

# 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

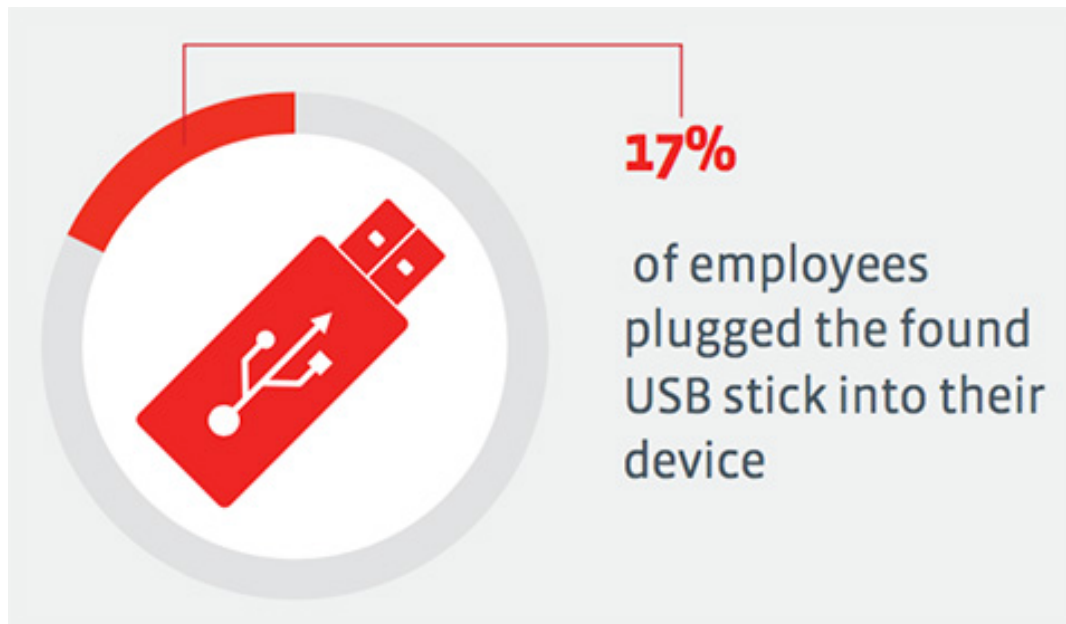




“ Мир полон очевидных вещей, которых никто не замечает.”

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



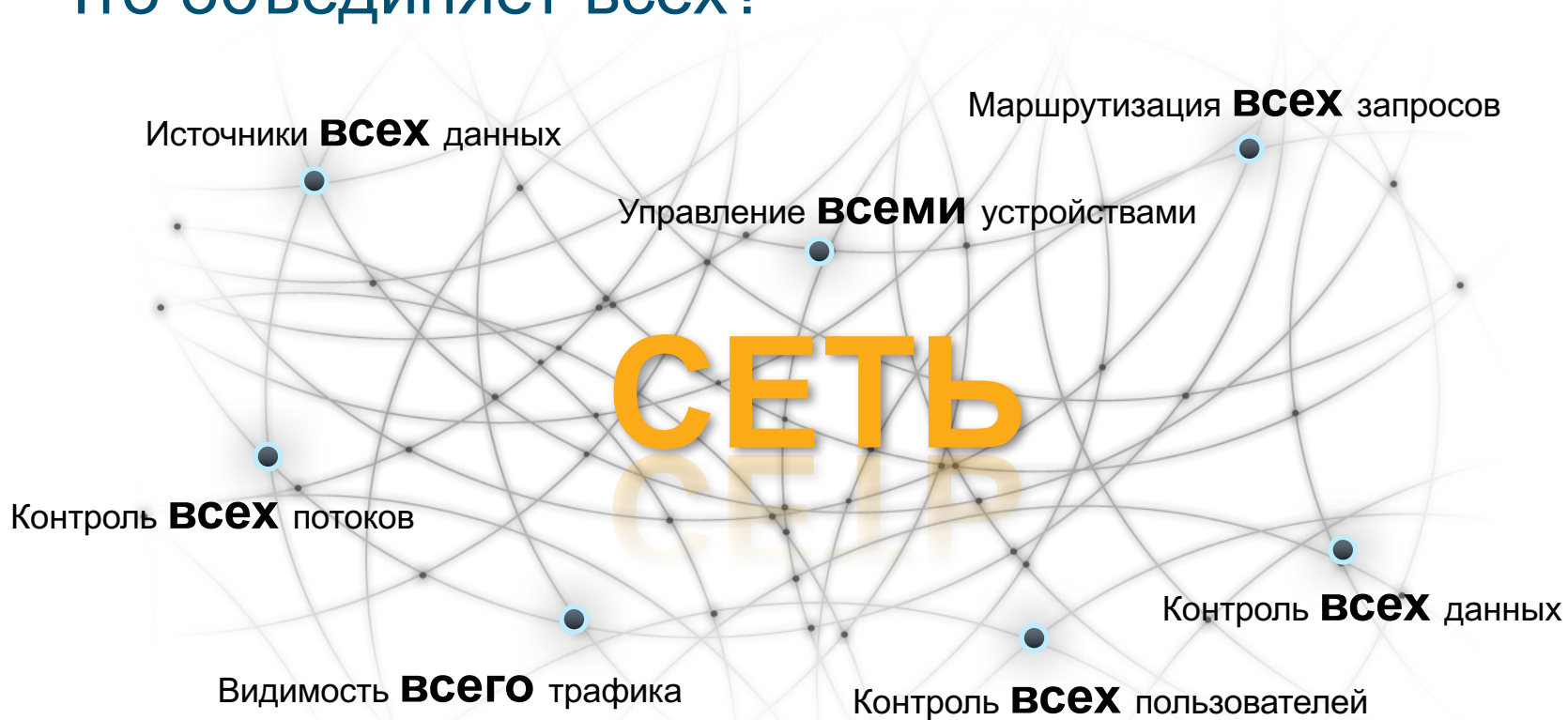
# Об этой сессии: Видимость через изучение данных



Возможность понять:

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

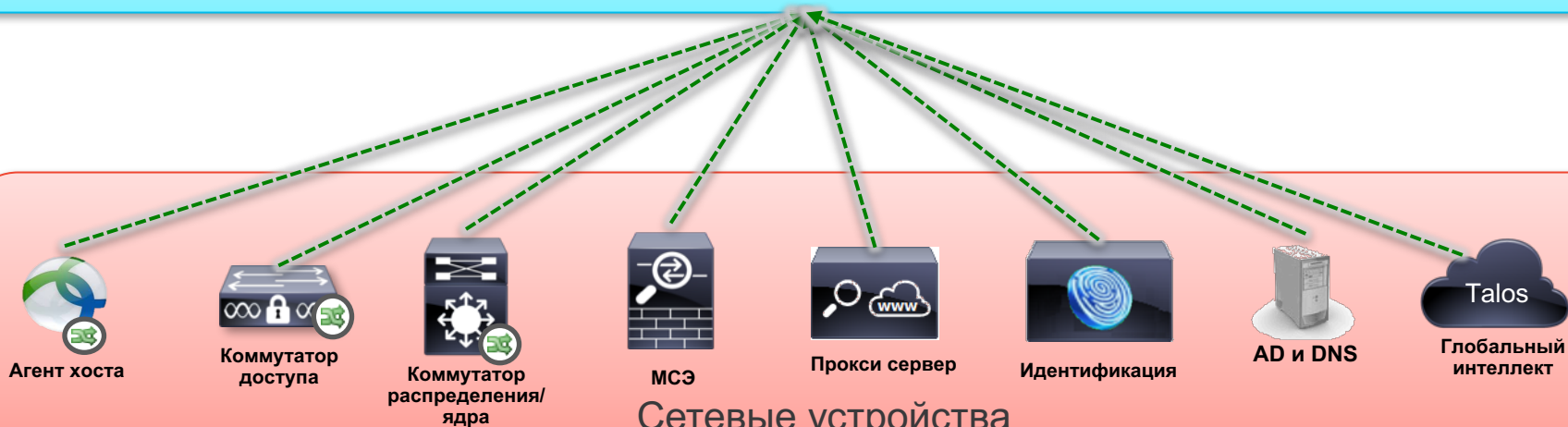
# Что объединяет всех?



# 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>



Изолированные знания основанные на функции и расположении

# Аналитика данных с помощью телеметрии:

## Обнаружение

- Идентификация бизнес-критичных приложений и сервисов в сети

## Идентификация дополнительных Индикаторов Компрометации (IoC)

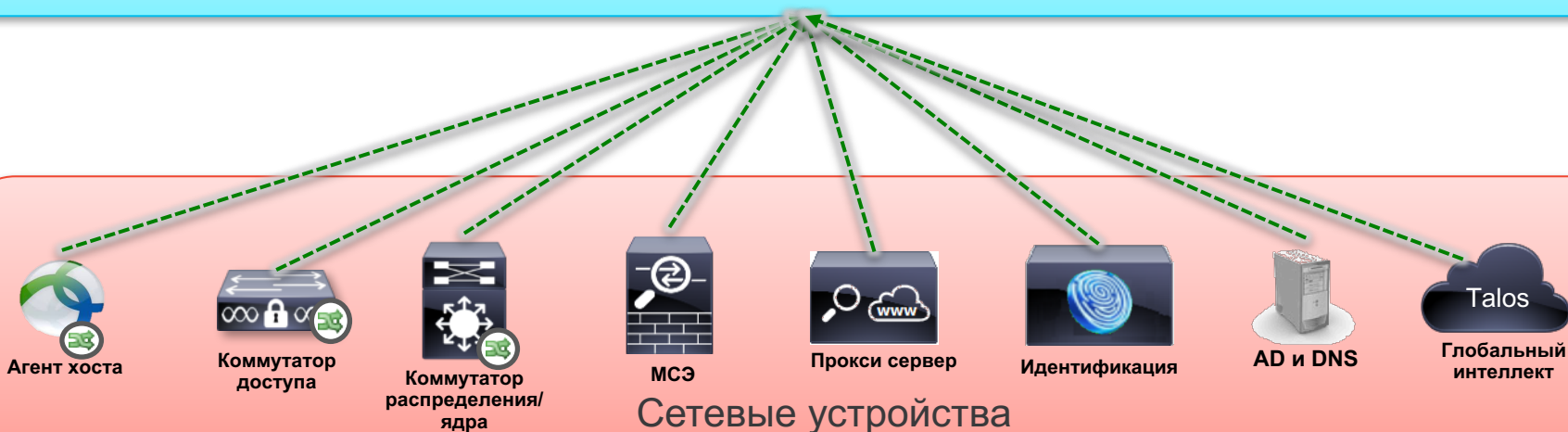
- Политики и Сегментация
- Сетевое поведение и Обнаружение Аномалий (NBAD)

## Лучше понимать / реагировать на IOС:

- Аудит всех коммуникаций между хостами

# Cisco Stealthwatch

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



Сетевые устройства

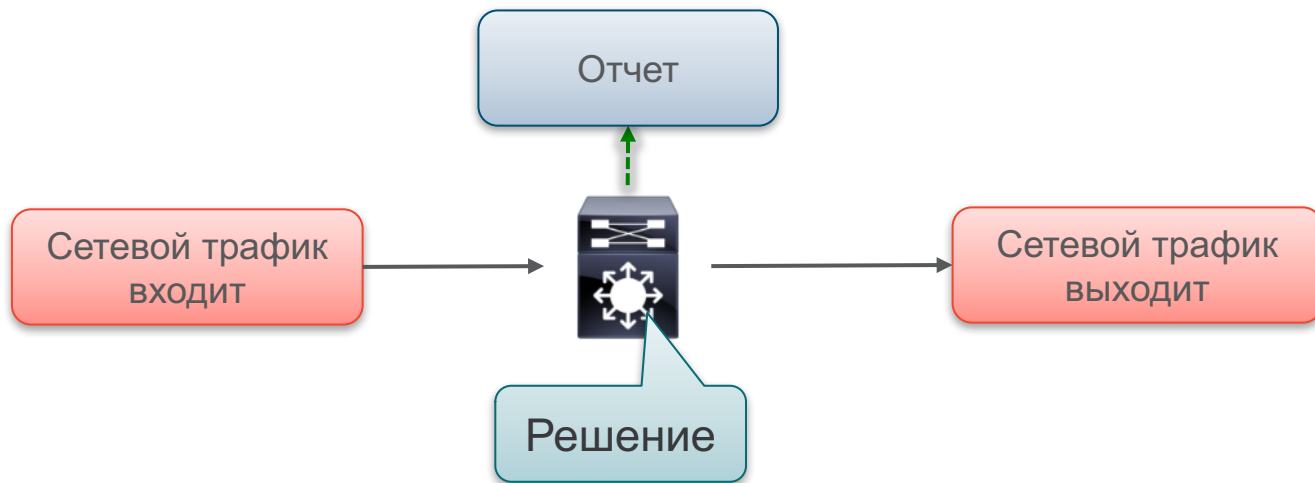
Изолированные знания основанные на функции и расположении

# 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

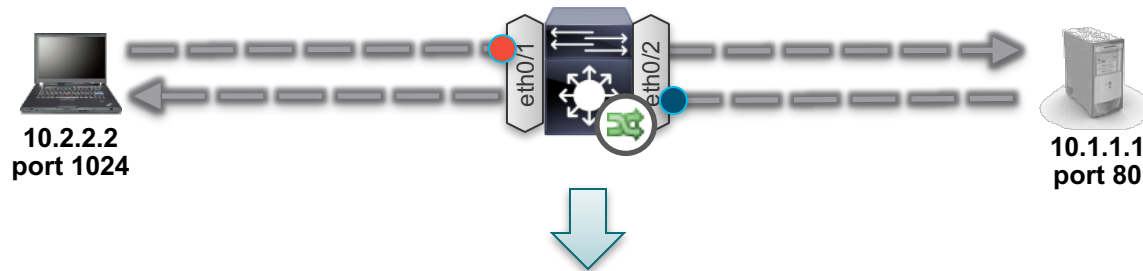
## IPFIX

Стандартизована  
Шаблонная

Поля изменяемой  
длины

**450+** Заданных полей

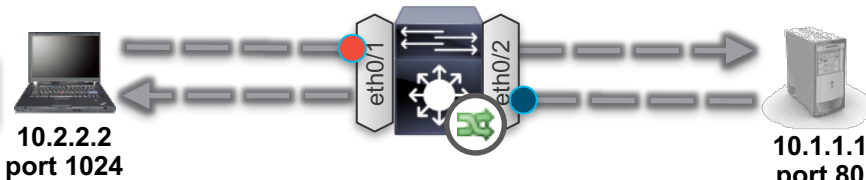
# Транзакционная телеметрия с NetFlow



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

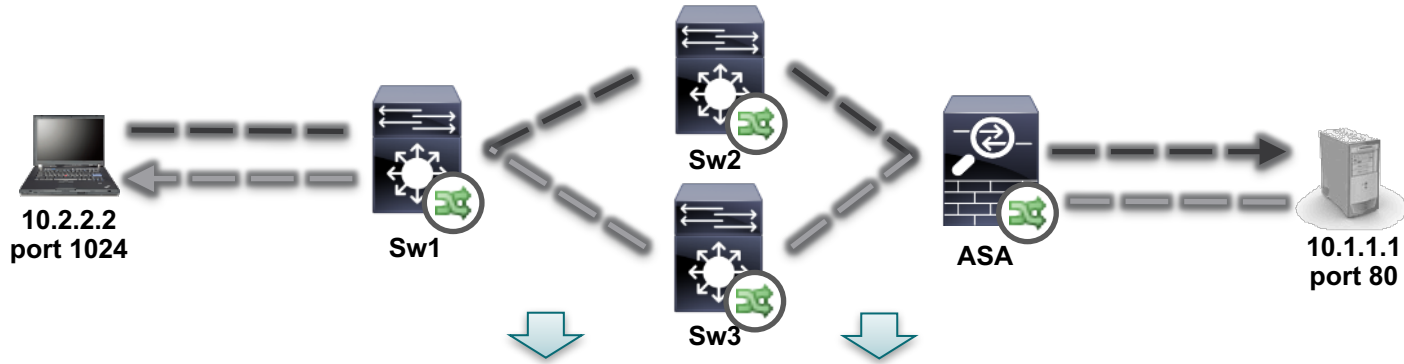


Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Client SGT	Server SGT	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	100	1010	eth0/1 eth0/2

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



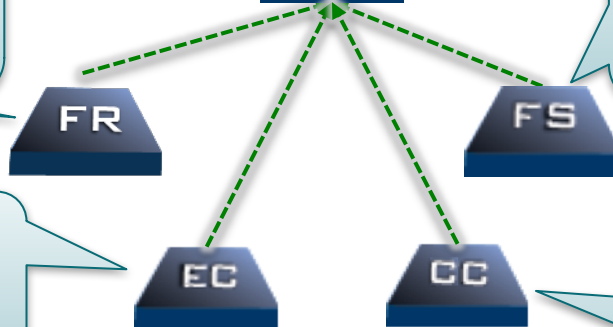
## Endpoint License Concentrator

- Собирает AnyConnect 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





DURATION	SUBJECT	PORT / PROTOCOL	TRAFFIC SUMMARY	PORT / PROTOCOL	PEER
▶ Start: 06/12 - 03:19:12 PM End: 06/12 - 03:21:06 PM Duration: 1m 54s	 209.182.184.7 <a href="#">View URL Data</a> United States aip03-pxe01-px1.lancope.com	13298/TCP	1.14MB   29.91K packets → HTTP ← 67.05MB   54.09K packets	80/TCP	 70.38.0.134 Canada
▶ Start: 06/12 - 03:23:34 PM End: 06/12 - 03:25:36 PM Duration: 2m 2s	 10.201.3.3 <a href="#">View URL Data</a> RFC 1918	2175/TCP	1.03MB   27.03K packets → HTTP ← 65.05MB   52.48K packets	80/TCP	 70.38.0.134 Canada

Таблица Потоков

Идентификация Пользователя/ Устройства

Данные интеллекта угроз

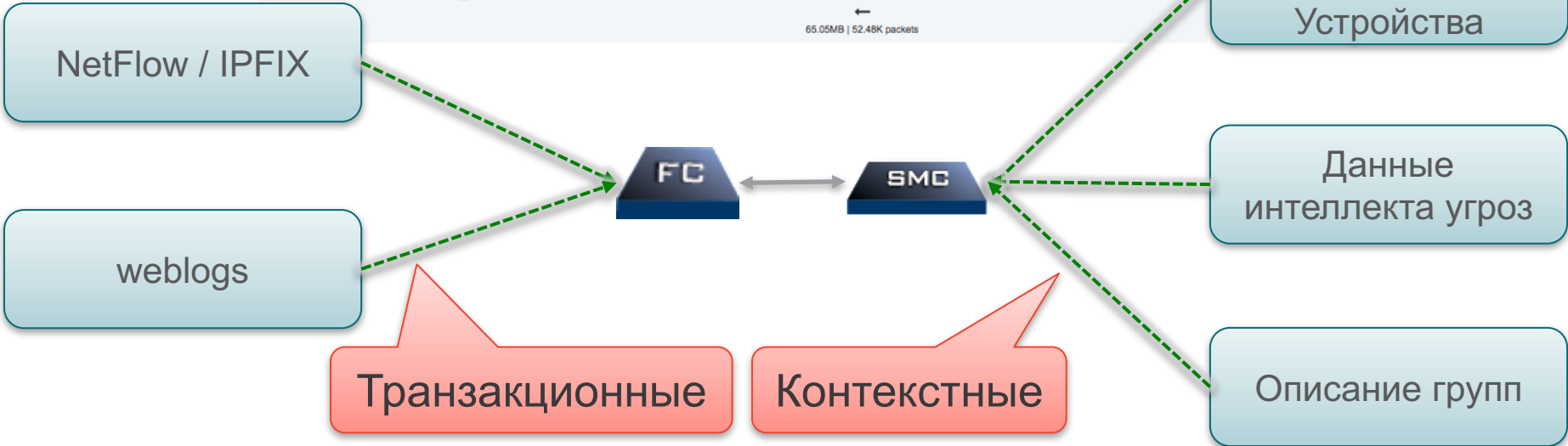
Описание групп

NetFlow / IPFIX

weblogs

Транзакционные

Контекстные



# Двусторонняя запись потока

<b>Кто</b>	<b>Что</b>	<b>Кто</b>			
<b>Duration</b>	<b>Search Subject</b>	<b>Port</b>	<b>Traffic S</b>	<b>Port</b>	<b>Peer</b>
Start: 05/29 - 12:19:18 PM End: 05/29 - 12:20:58 PM Duration: 1m 40s	10.10.18.102 RFC 1918 employee1 00:50:56:b4:3f:af	4866/TCP	11.49KB   285 packets → HTTP ← 1.62MB   1.15K packets	80/TCP	216.191.247.145 Canada crl.entrust.net
<b>Когда</b>	<b>Где</b>	<b>Как</b>	<b>Больше контекста</b>		

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

## Flow Detailed Summary: 10.10.18.102

### Search Subject Details

Packets: 285  
Packet Rate: 2.85pps  
Bytes: 11.49KB  
Byte Rate: 117.69bps  
Percent Transfer:  
0.6879458949171267%  
Host Groups: Desktops  
TrustSec ID: 100  
TrustSec Name: Employees  
Payload: GET http://crl.entrust.net/2048ca.crl

### Totals

Packets: 1.44K  
Packet Rate: 14.37pps  
Bytes: 1.63MB  
Byte Rate: 17.11Kbps  
Search Subject/Peer  
Ratio: 0.01  
TCP Connections: 2  
RTT: 2ms  
SRT: 498ms

### Peer Details

Packets: 1.15K  
Packet Rate: 11.52pps  
Bytes: 1.62MB  
Byte Rate: 16.99Kbps  
Percent Transfer:  
99.31205410508288%  
Host Groups: Canada  
Payload: 200 OK  
TrustSec ID: 0  
TrustSec Name: Unknown

Close

# Контекстная телеметрия



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

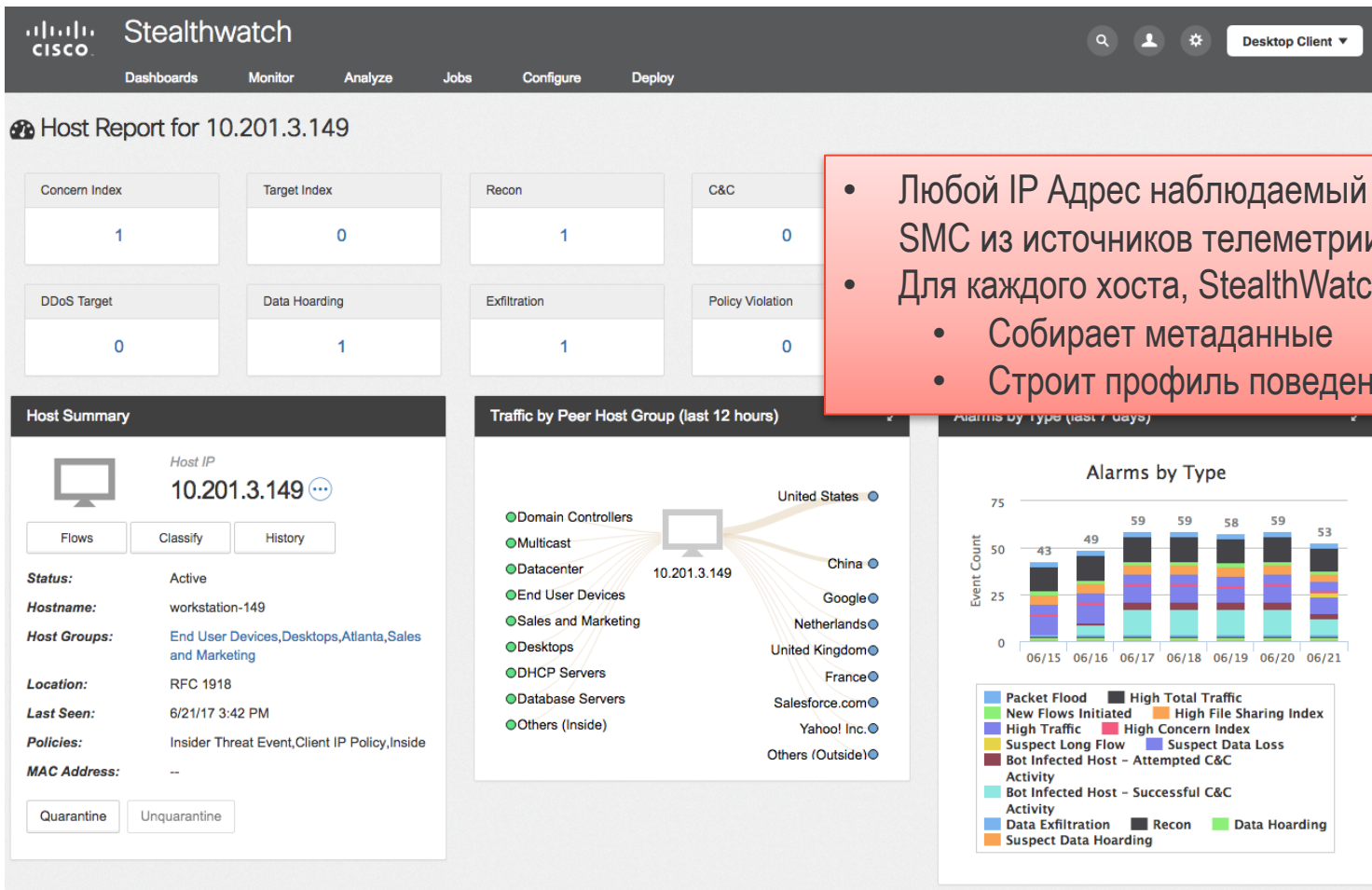
Кто?

IP Адрес: 10.10.10.10

Что?

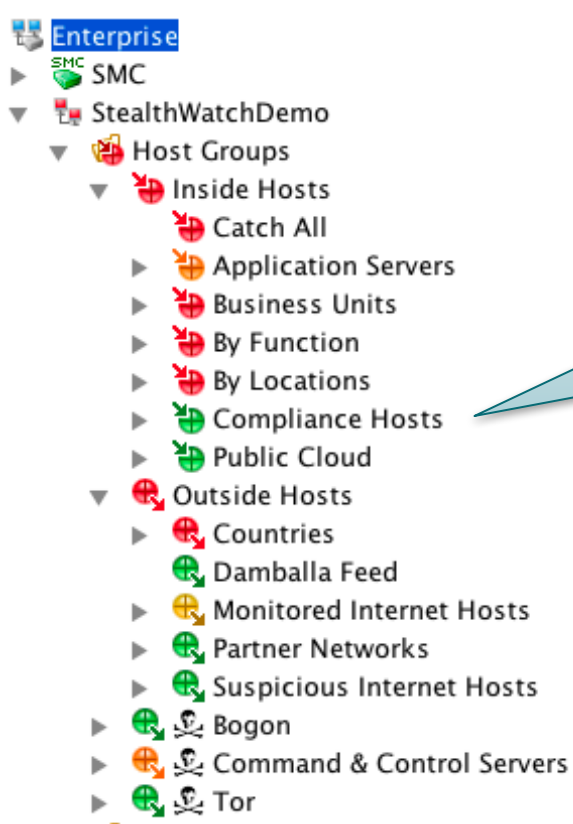
Где?

# 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

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



- Известные C&C Сервера
- Тор Входы и Выходы

A screenshot of a network management interface showing a list of host groups. The list is organized into a tree structure with expandable folders. The visible items are:

- Host Groups
  - Inside Hosts
  - Outside Hosts
  - Command & Control Servers
    - Agent.nfx
    - Aldibot
    - Armageddon
    - Banload
    - Barracuda
    - Bho-jba
    - Blackenergy
    - Colddeath
    - Darkcomet
    - Darkshell
    - Ddoser
    - Dirtjumper
    - Dofoil
    - Drive
    - Emo
    - Graybird
    - Gumblar
    - Haxdoor
    - Hitpop
    - Hitpop Checkin
    - Http Post
    - Icepack
    - Illusion
    - Ircbot
    - Mpack

# “Обогащенная” запись сессии

Geo-IP

NBAR

Start: 01/10 - 02:18:15 PM  
End: 01/10 - 02:18:20 PM  
Duration: 5s



10.201.3.149  
RFC 1918  
ken

[View Details](#)

53455/TCP

16.57KB | 321 packets

80/TCP



89.108.67.143  
Russian Federation  
cp117.agava.net

→  
HTTP  
←

672.77KB | 541 packets

ISE  
Телеметрия

## Flow Detailed Summary: 10.201.3.149

### Search Subject Details

Packets: 321  
Packet Rate: 64.2pps  
Bytes: 16.57KB  
Byte Rate: 3.39Kbps  
Percent Transfer: 2.4%

Host Groups: Atlanta, Sales and Marketing, Desktops

Payload: GET http://allstadiums.ru/parfumin/config.bin

Process Name: taskhost.exe

### Totals

Packets: 862  
Packet Rate: 172.4pps  
Bytes: 689.34KB  
Byte Rate: 141.18Kbps  
Search Subject/Peer Ratio: 0.02  
TCP Connections: 1  
RTT: 166ms  
SRT: 797ms

### Peer Details

Packets: 541  
Packet Rate: 108.2pps  
Bytes: 672.77KB  
Byte Rate: 137.78Kbps  
Percent Transfer: 97.6%  
Host Groups: Russian Federation, Gumbler  
Payload: 200 OK

Применяем группировку

Flow Sensor

AnyConnect NVM

Threat Intelligence

# Программа

- Введение
- Использование сетевой телеметрии
- Организация данных



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

The screenshot displays the StealthWatch Management Console interface. On the left is a navigation tree for the Enterprise environment. The main area shows several reports under the 'Cyber Threats' tab, including 'Suspectious Internal Hosts', 'Suspectious Outside Hosts', and 'Possible Victims'. Each report contains a table of host data with columns for Country, Host, CI%, and Alerts. A search bar is visible at the bottom left, and a refresh timestamp is at the bottom center.

Country	Host	CI%	Alerts
United States	69.160.42.248	...	Port_Scan, Rejects, Spoof, TCP_Scan, TCP_Stealth
China	58.221.60.166	...	Rejects, Spoof, TCP_Scan
Turkey	78.187.95.226	...	Rejects, Spoof, TCP_Scan
	61.175.101.118	...	Rejects,

Host Gr...	Host	CI%	Alerts
Atlanta, Infrastructure, Desktops, Virtual Desktop	10.201.3.83	...	Ping, TCP_Scan
Catch All	199.204.23.227	...	Port_Scan, Rejects, Spoof, TCP_Scan, TCP_Stealth
New York, Desktops	10.10.101.24	...	Ping, TCP_Scan
Sales and	wkstation50	...	Spoof, TCP_Scan

Country	Host	CI%	Alerts
Atlanta	wanrt01 (209.182.184.1)	8...	
Firewalls	10.240.200.1	7...	
Atlanta	wanrt02 (209.182.184.3)	6...	
New York, Desktops	10.20.30.40	5...	
Engineering	10.165.254.12	5...	

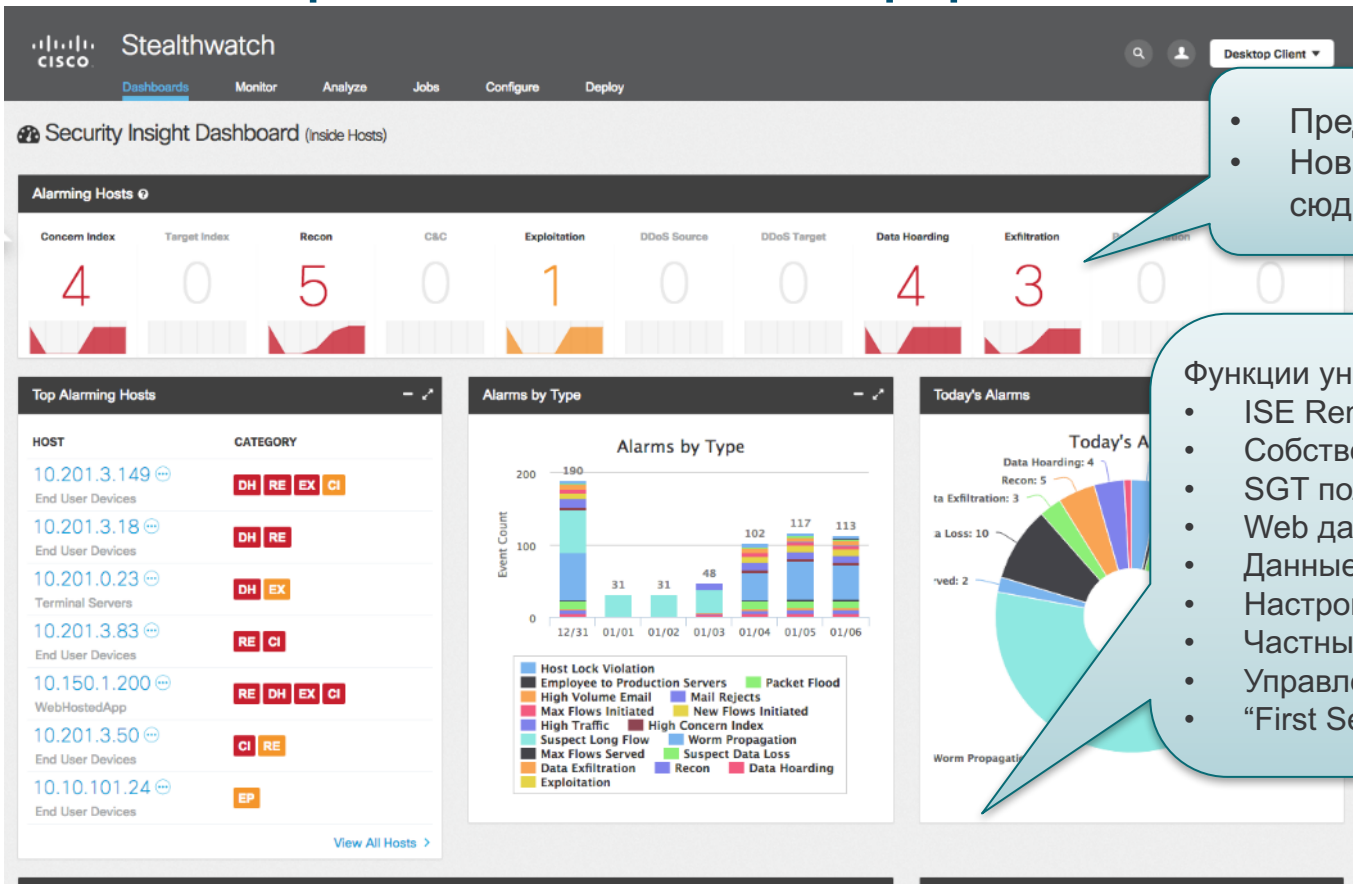
Touched ...	Touched ...	CI Co...	Host
New York, Desktops	10.20.10.254	RFC 1918	
Servers	10.201.0.28	RFC 1918	
Servers	10.201.0.19	RFC 1918	(10.201.3.50)
Domain Controller/DNS	10.201.0.16	RFC 1918	wkstation50 (10.201.3.50)
Atlanta, Infrastructure, Desktops	10.201.3.83	RFC 1918	wkstation50 (10.201.3.50)

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

Дерево Enterprise

Просмотр отчетов

# Со стороны: SMC Интерфейс 2: “Web” Интерфейс

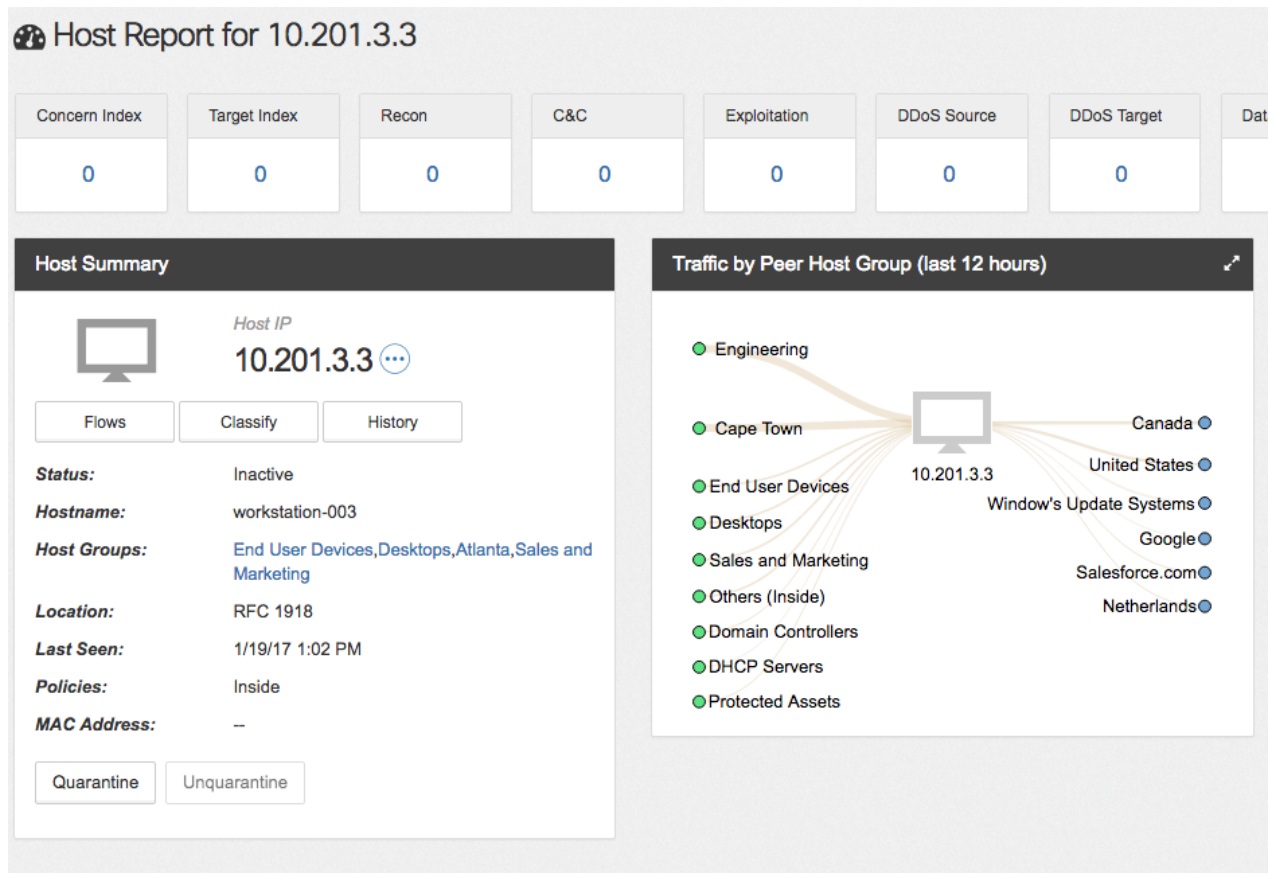


- Представлен в Stealthwatch 6.5
- Новые функции добавляются сюда

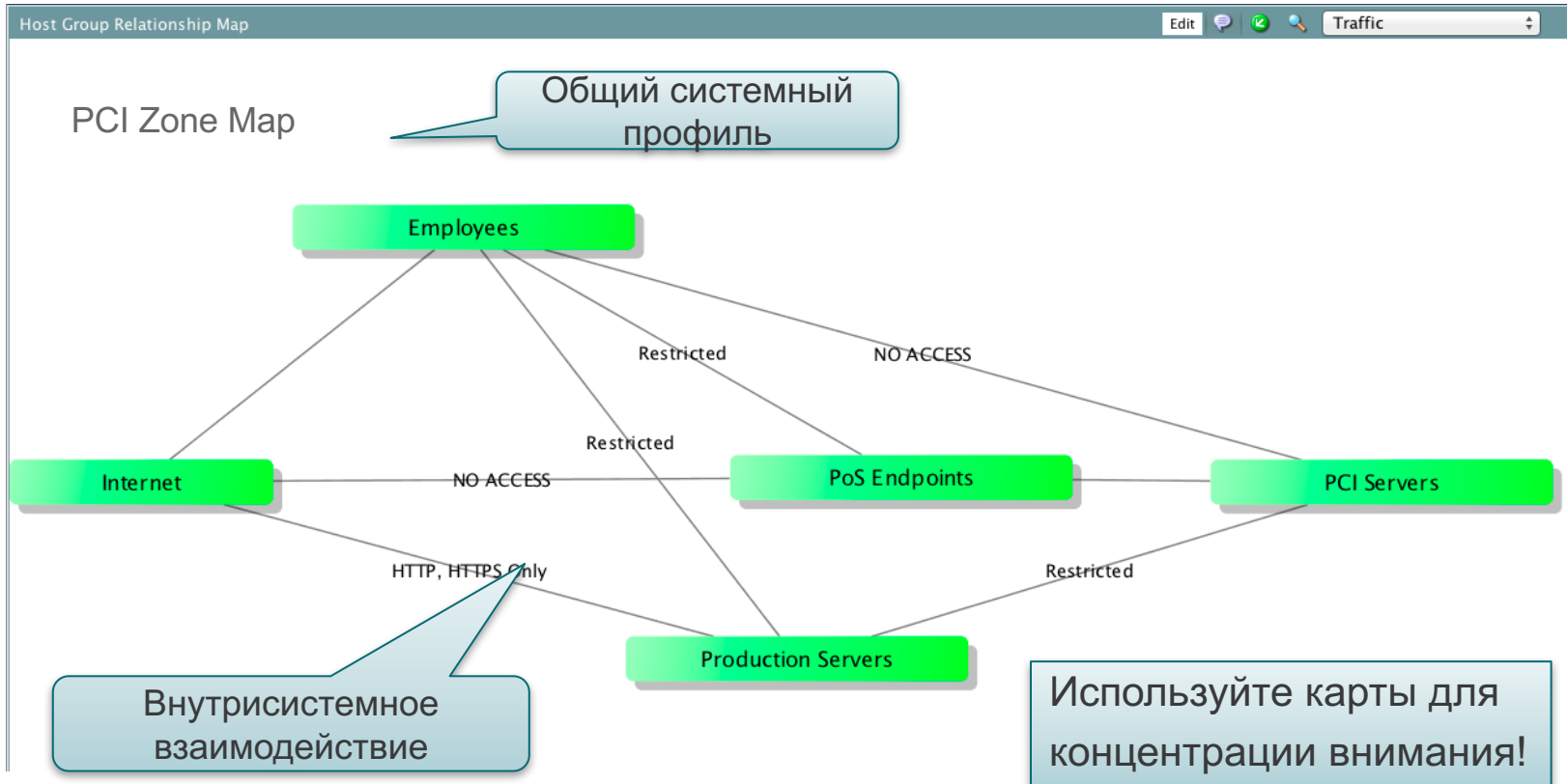
Функции уникальные для WEB интерфейса:

- 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 компрометации

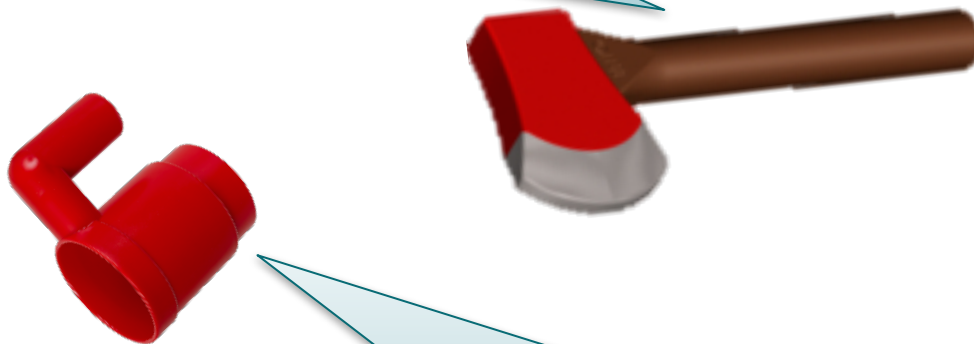
- [http://en.wikipedia.org/wiki/Indicator\\_of\\_compromise](http://en.wikipedia.org/wiki/Indicator_of_compromise)



# IoS 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")

Security  
Event

Security  
Event

Security  
Event

Security  
Event

Security  
Event

## События безопасности ("Алгоритмы")

Security  
Event

Security  
Event

Security  
Event

Security  
Event

Security  
Event

## Категории ("Индексы")

CI

TI

---

C&C

Recon

## События безопасности ("Алгоритмы")

Security  
Event

Security  
Event

Security  
Event

Security  
Event

Security  
Event

## Категории ("Индексы")

CI

TI

---

C&C

Recon

## Тревоги ("Уведомления")

Alarm

Alarm

Alarm

Alarm

Alarm

## События безопасности ("Алгоритмы")

Security Event

Security Event

Security Event

Security Event

Security Event

## Категории ("Индексы")

CI

TI

C&C

Recon

## Тревоги ("Уведомления")

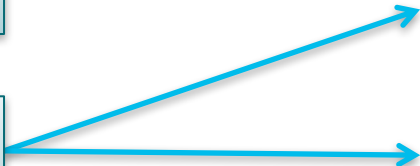
Alarm

Alarm

Alarm

Alarm

Alarm



## События безопасности ("Алгоритмы")

Security Event

Fake Application

Security Event

Security Event

Security Event

## Категории ("Индексы")

CI

TI

C&C

Recon

## Тревоги ("Уведомления")

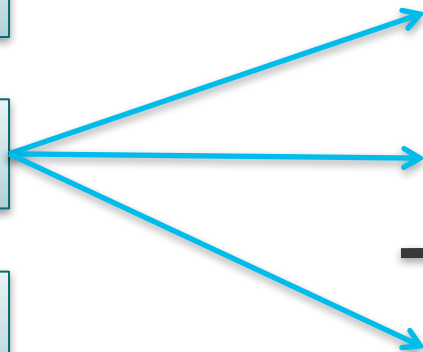
Alarm

Alarm

Alarm

Alarm

Alarm



## События безопасности ("Алгоритмы")

Security Event

Fake Application

Security Event

Security Event

Security Event

## Категории ("Индексы")

CI

TI

C&C

Recon

## Тревоги ("Уведомления")

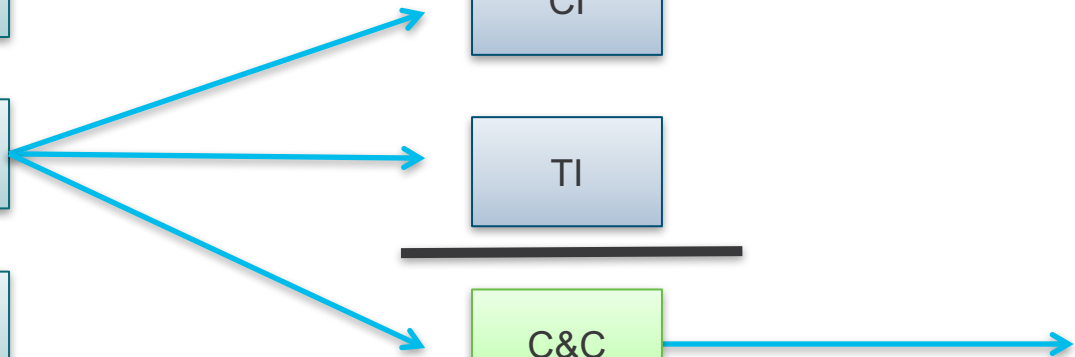
Alarm

Alarm

Alarm

Alarm

Alarm



## События безопасности ("Алгоритмы")

Security Event

Security Event

Security Event

Security Event

SQLF

## Категории ("Индексы")

CI

TI

---

C&C

Recon

## Тревоги ("Уведомления")

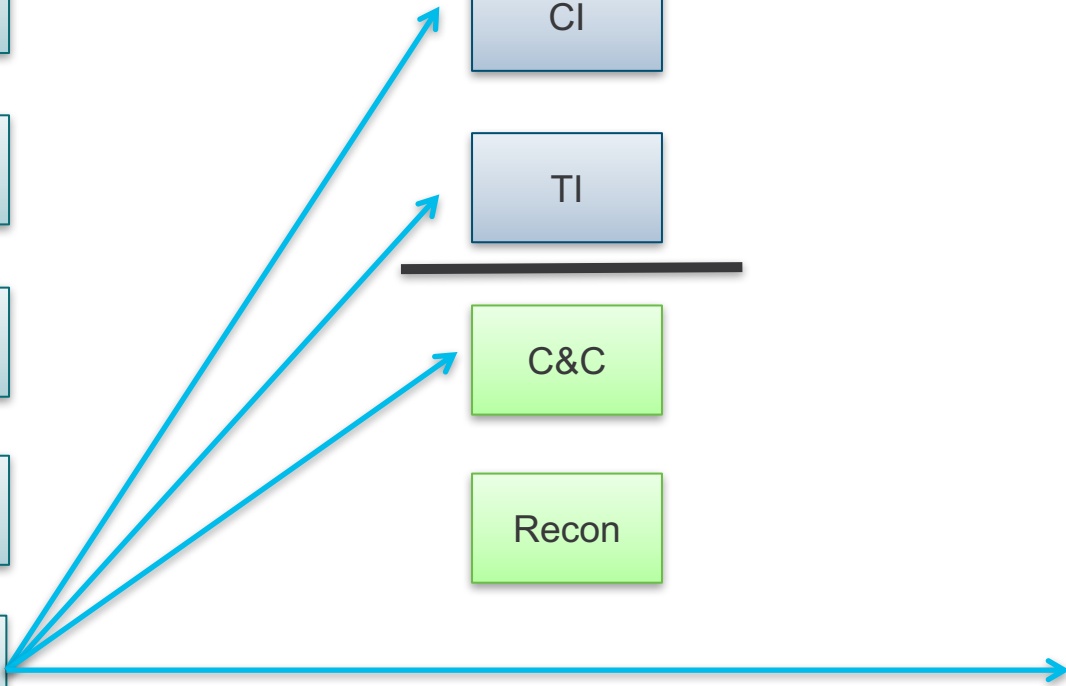
Alarm

Alarm

Alarm

Alarm

Alarm



# Категории тревог

Concern Index
57 active
76 total

Target Index
11
20

Recon
43
65

Command & Control
1
4

Exploitation
37
50

DDoS Source
0
0

DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	1	0	1	0
1	5	4	45	0

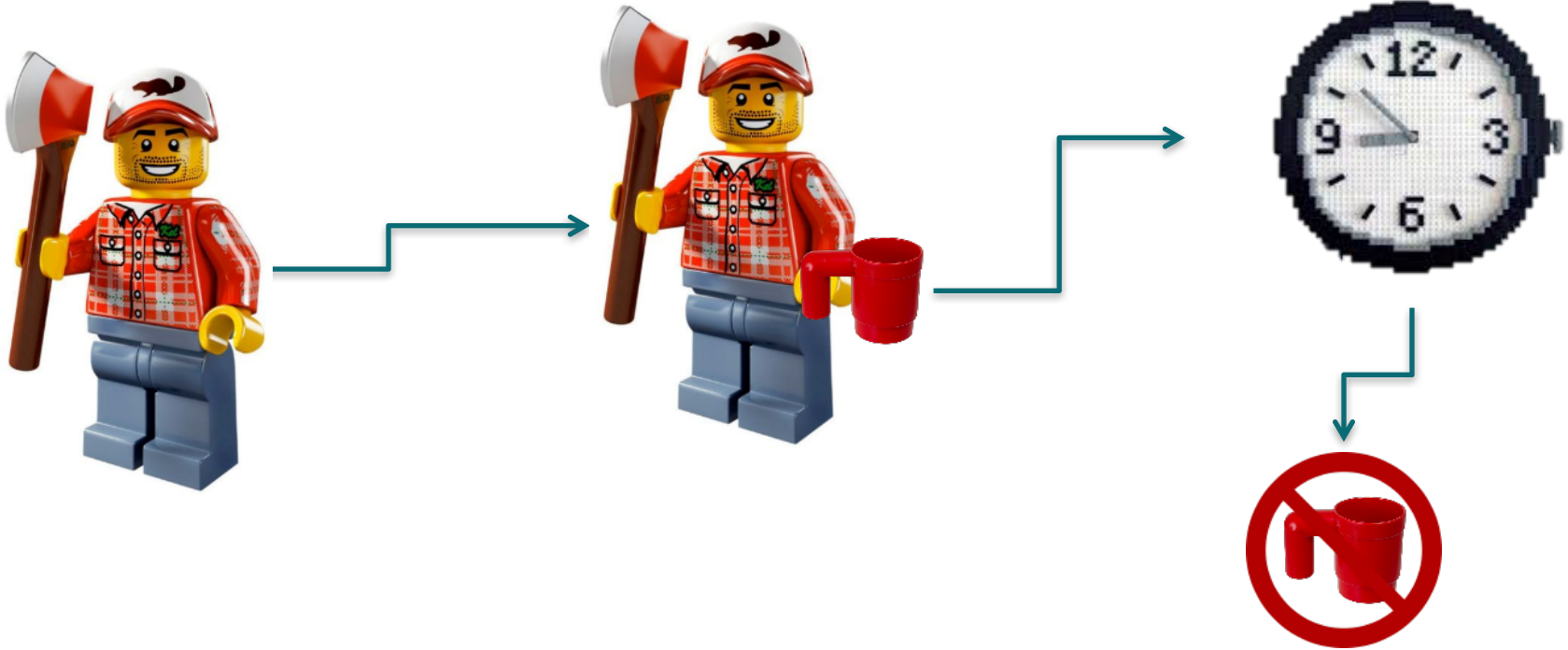
Каждая категория набирает очки

# Stealthwatch: Тревоги

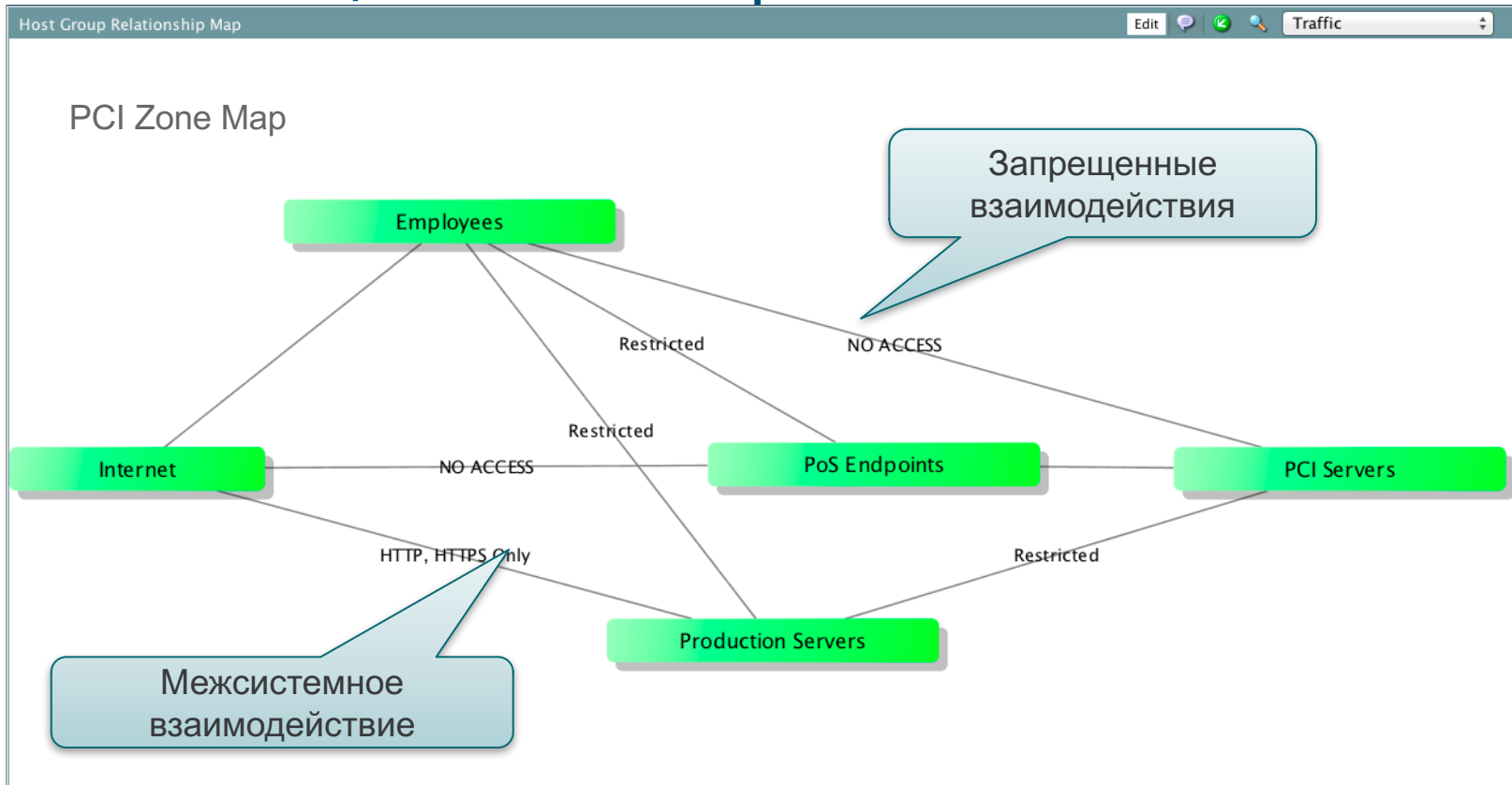
- Показывает серьезные отклонения в поведении и нарушение политики
- Известные и неизвестные атаки генерируют тревоги
- Активность выбивающаяся из нормы, разрешенного поведения или установленных политик

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

**Host Locking: Edit Rule**

Name: Employees to Confidential Servers

Description: Unauthorized Traffic: A host in the employee group should not communicate with hosts in the confidential server group.

Client Host Group: Inside Hosts -> By Function -> Employees

Server Host Group: Inside Hosts -> By Function -> Servers -> Confidential Servers

Disallow all traffic except  
 Allow all traffic except

Services

- 0-hop
- 3pc
- a/n
- afs
- ah
- aol-im
- apple-net-assistant
- appleshare

Applications

- 3com AMP3
- 3Com TSMUX
- ACAP
- AccessBuilder
- ActiveX
- Adobe Connect
- Adobe EchoSign
- AFS

Unidirectional UDP traffic triggers alarm

Unidirectional TCP traffic triggers alarm

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

Alarm Table - 1 record

Policy	Start Active Time	Alarm	Source	Source Host Groups	Source Use...	Target	Target Host ...	Details
Inside Hosts	Jun 23, 2017 10:45:00 AM (7 minutes 10s ago)	Host Lock Violation	10.90.90.102	Employees	employee1	10.50.50.100	Confidential Servers, PCI Servers	Rule #1 Employees to Confidential Servers Source Host is using http (80/tcp) as client to 10.50.50.100 (Double-click for details)

# Нарушение политик: Собственные события

demo.local | Alarm Dashboard : Policy Violation (1)

Экран тревог показывает все тревоги

Alarms

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	<a href="#">Employee to Production Servers</a>	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.

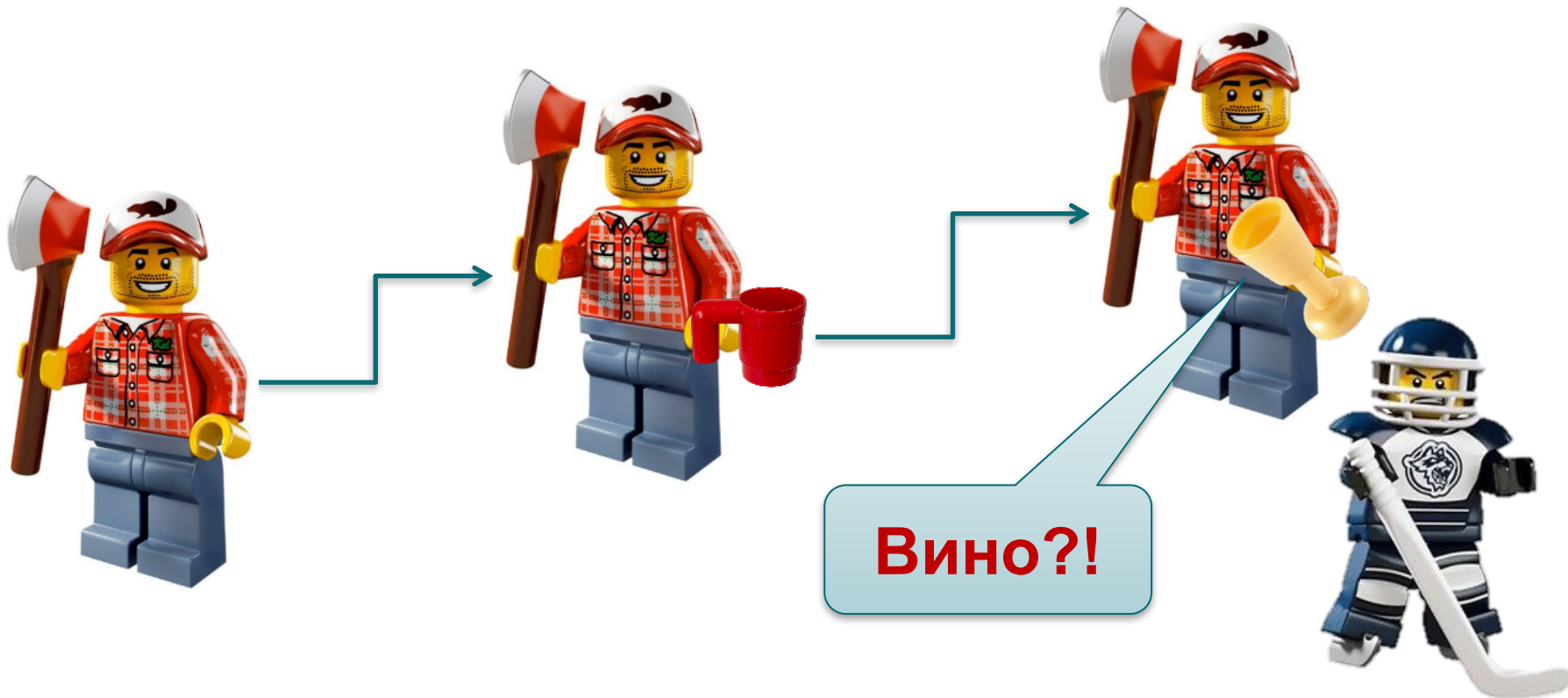
demo.local | Alarms : Employee to Production Servers for 5/25/2015 (1)

Показаны детали по “Employee to Productions Servers” тревоги

Alarms



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	<a href="#">View Details</a>	Current	Yes	No

# Обнаружение аномалий: Отклонение от нормы



# Пример категории тревог: Concern Index

**Concern Index:** Отслеживает hosts, 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, Recon	No settings	
Addr_Scan/udp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, Recon	No settings	
Bad_Flag_ACK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index, Anomaly	No settings	
Bad_Flag_All	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index, Anomaly	No settings	
Bad_Flag_NoFlg	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index, Anomaly	No settings	
Bad_Flag_Rsrvd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index, Anomaly	No settings	
Bad_Flag_RST	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index, Anomaly	No settings	
Bad_Flag_SYN_FIN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	High Concern Index, High Target Index,	No settings	

# High Concern Index

Отклонение от базового уровня на 2,432%!

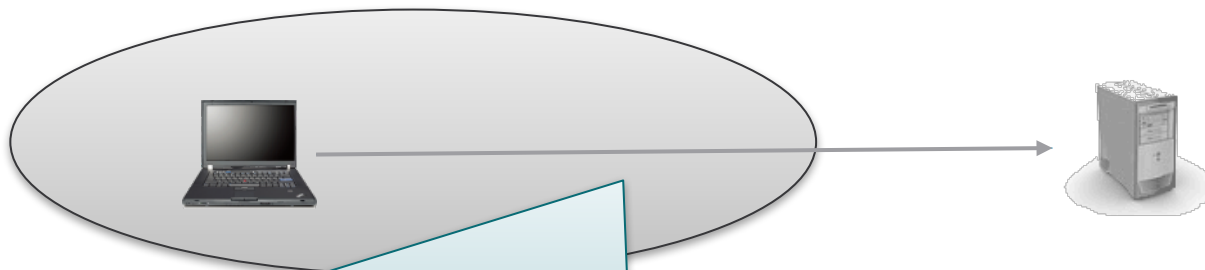
Concern Index x

Filter Domain : ACME Time : Today

Summary - 92 records summarized into 92 records

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

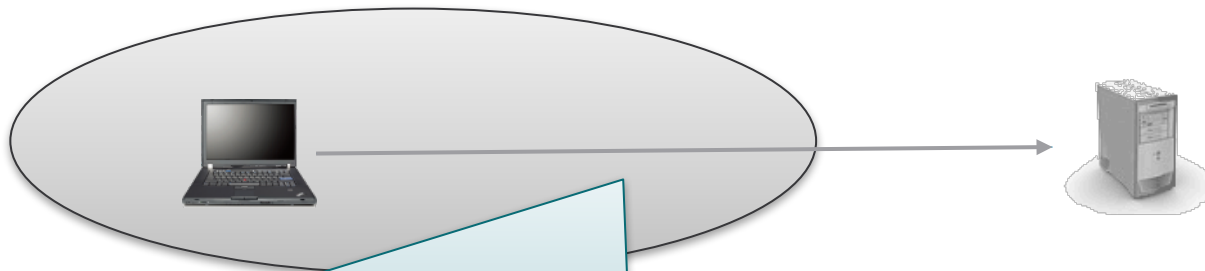
Политика по-умолчанию

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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.

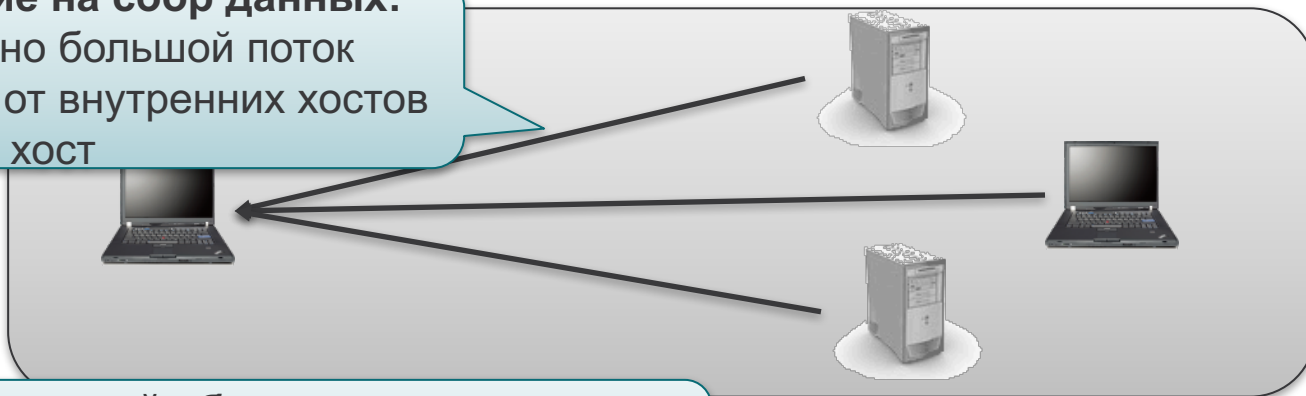
Политика по-умолчанию

Type	Enable Source	Alarm Source	Enable Target	Alarm Target	Alarm Categories	Settings	Mitigation
Suspect Data Loss	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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

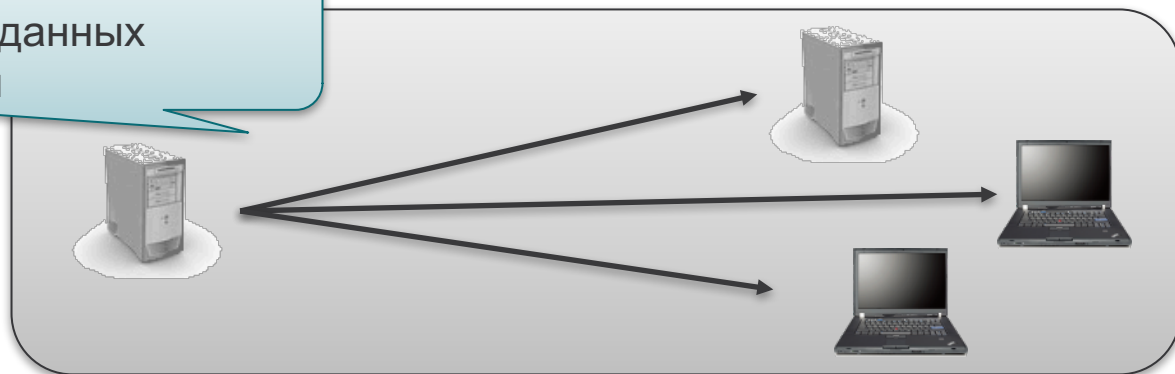
## Подозрение на сбор данных:

- Необычно большой поток данных от внутренних хостов на один хост



## Таргетированный сбор данных:

- Необычно большой объем данных исходящий на многие 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

Host Policy Manager for Domain "Lancopse"

Host Policies

IP Address:

Host Policy Report Remove Edit... Show Effective Policy...

Role Policies

Name	Description	Assigned to Host Groups	Assigned to Ranges
Alex		Email CRM	
Asia		Asia	
Business Critical Application		Business Critical App	
Compliance Hosts Policy	Policy for compliance hosts	Compliance Hosts	
Policy Target			
Ecommerce		Ecommerce	
User Policy	Policy for end users within network	Sales and Marketing	
Engineering Policy	Policy for engineering segment	Engineering	
Firewall & Proxy Policy	Policy set for network firewall & proxies	Firewalls Proxies-NAT	
High Target Index Suppress		Catch All HoneyNet Infrastructure By Locations Users	

Duplicate... Add...

Default Policies

Name	Description
Inside Hosts	All hosts in Inside Hosts
Outside Hosts	All hosts in Outside Hosts

Edit... Help Close

Проверка применяемых политик

Назначение политики группам

Создать ролевые политики для отдельных групп

Политики по-умолчанию для внутренних и внешних хостов

# Создание и изменение ролевой политики

Edit Role Policy - Network Management & Scanners

Name:

Description:

Assign to: Host Groups:

Задать ролевую политику

Назначить Хостовые группы на Ролевую политику

Назначить категории тревог и событий на роль

IP Address Ranges:

Alarm Categories **Security Events**

Type	Impact Source Policy	Enable Source	Alarm Source	Impact Target Policy	Enable Target	Alarm Target	Alarm Categories	Settings	Mitigation
Addr Scan/tcp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Recon, High Concern Index	No settings	No settings
Addr Scan/udp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Recon, High Concern Index	No settings	No settings
Bad Flag ACK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High Target Index, Recon, High Concern Index	No settings	No settings
Bad Flaq All							Hiah Targa Index.	No settinas	No settings

Включить/Выключить события безопасности – Подумайте над направлением!

Help

Export...

Import...

Apply

Edit Mitigation...

Enable All Events

Disable All Events

Close

OK

# Установка граничных значений событий

Включить и выдавать тревоги

Type	Enable Source	Alarm Source	Enable Target	Alarm Target	Alarm Categories	Settings
Suspect Data Loss	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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

Аномалии и политики

Приемлемое отклонение от нормы

Behavioral and Threshold  Threshold Only

Tolerance:



75

Never trigger alarm when less than:

1,000,000,000

client payload bytes in 24 hours

Always trigger alarm when greater than:

5,000,000,000,000

client payload bytes in 24 hours

Указать границы

Close

OK

# Реагирование на обнаружение аномалий

Ранжирование по приоритету

Используется классификация!

HOST	CATEGORY
10.201.3.149 ⓘ End User Devices	DH RC CI EX
10.201.3.18 ⓘ End User Devices	DH RC
10.201.0.23 ⓘ Terminal Servers	DH EX
10.150.1.200 ⓘ WebHostedApp	RC DH EX CI
10.10.101.24 ⓘ End User Devices	EP
10.10.30.15 ⓘ DNS Servers	DT
10.201.3.50 ⓘ End User Devices	CI RC

[View All Hosts >](#)

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



# Расследование ИОС: Пример

Обнаружен новый сервер  
Malware!



Zeus C&C Server:  
**128.107.78.8**

# Шаг 1: Мы этот хост видели?

Ищем по IP адресу



Stealthwatch

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

128.107.78.8

Hosts

Известен и недавно его видели

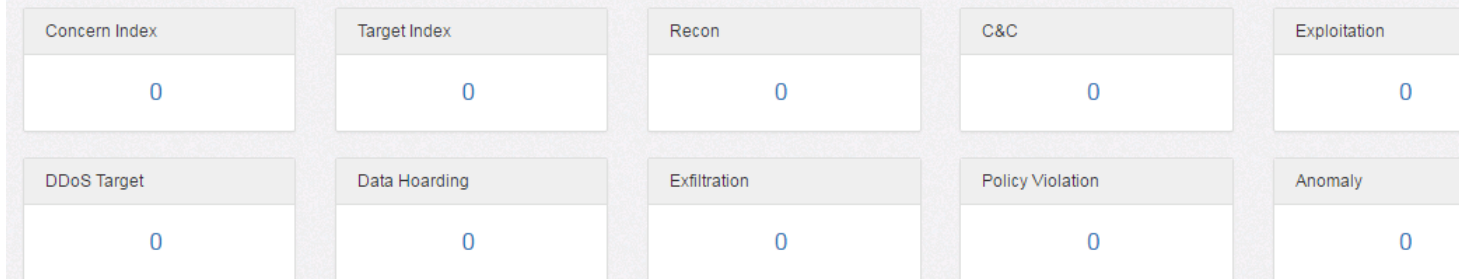
Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

First Previous **1** Next Last

# Шаг 2: Расследование вторжения

Host Report for 128.107.78.8



## Host Summary



Host IP

128.107.78.8

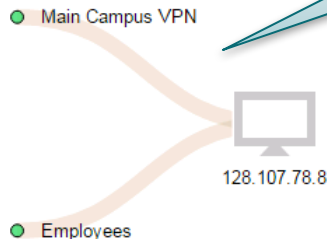
Flows

Classify

History

**Status:** Inactive  
**Hostname:** -  
**Host Groups:** United States  
**Location:** United States  
**Last Seen:** 1/27/17 9:13 PM  
**Policies:** Outside

## Traffic by Peer Host Group (last 12 hours)



Недавние связи с хостами внутри сети

# Шаг 2: Классификация

The screenshot displays the 'Host Report for 128.107.78.8' interface. At the top, there are several summary cards for metrics like Concern Index, Target Index, Recon, C&C, Exploit, DDoS Target, Data Hoarding, Exfiltration, Policy Violation, and Anoma. Below these is the 'Host Summary' section, which includes a host icon, IP address (128.107.78.8), and buttons for 'Flows', 'Classify', and 'History'. The 'Classify' button is highlighted with a red box. To the right, a 'Traffic by Peer Host Group (last 12 hours)' chart shows connections from 'Main C...' and 'Employees' to the host. On the far right, a search and filter panel is open, showing a tree view of host groups. The 'United States' group is expanded, and 'Matt's Zeus Server' is selected, also highlighted with a red box. A light blue callout bubble with the text 'Назначение в хост-группу' (Assignment to host group) points to the 'Matt's Zeus Server' selection. At the bottom right of the filter panel, there are 'Cancel' and 'Classify' buttons.

Host Report for 128.107.78.8

Concern Index: 0

Target Index: 0

Recon: 0

C&C: 0

Exploit: 0

DDoS Target: 0

Data Hoarding: 0

Exfiltration: 0

Policy Violation: 0

Anoma: 0

Host Summary

Host IP: 128.107.78.8

Flows | **Classify** | History

Status: Inactive

Hostname: --

Host Groups: United States

Location: United States

Last Seen: 1/27/17 9:13 PM

Policies: Outside

MAC Address: --

Quarantine | Unquarantine

Traffic by Peer Host Group (last 12 hours)

Main C... | 128.107.78.8 | Employees

Search

- Inside Hosts
- Outside Hosts
  - Countries
    - Africa
    - Americas
      - Caribbean
      - Central America
      - Northern America
        - Bermuda
        - Canada
        - Greenland
        - St. Pierre and Miquelon
        - United States
      - South America
    - Asia
    - Europe
    - Oceania
    - Other
      - Matt's Zeus Server**
    - Trusted Internet Hosts
    - Command & Control Servers
    - Tor
    - Recon

Cancel | **Classify**

Назначение в хост-группу

# Шаг 3: Поиск инфицированных хостов

Построение запроса потока, включающего C&C Сервер

Q Flow Search ⓘ

Clear All

Time Range: Last 12 Hours

Subject:

128.107.78.8 ✕

Orientation: Either

Peer:

Host Groups: Employees ✕

Начнем с определенного временного диапазона

Направление изначально в привилегированные группы

SEARCH TYPE

Flow

TIME RANGE

Last 12 Hours

SEARCH NAME

Flow on 1/

Subject

HOST IP ADDRESS OR RANGE

128.107.78.8 ✕

Connecti

APPLICATION

Select

PORT / PROTOCOL

ex. 80/tcp or 180/tcp

# Шаг 4: Анализ возвращенных результатов

Загрузка  
Вредноса

START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER PROCESS NAME	PEER FILE HASH
▶ Jan 27, 2017 8:13:10 PM	1m 32s	128.107.78.8 <a href="#">View URL</a> <a href="#">Data</a>	80/TCP	United States	494.11K	HTTP (unclassified)	496.57K	10.100.10.101	49271/TCP	Main Campus VPN,Employees	firefox.exe	BE0B500D92C2A93E2E
▶ Jan 27, 2017 9:13:55 PM	2s	128.107.78.8 <a href="#">View URL</a> <a href="#">Data</a>	80/TCP	United States	37.07K	HTTP (unclassified)	37.36K	10.100.10.101	49787/TCP	Main Campus VPN,Employees	taskhost.exe	473866333D2241BAD6S

C&C Сервер

Зараженный хост

Звонок "домой"

# Шаг 5: Расследование зараженных хостов

Host Report for 10.100.10.101

Открыть и  
исследовать отчет  
хоста

The screenshot displays a host report for IP 10.100.10.101. At the top, there are eight summary cards showing zero values for Concern Index, Target Index, Recon, C&C, DoS Target, Data Hoarding, Exfiltration, and Policy Violation. Below these is a 'Host Summary' section with a computer icon and the IP address 10.100.10.101. It includes tabs for Flows, Classify, and History, and lists details such as Status (Active), Hostname (--), Host Groups (Main Campus VPN, Employees), Location (RFC 1918), Last Seen (1/27/17 10:17 PM), Policies (Inside), and MAC Address (00:50:56:b6:4b:1a (VMware, Inc.)). At the bottom of this section are 'Quarantine' and 'Unquarantine' buttons. To the right is a 'Traffic by Peer Host Group (last 12 hours)' section featuring a network diagram. The diagram shows the host 10.100.10.101 connected to various host groups: StealthWatch System, Main Campus VPN, Employees, DHCP Servers, Domain Controllers, DNS Servers, Confidential Servers, PCI Servers, and Development Servers. The host is also shown with connections to 'United States' and 'Canada'.

# Шаг 5: Расследование инфицированных хостов

The screenshot displays the Cisco StealthWatch interface for a host with IP 10.100.10.101. The interface is divided into several sections:

- Host Summary:** Shows host details such as IP, status (Inactive), hostname, host groups (Main Campus VPN, Employees), location (RFC 1918), last seen time (1/27/17 10:20 PM), policies (Inside), and MAC address.
- Traffic by Peer Host Group (last 12 hours):** A network diagram showing connections from various host groups to the target host. A red box highlights 'DNS Servers' and 'Confidential Servers'.
- Users & Sessions:** A table showing user sessions associated with the host's MAC address. A red box highlights the session for user 'employee1'.
- Application Traffic:** A table showing traffic for applications like NetFlow and NetBIOS.

Определение пользователя и устройства

Касательно ущерба: Требуется мгновенная реакция и глубокого расследования, реагирования на инцидент

# Шаг 6: Rapid Threat Containment

The screenshot displays the Cisco StealthWatch interface for a host report. A white dialog box with the title "Success" is overlaid on the screen, containing the text: "Quarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the ISE appliance or contact your ISE administrator." Below the text is a blue "Ok" button. In the background, the "Host Report for 10.100.10.101" is visible, showing various metrics like Concern Index, Target Index, DDoS Target, and Data Hoarding, all with a value of 0. The "Host Summary" section shows the host IP 10.100.10.101, status "Active", and a red box highlighting the "Quarantine" button. The "Traffic by Peer Host" section shows a network diagram with various server categories and a map of the United States.

Success

Quarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the ISE appliance or contact your ISE administrator.

Ok

Host Report for 10.100.10.101

Concern Index 0

Target Index 0

DDoS Target 0

Data Hoarding 0

Host Summary

Host IP 10.100.10.101

Flows Classify History

Status: Active

Hostname: --

Host Groups: Main Campus VPN, Employees

Location: RFC 1918

Last Seen: 1/27/17 10:20 PM

Policies: Inside

MAC Address: 00:50:56:b6:4b:1a (VMware, Inc.)

Quarantine Unquarantine

Traffic by Peer Host

StealthWatch Sys

Main Campus VPN

Employees

DHCP Servers

Domain Controllers

DNS Servers

Confidential Servers

PCI Servers

Development Servers

United States

10.100.10.101

Canada

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

Subject: File Hash: 47386633D2241BAD6918D21EBCBE8F8EEA9344D816788300BCA290A89FBD3DD Orientation: Either

Connection: Direction: Total

DURATION	SUBJECT	PORT/PROTOCOL	TRAFFIC SUMMARY	PORT/PROTOCOL	PEER
▶ Start: 01/27 - 10:13:00 PM End: 01/27 - 10:17:15 PM Duration: 4m 15s	 10.100.10.101 ⓘ <a href="#">View URL Data</a>  RFC 1918 employee1 00:50:56:b6:4b:1a	49327/TCP	3.89KB   10 packets → HTTPS (unclassified) ← 409.25KB   908 packets	443/TCP	 173.194.203.105 ⓘ  United States pg-in-f105.1e100.net
▶ Start: 01/27 - 10:13:55 PM End: 01/27 - 10:13:57 PM Duration: 2s	 10.100.10.101 ⓘ <a href="#">View URL Data</a>  RFC 1918 employee1 00:50:56:b6:4b:1a	50183/TCP	295B   2 packets → HTTP (unclassified) ← 37.07KB   82 packets	80/TCP	 128.107.78.8 ⓘ  United States

# Шаг 7: Продолжение расследования и мониторинга

Создать правило для уведомления о будущих связях

Custom Event: Communication to Matt's Zeus Servers

Rule/Event Name:

Communication to Matt's Zeus Servers

Description:

ex. Event will trigger based on this rule.

Object

Host:

includes

Host Groups

Host Groups

Select

Inside Hosts

User:

Devices:

Peer

Host:

includes

Host Groups

Host Groups

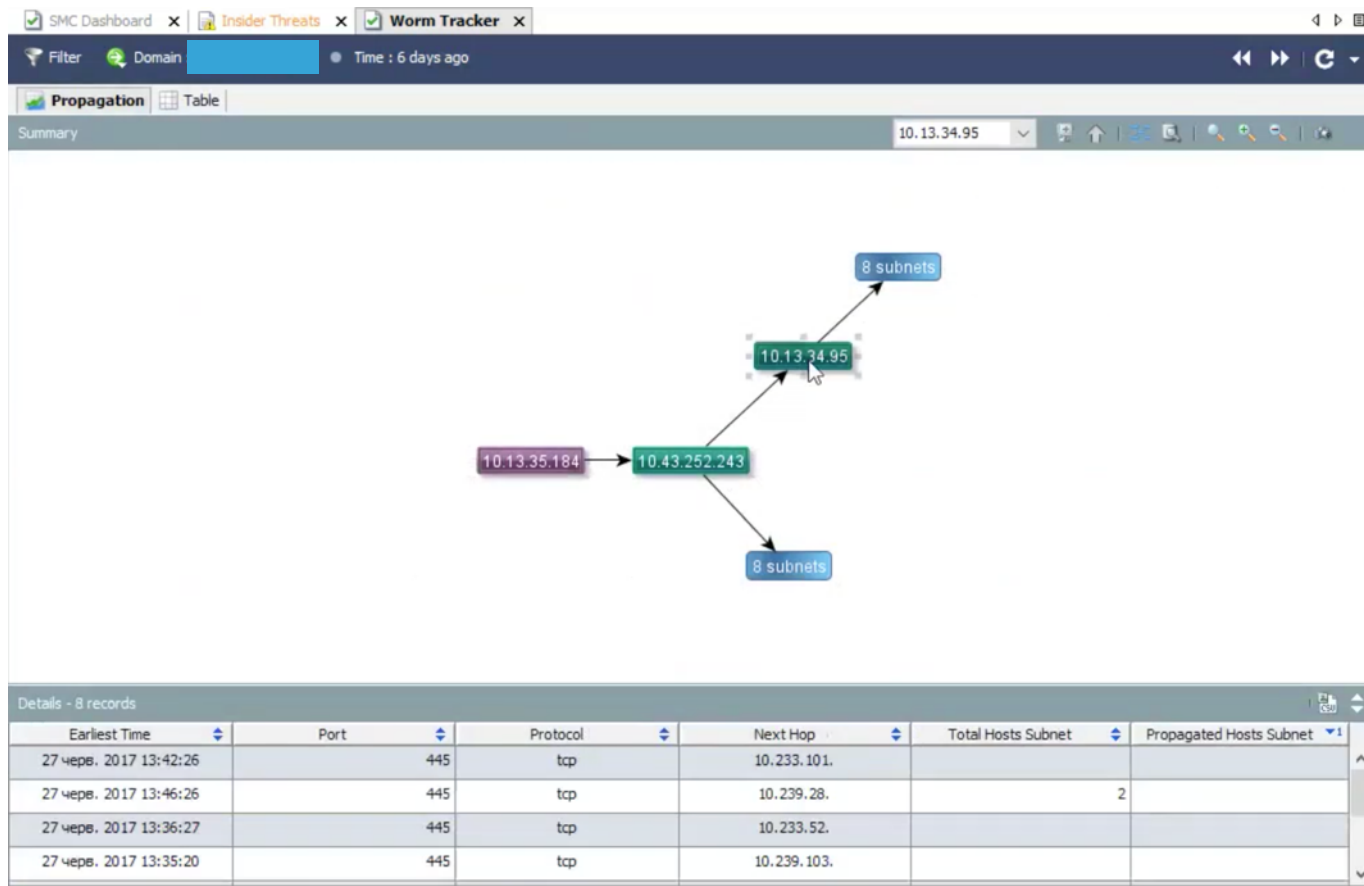
Select

Matt's Zeus Server

User:

Devices:

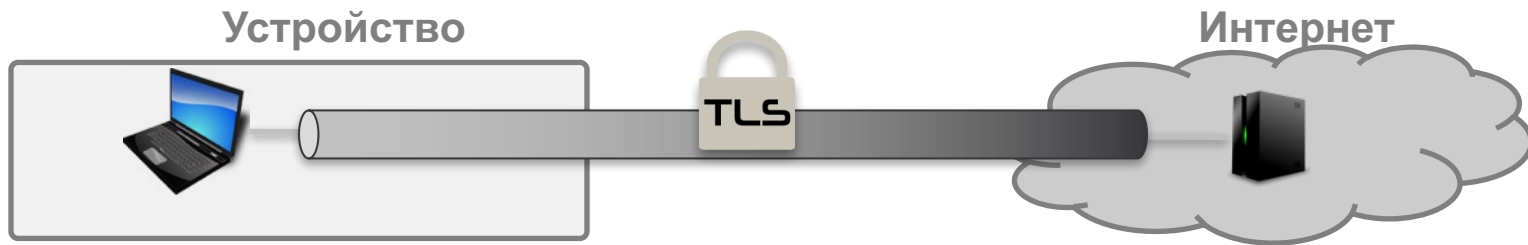
# Решение Cisco StealthWatch в анализе атаки Pyetya/Nyetya





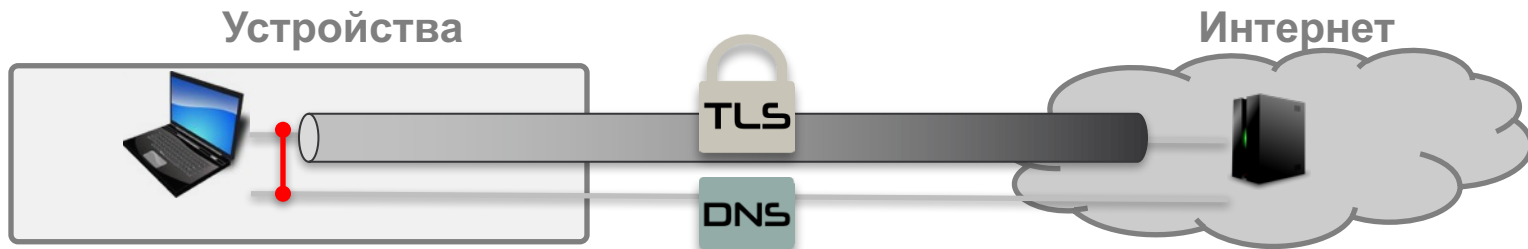
# Анализ зашифрованного трафика

# 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, ...

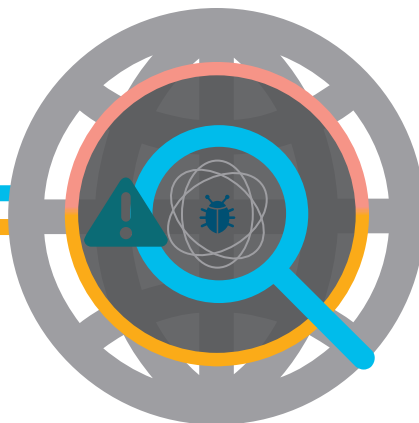
**DNS данные:** имена, типы запросов, временные параметры запросов

**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

Зашифрованный  
трафик



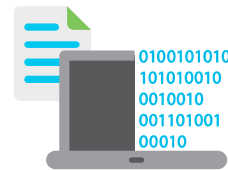
Незашифрованный  
трафик



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

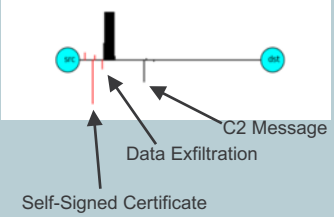



“Identifying encrypted malware traffic with contextual flow data”

AISeC '16 | Blake Anderson, David McGrew (Cisco Fellow)

# Возможности данных ETA

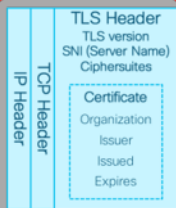
Исследования Cisco

	TCP/IP	DNS	TLS	SPLT
Malware traffic	Наблюдаемый адрес	c15c0.com afb32d75.com	Необычный отпечаток Необычный сертификат	 <p>Self-Signed Certificate Data Exfiltration C2 Message</p> <p>Bestafera</p>
Benign traffic	Превалирующий адрес	cisco.com	Типичный отпечаток Типичный сертификат	 <p>Google search</p>

# Как мы инспектируем трафик?

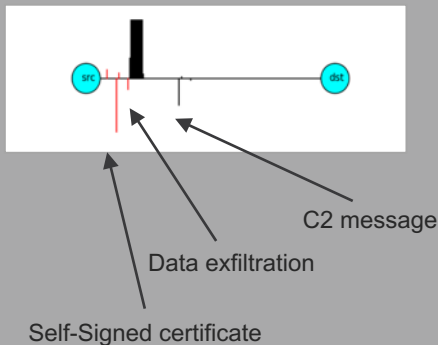
## Первоначальный пакет

Получить как можно больше из незашифрованных пакетов



## Sequence of packet lengths and times

Идентифицировать содержимое с помощью размера и последовательности пакетов



## 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 Cisco

Расширенная аналитика и машинное обучение

Глобальная корреляция знаний

Постоянное соответствие

# Немного науки

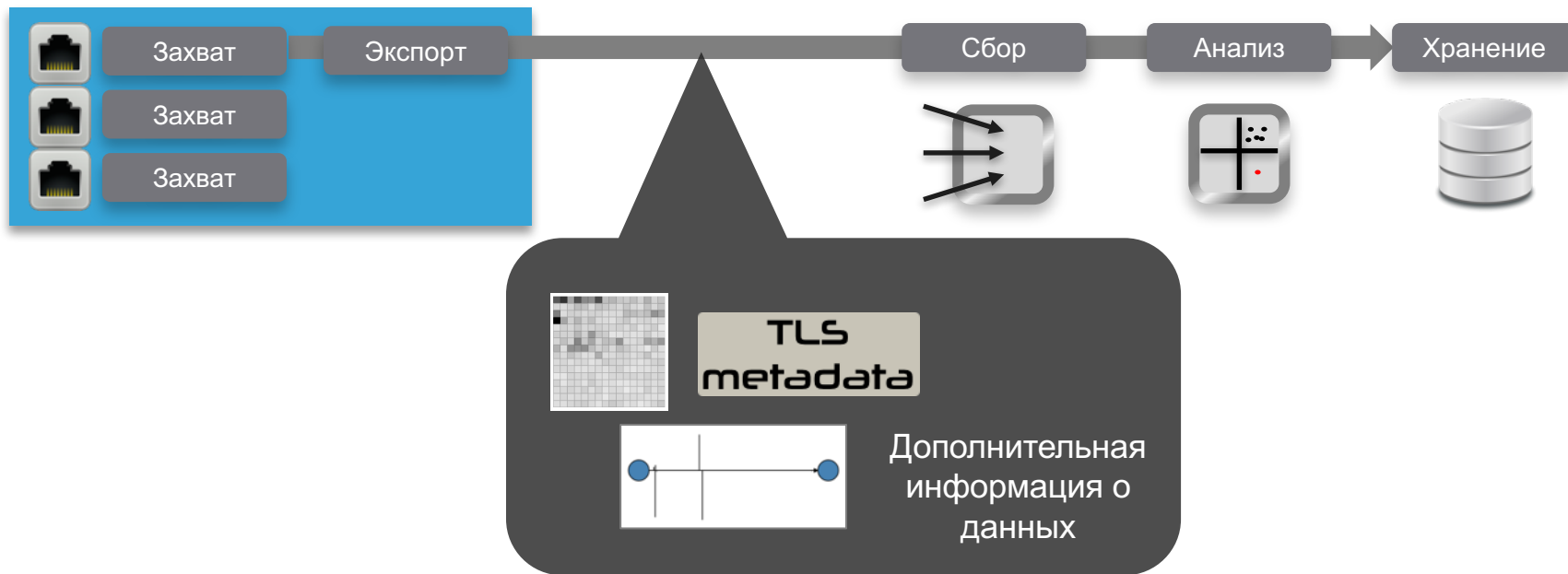
# Традиционный анализ сетевых потоков

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



# Сбор расширенной телеметрии

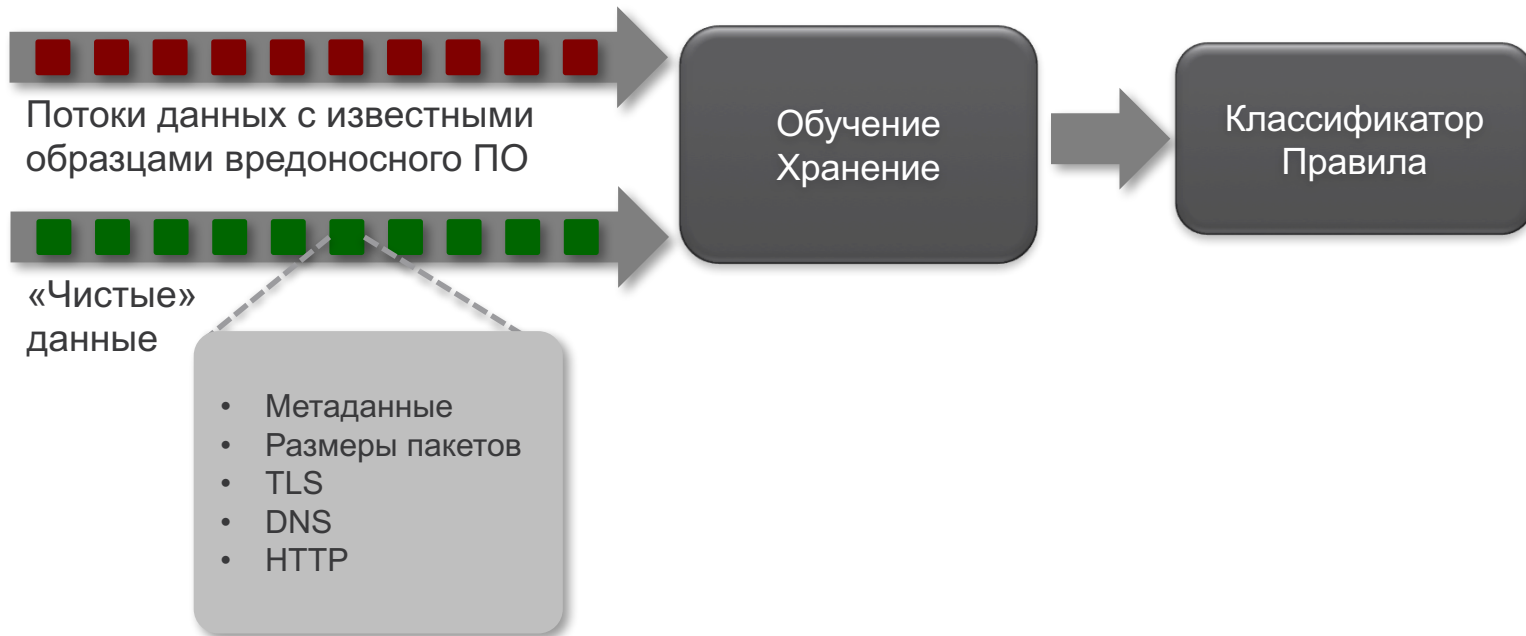
**srcIP, dstIP, srcPort, dstPort, prot, startTime, stopTime, numBytes, numPackets**



# Обзор решения



# Набор данных, использованный в исследовании



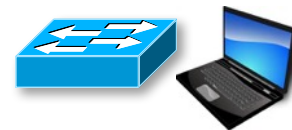
# Потоки данных с известными образцами ВПО

- 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



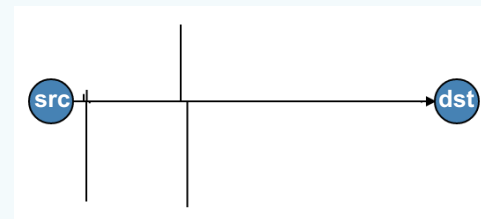
# «Чистые» данные

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

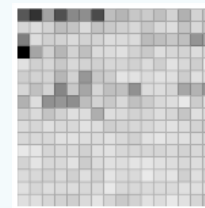


# Типы данных, использованные из расширенной телеметрии

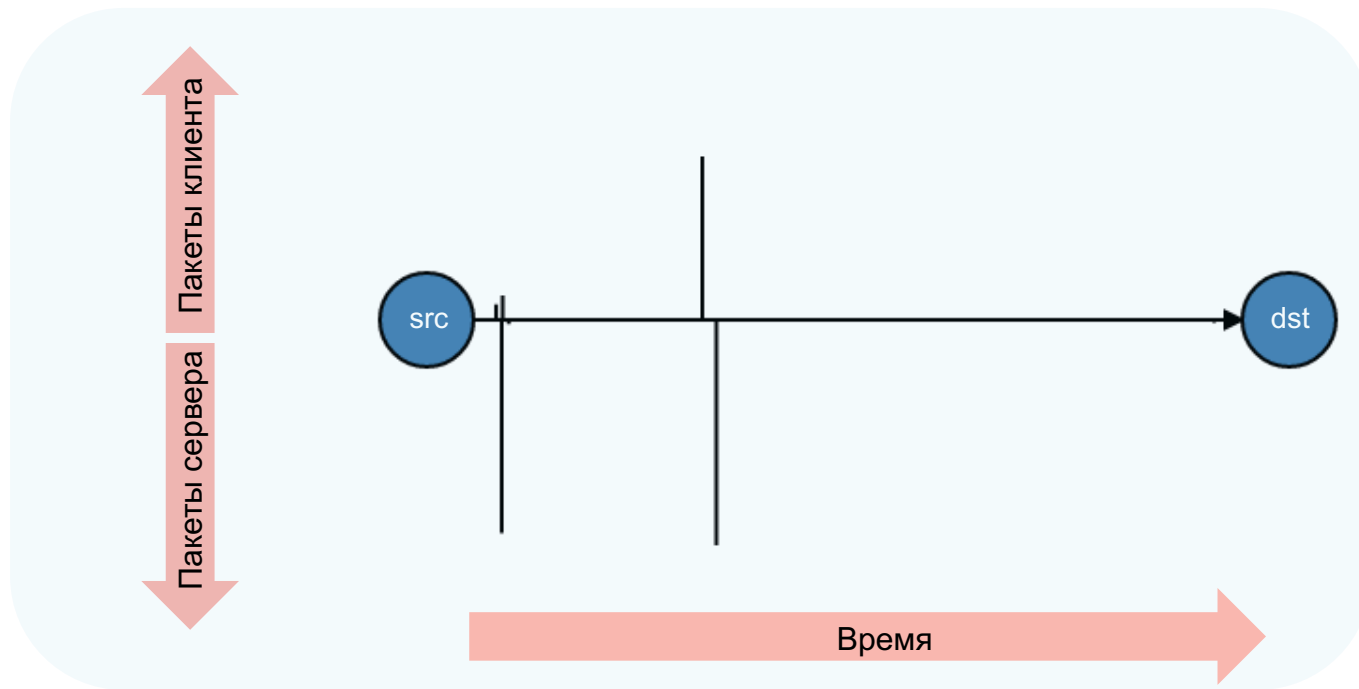
- **SPLT** – Sequence of Packet Lengths and Arrival Times, или распределение пакетов и их последовательностей с учётом временных интервалов



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



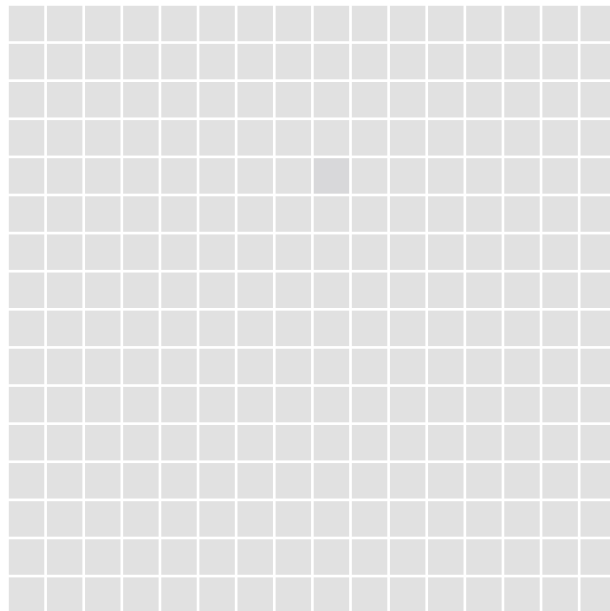
# SPLT - распределение пакетов и их последовательностей с учётом временных интервалов



# VD - побайтное распределение

Н Т Т Р / 1 . 1 2 0 0 0 К

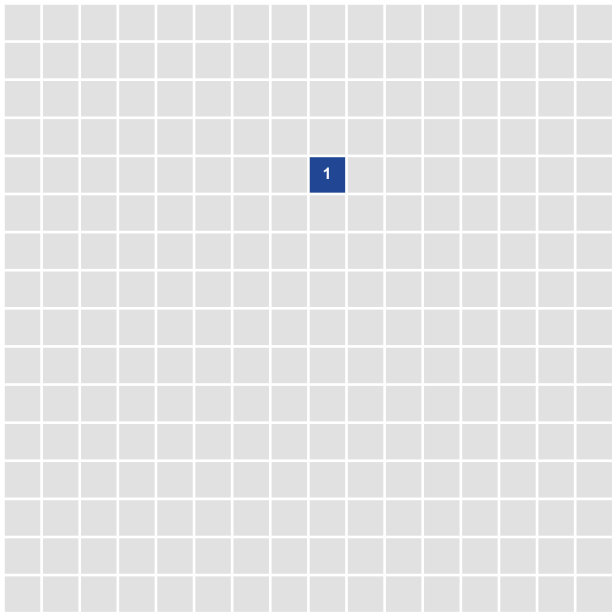
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b



# BD - побайтное распределение

Н Т Т Р / 1 . 1 2 0 0 0 К

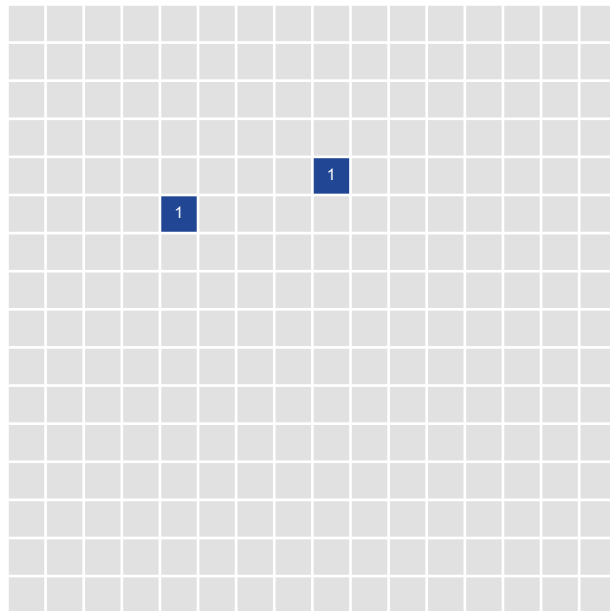
□□ 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b



# BD - побайтное распределение

Н Т Т Р / 1 . 1 2 0 0 0 К

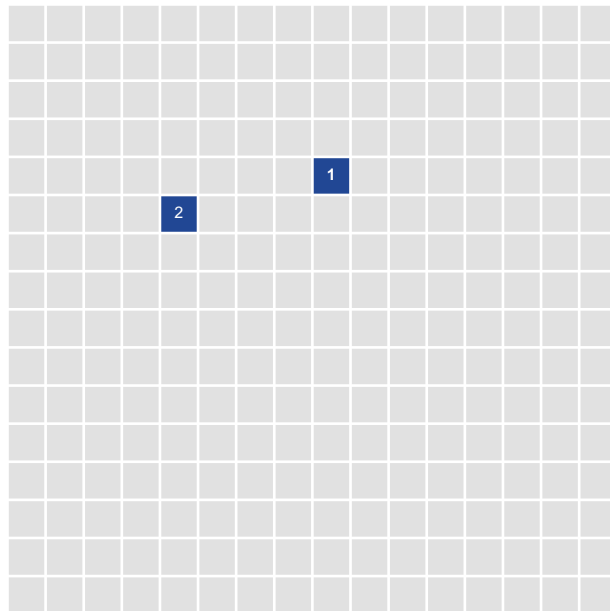
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b



# BD - побайтное распределение

Н Т **Т** Р / 1 . 1 2 0 0 0 К

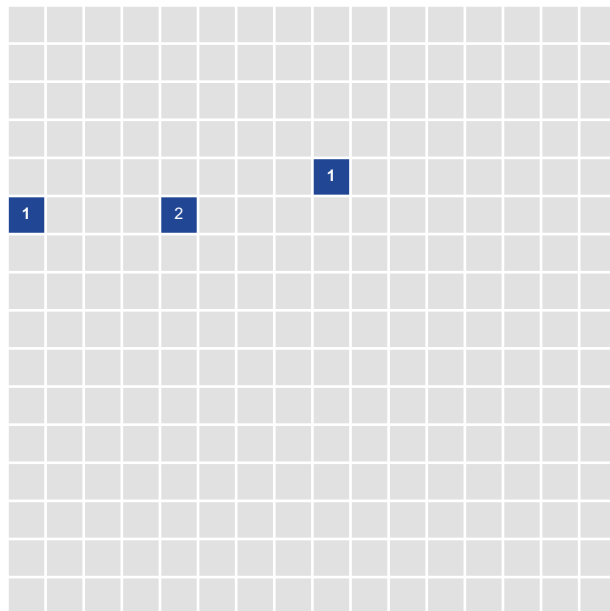
□□48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b



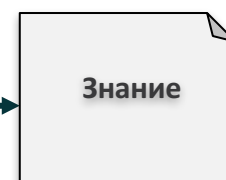
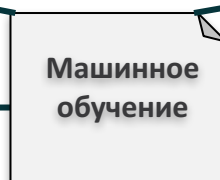
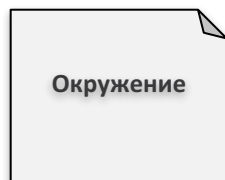
# BD - побайтное распределение

Н Т Т **Р** / 1 . 1 2 0 0 0 К

□□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

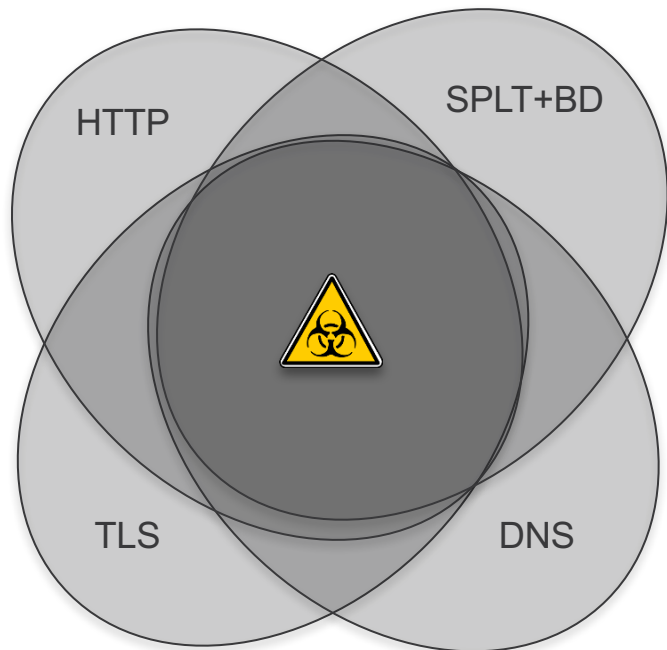
- HTTP

- 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.	FDR
SPLT+BD+TLS+HTTP+DNS	99.993%	0.00%
SPLT+BD+TLS+HTTP	99.978%	0.00%
SPLT+BD+TLS+DNS	99.983%	99.956%
SPLT+BD+TLS	99.968%	98.043%
SPLT+BD+HTTP	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!**