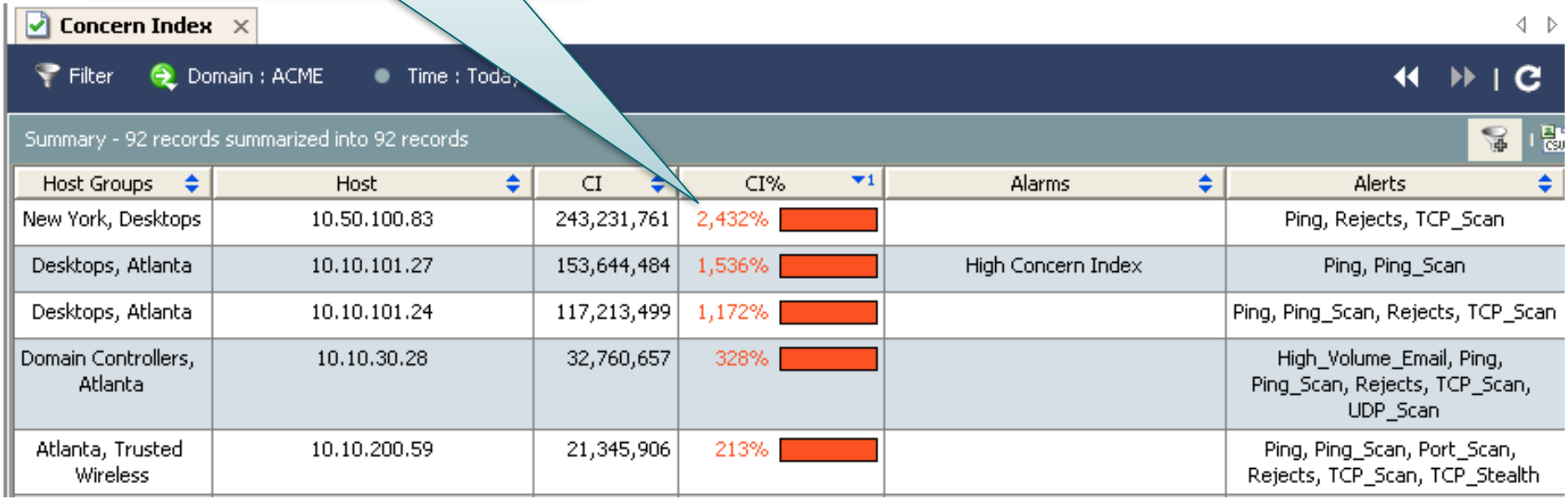
87 различных алгоритмов составляют CI начиная с v6.9.1

Alarm Categories | Security Events

Type	Enabled	Alarm	Alarm Categories	Settings
Addr_Scan/tcp	☑	☐	High Concern Index, Recon	No settings
Addr_Scan/udp	☑	☐	High Concern Index, Recon	No settings
Bad_Flag_ACK	☑	☐	High Concern Index, High Target Index, Anomaly	No settings
Bad_Flag_All	☑	☐	High Concern Index, High Target Index, Anomaly	No settings
Bad_Flag_NoFlg	☑	☐	High Concern Index, High Target Index, Anomaly	No settings
Bad_Flag_Rsrvd	☑	☐	High Concern Index, High Target Index, Anomaly	No settings
Bad_Flag_RST	☑	☐	High Concern Index, High Target Index, Anomaly	No settings
Bad_Flag_SYN_FIN	☑	☐	High Concern Index, High Target Index,	No settings

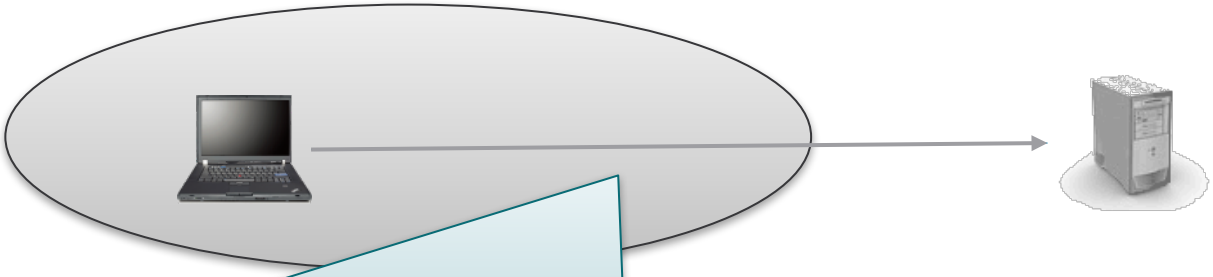
High Concern Index

Отклонение от базового уровня на 2,432%!



Host Groups	Host	CI	CI%	Alarms	Alerts
New York, Desktops	10.50.100.83	243,231,761	2,432%		Ping, Rejects, TCP_Scan
Desktops, Atlanta	10.10.101.27	153,644,484	1,536%	High Concern Index	Ping, Ping_Scan
Desktops, Atlanta	10.10.101.24	117,213,499	1,172%		Ping, Ping_Scan, Rejects, TCP_Scan
Domain Controllers, Atlanta	10.10.30.28	32,760,657	328%		High_Volume_Email, Ping, Ping_Scan, Rejects, TCP_Scan, UDP_Scan
Atlanta, Trusted Wireless	10.10.200.59	21,345,906	213%		Ping, Ping_Scan, Port_Scan, Rejects, TCP_Scan, TCP_Stealth

Пример события: Suspect Quiet Long Flow



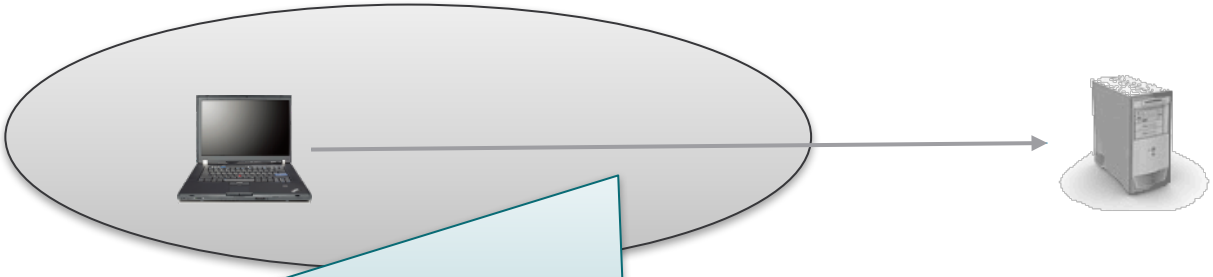
Соединение между внутренней и внешней сетью (с трафиком в обе стороны), которое превышает длительность “Секунды для квалификации потока как длинного” и передает подозрительно маленький объем информации

Политика по-умолчанию

Seconds required to qualify a flow as long duration: 32.4k

Type	Enable Source	Alarm Source	Enable Target	Alarm Target	Alarm Categories	Settings	Mitigation
Suspect Quiet Long Flow	☑	☐	☑	☐	Command & Control, High Target Index, High Concern Index	No settings	None

Пример события: Suspect Data Loss



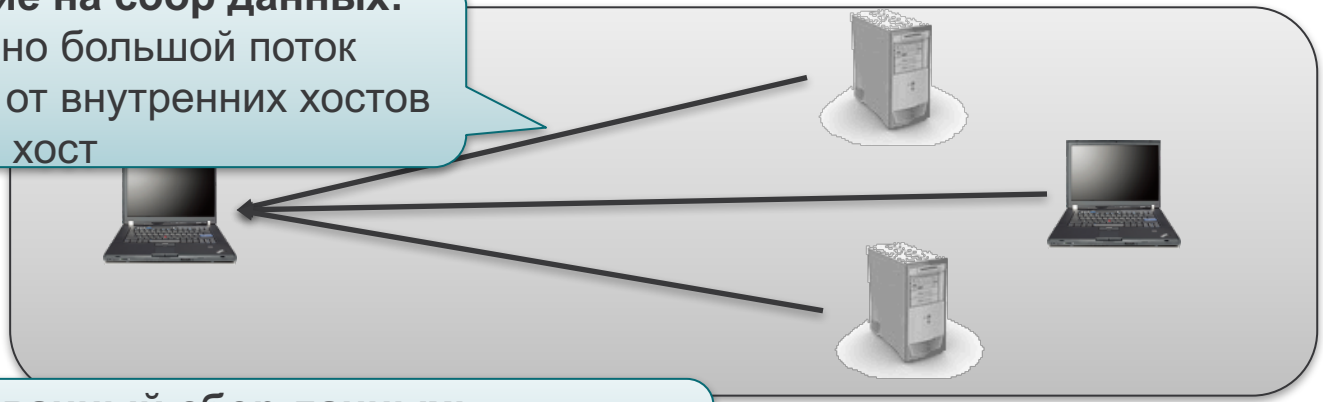
Указывает что внутренний хост выгрузил необычно большое количество данных наружу.

Политика по-умолчанию

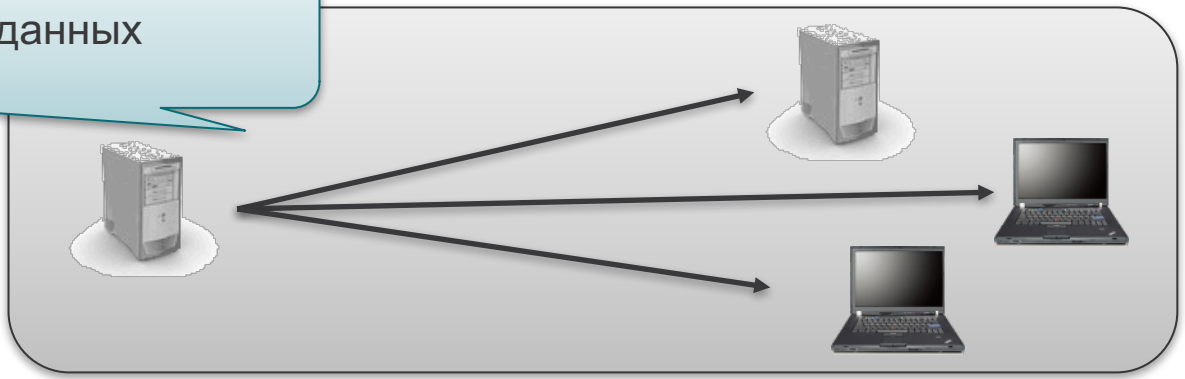
Type	Enable Source	Alarm Source	Enable Target	Alarm Target	Alarm Categories	Settings	Mitigation
Suspect Data Loss	☑	☑	☑	☐	Data Exfiltration, High Concern Index	Tolerance: **75** Never trigger alarm when less than: **1G** client payload bytes in 24 hours Always trigger alarm when greater than: **5T** client payload bytes in 24 hours	None

Пример алгоритма: Data Hoarding

Подозрение на сбор данных:
- Необычно большой поток данных от внутренних хостов на один хост



Таргетированный сбор данных:
- Необычно большой объем данных исходящий намногие хосты



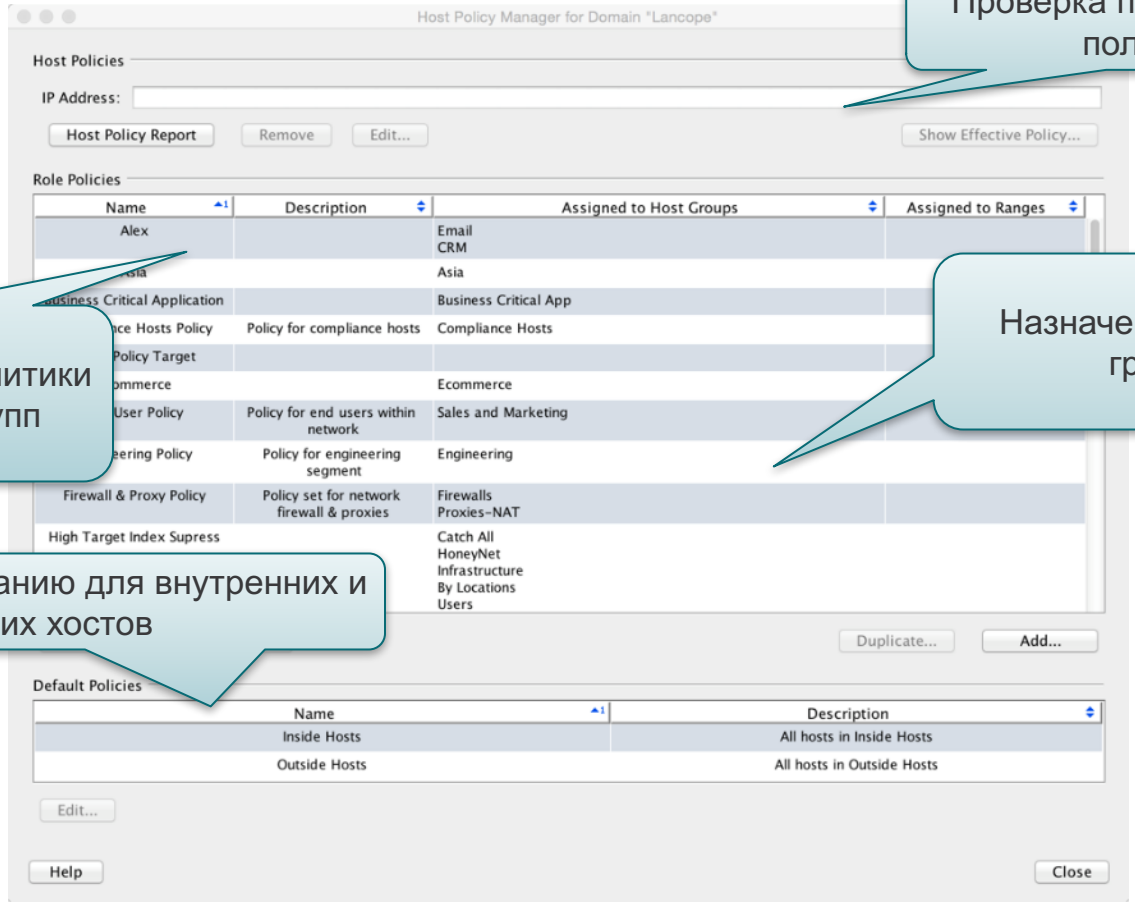
Suspect Data Hoarding

Сбор данных

- Необычно большой поток данных от внутренних хостов на один хост
- Политики и поведение

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active
5/29/15 12:00 PM	Atlanta, Sales and Marketing, Desktops	10.201.3.18	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.18	--	Observed 23.9G bytes. Policy maximum allows up to 50M bytes.	5/29/15 1:05 PM
5/29/15 11:20 AM	Terminal Server, Datacenter	10.201.0.23	--	Multiple Hosts	Suspect Data Hoarding	10.201.0.23	--	Observed 38.45G bytes. Policy maximum allows up to 50M bytes.	5/29/15 2:40 PM

Менеджер политик хостов



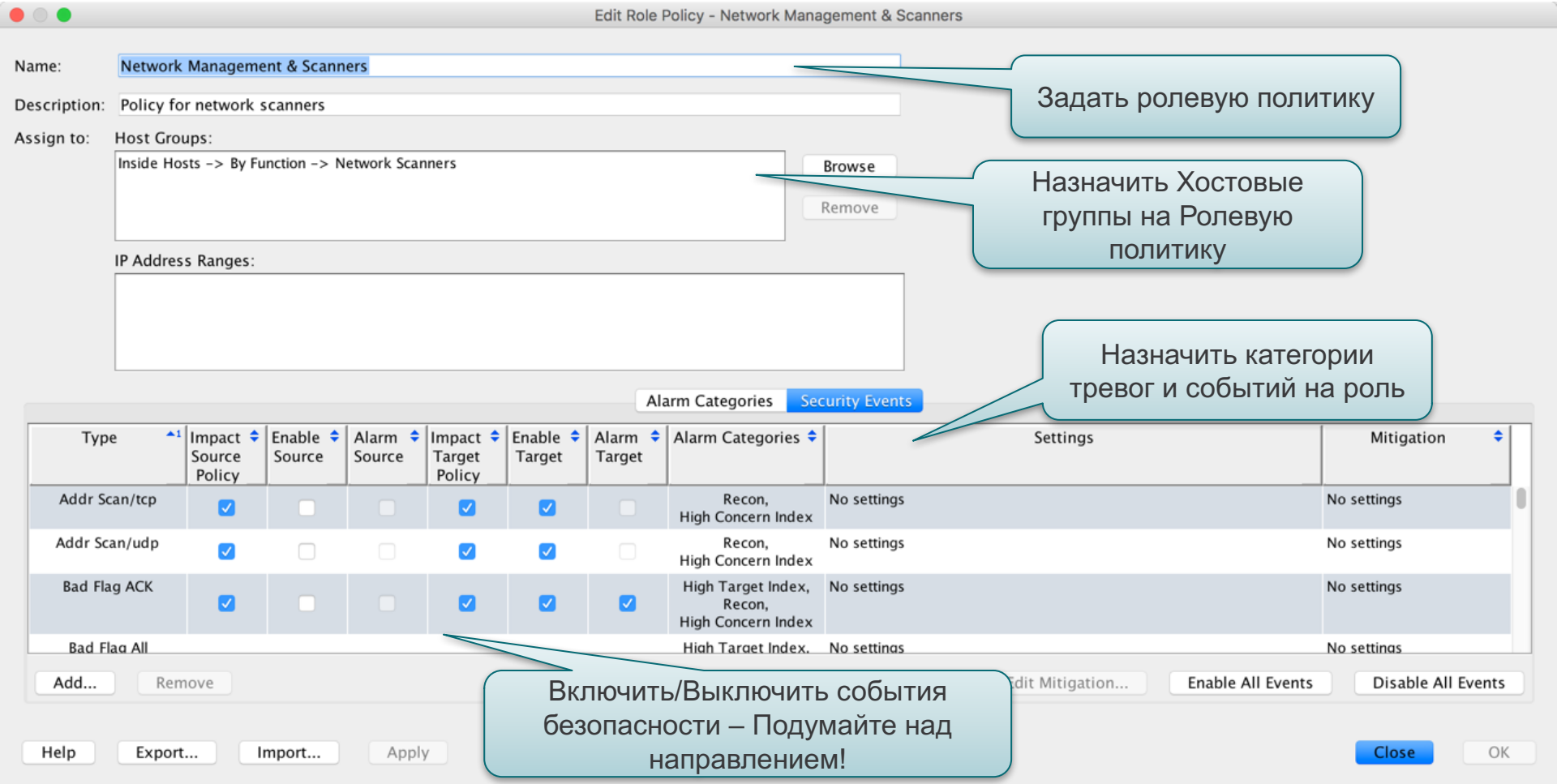
Проверка применяемых политик

Создать ролевые политики для отдельных групп

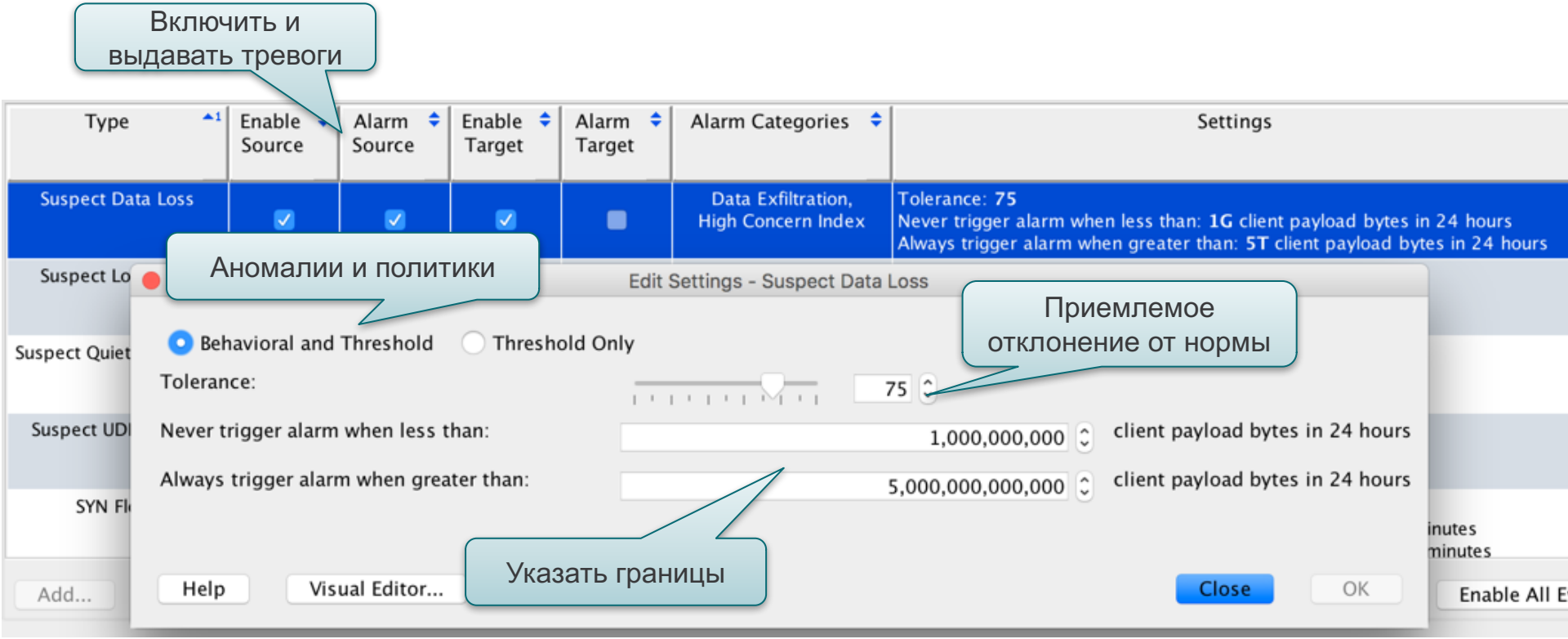
Назначение политики группам

Политики по-умолчанию для внутренних и внешних хостов

Создание и изменение ролевой политики



Установка граничных значений событий



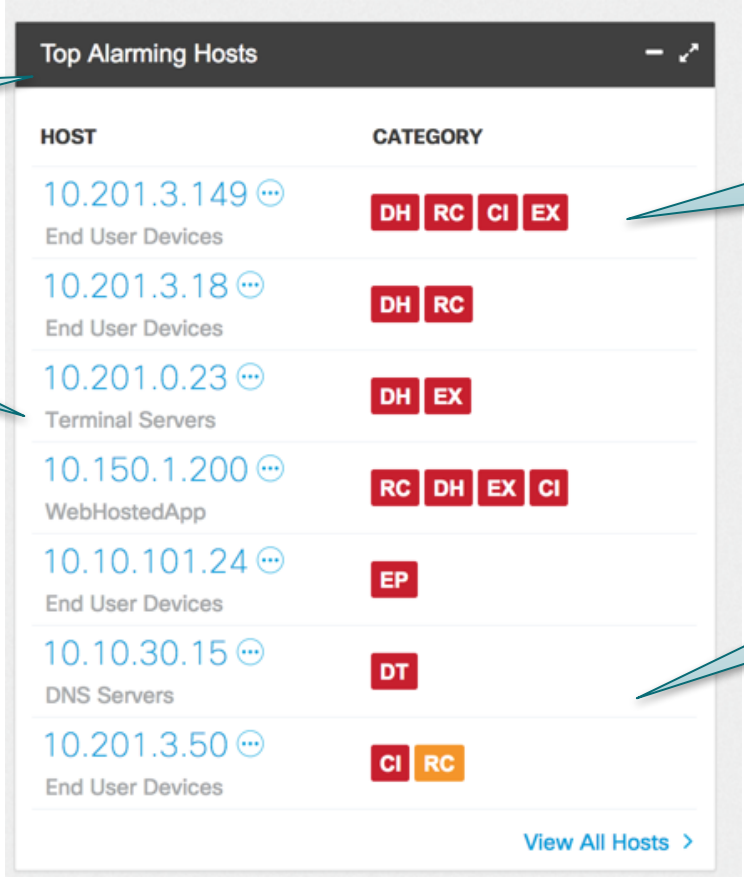
Реагирование на обнаружение аномалий

Ранжирование по приоритету

Используется классификация!

Этот хост НАИБОЛЕЕ странно себя ведет

Работаем сверху вниз



Программа

- Введение
- Использование сетевой телеметрии
- Организация данных
- Обнаружение Индикаторов Компрометации
- Расследование вторжения

Расследование вторжения

1. Понимать предыдущие шаги
2. Мониторинг и контроль происходящего вторжения

“Наука о дедукции.”
Глава 1: Знак четырёх

Наука о дедукции

Сбор улик

IOC

Что они смогли получить?

Куда они смогли пробраться?

Когда они получили туда доступ?

Элементы данных

Кто они?

Они все еще здесь?

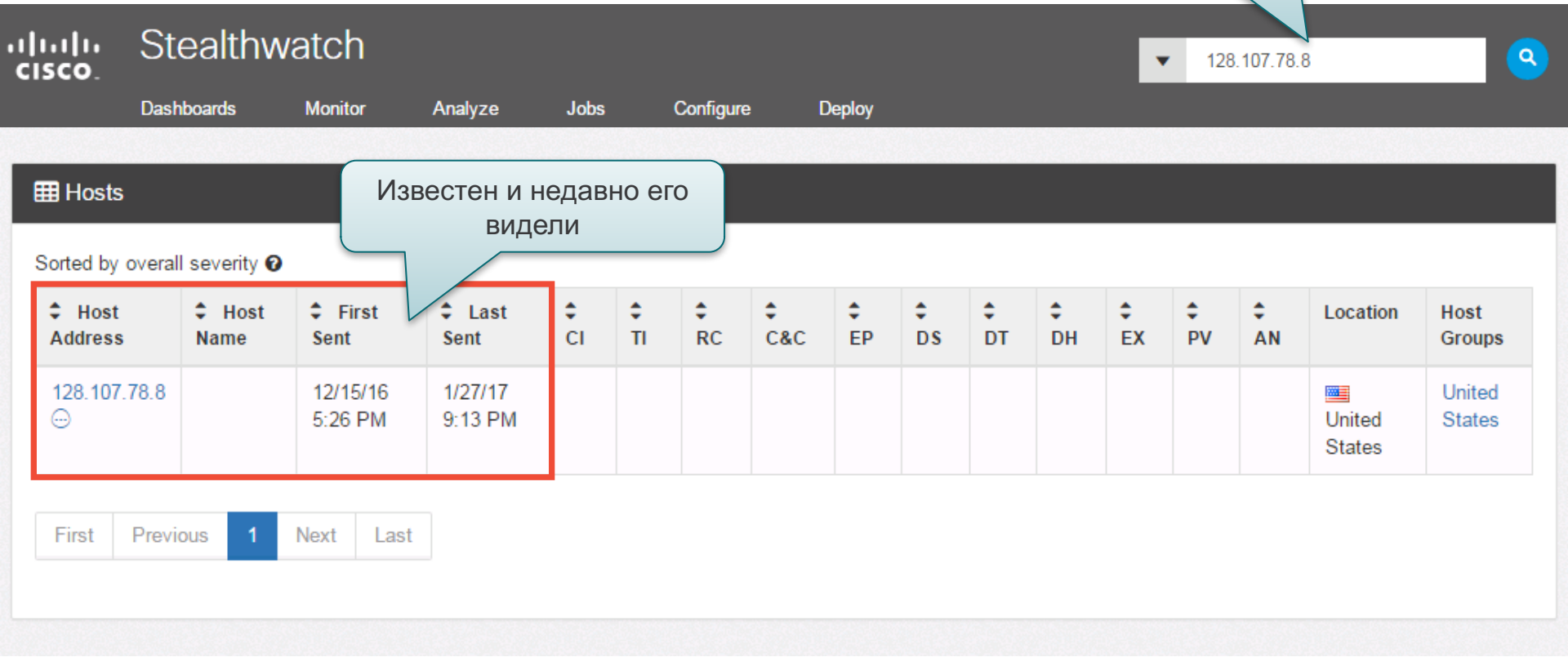
Расследование IOC: Пример

Обнаружен новый сервер Malware!

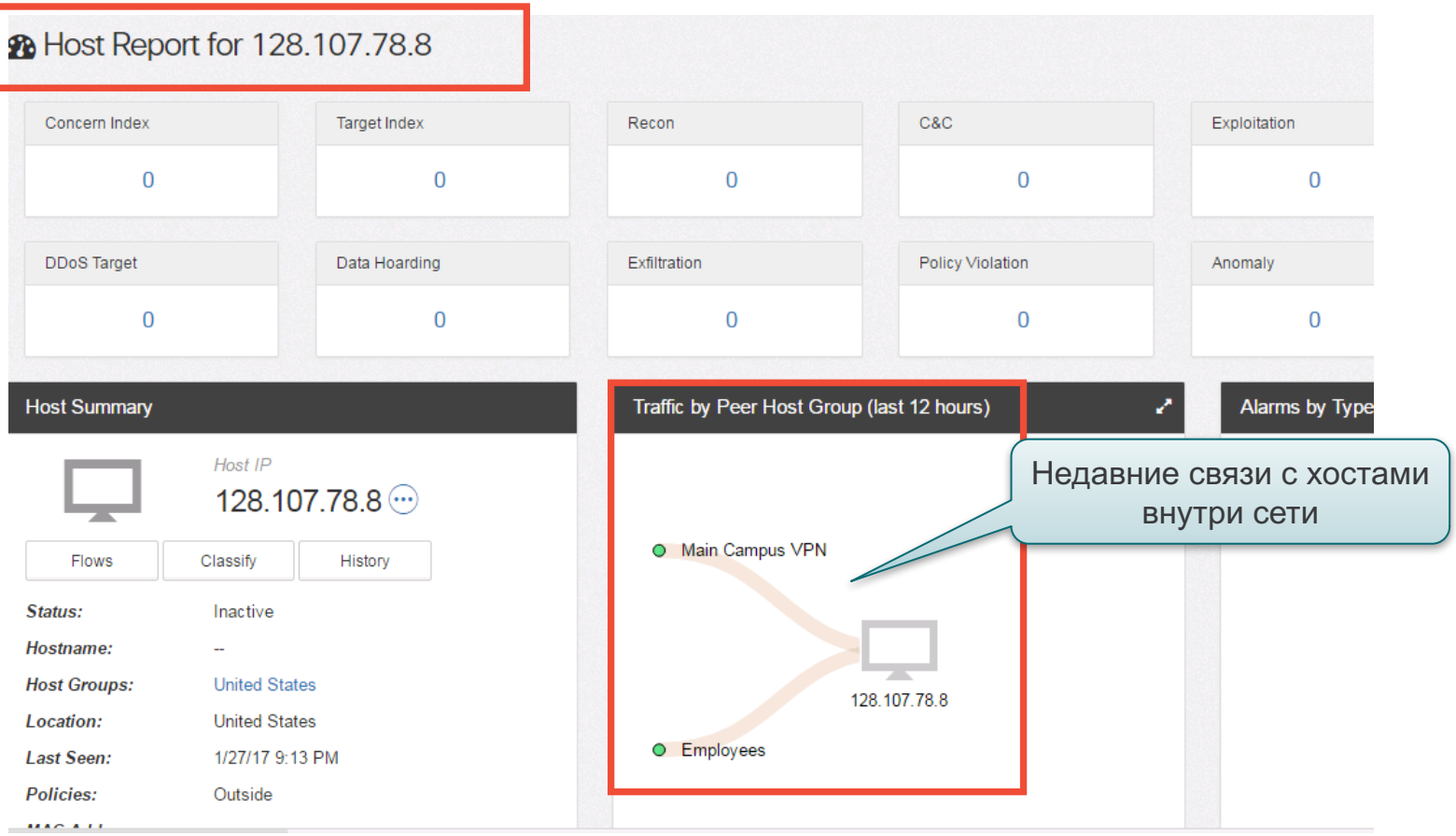
Zeus C&C Server:
128.107.78.8

Шаг 1: Мы этот хост видели?

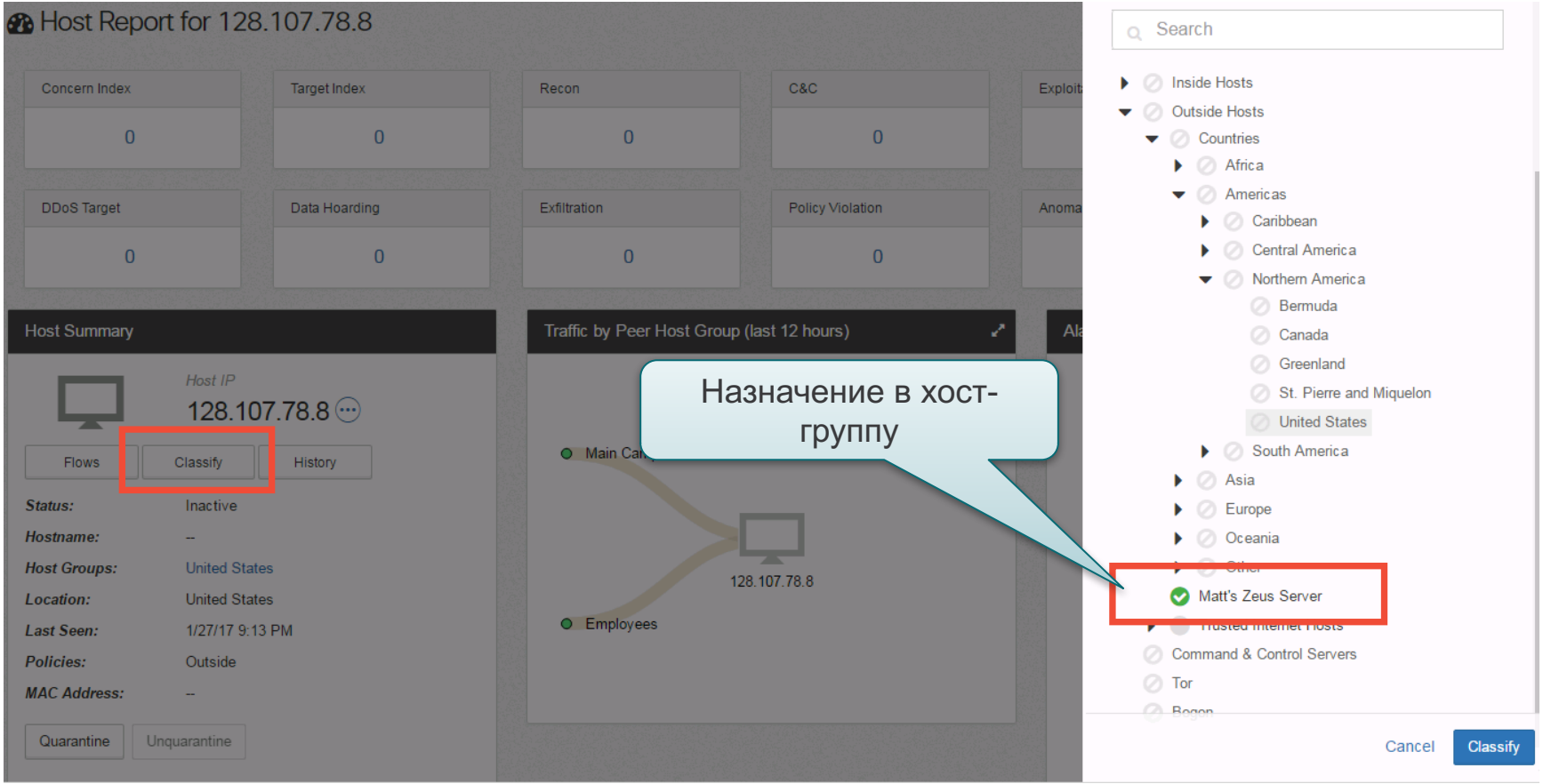
Ищем по IP адресу



Шаг 2: Расследование вторжения

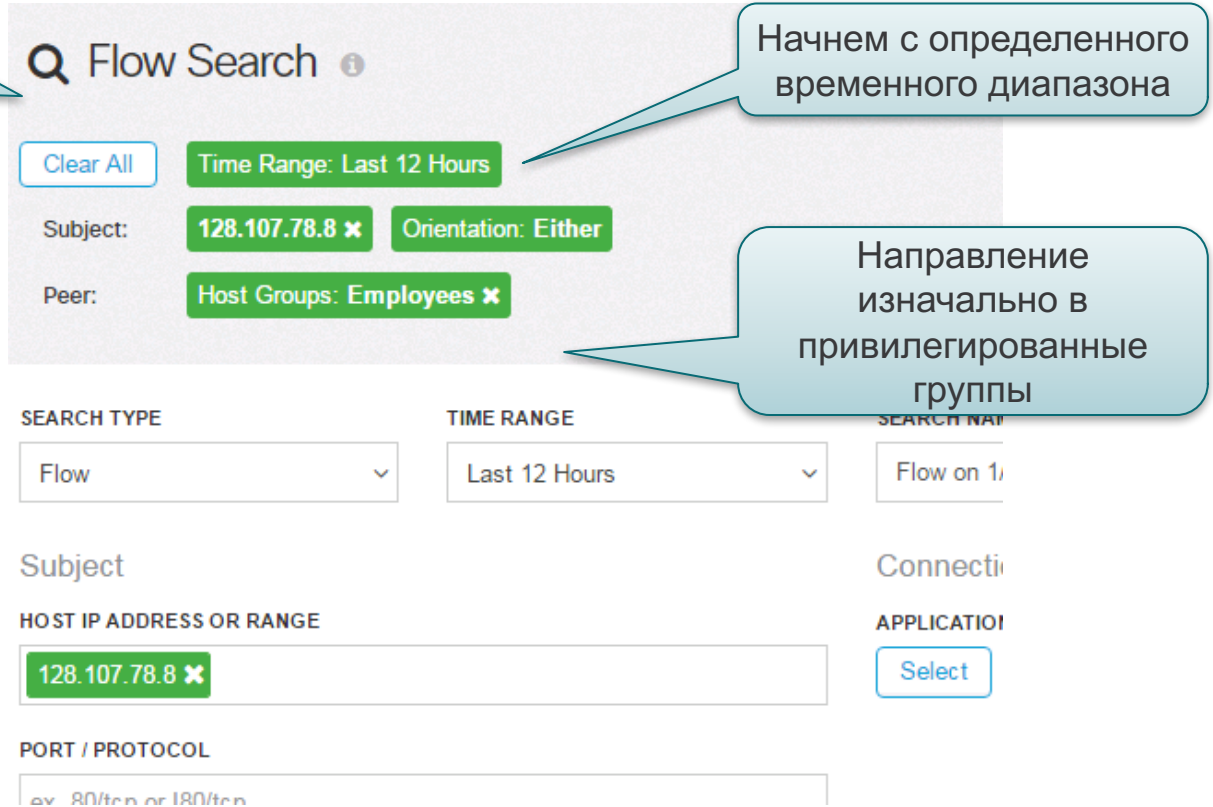


Шаг 2: Классификация



Шаг 3: Поиск инфицированных хостов

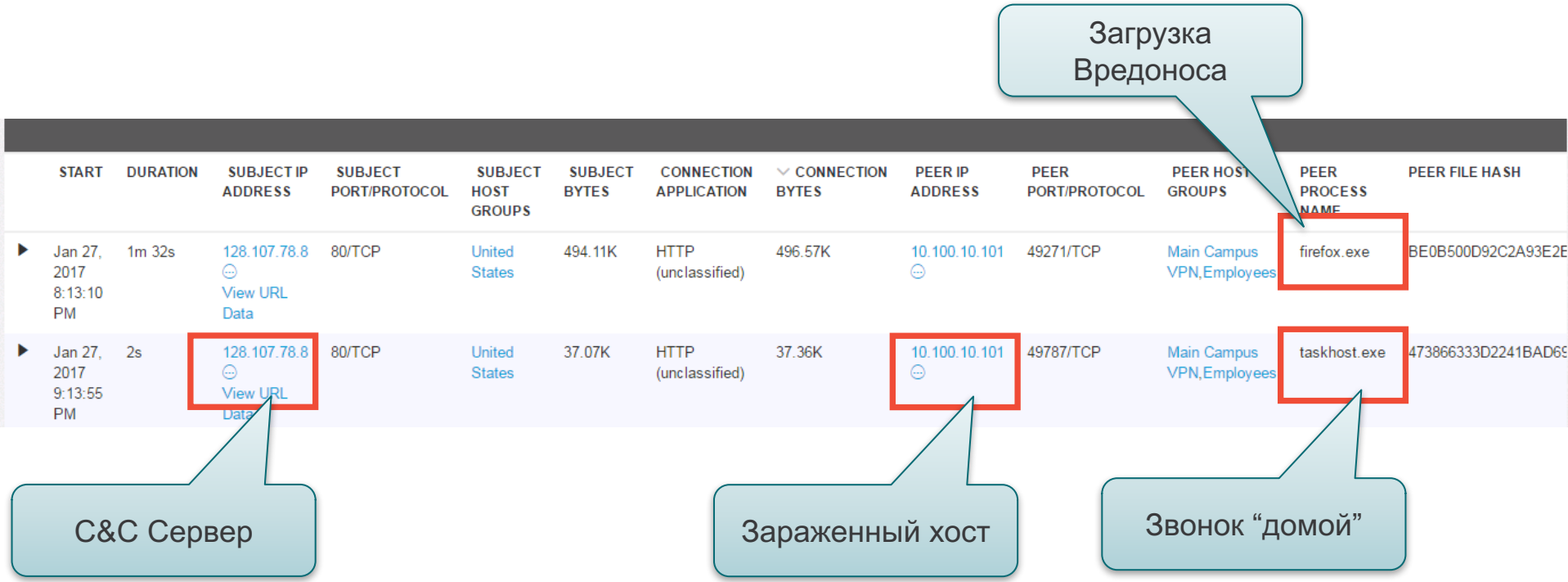
Построение запроса потока, включающего C&C Сервер



Начнем с определенного временного диапазона

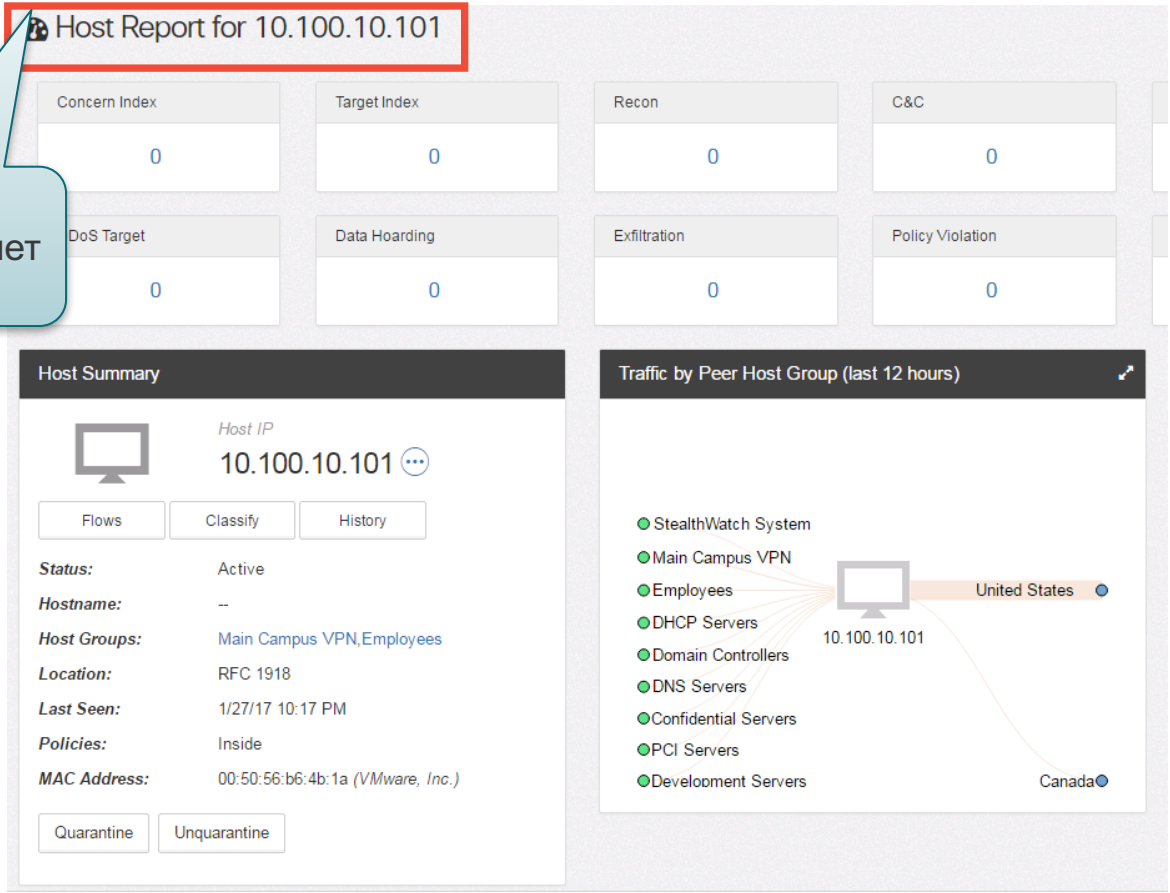
Направление изначально в привилегированные группы

Шаг 4: Анализ возвращенных результатов

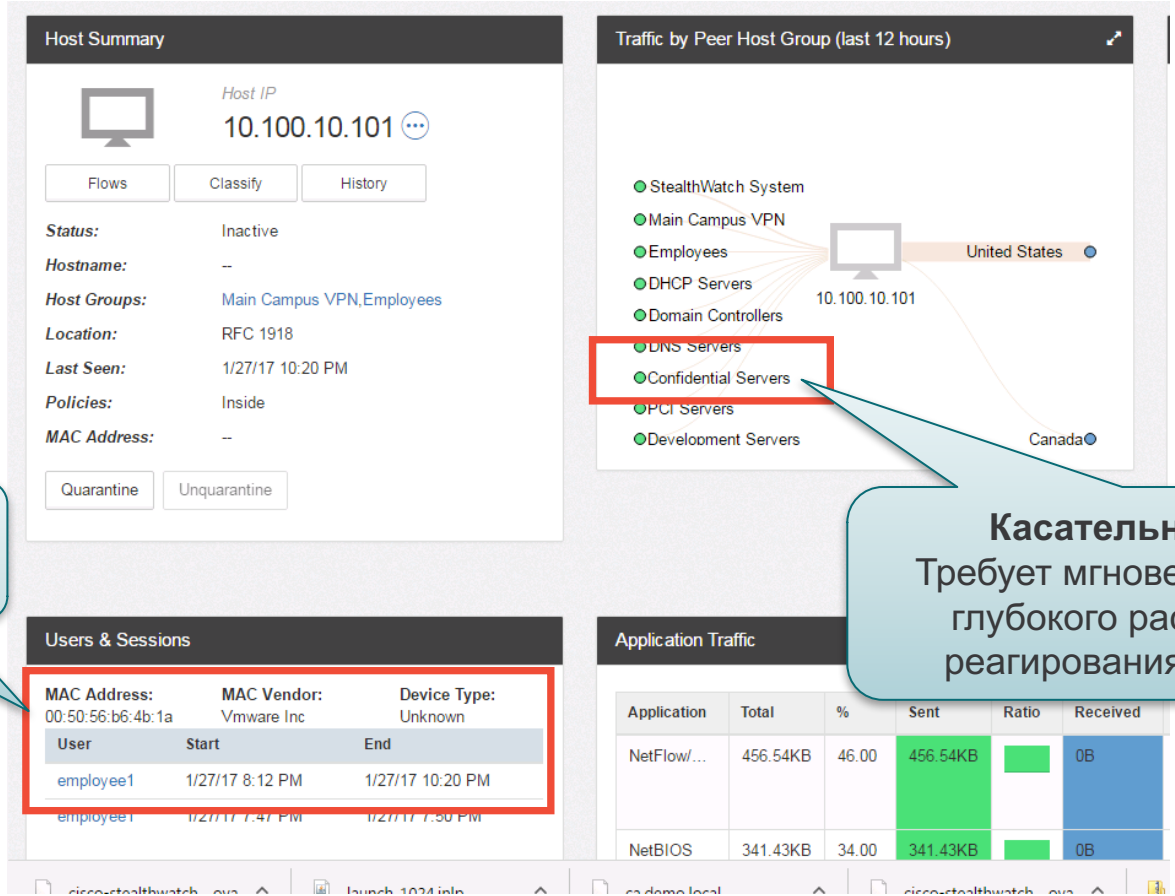


Шаг 5: Расследование зараженных хостов

Открыть и исследовать отчет хоста



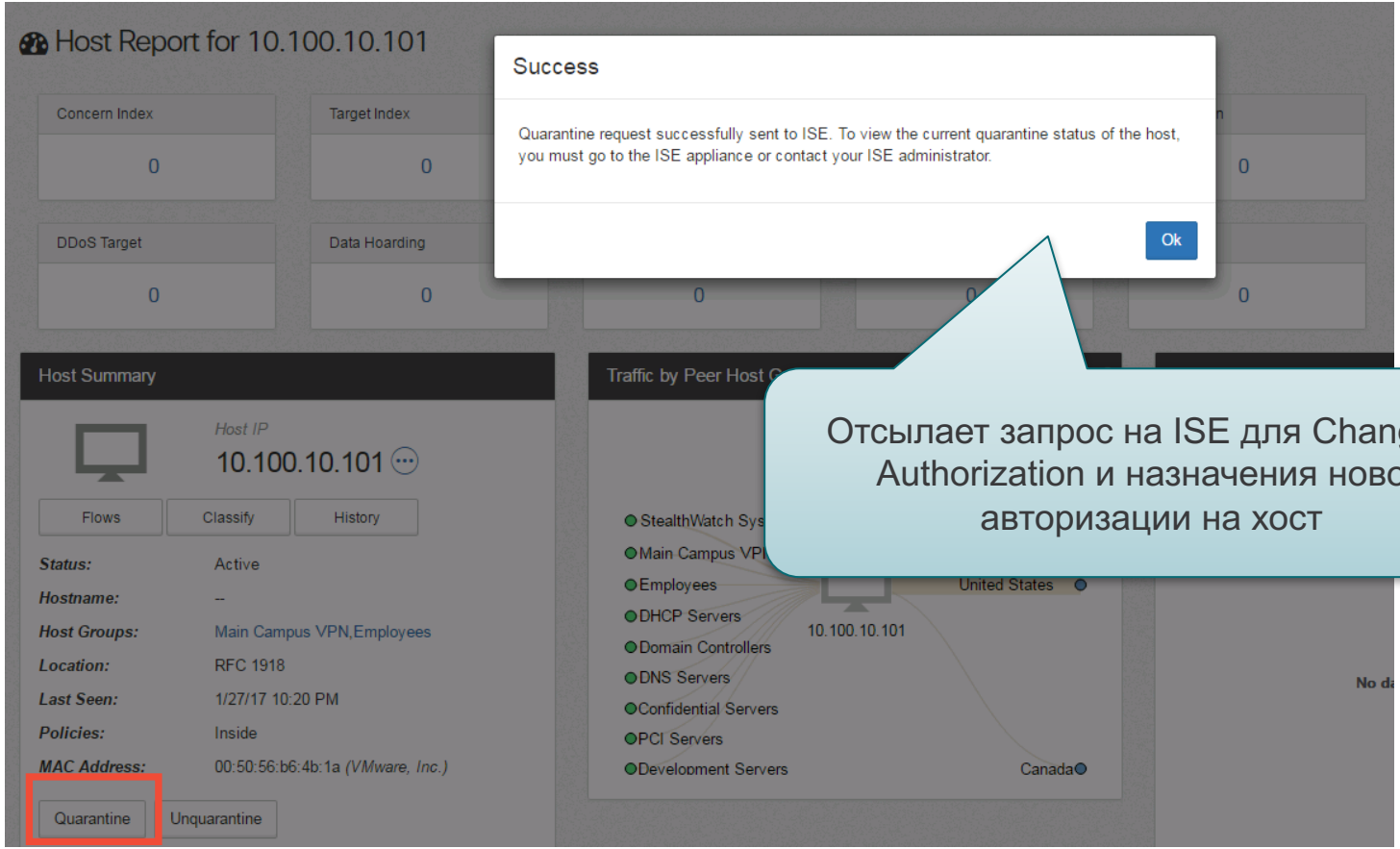
Шаг 5: Расследование инфицированных хостов



Определение пользователя и устройства

Касательно ущерба: Требует мгновенной реакции и глубокого расследования, реагирования на инцидент

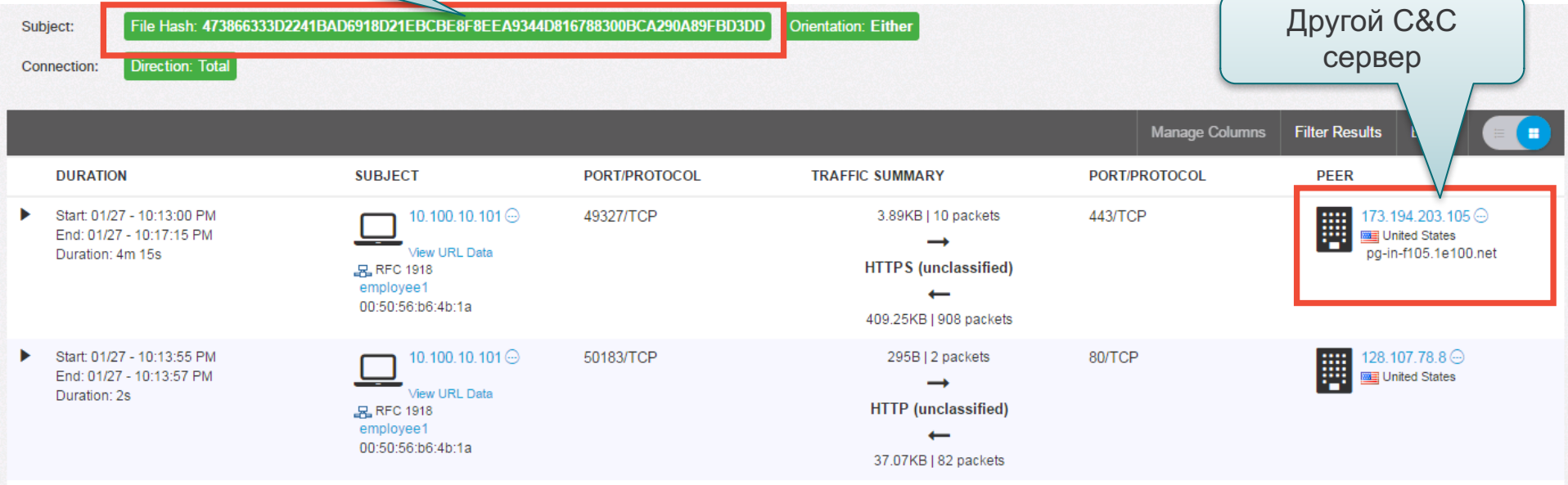
Шаг 6: Rapid Threat Containment



Отсылает запрос на ISE для Change of Authorization и назначения новой авторизации на хост

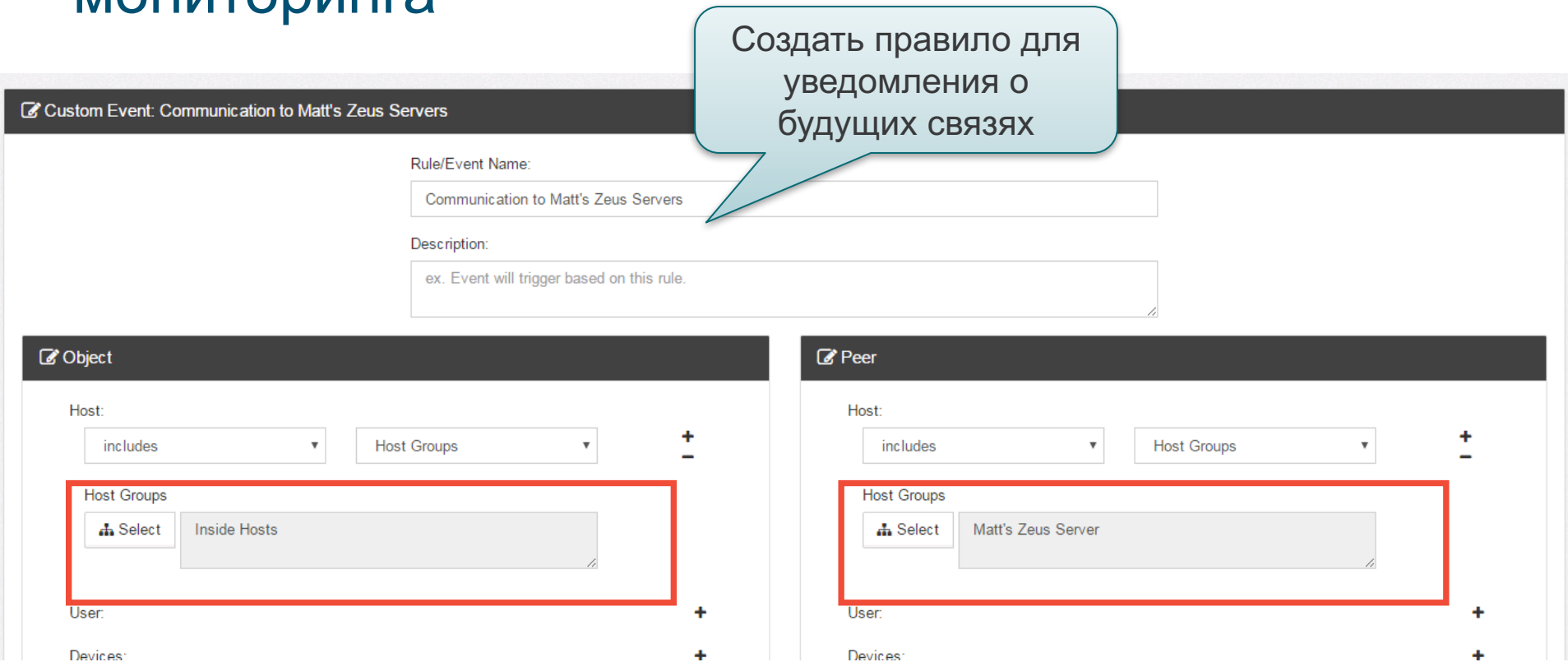
Шаг 7: Продолжение расследовани и мониторинг

Поиск Malware по его хэшу

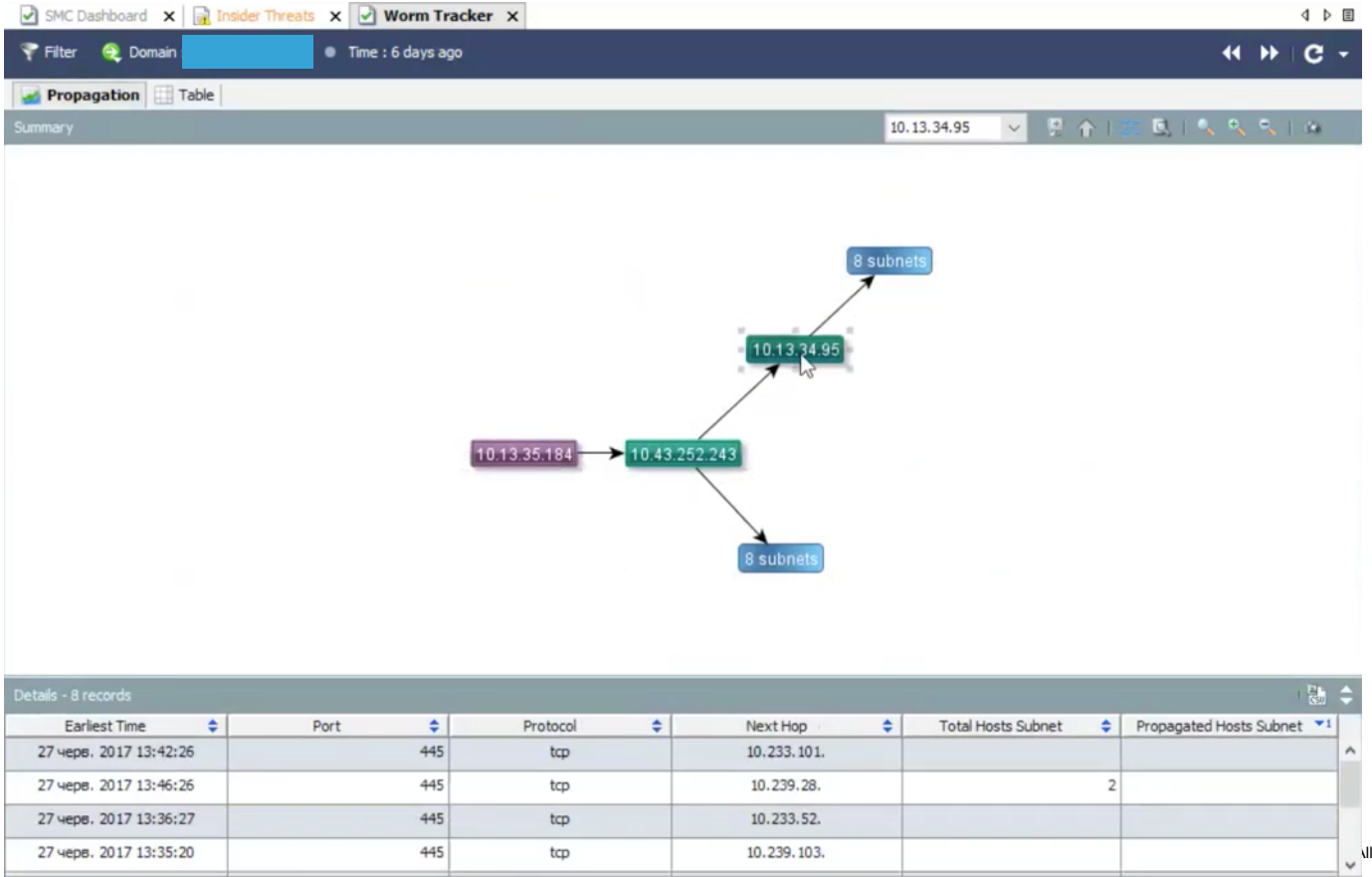


Другой C&C сервер

Шаг 7: Продолжение расследования и мониторинга

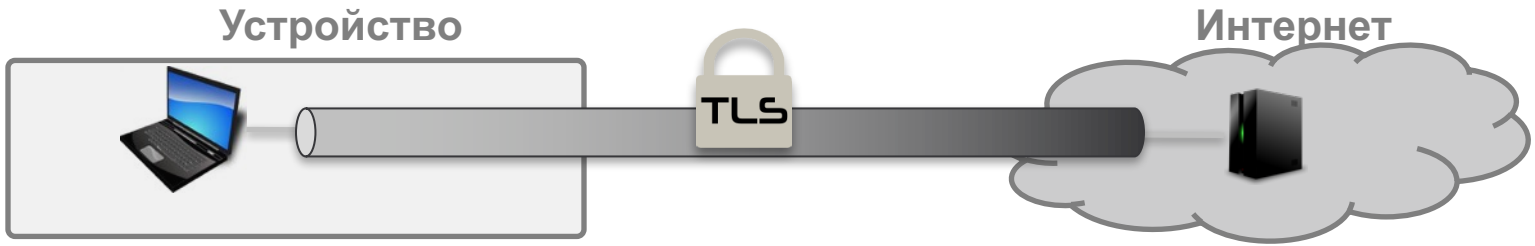


Решение Cisco StealthWatch в анализе атаки Pyetya/Nyetya



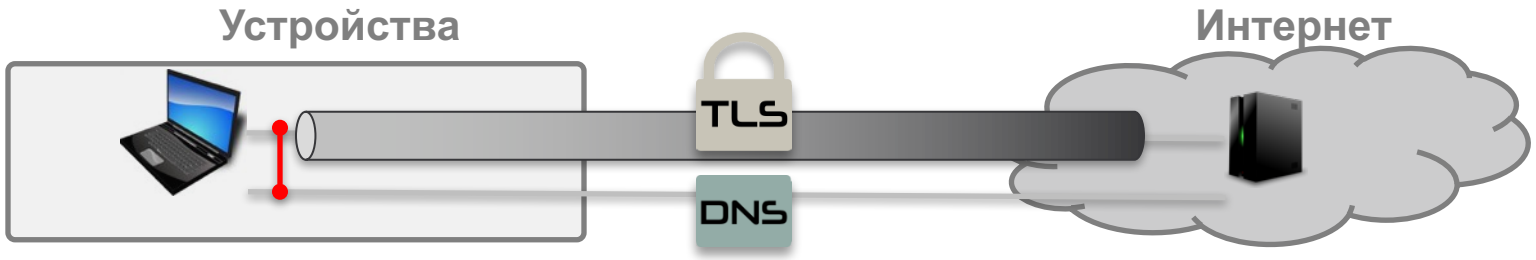
Анализ зашифрованного трафика

Проблема: зловредный код активно использует TLS-шифрование



- Шифрование с помощью TLS активно используется (само по себе это не плохо!)
- Решения, основанные на анализе строк, становятся менее эффективными
- Проблемы внедрения расшифровки (MITM) для анализа:
  - Приватность; юридические проблемы; внедрение; стоимость; отсутствие у клиентов желания сотрудничать

Наш подход: использовать все доступные данные



Netflow данные: SrcIP, DstIP, SrcPort, DstPort, Proto, #Bytes, #Packets

Intraflow данные: размеры пакетов & временные параметры, распределение байтов, …

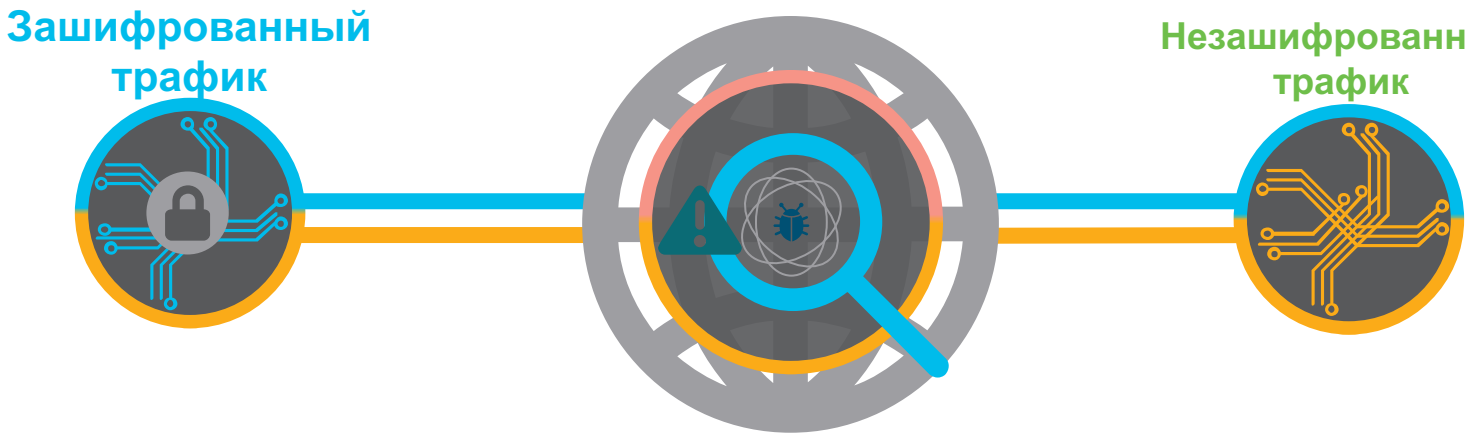
TLS метаданные: расширения, наборы шифров, SNI, поля сертификатов, …

DNS данные: имена, типы запросов, временные параметры запросов

HTTP данные: заголовки и сопутствующие поля, в том числе других http-запросов с этого же хоста

Расширенная аналитика

Первая сеть с возможностью находить угрозы в зашифрованном трафика без расшифровки



Защитите и управляйте сетью в реальном времени

Encrypted Traffic Analytics (ETA)

Видимость и обнаружение malware без расшифровки

Malware в зашифрованном трафике

Являются ли данные в TLS сессии вредоносными?

- Конфиденциальность
- Целостность канала без инспекции
- Адаптация. к стандартам шифрования

Криптографическое соответствие

Сколько из моего бизнеса использует сильное шифрование?

- Аудит нарушений TLS политик
- Пассивное обнаружение уязвимостей библиотек
- Постоянный мониторинг прозрачности сети

Encrypted Traffic Analytics (ETA)

Исследования Cisco

Известный трафик malware

Known benign traffic

Извлечь наблюдаемые особенности из данных

Применить машинное обучение для создания детекторов

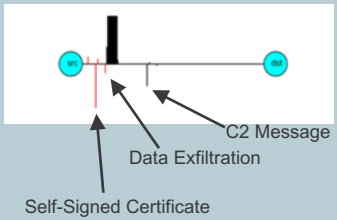
Известные malware сессии детектируются с точностью 99%^

“Identifying encrypted malware traffic with contextual flow data”

AISec ’16 | Blake Anderson, David McGrew (Cisco Fellow)

Возможности данных ETA

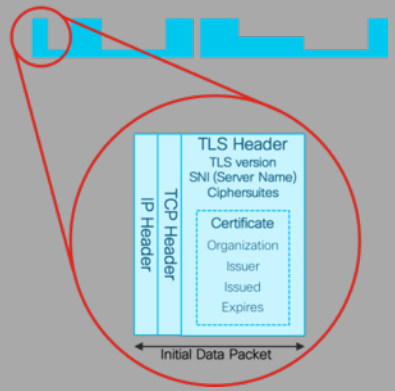
Исследования Cisco

	TCP/IP	DNS	TLS	SPLT
Malware traffic	Наблюдаемый адрес	c15c0.com afb32d75.com	Необычный отпечаток Необычный сертификат	 Bestafera
Benign traffic	Превалирующий адрес	cisco.com	Типичный отпечаток Типичный сертификат	 Google search

Как мы инспектируем трафик?

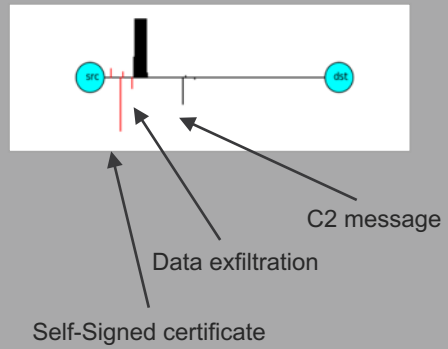
Первоначальный пакет

Получить как можно больше из незашифрованных пакетов



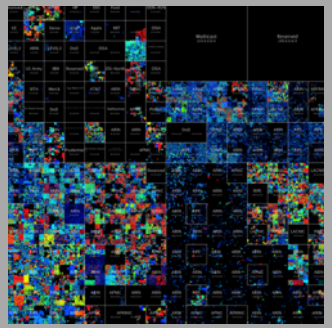
Sequence of packet lengths and times

Идентифицировать содержимое с помощью размера и последовательности пакетовpackets



Threat intelligence map

Кто есть кто в dark internet



Поведенческая информация о серверах в Internet

Найти вредоносную активность в зашифрованном трафике

Новый Catalyst 9K*

Cisco Stealthwatch

Улучшенная сеть	Быстрое расследование	Высокая точность	Усиленная защита
Расширенный Netflow от новых коммутаторов и маршрутизаторов Ciso	Расширенная аналитика и машинное обучение	Глобальная корреляция знаний	Постоянное соответствие

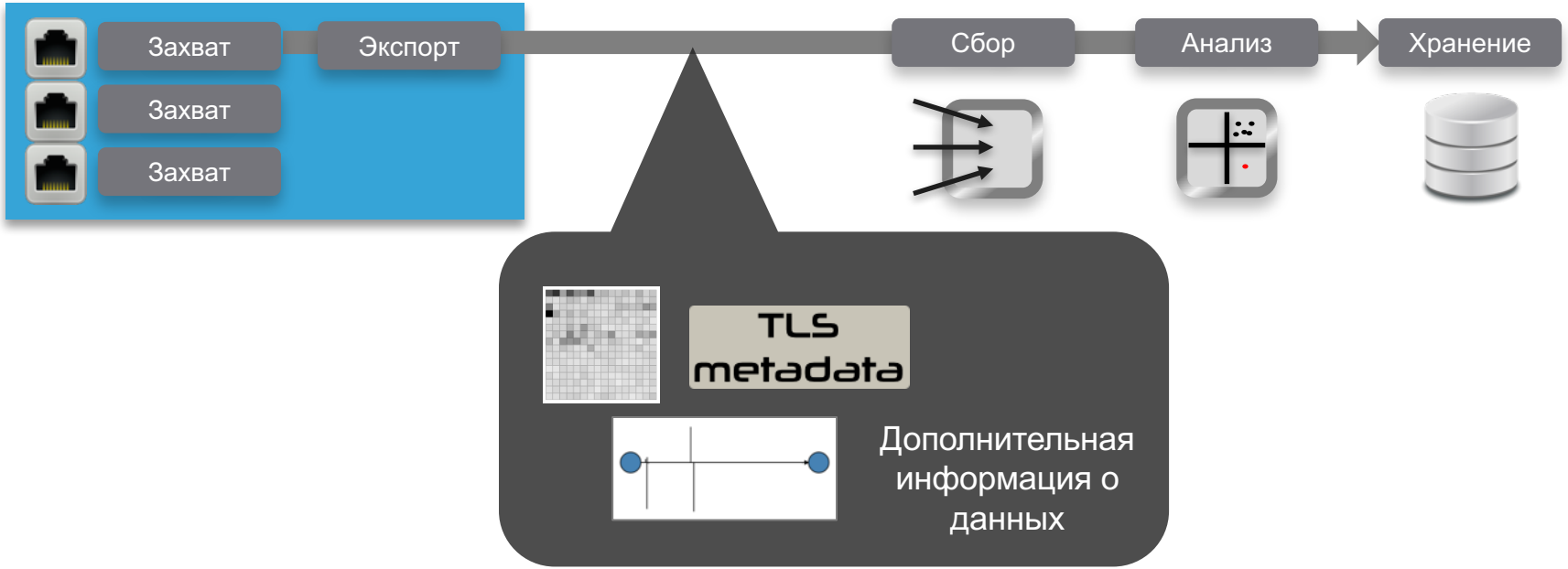
Немного науки

Традиционный анализ сетевых потоков

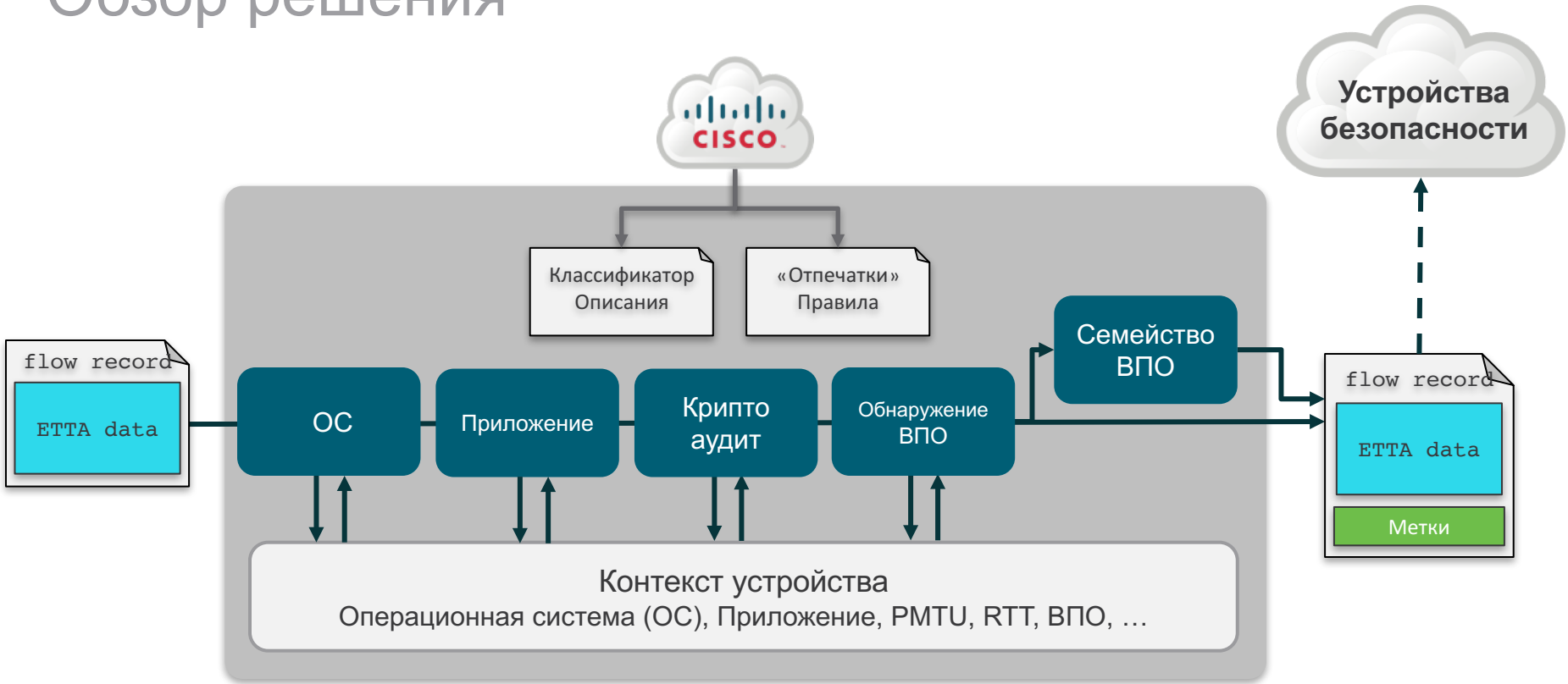
srcIP, dstIP, srcPort, dstPort, prot, startTime, stopTime, numBytes, numPackets

Сбор расширенной телеметрии

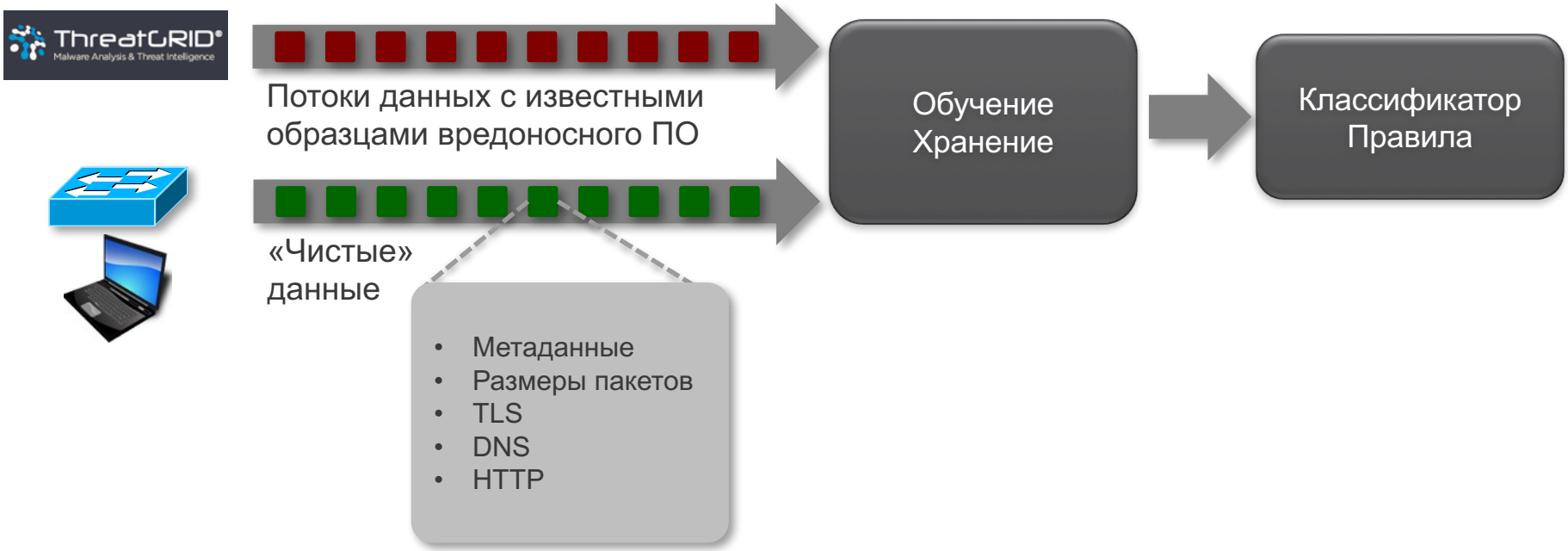
srcIP, dstIP, srcPort, dstPort, prot, startTime, stopTime, numBytes, numPackets



Обзор решения



Набор данных, использованный в исследовании



Потоки данных с известными образцами ВПО

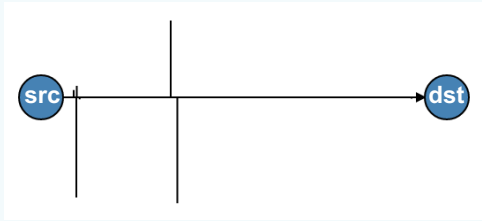
- Записи сетевого обмена из системы динамического анализа Cisco ThreatGRID (в формате pcap):
  - 5-ти минутные сессии анализа;
  - Образцы с Threat Score = 100/100;
- Миллионы pcap-файлов:
  - ~5,000-15,000 новых каждый день;
  - Сотни миллионов потоков

«Чистые» данные

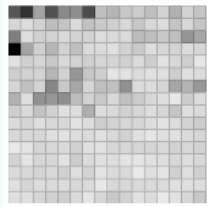
- Демилитаризованная зона сети крупной компании:
  - ~10-15 миллионов потоков в день;
  - ~500 пользователей
- IP-адреса анонимизированы.

Типы данных, использованные из расширенной телеметрии

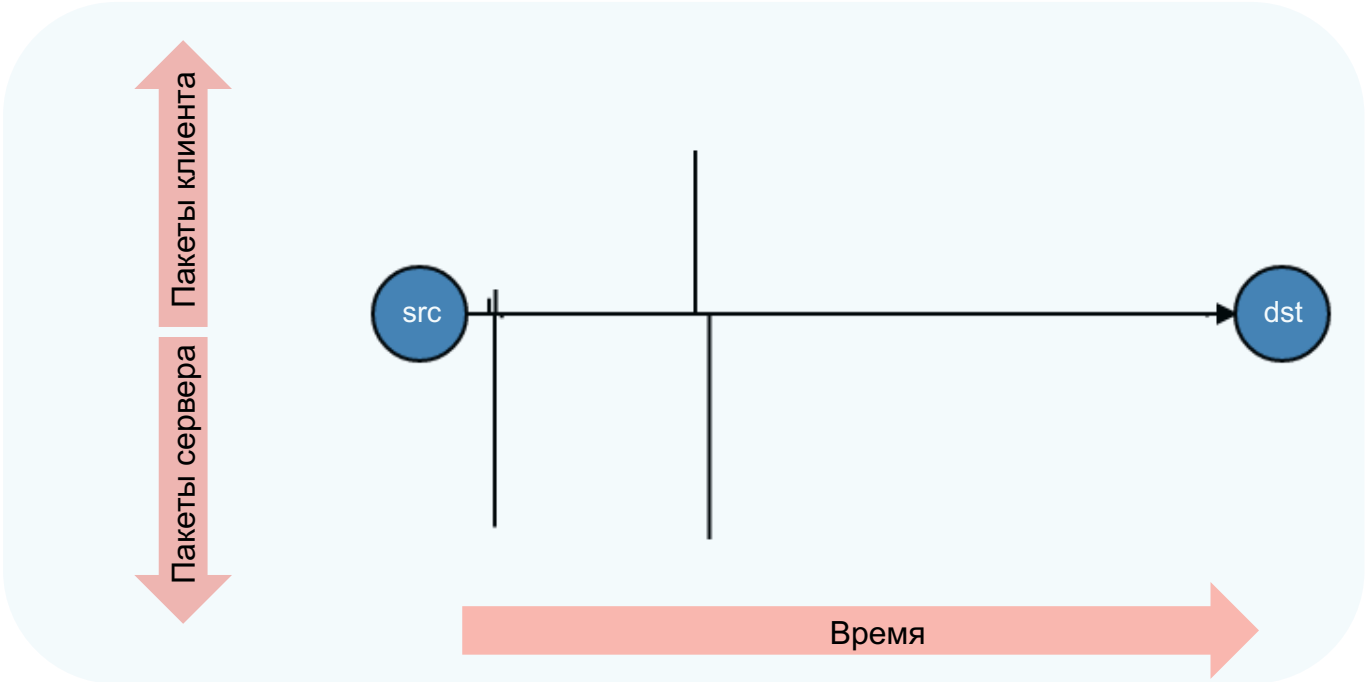
- **SPLT** – Sequence of Packet Lengths and Arrival Times, или распределение пакетов и их последовательностей с учётом временных интервалов



- **BD** - Byte Distribution или побайтное распределение
- **BE** - Byte Entropy или побайтная энтропия



SPLT - распределение пакетов и их последовательностей с учётом временных интервалов



BD - побайтное распределение

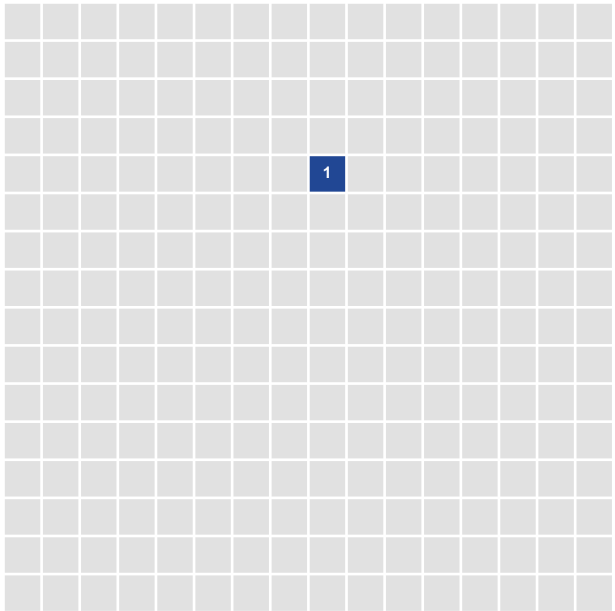
```
H  T  T  P  /  1  .  1     2  0  0     O  K
```

```
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b
```

BD - побайтное распределение

H	T	T	P	/	1	.	1		2	0	0		O	K

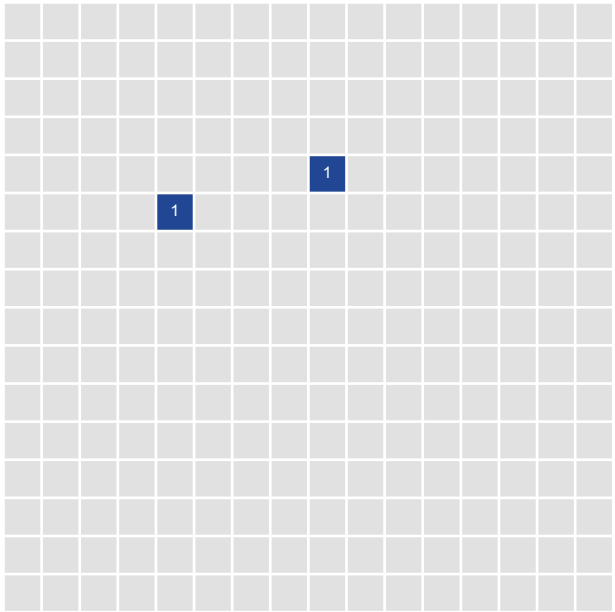
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b



BD - побайтное распределение

```
H  T  T  P  /  1  .  1     2  0  0     O  K
```

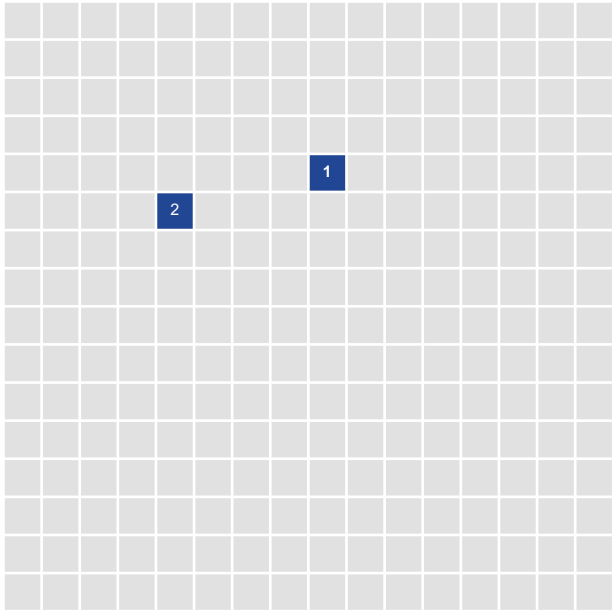
```
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b
```



BD - побайтное распределение

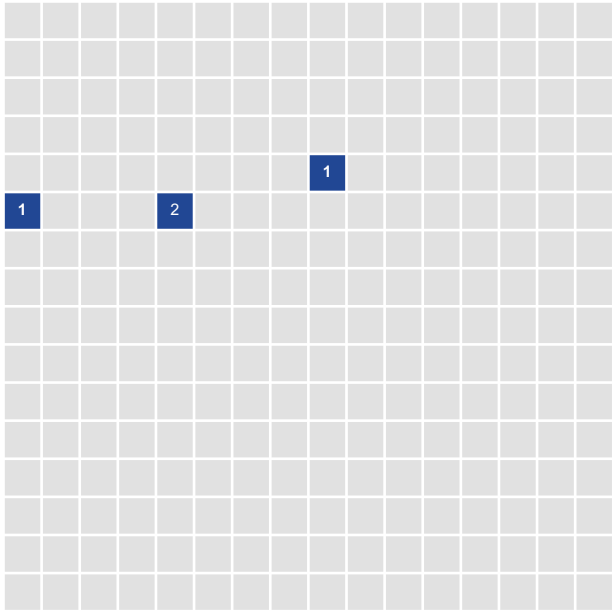
```
H  T  T  P  /  1  .  1     2  0  0     O  K

□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b
```

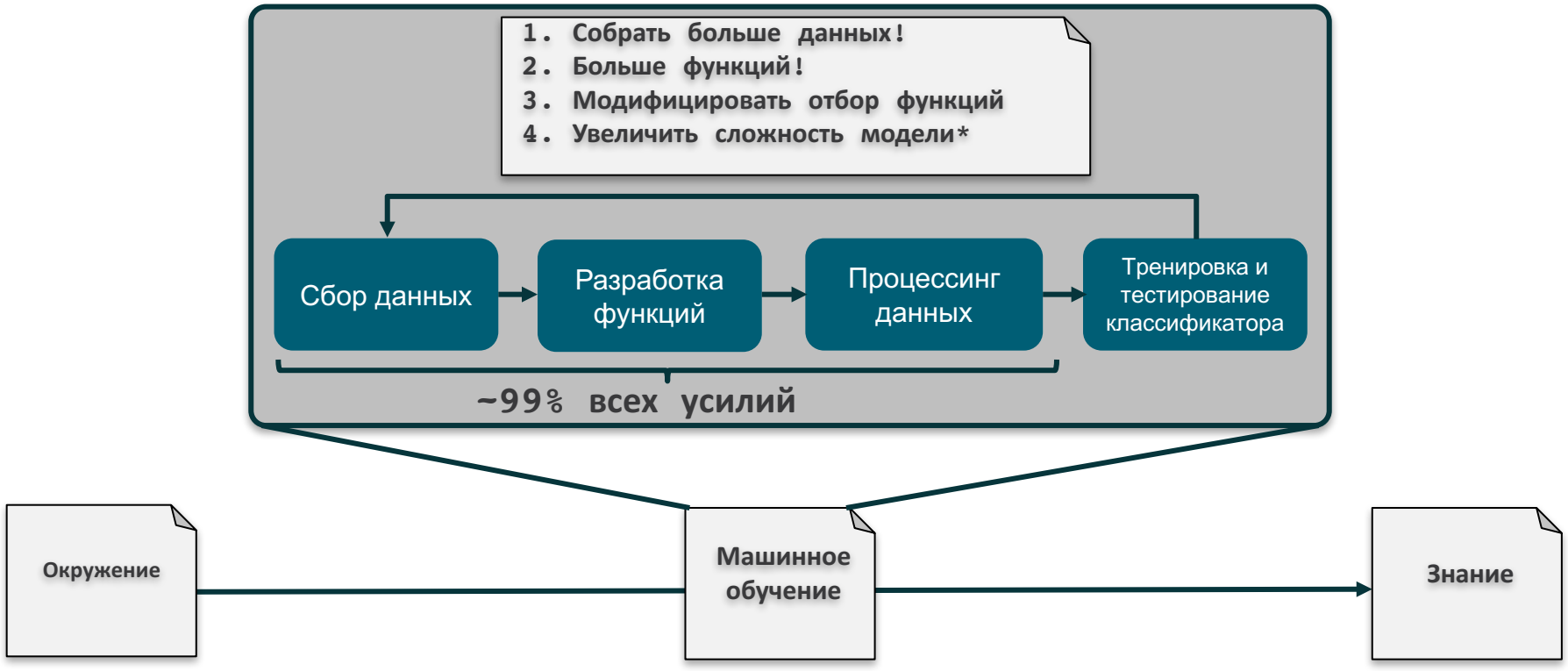


BD - побайтное распределение

```
H  T  T  P  /  1  .  1     2  0  0     O  K
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b
```



Управляемое данными обучение



* Если больше ничего не помогает

Тестовый набор данных

- Вредоносный код
  - Записи сетевого обмена (pcap) с августа 2015 по май 2016 из Cisco ThreatGRID;
  - Трафик TLS (443), больше 100 байт на вход и выход;
  - 225,740 потоков; сетевая телеметрия обогащалась информацией о TLS-extensions, шифр-наборах, и размерах публичных ключей;
- «Хороший трафик»
  - Трафик взят из DMZ крупной компании
  - Трафик TLS (443), больше 100 байт на вход и выход;
  - 225,000 потоков; сетевая телеметрия обогащалась информацией о TLS-extensions, шифр-наборах, и размерах публичных ключей;
- 10-кратная перекрёстная проверка данных

Добавлена контекстная информация

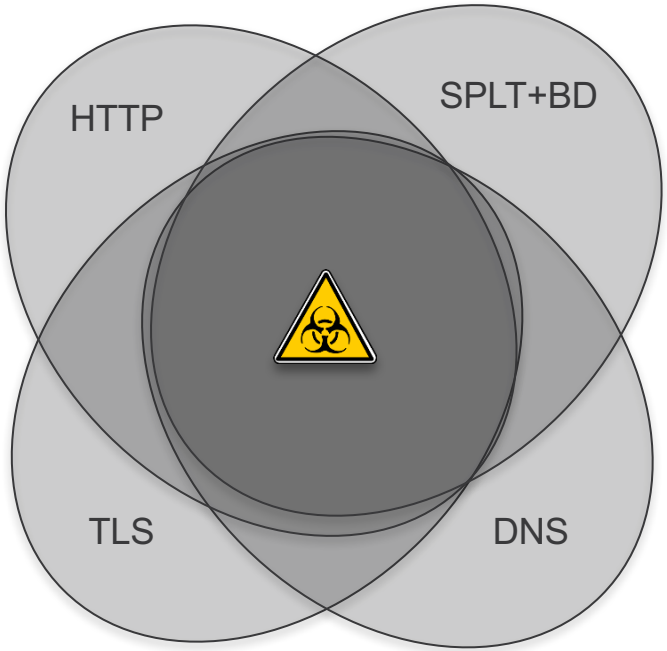
- DNS
  - Alexa Lists
  - Lengths of DN and FQDN
  - Suffix
  - TTL
  - % Numerical Characters
  - % Non-alphanumeric Chars
- HTTP
  - Outbound/inbound header fields
  - Content-Type
  - User-Agent
  - Accept-Language
  - Server
  - code

Интересные факты:

- Зловреды наиболее часто используют:
  - DNS Suffix: org
  - DNS TTL: 3600
  - TLS_RSA_WITH_RC4_128_SHA
  - HTTP Field: location
  - DNS Alexa: Not Found
  - HTTP Server: nginx
  - HTTP Code: 404

- Легитимный трафик наиболее часто использует:
  - TLS Ext: extended_master_secret
  - Content type: application/octet-stream
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - HTTP Server: Microsoft-IIS/8.5
  - DNS Alexa: top-1,000,000
  - HTTP User-Agent: Microsoft-CryptoAPI/6.1

Обнаружение зашифрованного ВПО



	Acc.	0.00% FDR
SPLT+BD+TLS+HTTP+DNS	99.993%	99.978%
SPLT+BD+TLS+HTTP	99.983%	99.956%
SPLT+BD+TLS+DNS	99.968%	98.043%
SPLT+BD+TLS	99.933%	70.351%
HTTP+DNS	99.985%	99.956%
TLS+HTTP	99.955%	99.660%
TLS+DNS	99.883%	96.551%
HTTP	99.945%	98.996%
DNS	99.496%	94.654%
TLS	94.836%	50.406%

Спасибо за внимание!