



Защита от современных угроз с помощью SourceFire FirePOWER и Cisco CTD

Андрей Москвитин

Специалист по решениям ИБ, Cisco

amoskvit@cisco.com

Текущие проблемы безопасности



Изменение бизнес-моделей



Динамический ландшафт угроз



Сложность и фрагментация

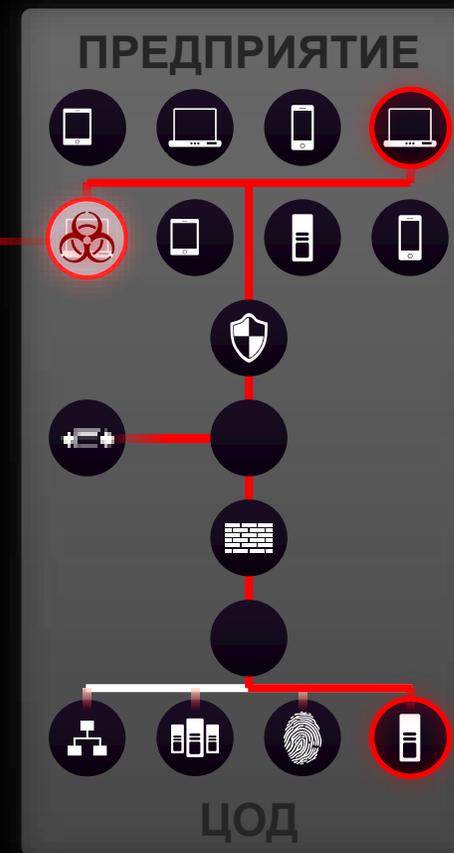
Анатомия современной угрозы



Заражение точки входа происходит за пределами предприятия

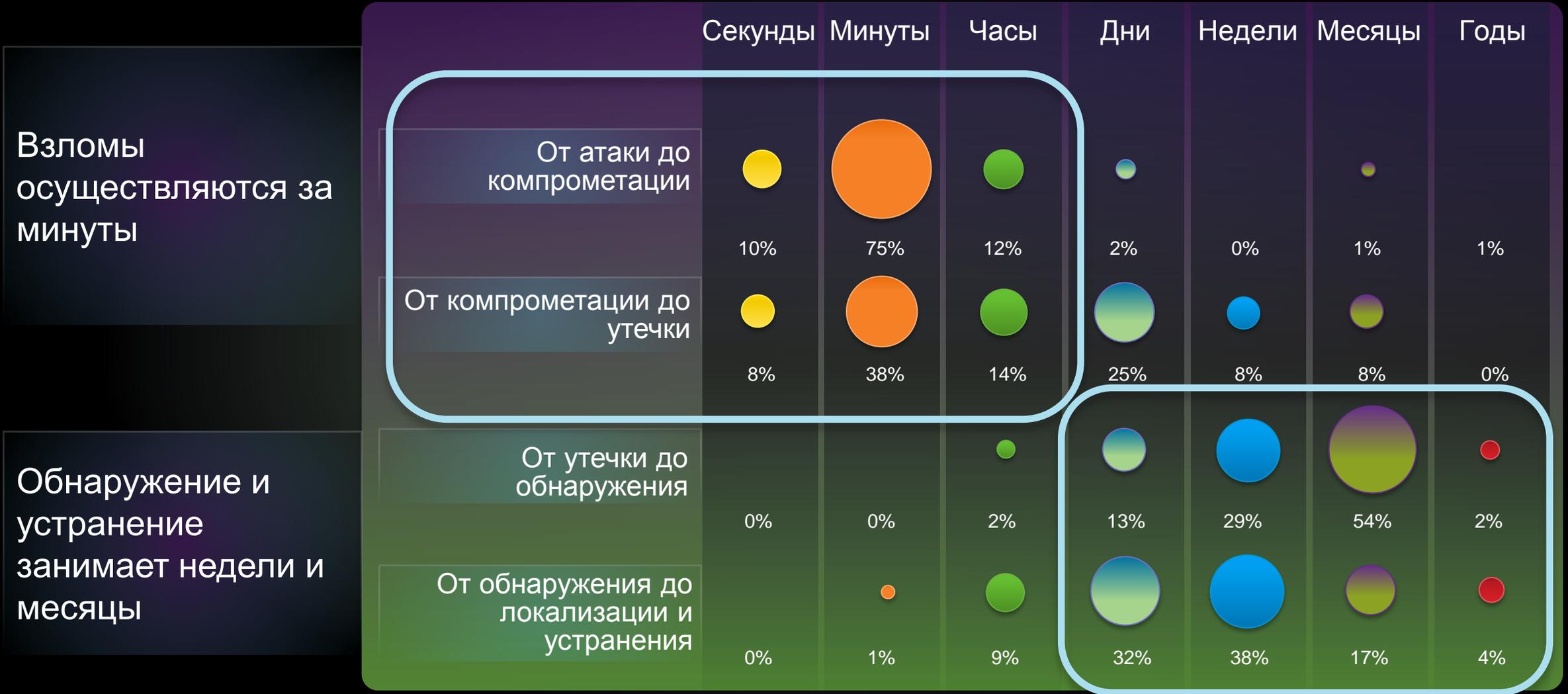


Продвинутые угрозы обходят средства защиты периметра



Угроза распространяется по сети и захватывает как можно больше данных

Время не на нашей стороне



Временная шкала событий в % от общего числа взломов

Источник: 2012 Verizon Data Breach Investigations Report

Если бы Вы знали что будете
взломаны действовали ли бы
Вы иначе?

Новая модель безопасности



Всеобъемлющий портфель решений в области ИБ

МСЭ и NGFW

- Cisco ASA / ASA-SM
- Cisco ISR / ASR Sec
- FirePOWER NGFW
- Meraki MX

IPS и NGIPS

- Cisco IPS
- Cisco wIPS
- Cisco ASA Module
- FirePOWER NGIPS

Advanced Malware Protection

- FireAMP
- FireAMP Mobile
- FireAMP Virtual
- AMP для FirePOWER

Интернет-безопасность

- Cisco WSA / vWSA
- Cisco Cloud Web Security

Безопасность электронной почты

- Cisco ESA / vESA
- Cisco Cloud Email Security

NAC + Identity Services

- Cisco ISE / vISE
- Cisco ACS

VPN

- Cisco AnyConnect
- Cisco ASA
- Cisco ISR / RVPN

UTM

- Meraki MX

Мониторинг инфраструктуры

- Cisco Cyber Threat Defense

Policy-based сеть

- Cisco TrustSec
- Cisco ISE
- Cisco ONE

Secure DC

- Cisco ASA / 1000v / ASA v / VSG
- Cisco TrustSec

Контроль приложений

- Cisco ASA NGFW / AVC
- Cisco IOS AVC / NBAR
- Cisco SCE / vSCE
- FirePOWER NGFW

#1 на рынке
сетевой безопасности
(Источник: Infonetics)

Лидер Gartner
Magic Quadrant
(Email Security, Web Security,
Network Access, SSL, IPS)

#1 на рынке ИБ
ЦОДов
(Источник:
Infonetics)

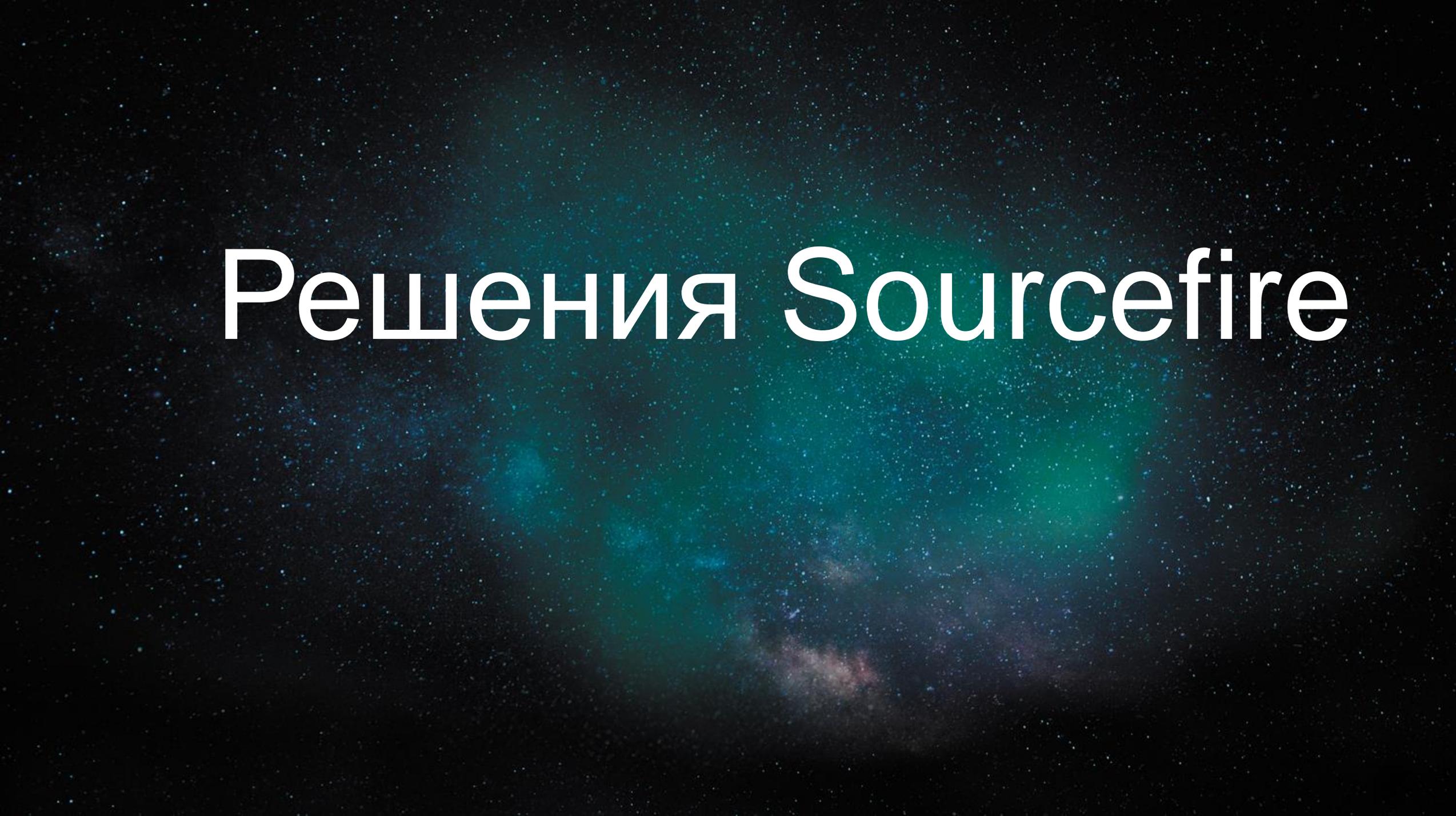
Безопасность
стала одним из 5-ти
основных
приоритетов
компании

Существенные
инвестиции
в R&D, M&A &
людей



Cisco Security Momentum

Решения Sourcefire

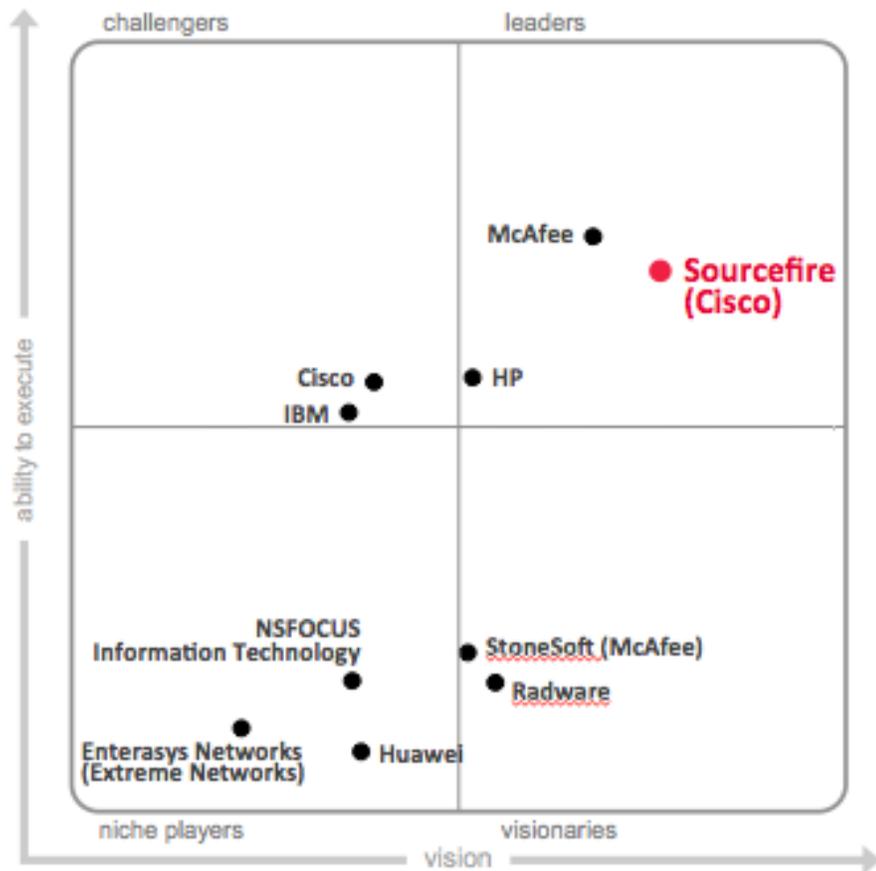


Sourcefire – эксперты в области ИБ

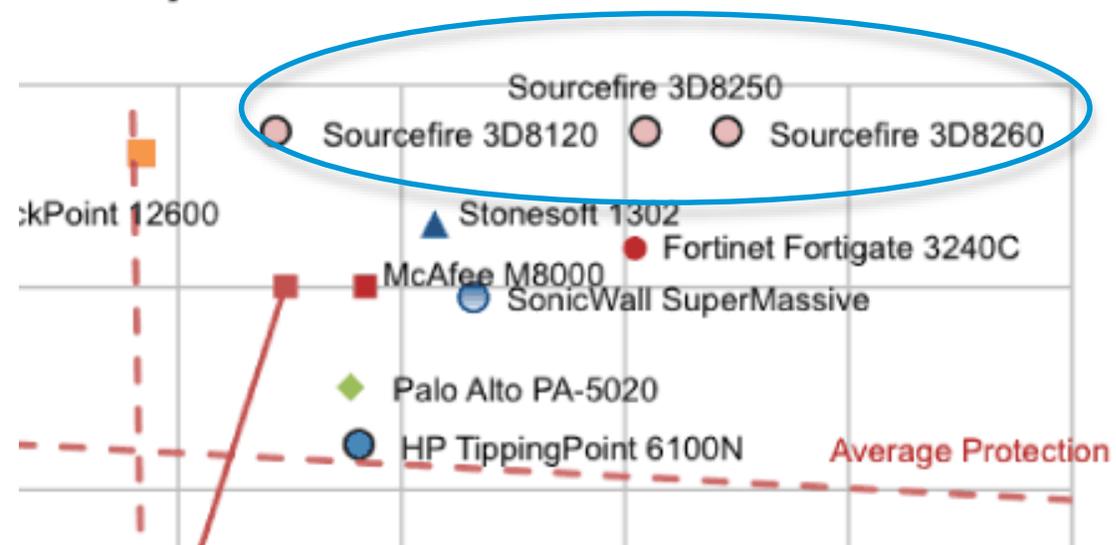
- Гениальная команда
- Больше 10 лет на рынке
- 6 лет подряд лидирует в квадратах Gartner
- Защищает компании в более чем 180 странах
- Инновации: 41+ патент получен или в разработке
- Open source проекты - Snort, ClamAV, Razorback, OpenAppID



Почему лучшие?



on Systems (IPS)

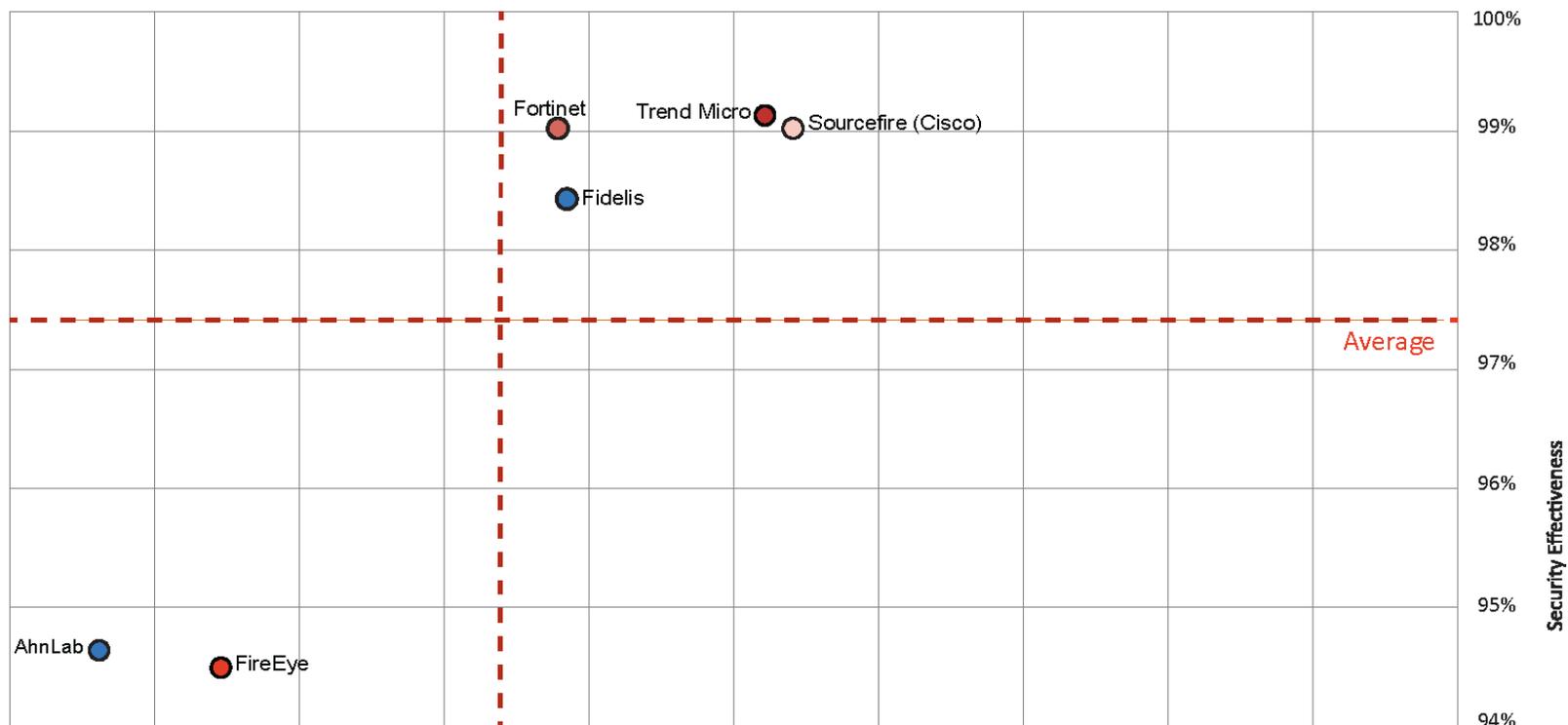


Лидер Gartner Magic Quadrant for IPS с 2006

Самый низкий TCO за защищаемый Мбит/с

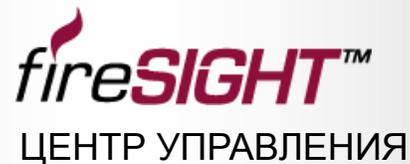
Почему лучшие? (продолж.)

NSS Labs Breach Detection Systems (BDS) Security Value Map™



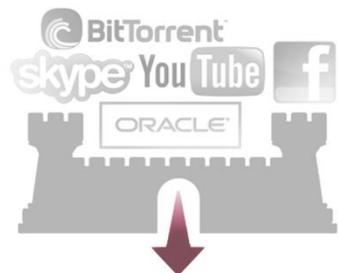
99% защита от угроз, обнаружение
100% exploits, самый низкий TCO
за Мбит/с

Sourcefire – решения по обеспечению безопасности



ДО

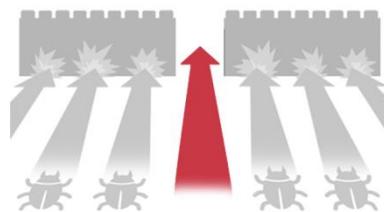
Вы видите,
вы контролируете



NGFW

ВО ВРЕМЯ

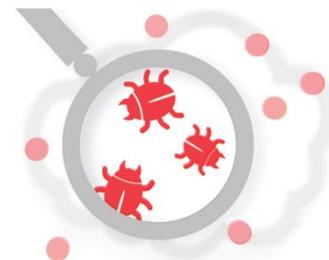
Интеллектуальное
противодействие
и с учетом контекста



NGIPS

ПОСЛЕ

Ретроспективные
средства безопасности



AMP

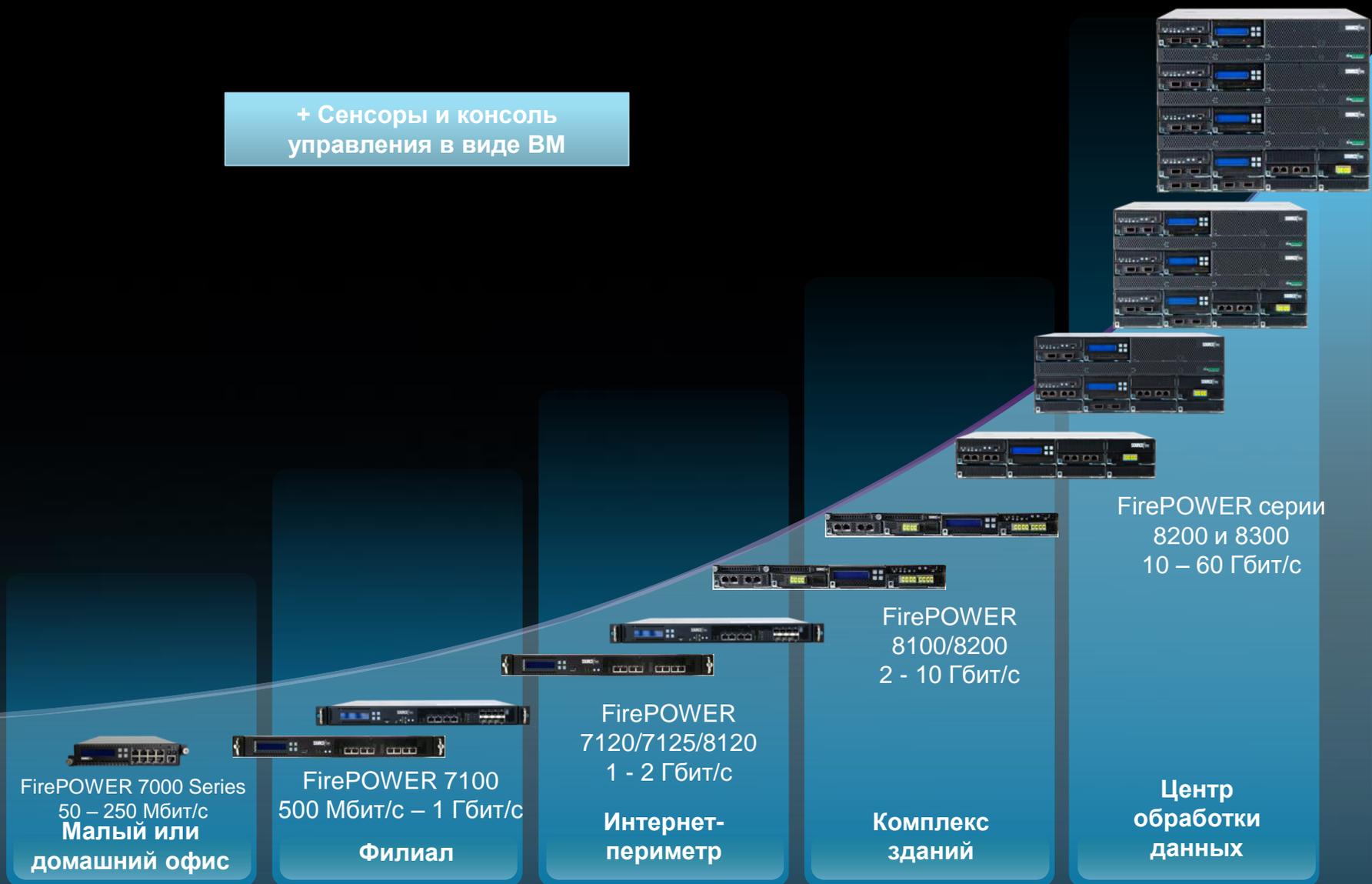


firePOWER™
УСТРОЙСТВА | VM

Платформы и размещение в сети

Производительность и масштабируемость системы предотвращения вторжений

+ Сенсоры и консоль управления в виде VM



FirePOWER 7000 Series
50 – 250 Мбит/с
Малый или домашний офис

FirePOWER 7100
500 Мбит/с – 1 Гбит/с
Филиал

FirePOWER 7120/7125/8120
1 - 2 Гбит/с
Интернет-периметр

FirePOWER 8100/8200
2 - 10 Гбит/с
Комплекс зданий

FirePOWER серии 8200 и 8300
10 – 60 Гбит/с
Центр обработки данных

Подход Sourcefire:

... непрерывный процесс до, во время и после атаки

Вы не можете
защитить то, что
не видите

Автоматическая
настройка системы
безопасности



В первую очередь необходимо знать, что у вас есть
Невозможно обеспечить защиту того, о чем вы не знаете



fireSIGHT™

Все время
в режиме
реального времени

Понимание контекста

Внутри ВАШЕЙ сети

ЛОКАЛЬНО
Бизнес Контекст

-  Кто
-  Что
-  Как
-  Откуда
-  Когда

А В С
1 2 В 1 4

Снаружи ВАШЕЙ сети

ГЛОБАЛЬНО
Ситуационный
анализ угроз

-  Репутация
-  Взаимодействие
-  Приложения
-  Сайты

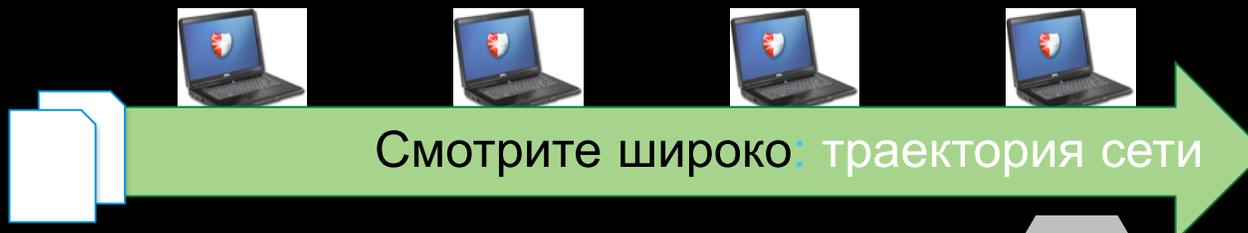
Реализация безопасности с **ЛОКАЛЬНЫМ**
и **ГЛОБАЛЬНЫМ** контекстом

Понимание контекста (продолж.)

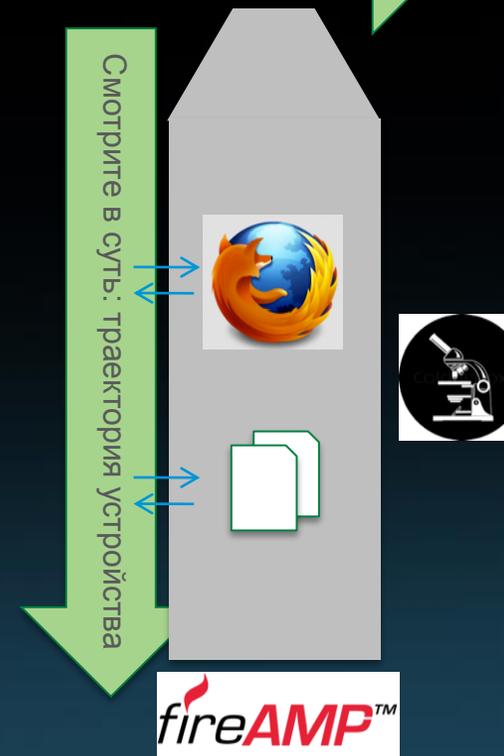
| | |
|---|--|
| Событие + сеть и контекст пользователя | Событие: Попытка получения доступа Цель: 96.16.242.135 (уязвимо) ОС хоста: Blackberry Приложения: электронная почта, браузер, Twitter Местоположение: Белый дом, США Идентификатор пользователя: bobama Ф. И. О.: Барак Обама Департамент: административный |
| Событие + контекст сети | ОС хоста: Blackberry Приложения: электронная почта, браузер, Twitter Местоположение: Белый дом, США |
| Событие | Цель: доступа 96.16.242.135 |

Контекст способен фундаментально изменить интерпретацию данных события

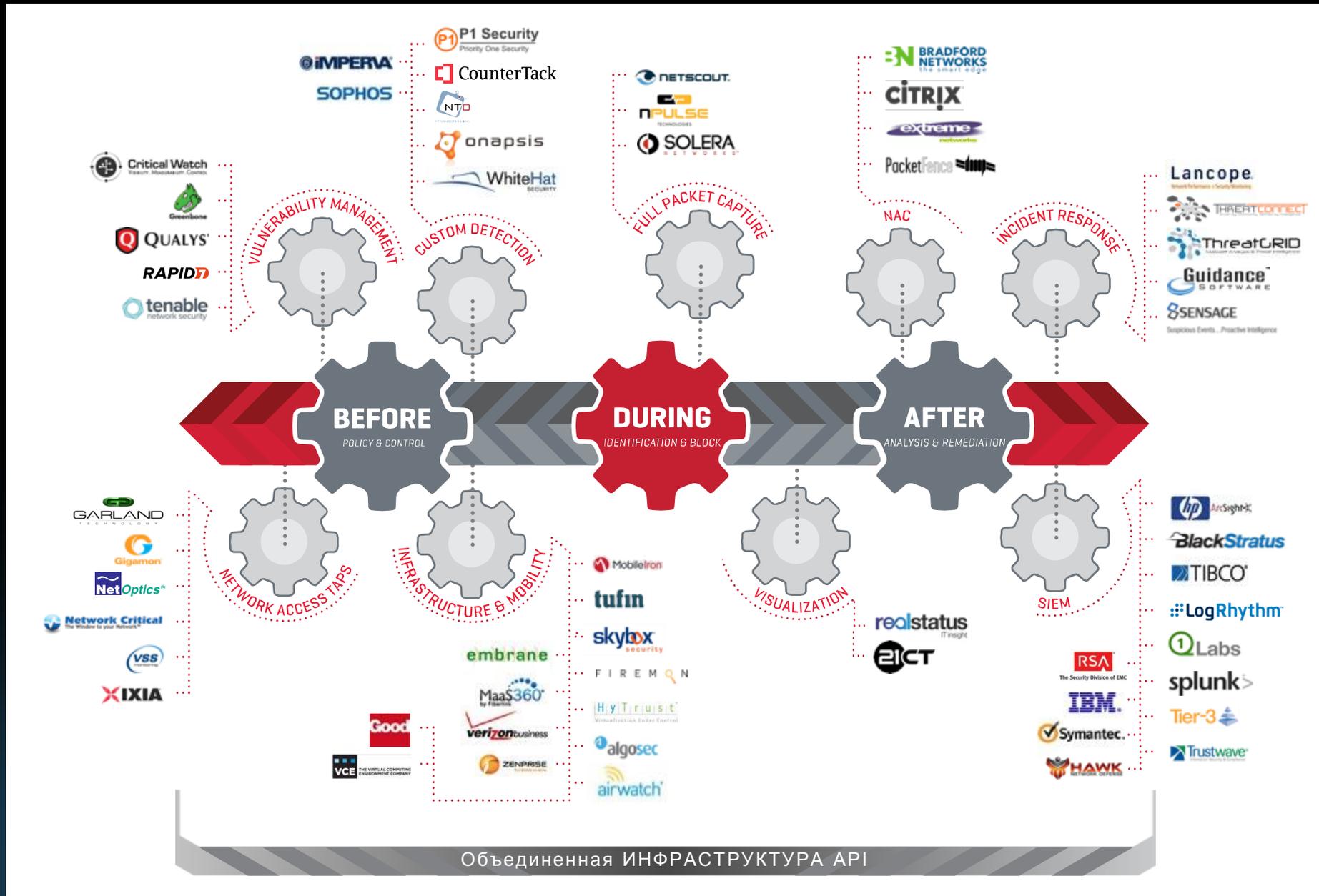
Анализ траектории файла и устройства – поиск источника заражения



- Какие системы были заражены?
- Почему это произошло?
- Где источник заражения?
- За что еще он отвечает?
- С кем он еще взаимодействовал?



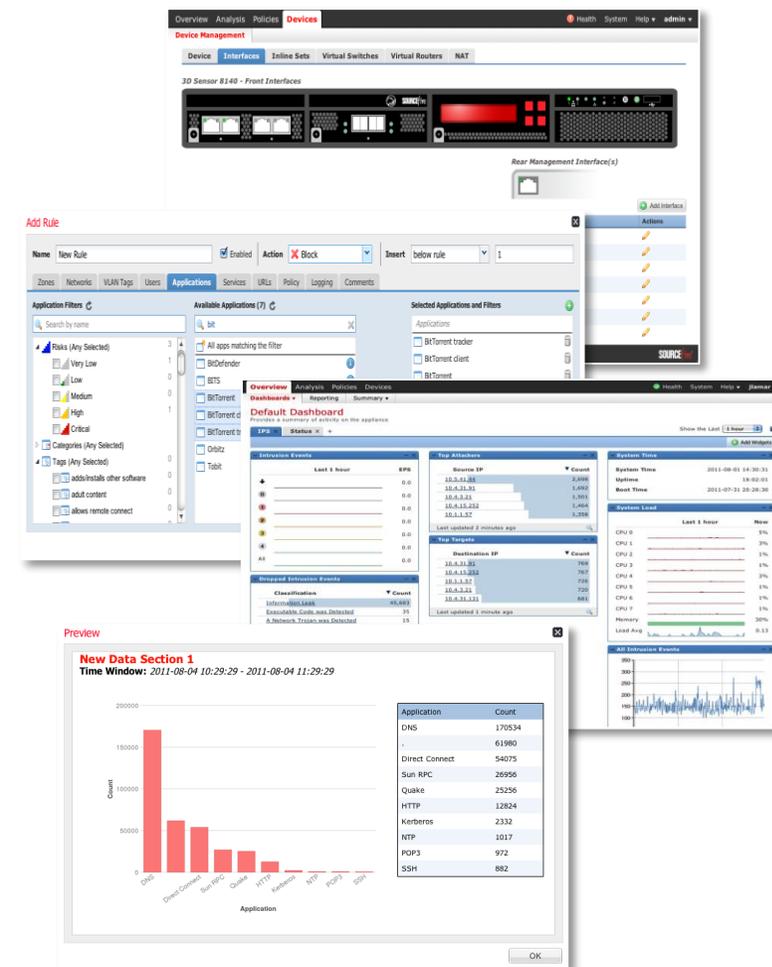
Объединенная партнерская программа Sourcefire и Cisco



Sourcefire Defense Center®



- Настраиваемая инструментальная панель
- Комплексные отчеты и оповещения
- Централизованное управление политиками
- Иерархическое управление
- Обеспечение высокой доступности
- Интеграция с существующими системами безопасности



Устройства центра обеспечения защиты



| | DC750 | DC1500 | DC3500 |
|--|--------------------------------|---|---|
| Макс. число управляемых устройств* | 10 | 35 | 150 |
| Макс. число событий системы предотвращения вторжений | 20 млн. | 30 млн. | 150 млн. |
| Система хранения событий | 100 Гб | 125 Гб | 400 Гб |
| Макс. сетевая карта (хосты пользователи) | 2 тыс. 2 тыс. | 50 тыс. 50 тыс. | 300 тыс. 300 тыс. |
| Макс. кол-во Netflow (потоков/с) | 2000 потоков/с | 6000 потоков/с | 10000 потоков/с |
| Возможности высокой доступности | Дистанционное управление (LOM) | RAID 1, LOM, High Availability pairing (HA) | RAID 5, LOM, HA, резервный источник питания пер. тока |

* Макс. число устройств зависит от типа сенсора и частоты событий

The background is a deep black space filled with numerous small, bright white and blue stars. A prominent feature is a large, glowing nebula in shades of teal and blue, which is slightly out of focus. In the lower center, there is a faint, elongated galaxy or star cluster with a reddish-pink hue. The overall composition is centered and evokes a sense of vastness and cosmic wonder.

DEMO TIME!

Одна консоль – множество ролей

The image displays two overlapping screenshots of the Cisco Sourcefire management console. The top screenshot shows the 'User Roles' page, which includes a navigation menu with 'Users', 'User Roles', and 'Login Authentication'. A list of user roles is visible on the left, such as 'Access Admin', 'Administrator', and 'External Database User'. The bottom screenshot shows the 'User Role Editor' form, which includes fields for 'Name' and 'Description', and sections for 'Menu Based Permissions' and 'System Permissions'. The 'Menu Based Permissions' section contains a tree view of permissions like 'Searches', 'Bookmarks', 'Policies', 'Intrusion', and 'Access Control'. The 'System Permissions' section includes 'External Database Access'. Both screenshots show the top navigation bar with 'Overview', 'Analysis', 'Policies', and 'Devices' tabs, and a user profile 'admin'.

User Roles

Users | **User Roles** | Login Authentication

Configure Permission Escalation | Create User Role

User Role

- Access Admin
Sourcefire Provided
- Administrator
Sourcefire Provided
- External Database User
Sourcefire Provided
- Intrusion Admin
Sourcefire Provided
- Maintenance User
Sourcefire Provided
- Network Admin
Sourcefire Provided
- Reporting Admin
Sourcefire Provided
- Security Approver
Sourcefire Provided
- Security Event Analyst
Sourcefire Provided
- Security Event Analyst
Sourcefire Provided

1 Row Selected

User Role Editor

Users | **User Roles** | Login Authentication

Name:

Description:

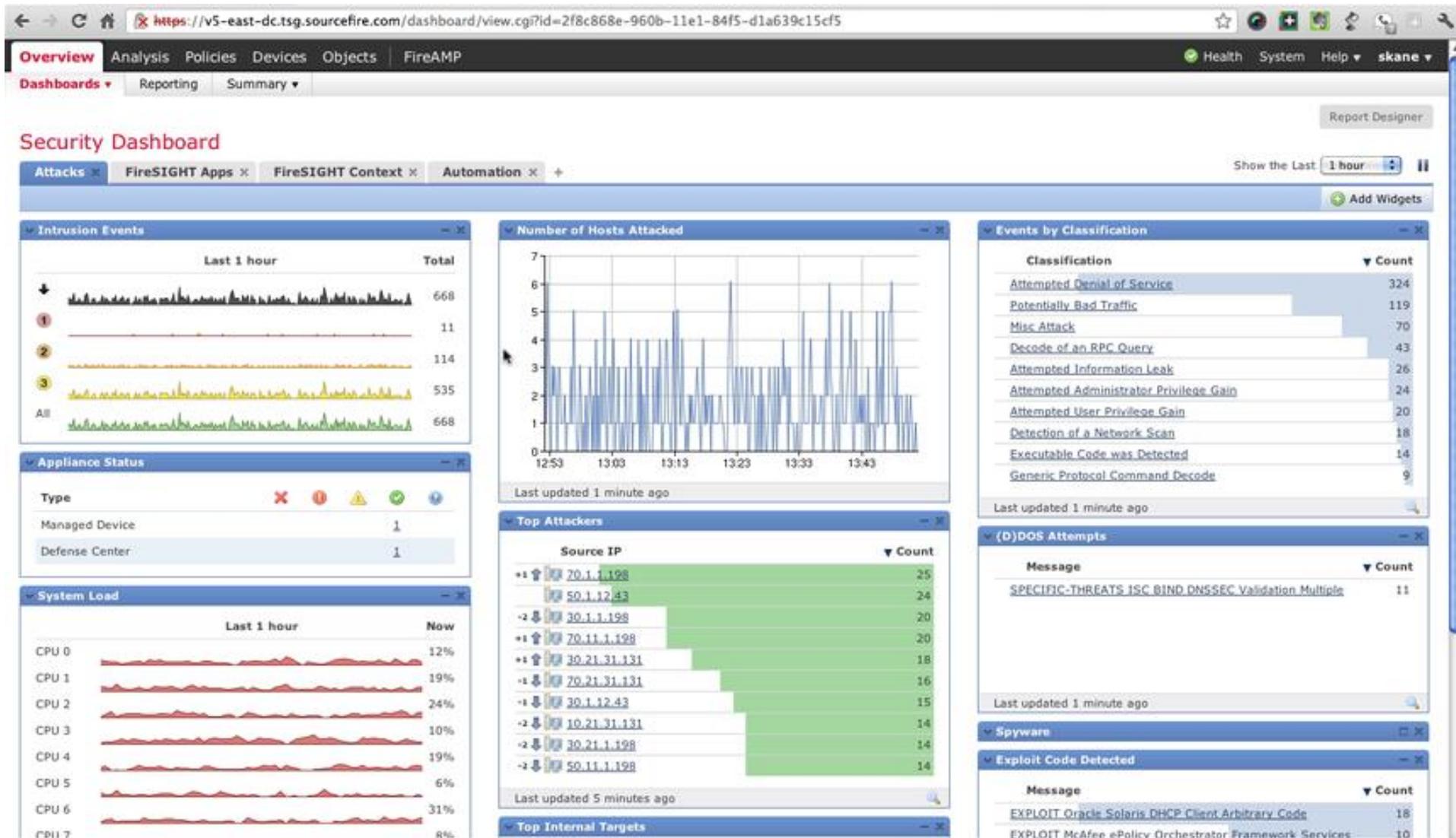
Menu Based Permissions

- Searches
- Bookmarks
- Policies
 - Intrusion
 - Access Control
 - Access Control List
 - Access Control Policy Editing
 - Allow changes to Administrator Rules
 - Allow Changes to Root Rules
 - Apply Intrusion Prevention Policies
 - Custom Applications
 - Network Discovery

System Permissions

- External Database Access

Save | Cancel



Автоматизация создания политик и правил

The screenshot displays the 'Intrusion Events' management interface. On the left, a vertical navigation pane shows event history with a bar chart and a list of items labeled 1, 2, 3, 4, and All. The main area is titled 'Last 1 hour' and 'Total'. A 'Policy Information' dialog box is open, showing the configuration for the 'Default Production Demo Lab IPS Policy'. The dialog includes fields for Name, Description, and a checked 'Drop when Inline' option. It also shows the 'Base Policy' as 'Security Over Connectivity' and provides status information: 'This policy defines 0 variables', 'This policy has 9038 enabled rules' (558 generate events, 8480 drop and generate), and 'FireSIGHT recommends 7154 rule state settings for 7430 hosts' (214 generate, 3550 drop and generate, 3390 disabled). At the bottom of the dialog are 'Commit Changes' and 'Discard Changes' buttons.

Intrusion Events

Last 1 hour Total

Policy Information

Name: Default Production Demo Lab IPS Policy

Description: Sourcefire Provided. For best results, do not modify.

Drop when Inline:

Base Policy: Security Over Connectivity

✓ The base policy is up to date (Rule Update 2013-10-09-004-vrt)

🛡️ This policy defines 0 variables

📊 This policy has 9038 enabled rules

- ➔ 558 rules generate events
- ✗ 8480 rules drop and generate events

🌐 FireSIGHT recommends 7154 rule state settings for 7430 hosts

- ➔ Set 214 rules to generate events
- ✗ Set 3550 rules to drop and generate events
- ➔ Set 3390 rules to disabled

Policy is not using the recommendations. Click to change recommendations

Last generated: 2013 Oct 10 10:15:33

Commit Changes Discard Changes



Application Statistics

Provides traffic and intrusion event statistics by application

Show the Last 1 hour

Connections x Intrusion Events x +

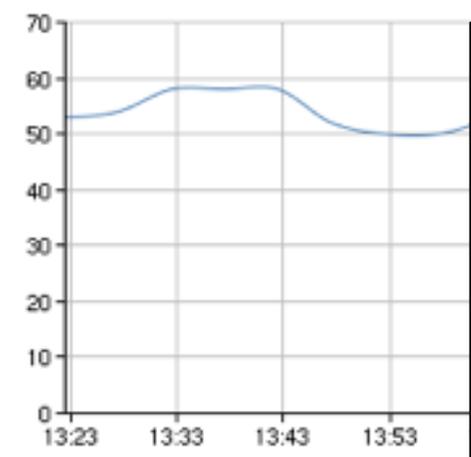
Add Widgets

Allowed Connections by Application

| Application | Allowed Connections |
|----------------|---------------------|
| Sun RPC | 191,962 |
| Sun RPC client | 191,962 |
| DNS | 177,792 |
| HTTP | 80,881 |
| HTTPS | 41,480 |
| Direct Connect | 23,586 |
| Direct Connect | 23,586 |
| SNMP | 20,094 |
| Dropbox | 13,369 |
| SSL | 9,756 |

Last updated less than a minute ago

Unique Applications over Time



Last updated less than a minute ago

Risky Applications

Risky Applications

Title: Risky Applications

Preset: None

Table: Application Statistics

Field: Application

Aggregate: Total Bytes (KB)

Filter: High Risk Applications with Low Bl

Show: Top

Results: 10

Show Movers:

Color: ■ ■ ■ ■ ■ ■ ■

| Application | Total Bytes (KB) |
|---------------|------------------|
| BitTorrent | 41,077.00 |
| eDonkey | 320.16 |
| Ustream.tv | 81.63 |
| Facebook | 34.69 |
| Yet ABC | 8.89 |
| Facebook Apps | 4.16 |
| QQ | 1.98 |
| MySpace | 0.70 |
| Gnutella | 0.53 |

Last updated 4 minutes ago

Allowed Connections by Business

| Business Relevance | Allowed Connections |
|--------------------|---------------------|
| High | 410,375 |
| Medium | 331,579 |
| Very High | 53,575 |
| Very Low | 6,905 |
| Low | 28 |

Allowed Connections by Application

| Risk | Allowed |
|-----------|---------|
| High | |
| Very Low | |
| Medium | |
| Very High | |
| Low | |

Total Bytes (KB)

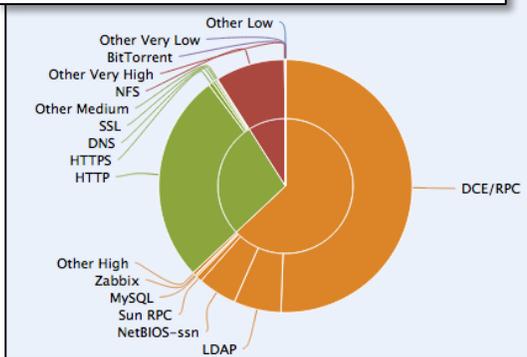
| |
|-----------|
| 41,077.00 |
| 320.16 |
| 81.63 |
| 34.69 |
| 8.89 |
| 4.16 |
| 1.98 |
| 0.70 |
| 0.53 |

Total Traffic (KB/s)

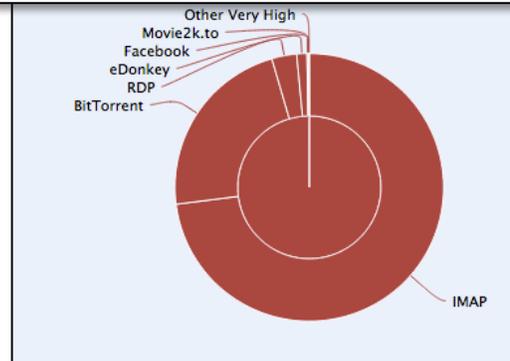
| |
|----------|
| 4,412.25 |
| 3,852.30 |
| 2,721.11 |
| 1,723.48 |
| 1,354.04 |
| 404.91 |

Понимание контекста в FireSIGHT

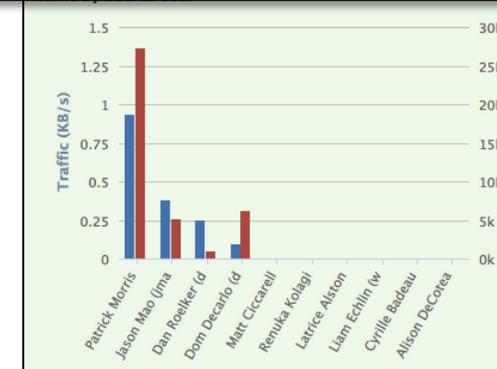
Просмотр всего трафика приложения...



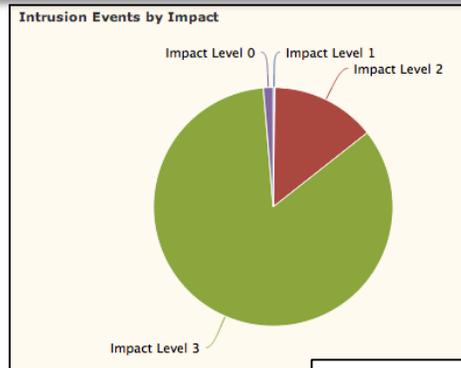
Поиск приложений с высокой степенью риска...



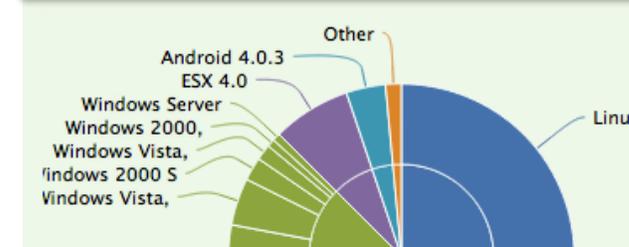
Кто их использует?



Чем еще занимались эти пользователи?



Какие использовались операционные системы?



Как выглядит их трафик за период времени?



Информация о хосте и истории его действий

The screenshot shows a network security interface with several key sections:

- Host Details:** Hostname, NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type, Last Seen, Events, Intrusion Events, Current User, and Operating System (Vendor, Product, Version).
- User Identity:** Username, Authentication Protocol, First Name, Last Name, Email, Department, and Phone.
- Host History:** A table showing connections from various IP addresses over time.
- Applications:** A list of installed applications with their versions and client types.

Callouts provide context for the data:

- Кто на хосте:** Points to the 'Current User' field.
- Идентифицированная операционная система и ее версия:** Points to the 'Operating System' table.
- Серверные приложения и их версия:** Points to the 'Applications' table.
- Клиентские приложения:** Points to the 'Client' column in the applications list.
- Версия клиентского приложения:** Points to the 'Version' column in the applications list.
- Приложение:** Points to the application name in the list.
- Какие еще системы / IP-адреса использует пользователь? Когда?:** Points to the 'Host History' table.

Управление политиками

Overview Analysis **Policies** Devices Health System Help jamar

Intrusion Access Control Network Discovery Custom Applications Users Correlation Actions

Interesting Use Cases

Enter a description

Save Cancel Save and Apply + Add Category + Add Rule Search Rules ✕

Device Targets: 0 devices

| # | Name | Source Zones | Dest Zones | Sou... Net... | Dest Net... | VLA... | U... | Applications | Services | URLs | Action | Shield | Document | Count | Tools |
|---|-----------------------|--------------|------------|---------------|-------------|--------|------|---|----------|--|-----------------------------------|--------|----------|-------|-------|
| Administrator Rules | | | | | | | | | | | | | | | |
| This category is empty. | | | | | | | | | | | | | | | |
| Standard Rules | | | | | | | | | | | | | | | |
| 1 | Mobile Security 1 | Intern | any | any | Ten | any | any | <input type="checkbox"/> Android browser <input type="checkbox"/> Blackberry browser <input type="checkbox"/> Mobile Safari | any | any | ✗ Block | Shield | Document | 1 | Tools |
| 2 | Read Only Facebook | Intern | Extern | any | any | any | any | <input type="checkbox"/> Facebook Status Update <input type="checkbox"/> Facebook Send Email <input type="checkbox"/> Facebook Comment <input type="checkbox"/> Facebook Chat <input checked="" type="checkbox"/> Tags: Facebook game; Fill | any | any | ✗ Block | Shield | Document | 0 | Tools |
| 3 | Web Block List | Intern | Extern | any | any | any | any | any | any | <input checked="" type="checkbox"/> Adult and Pornography (Any Reputation) <input checked="" type="checkbox"/> Bot Nets (Any Reputation) <input checked="" type="checkbox"/> Confirmed SPAM Sources (Any Reputati <input checked="" type="checkbox"/> Gambling (Any Reputation) (13 more...) | ✗ Block | Shield | Document | 0 | Tools |
| 4 | Block All P2P | Intern | Extern | any | any | any | any | Categories: peer to peer | any | any | ✗ Block | Shield | Document | 0 | Tools |
| 5 | Inbound Email | Extern | Intern | any | any | any | any | SMTP | SMTP | any | ✓ Allow | Shield | Document | 0 | Tools |
| 6 | Outbound Web Browsing | Extern | Intern | any | any | any | any | HTTP | any | any | ✓ Allow | Shield | Document | 0 | Tools |
| Root Rules | | | | | | | | | | | | | | | |
| This category is empty. | | | | | | | | | | | | | | | |
| Default Action | | | | | | | | | | | Access Control: Block All Traffic | | | | |
| 1 Row Selected Displaying 1 - 6 of 6 rules Page 1 of 1 | | | | | | | | | | | | | | | |

Фильтрация URL

Editing Rule - Web Block List

Name: Web Block List | Enabled | Action: Block | Move

Zones | Networks | VLAN Tags | Users | Applications | Services | **URLs** | Policy | Logging | Comments

Categories and URLs

- Any
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy
- CDNs
- Computer and Internet Info
- Computer and Internet Security

Reputations

- Any
- 5 - Well known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High risk

Add to Rule

Selected URLs

- Adult and Pornography (Any Reputation)
- Bot Nets (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Gambling (Any Reputation)
- Keyloggers and Monitoring (Any Reputation)
- Malware Sites (Any Reputation)
- Marijuana (Any Reputation)
- Nudity (Any Reputation)
- Open HTTP Proxies (Any Reputation)
- Parked Domains (Any Reputation)
- Pay to Surf (Any Reputation)

Enter URL Add

Save Cancel

Различные категории URL

URLs категорированы по уровню рисков

Контроль по типам файлов

The screenshot shows the 'Add File Rule' configuration window. Three callout boxes illustrate the available options for the configuration fields:

- Application Protocol:** Any, HTTP, SMTP, IMAP, POP3
- Direction of Transfer:** Any, Upload, Download
- Action:** Detect, Malware Cloud Lookup, Block

The main window configuration is as follows:

- Application Protocol:** Any
- Direction of Transfer:** Any
- Action:** Malware Cloud Lookup

File Type Categories:

| Category | Count |
|---|-------|
| <input type="checkbox"/> Office Documents | 7 |
| <input type="checkbox"/> Archive | 1 |
| <input type="checkbox"/> Multimedia | 1 |
| <input checked="" type="checkbox"/> Executables | 2 |
| <input type="checkbox"/> PDF files | 1 |
| <input type="checkbox"/> Encoded | 0 |
| <input type="checkbox"/> Graphics | 0 |
| <input type="checkbox"/> System files | 0 |

File Types:

- Search name and description
- All types in selected Categories
- MSEXE
- JARPACK

Selected File Categories and Types:

- MSEXE
- JARPACK

Buttons: Add, Save, Cancel

Анализ траектории файла

Trajectory

Oct 28

11:55

10.0.164.79

10.0.202.94

10.131.14.58

10.131.12.247

10.0.30.0

10.131.12.233

10.0.231.66

10.0.112.64

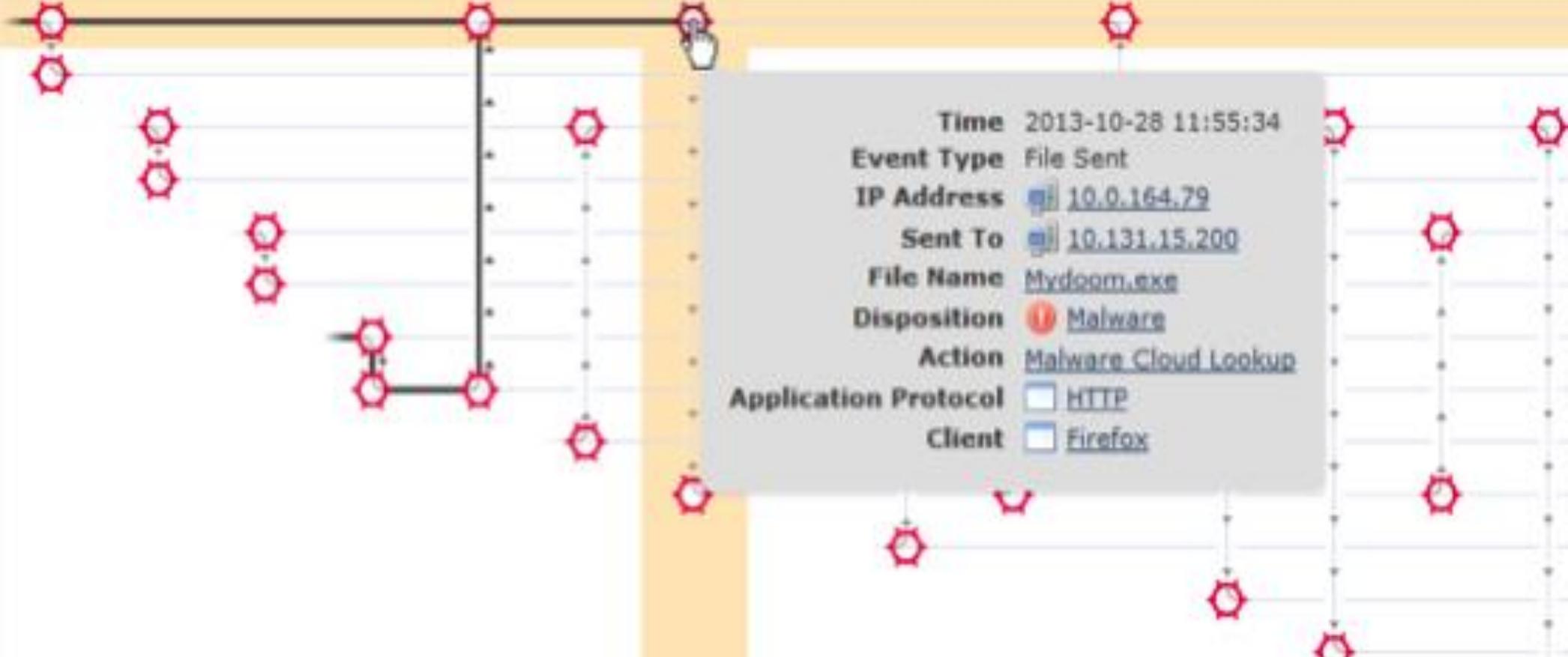
10.0.168.95

10.131.15.200

218.212.144.140

10.0.57.108

255.255.255.255



| | |
|----------------------|--|
| Time | 2013-10-28 11:55:34 |
| Event Type | File Sent |
| IP Address | 10.0.164.79 |
| Sent To | 10.131.15.200 |
| File Name | Mydoom.exe |
| Disposition | ! Malware |
| Action | Malware Cloud Lookup |
| Application Protocol | <input type="checkbox"/> HTTP |
| Client | <input type="checkbox"/> Firefox |

«Черные списки»

■ Что это?

Сигналы тревоги и правила блокирования:

Трафик ботнетов и C&C / Известные злоумышленники / открытые прокси/релеи

Источники вредоносного ПО, фишинга и спама

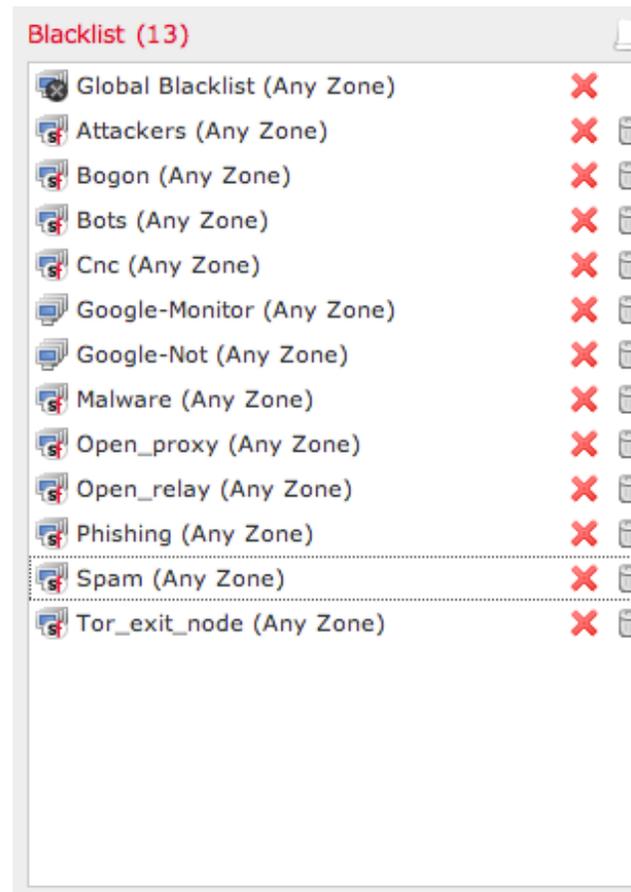
Возможно создание пользовательских списков

Загрузка списков от Sourcefire или иных источников

■ Как это может помочь?

Блокировать каналы вредоносных коммуникаций

Непрерывно отслеживать любые несанкционированные и новые изменения



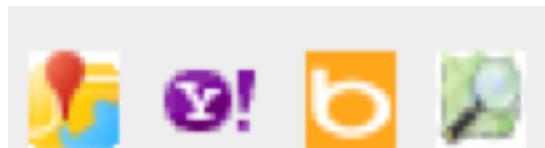
Геолокация



| Country Name | Count |
|---------------|-------|
| United States | 162 |
| Germany | 36 |
| China | 18 |
| Japan | 13 |
| France | 11 |
| Russia | 4 |
| North Korea | 2 |
| Pakistan | 1 |
| Iraq | 1 |
| Iran | 1 |

Last updated 1 minutes ago

| Initiator IP | Initiator Location | Responder IP |
|--------------------------------|--------------------|-----------------------------|
| 76.100.209.66 | USA | 10.4.32.112 |
| 10.4.10.131 | | 10.4.32.112 |
| 10.4.10.131 | | 10.4.32.112 |
| 10.4.33.95 | | 10.5.32.206 |
| 89.188.101.82 | ISR | 10.5.32.206 |
| 200.189.215.85 | BRA | 10.4.33.44 |
| 10.4.31.237 | | 10.5.32.206 |
| 10.4.11.216 | | 10.5.39.206 |



- Визуализация карт, стран и городов для событий и узлов

Детали по геолокации

- IP –адреса должны быть маршрутизируемыми
- Два типа геолокационных данных
 - Страна – включено по умолчанию
 - Full – Может быть загружено после Установки:
 - Почтовый индекс, координаты, TZ, ASN, ISP,
 - организация, доменное имя и т.д.
 - Ссылки на карты (Google, Bing и другие)
- Страна сохраняется в запись о событии
 - Для источника & получателя

Geolocation for **94.236.27.33**

| | |
|---------------------------|---|
| Country | United Kingdom  (Europe) |
| Region | Lnd |
| City | London |
| Postal Code | wc2n 5 |
| Latitude/Longitude | 51.5073, -0.12601 |
| Maps |     |
| Timezone | GMT:+0 |

▼ **Additional Information**

| | |
|------------------------|-----------------------|
| ASN | 15395 (Uk Rackspace) |
| ISP | Cogent Communications |
| Home/Business | Business |
| Domain Name | hayward.co.uk |
| Connection Type | Broadband |

Дизайнер пользовательских отчетов

The screenshot displays a web-based report designer interface. At the top, there is a navigation bar with tabs for 'Overview', 'Analysis', 'Policies', and 'Devices'. A secondary navigation bar includes 'Dashboards', 'Reporting', and 'Summary'. The main area is titled 'Report Sections' and contains a configuration panel for 'New Data Section 1' and a 'Preview' window.

Report Configuration Panel:

- Table:** Intrusion Events
- Preset:** None
- Format:** [Bar Chart]
- Search:** None
- X-Axis:** Time
- Y-Axis:** Count

Preview Window:

New Data Section 1
Time Window: 2011-08-04 10:29:29 - 2011-08-04 11:29:29

| Application | Count |
|----------------|--------|
| DNS | 170534 |
| . | 61980 |
| Direct Connect | 54075 |
| Sun RPC | 26956 |
| Quake | 25256 |
| HTTP | 12824 |
| Kerberos | 2332 |
| NTP | 1017 |
| POP3 | 972 |
| SSH | 882 |

Cyber Threat Defense

aka Lancope Stealthwatch

Немного фактов

- На установление факта заражения уходит в среднем 9-18 месяцев (US CERT)
Как правило об этом узнают от третьей стороны
- При реагировании на инцидент 75% времени тратится на поиск причины – счёт идёт на дни и недели (Forrester)
- У большинства компаний нет установленного процесса реагирования на инциденты

Как минимизировать ущерб?



Знать атакующего

Кто?

- Страна? Конкуренты? Частные лица?

Что?

- Что является целью?

Когда?

- Когда атака наиболее активна и с чем это связано?

Где?

- Где атакующие? Где они наиболее успешны?

Зачем?

- Зачем они атакуют – что конкретно их цель?

Как?

- Как они атакуют – Zero-day? Известные уязвимости? Инсайдер?

Знать себя

Кто?

- Кто в моей сети?

Что?

- Что делают пользователи? Приложения?
- Что считать нормальным поведением?

Когда?

- Устройства в сети? Что считать нормальным состоянием?

Где?

- Где и откуда пользователи попадают в сеть?
- Внутренние? eCommerce? Внешние?

Зачем?

- Зачем они используют конкретные приложения?

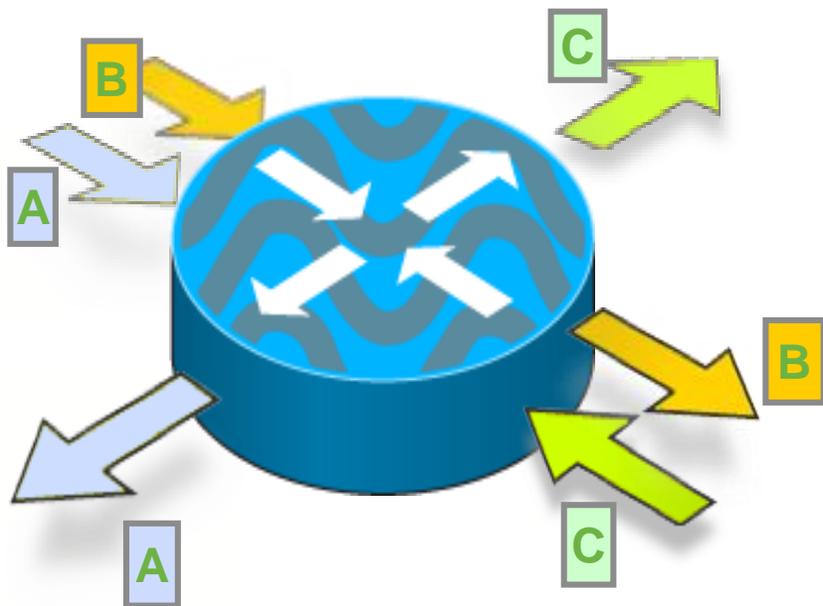
Как?

- Как всё это попадает в сеть?

Варианты решений



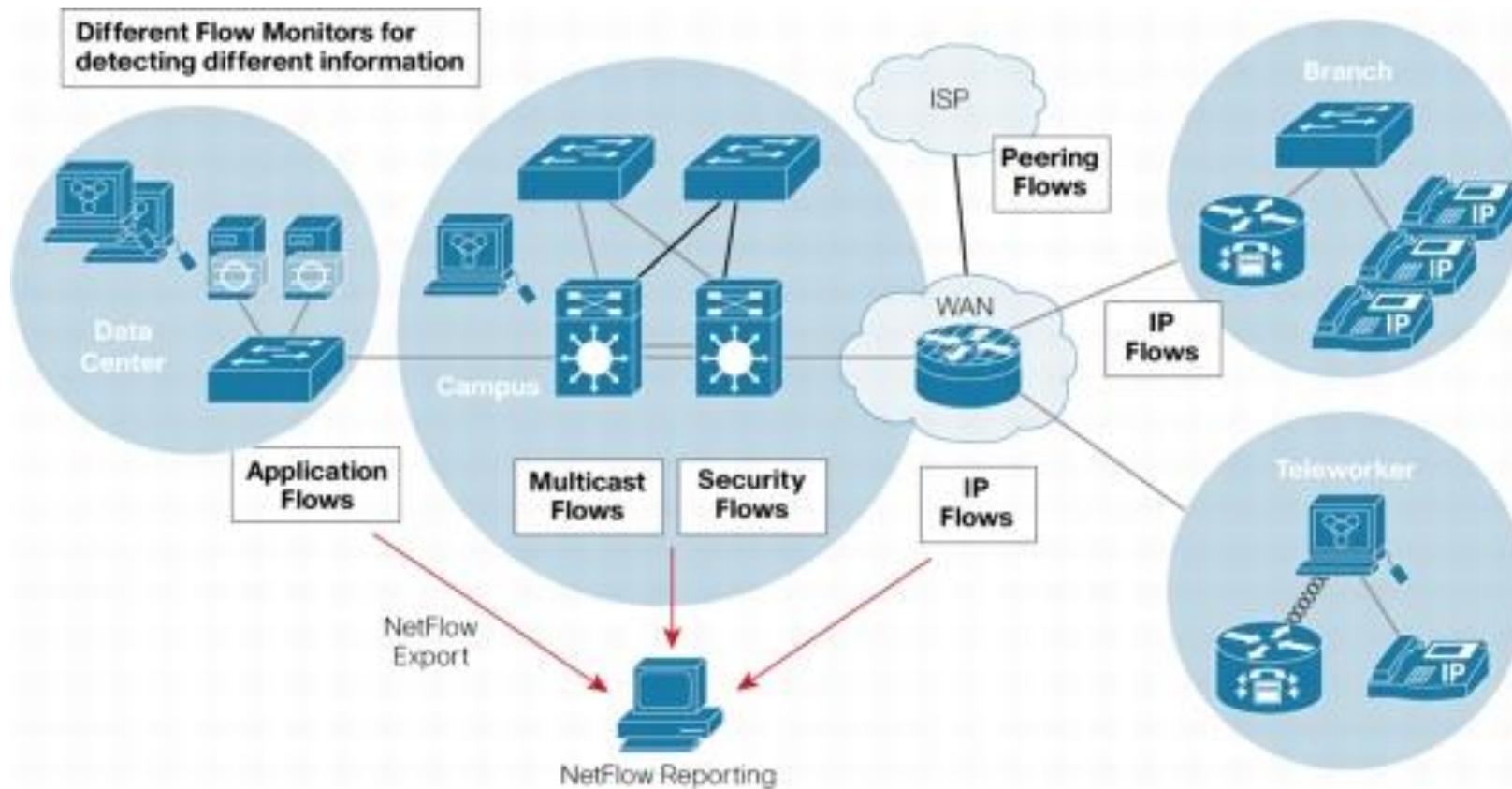
Не везде есть IPS, но везде есть NetFlow



| | Source IP: Port | Destination IP: Port | Packets | Date/Time |
|----------|-------------------|----------------------|---------|-------------------------|
| A | 192.168.15.7:2068 | 211.160.17.195:8080 | 7 | 5/7/2009 8:11:13 GMT |
| B | 192.168.21.5:1042 | 72.18.45.223:21 | 219 | 5/7/2009 9:00:03 GMT |
| C | 192.168.6.22:3161 | 172.18.15.188:80 | 1 | 5/7/2009 9:05:16 GMT |

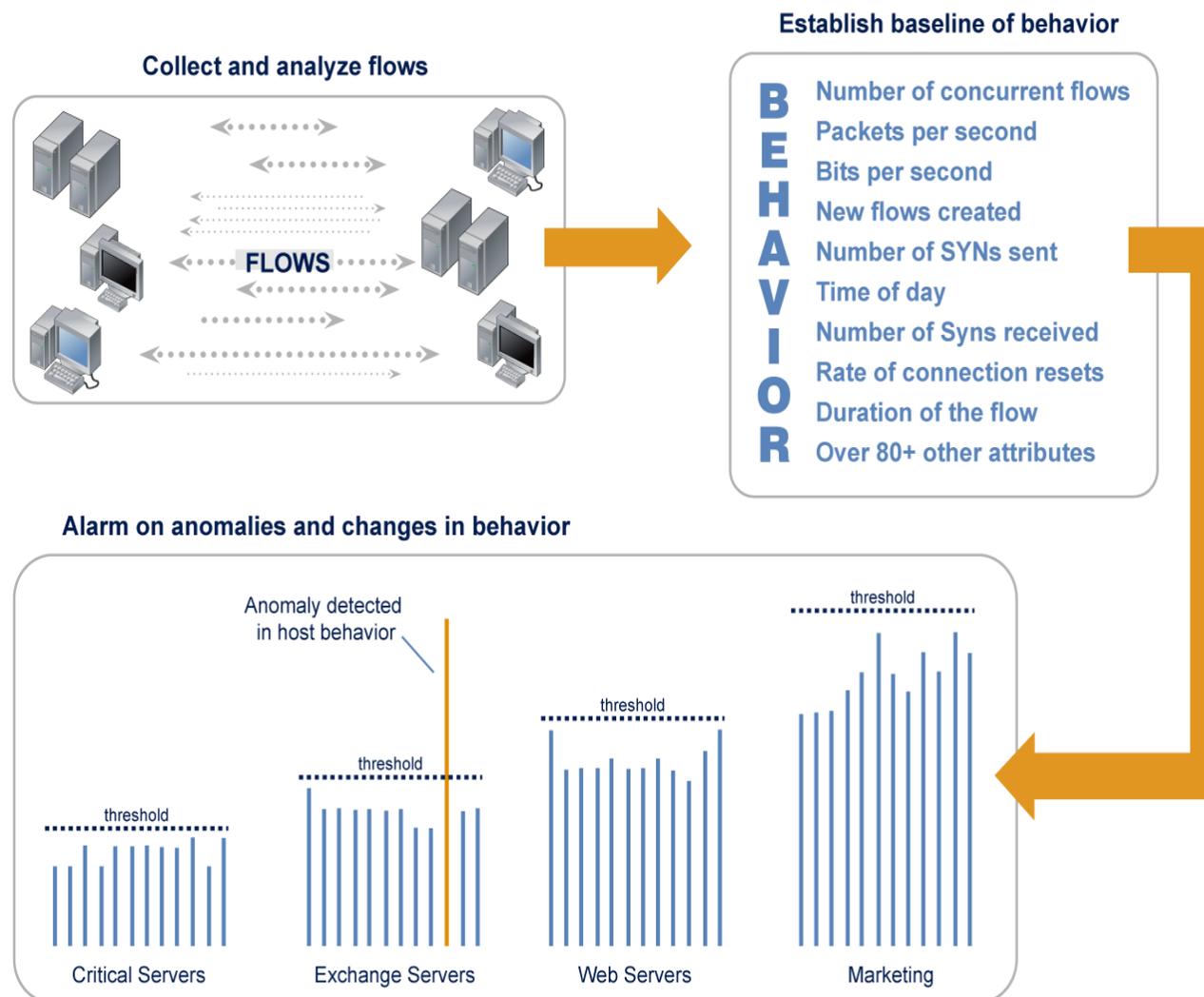


Сеть как сенсор



- NetFlow можно взять из всех критичных и важных точек

Возможности STD – Поведенческий анализ



Возможности CTD (ч.2)

- Обнаружение сетевых сканирований
- Обнаружение компьютеров-зомби и червей
- Помощь в устранении эпидемий
 - Кто нулевой пациент ?
 - С кем он контактировал ?
 - Кто из контактов заразился ?
 - Кого теперь пытаются заразить контакты ?
- Предотвращение утечек данных – превышение заданного порога по отправке данных
- Профилирование сети, инвентаризация хостов и приложений, анализ структуры трафика
- Обнаружение нелегальных серверов и P2P-трафика внутри сети

Возможности CTD (ч.3)

- Автоматическое или полуавтоматическое блокирование
В т.ч. на устройствах других производителей
- Сбор информации о потоках по NetFlow-like протоколам
NBAR, AVS, NSEL, jflow, sflow, и др.
В т.ч. с устройств других производителей
- Интеграция с системами SIEM, сканерами уязвимостей
- Подробнее
<http://www.lancope.com/resource-center/partner-integration-briefs/sw-integrations/>

Типы NetFlow

Sampled

- Маленькое подмножество трафика, менее 5%, собирается и используется для генерирования телеметрии. Дает покадровый обзор активности в сети, похоже на чтение книги, просматривая каждую 100-ю страницу.

Unsampled

- Телеметрия генерируется всем трафиком, при этом получается общая картина активности в сети.

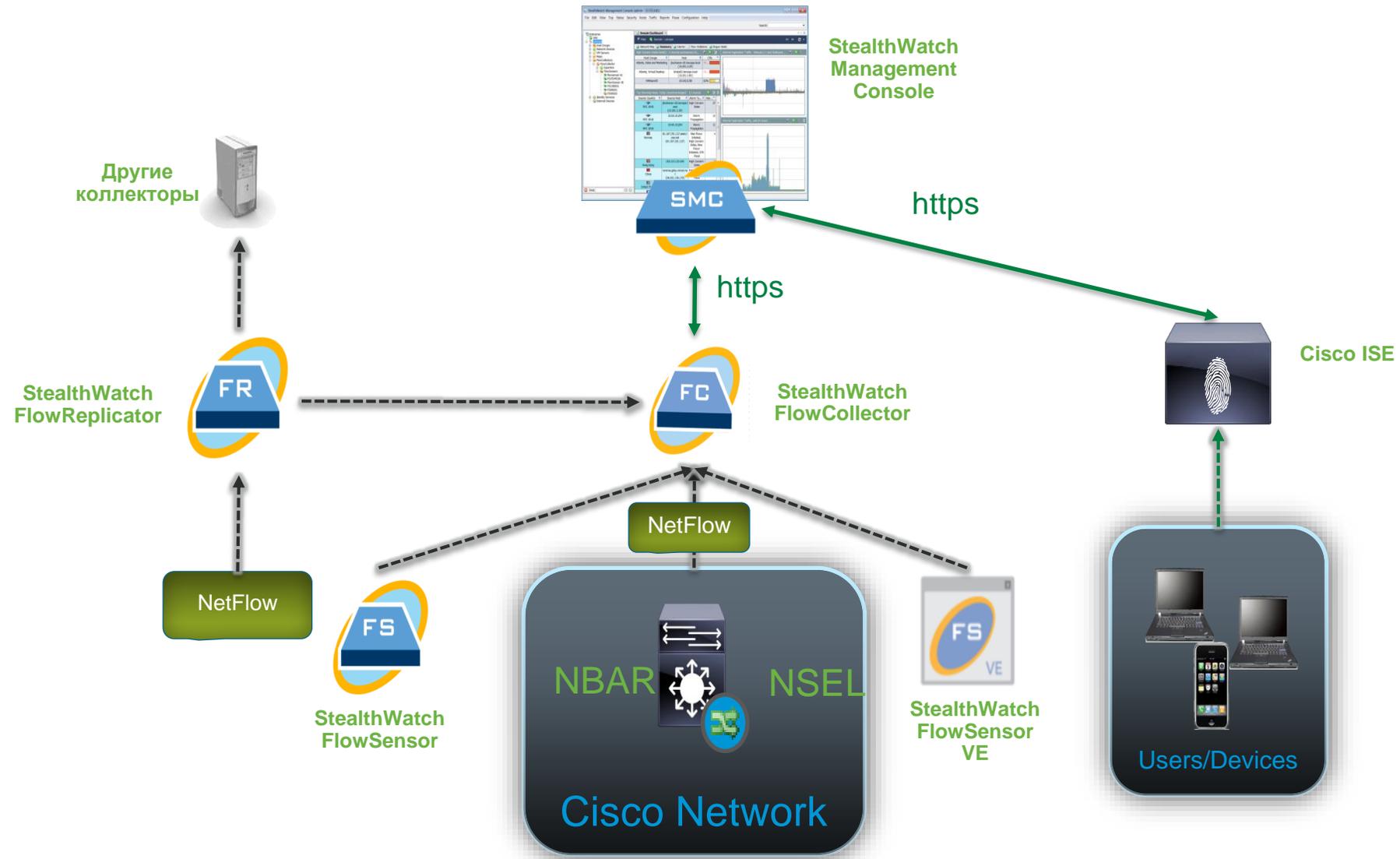
Индивидуальная, скрытая картина новых угроз требует полной информации о трафике в сети.

Только коммутаторы Cisco Catalyst могут дать информацию Unsampled NetFlow на полной скорости без влияния на производительность

Компоненты Cyber Threat Defense Solution 1.1

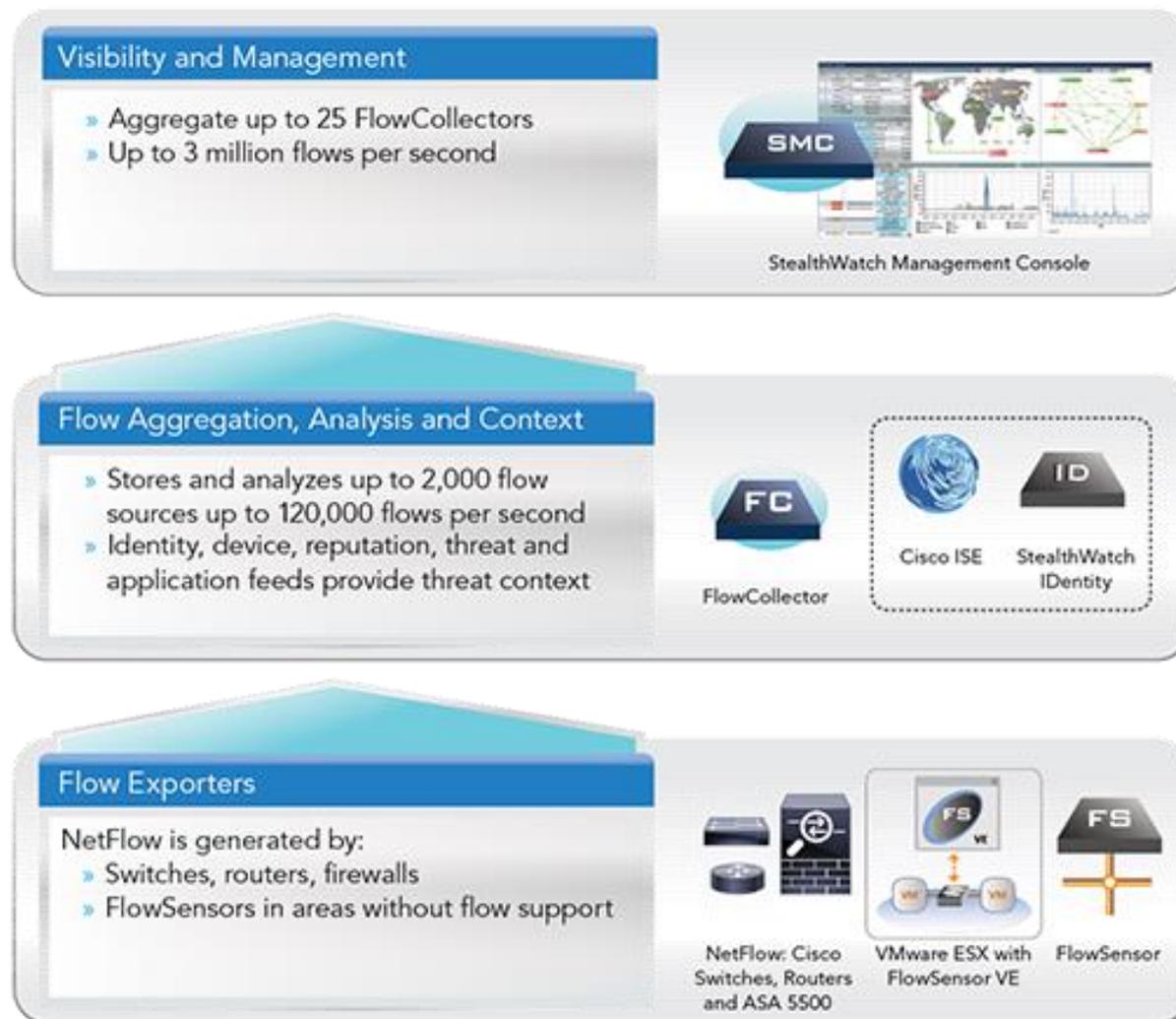
| Component | Hardware | Release | Image Type and License |
|--|--|------------------------|---|
| Catalyst 3500-X | Version ID: 02 Revision 0x03 10GE Service Module | 15.0(1)SE3 | Universal and IP Services |
| Catalyst 4500E Series | Supervisor 7E Supervisor 7L-E | 15.0(2)X0 15.0(2)X0 | Universal and IP Base Universal and IP Base |
| Catalyst 6500 Series | Supervisor 2T | 15.0(1)SY2 | Advanced Enterprise Services, Advanced IP Services and IP Base |
| ISR G2 | Any | 15.2(4)M2 | Universal and IP Base |
| ASR 1000 | RP1/RP2 | 15.2(1)S or XE3.5 | Universal and IP Base |
| Adaptive Security Appliance | Any | 8.4.4(1) | Any |
| NetFlow Generation Appliance | 3140 | 1.0 | Any |
| Identity Services Engine | Any | 1.1.1 | Any |
| Lancope StealthWatch Management Console | Any | 6.3 | Any |
| Lancope StealthWatch FlowCollector | Any | 6.3 | Any |
| Lancope StealthWatch FlowSensor | Any | 6.3 | Any |
| Lancope StealthWatch FlowReplicator | Any | 6.3 | Any |

Компоненты решения Cyber Threat Defense



Масштабируемая архитектура

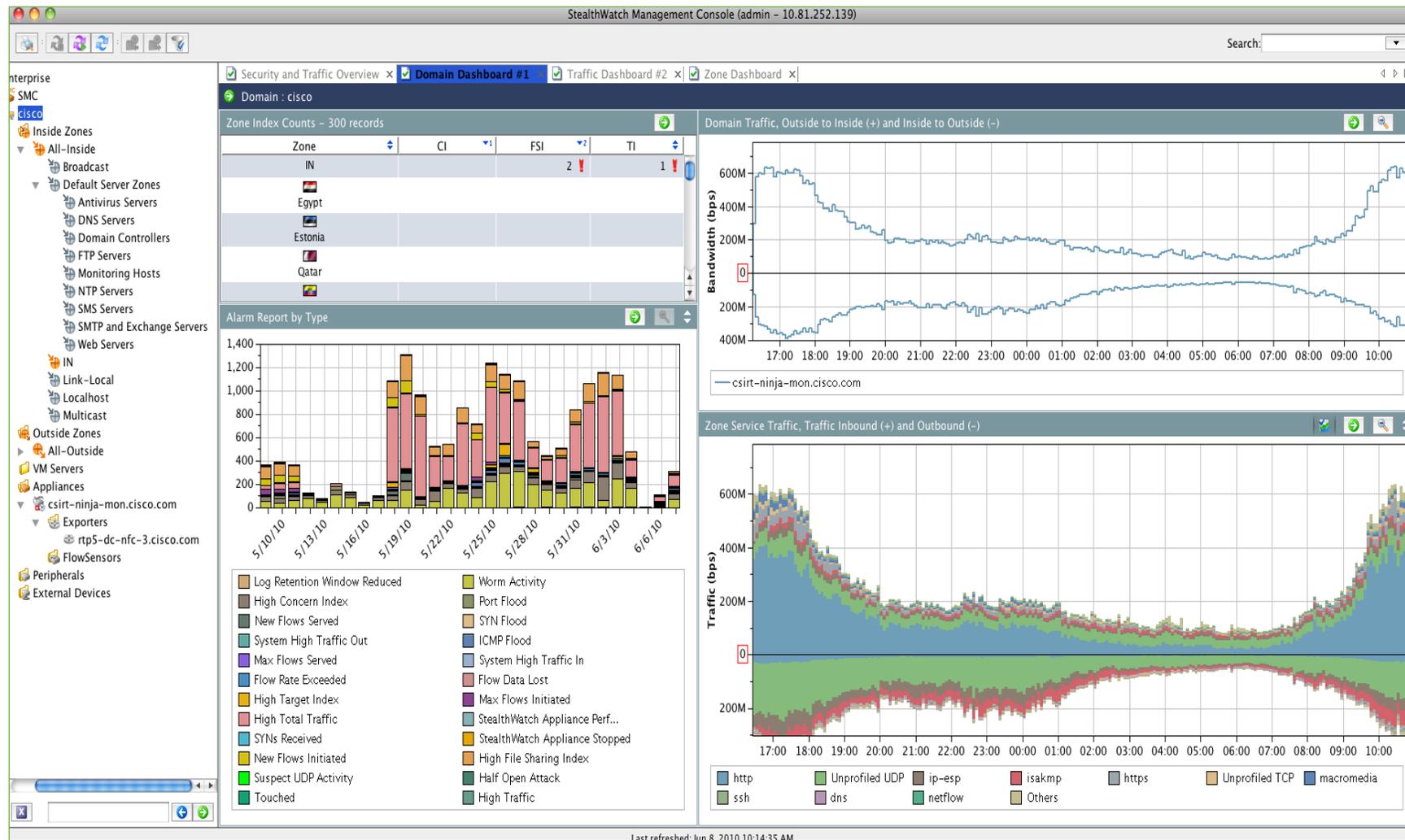
- Получение данные от сетевого оборудования с NetFlow, а также от сенсоров без поддержке NetFlow (например, VMware ESX)
- До 120.000 потоков в секунду на коллектор (до 3 миллионов на кластер)
- Понимание контекста



The background is a deep black space filled with numerous small, bright white and blue stars. A prominent feature is a large, glowing nebula in shades of teal and blue, which is more concentrated in the lower right quadrant. A faint, reddish-brown galaxy is visible in the lower center, appearing as a thin, curved band of light.

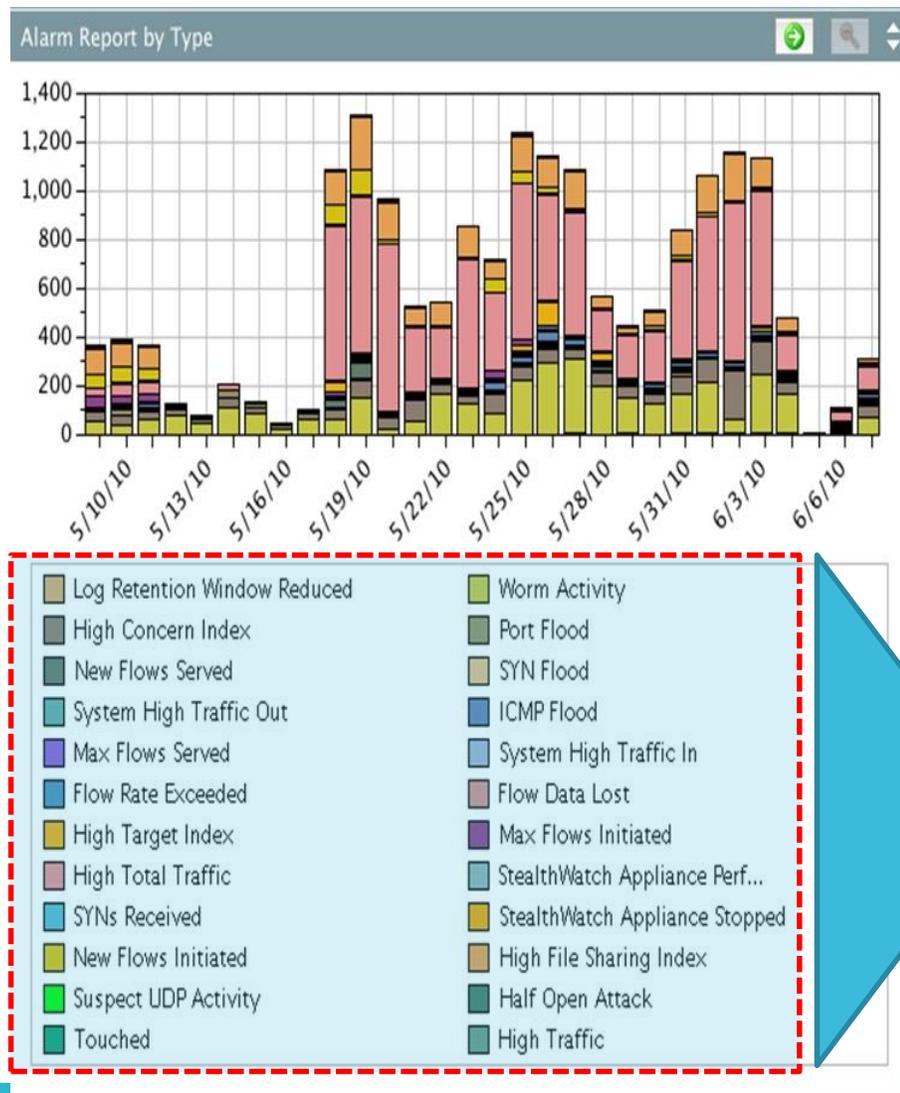
DEMO TIME!

Консоль управления STD



Last refreshed: Jun 8, 2010 10:14:35 AM

Крупным планом



Детальная статистика о всех атаках, обнаруженных в сети

Обнаружение разных типов атак, включая DDoS

Визуализация по разным срезам

StealthWatch Management Console (admin)

Domain: Lanclope

Internet Traffic Overview

Internet World Map

Top Internet Users, Last 5 Minutes - 12 records

| # | Host | Host Groups | Bytes | Peers |
|--------------|--------------------------|----------------------|---------|-------|
| 1 | 10.200.3.10 | DHCP Scopes | 6.6M | 12 |
| 2 | spyglass.lanclope.com | Atlanta, DMZ | 5.42M | 3,608 |
| 3 | 206.83.162.231 | SunGard | 2.23M | 2 |
| 4 | 10.200.0.71 | SunGard | 1.48M | 1 |
| 5 | lchqms05.lanclope.local | DNS Servers, Atlanta | 1.46M | 4,315 |
| 6 | 206.83.162.235 | SunGard | 1.46M | 1 |
| 7 | rchler-d3.lanclope.local | DHCP Scopes | 1.32M | 86 |
| 8 | 10.200.3.72 | DHCP Scopes | 1.03M | 92 |
| 9 | wallyn-l2.lanclope.local | DHCP Scopes | 973.12k | 44 |
| 10 | 206.83.162.232 | SunGard | 815.02k | 6 |
| Others (119) | | | 6.26M | 1,666 |
| Total (129) | | | 29.04M | 9,833 |

Top Internet Destinations, Last 5 Minutes - 12 records

| # | Peer | Peer Country | Bytes |
|---|--|---------------|---------|
| 1 | akamaitechnologies.com | United States | 330.51M |
| 2 | 02.mian.paetec.net | United States | 31.93M |
| 3 | 206.128/20.000.149.12.in-addr.a rpa | United States | 20.84M |
| 4 | 206.149.117.125 | United States | 20.57M |
| 5 | mian.paetec.net | United States | 11.9M |
| 6 | atl.llnw.net | United States | 9.01M |
| 7 | 206.100.144.1 | United States | 5.65M |
| 8 | 206.48.254.89 | United States | 4.77M |
| 9 | mediaserver-wt-02-1.pandora.c | United States | 4.13M |

Internet Application Traffic, Last 4 Hours

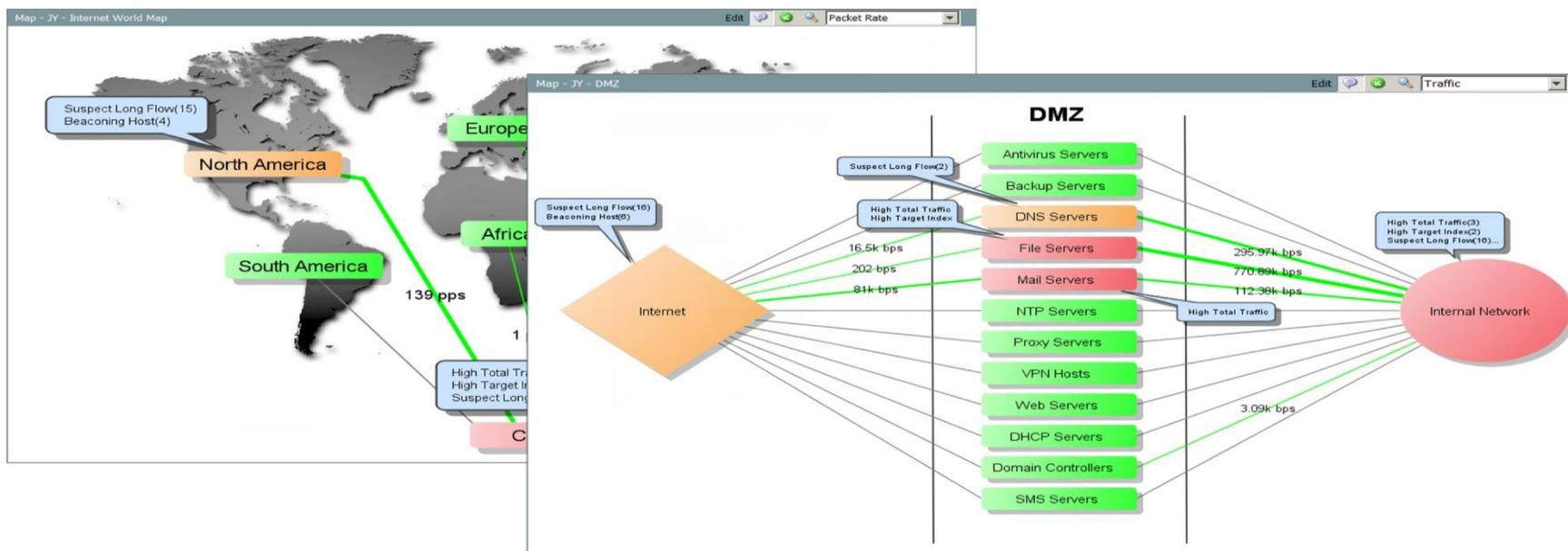
Traffic (bps)

11:00 12:00 13:00 14:00

P2P file
Inside Hosts -> Europe
16.77M bps (16,766,119)
Jan 4, 2011 2:48:00 PM

Last refreshed: Jan 5, 2011 9:39:38 AM

Визуализация по разным срезам



Cisco CTD: обнаружение атак без сигнатур

Высокий **Concern Index** показывает значительное количество подозрительных событий

Summary - 84 records summarized into 84 records

| Host Groups | Host | CI | CI% | Alarms | Alerts |
|--------------------|---------------|-------------|--------|---|------------------------------------|
| Atlanta, Desktops | 10.10.101.118 | 865,645,669 | 8,656% | High Concern Index | Ping, Ping_Scan, TCP_Scan |
| Atlanta, Desktops | 10.10.101.27 | 315,014,634 | 3,150% | High Concern Index, High Total Traffic | Ping, Ping_Scan |
| Desktops, New York | 10.50.100.83 | 180,149,569 | 1,801% | High File Sharing Index, High Total Traffic | Ping, Ping_Scan, Rejects, TCP_Scan |

| Группа узлов | Узел | CI | CI% | Тревога | Предупреждения |
|--------------|---------------|-------------|---------|--------------------|---------------------------|
| Desktops | 10.10.101.118 | 338,137,280 | 8,656 % | High Concern index | Ping, Ping_Scan, TCP_Scan |

Слежение за активностью как одного узла, так и группы узлов

Cisco CTD: обнаружение атак без сигнатур

| Policy | Start Active Time | Alarm | Source | Source Host Groups | Target | Details |
|-----------------------------|--|-------------------|--------------|------------------------------|----------------|---|
| Desktops & Trusted Wireless | Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desk | Multiple Hosts | Observed 515.84M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York | Multiple Hosts | Observed 515.84M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | Multiple Hosts | Observed 4.82G bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York, New York | Multiple Hosts | Observed 502.72M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago) | Suspect Data Loss | 10.10.101.68 | Atlanta, Desktops | Multiple Hosts | Observed 578.81M bytes. Policy maximum allows up to 500M bytes. |

Что делает 10.10.101.89?

| Политика | Время начала | Тревога | Источник | Source Host Groups | Цель | Детали |
|-----------------------------|--------------|-------------------------|--------------|--------------------|------------------|--|
| Desktops & Trusted Wireless | Янв 3, 2013 | Вероятная утечка данных | 10.10.101.89 | Атланта, Десктопы | Множество хостов | Наблюдается 5.33 Гб. Политика позволяет максимум до 500 Мб |

Предустановленные политики

Предполагаемая утечка данных

Слишком высокий показатель совместного использования файлов

Достигнуто максимальное количество обслуженных потоков

| Start Active Time | Alarm | Source | Source Host Groups | Details | Target | Target Host Groups |
|--|-------------------------|-----------------------------------|---|--|-----------------------------------|--------------------|
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | Suspect Data Loss | [REDACTED] | Private Addresses, [REDACTED], CRDC-VPN, CRDC-LAB | Observed 40.62M bytes. Expected 2.99M bytes, tolerance of 50 allows up to 10M bytes. | Multiple Hosts | |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | New Flows Served | Multiple Hosts | | Observed 2.05k flows. Expected 1 flows, tolerance of 50 allows up to 1k flows. | 83.218.20.202 | United Kingdom |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | High File Sharing Index | [REDACTED].cisco.com ([REDACTED]) | Private Addresses, [REDACTED] | Observed 61.75k points. Expected 24.96k points, tolerance of 50 allows up to 58.71k points. (Double-click for details) | Multiple Hosts | |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | High File Sharing Index | [REDACTED].cisco.com ([REDACTED]) | Private Addresses, [REDACTED] | Observed 58.25k points. Expected 7.62k points, tolerance of 50 allows up to 50k points. (Double-click for details) | Multiple Hosts | |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | New Flows Served | Multiple Hosts | | Observed 4.28k flows. Expected 16 flows, tolerance of 50 allows up to 4.09k flows. | 91.205.41.182 | United Kingdom |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | Max Flows Served | Multiple Hosts | | Observed 4.13k flows. Expected 14 flows, tolerance of 50 allows up to 4.12k flows. | 91.205.41.182 | United Kingdom |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | Max Flows Served | Multiple Hosts | | Observed 2.94k flows. Expected 2.05k flows, tolerance of 50 allows up to 2.91k flows. | [REDACTED].cisco.com ([REDACTED]) | ACL103, IPv4 |
| Apr 13, 2012 11:30:09 AM (2 minutes 11s ago) | Suspect Data Loss | [REDACTED] | Private Addresses, [REDACTED], CRDC-VPN, CRDC-LAB | Observed 44.51M bytes. Expected 3.27M bytes, tolerance of 50 allows up to 13.67M bytes. | Multiple Hosts | |
| Apr 13, 2012 11:30:04 AM (7 minutes 16s ago) | High File Sharing Index | [REDACTED].cisco.com ([REDACTED]) | [REDACTED], IPv4 | Observed 114.61k points. Expected 30.6k points, tolerance of 50 allows up to 136.61k points. | Multiple Hosts | |

Получение контекста от Cisco ISE

| Policy | Start Active Time | Alarm | Source | Source Host Groups | Source User ... | Source Devic... | Target | Details |
|-----------------------------|--|-------------------|--------------|------------------------------|-----------------|-----------------------|----------------|---|
| Desktops & Trusted Wireless | Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | ud0158 | Windows7-Wor kstation | Multiple Hosts | Observed 5.33G bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York, New York | ud0142 | Apple-iPad | Multiple Hosts | Observed 515.84M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | ud0158 | Windows7-Wor kstation | Multiple Hosts | Observed 4.82G bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York, New York | ud0142 | Apple-iPad | Multiple Hosts | Observed 502.72M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago) | Suspect Data Loss | 10.10.101.68 | Atlanta, Desktops | uc0123r | Windows7-Wor kstation | Multiple Hosts | Observed 578.81M bytes. Policy maximum allows up to 500M bytes. |

| Политика | Время старта | Тревога | Источник | Группа хостов источника | Имя пользователя | Тип устройства | Цель |
|-----------------------------|--------------|-------------------------|--------------|-------------------------|------------------|----------------|------------------|
| Desktops & Trusted Wireless | Янв 3, 2013 | Вероятная утечка данных | 10.10.101.89 | Атланта, Десктопы | Джон Смит | Apple-iPad | Множество хостов |

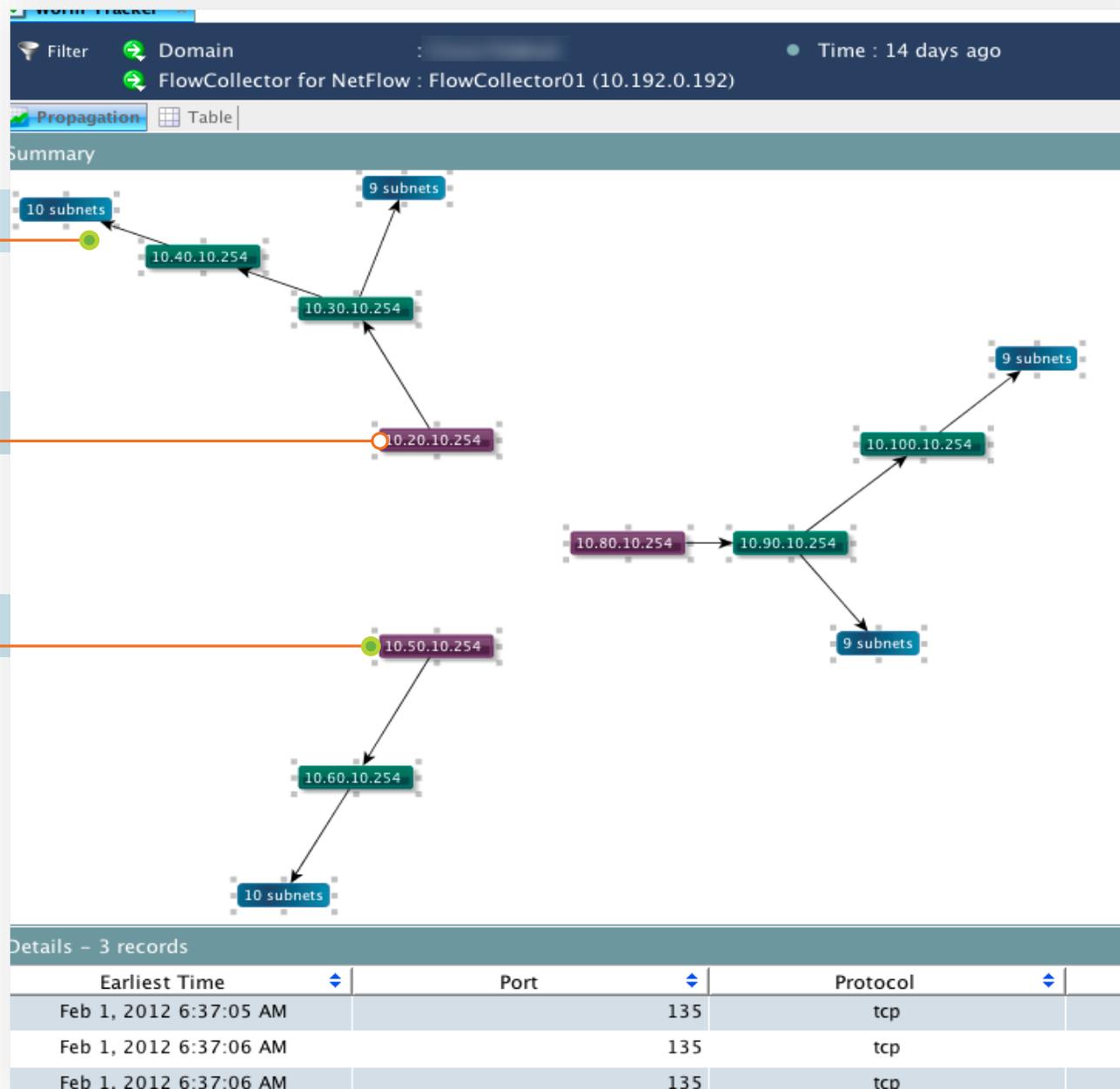
- Cisco ISE установлен в 1/3 всех проектов по Cisco Threat Defense (CTD)

Карта эпидемии

Третичное заражение

Вторичное заражение

«Нулевой пациент»



Получение контекста от Cisco ASA / ISR / ASR

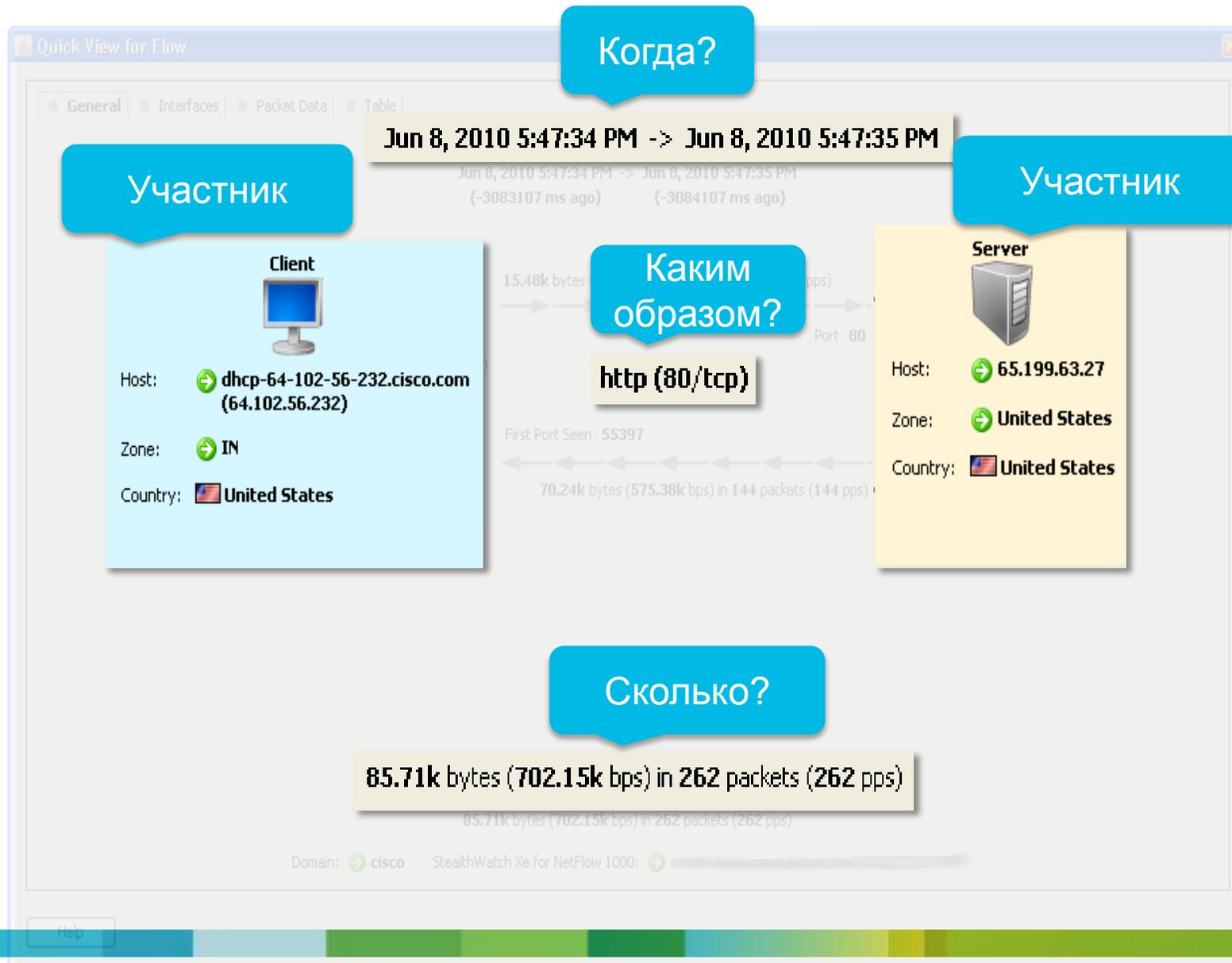
- Поле Flow Action может добавить дополнительный контекст
- NSEL-отчетность на основе состояний для поведенческого анализа
Сбор информации о отклоненных или разрешенных соединениях

| Flow Action | Client Host | Translated Host | Client Host Groups | Server Host | Server Host Groups |
|-------------|----------------|-----------------|--------------------|----------------|--------------------|
| Permitted | 192.168.203.10 | 168.192.203.10 | Web Servers | 168.192.200.22 | United States |
| Permitted | 192.168.203.10 | 168.192.203.10 | Web Servers | 168.192.200.22 | United States |
| Permitted | 168.192.200.22 | 168.192.203.10 | United States | 192.168.203.10 | Web Servers |
| Denied | 192.168.203.10 | 168.192.203.10 | United States | 192.168.203.10 | Web Servers |
| Denied | 168.192.200.22 | 168.192.203.10 | United States | 192.168.203.10 | Web Servers |

Permitted through ASA

Denied by ASA

Расследование инцидентов



Запрос интересующей информации

Выберите узел
для
исследования

Поиск
исходящего
трафика

Hosts

Filter by Host

Where the **Client or Server Host** is in:

All

Zone: ...

Include sub-zones

VMs: ...

Range:

IP Addresses:

and the **Other Host** is in:

All

Zone: ...

Include sub-zones

VMs: ...

Range:

IP Addresses:

Help OK Cancel

Результаты запроса

Flow Summary x Security and Traffic Overview x Flow Summary

Domain : cisco Active Time : From Jun 7, 2010 5:10:00 PM to Jun 7, 2010 5:10:00 PM

Client or Server Zone : Inside Zones

Client Hosts Server Hosts Services Conversations

Conversation - 2,000 records

| Client Zone | Client Host | Server Zone | Server Host | Service | Flow Count | Total Traffic (bps) | Client Traffic (bps) | Server Traffic (bps) | Adjusted Total... |
|-------------|--|---------------|---|---------------|------------|---------------------|----------------------|----------------------|-------------------|
| IN | rtp5-dmz-wsa-1.cisco.com (64.102.249.6) | United States | rdc-024-025-026-041.southeast.rr.com (24.25.26.41) | http (80/tcp) | 1 | 855.25k | 21.96k | 833.29k | 41.6M |
| All-Inside | rtp10-dmz-wsa-1.cisco.com (64.102.249.8) | United States | rdc-024-025-026-032.southeast.rr.com (24.25.26.32) | http (80/tcp) | 1 | 789.79k | 38.16k | 751.63k | 40.38M |
| IN | proxy.cisco.com (64.102.249.8) | United States | 208.111.161.254 | http (80/tcp) | 1 | 757.32k | 35.25k | 722.07k | 39.47M |
| IN | lwr02-00-acns-ce1.cisco.com (64.100.144.8) | United States | rdc-024-025-026-049.southeast.rr.com (24.25.26.49) | http (80/tcp) | 1 | 855.25k | 21.96k | 833.29k | 35.95M |
| IN | rtp5-dmz-wsa-1.cisco.com (64.102.249.6) | United States | rdc-024-025-026-032.southeast.rr.com (24.25.26.32) | http (80/tcp) | 1 | 789.79k | 38.16k | 751.63k | 30.59M |
| IN | rtp10-dmz-wsa-2.cisco.com (64.102.249.9) | United States | 208.111.161.254 | http (80/tcp) | 1 | 757.32k | 35.25k | 722.07k | 28.24M |
| IN | rtp10-dmz-wsa-1.cisco.com (64.102.249.8) | United States | rdc-024-025-026-116.southeast.rr.com (24.25.26.116) | http (80/tcp) | 1 | 705.75k | 27.90k | 677.76k | 27.08M |
| IN | lwr02-00-acns-ce1.cisco.com (64.100.144.8) | United States | rdc-024-025-026-049.southeast.rr.com (24.25.26.49) | http (80/tcp) | 1 | 855.25k | 21.96k | 833.29k | 25.74M |
| IN | rtp10-dmz-wsa-1.cisco.com (64.102.249.8) | United States | rdc-024-025-026-032.southeast.rr.com (24.25.26.32) | http (80/tcp) | 1 | 789.79k | 38.16k | 751.63k | 25.74M |
| IN | rtp-ksalhoff-8719.cisco.com (10.116.34.74) | IANA Reserved | 184.50.211.1 | http (80/tcp) | 1 | 459.95k | 27.65k | 432.30k | 25.74M |
| IN | dhcp-64-102-220-150.cisco.com (64.102.220.150) | United States | 184.50.211.1 | http (80/tcp) | 1 | 459.95k | 27.65k | 432.30k | 17.44M |
| IN | smokehouse.cisco.com (64.102.19.208) | IANA Reserved | 184.50.211.1 | http (80/tcp) | 1 | 8.09k | 474.67k | 466.58k | 17.26M |
| IN | rtp10-dmz-wsa-2.cisco.com (64.102.249.9) | United States | 208.111.161.254 | http (80/tcp) | 1 | 458.57k | 18.04k | 440.53k | 17.05M |
| IN | rtp5-dmz-wsa-2.cisco.com (64.102.249.7) | United States | 208.111.161.254 | http (80/tcp) | 1 | 423.40k | 23.83k | 399.57k | 16.34M |

Service Summary | Flow Count | Total Traffic (bps)

| | | |
|---------------|---|-------|
| http (80/tcp) | 1 | 1.16M |
|---------------|---|-------|

United States

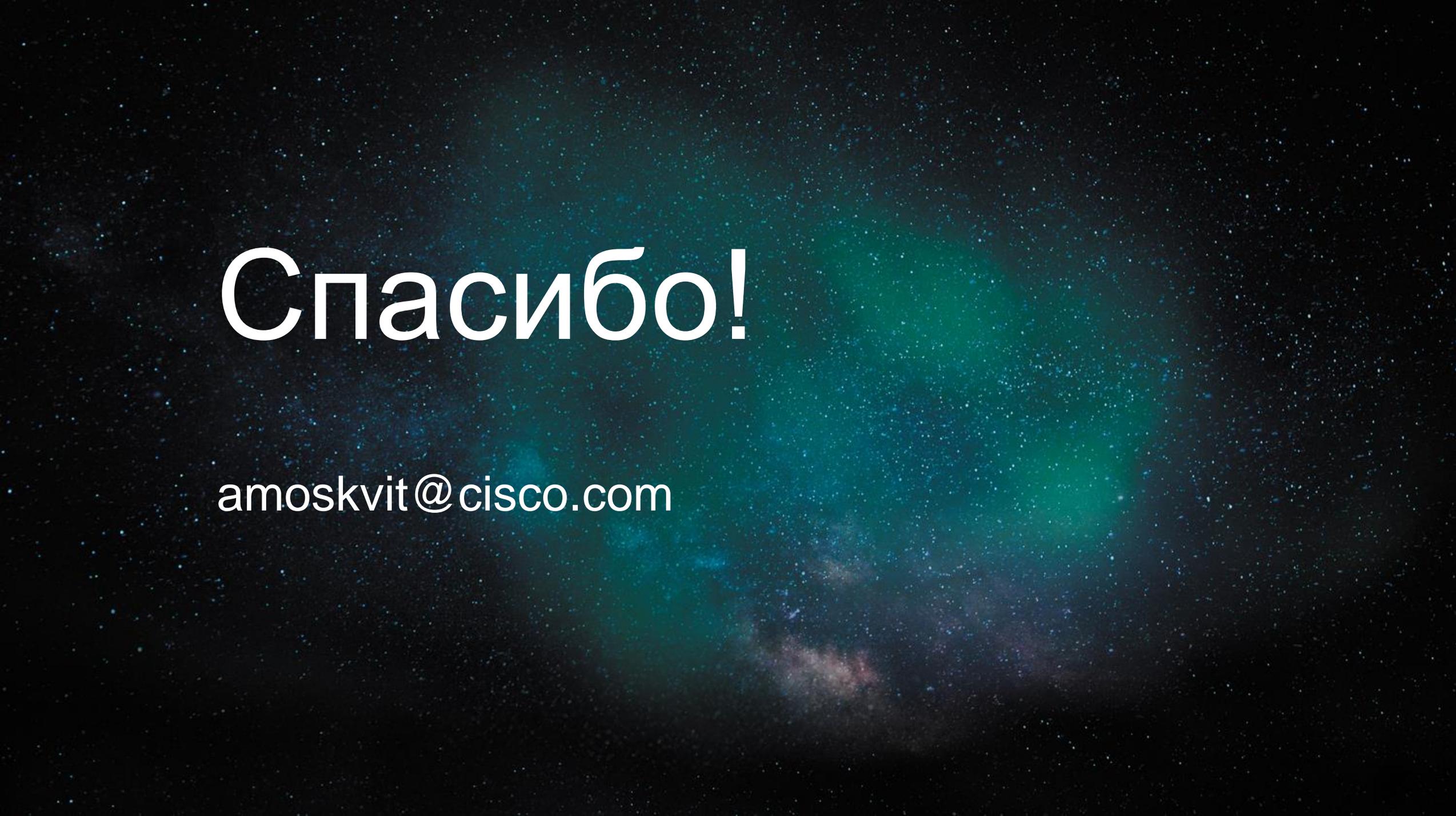
rdc-024-025-026-041.southeast.rr.com (24.25.26.41)

Тип трафика и объем

Last refreshed: Jun 7, 2010 5:32:02 PM

Начните с пилотного внедрения

- Оба решения доступны в виде VM и имеют временные лицензии
- Не требуют изменений в сети, только зеркальную копию трафика и NetFlow
- Разворачиваются в течение нескольких дней-недели
- Приносят ощутимые результаты
 - Обнаружение компьютеров-зомби и червей
 - Профилирование трафика и приложений
 - Инвентаризация хостов
 - Обнаружение нелегальных серверов и P2P-трафика внутри сети



Спасибо!

amoskvit@cisco.com

Решение по безопасности, встроенное, а не пристроенное



Sourcefire FireSIGHT «ВИДИТ ВСЕ»

| КАТЕГОРИИ | ПРИМЕРЫ | SOURCEFIRE СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И МЕЖСЕТВЫЕ ЭКРАНЫ НОВОГО ПОКОЛЕНИЯ | СТАНДАРТНАЯ СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ | СТАНДАРТНЫЙ МЕЖСЕТВЫЙ ЭКРАН НОВОГО ПОКОЛЕНИЯ |
|------------------------------|---|---|--|--|
| Угрозы | Атаки, аномалии | ✓ | ✓ | ✓ |
| Пользователи | AD, LDAP, POP3 | ✓ | ✗ | ✓ |
| Веб-приложения | Facebook Chat, Ebay | ✓ | ✗ | ✓ |
| Протоколы приложений | HTTP, SMTP, SSH | ✓ | ✗ | ✓ |
| Передача файлов | PDF, Office, EXE, JAR | ✓ | ✗ | ✓ |
| Вредоносное ПО | Conficker, Flame | ✓ | ✗ | ✗ |
| Серверы C&C | Интеллектуальная система безопасности C&C | ✓ | ✗ | ✗ |
| Клиентские приложения | Firefox, IE6, BitTorrent | ✓ | ✗ | ✗ |
| Веб-серверы | Apache 2.3.1, IIS4 | ✓ | ✗ | ✗ |
| Операционные системы | Windows, Linux | ✓ | ✗ | ✗ |
| Маршрутизаторы и коммутаторы | Cisco, Nortel, Wireless | ✓ | ✗ | ✗ |
| Мобильные устройства | iPhone, Android, Jail | ✓ | ✗ | ✗ |
| Принтеры | HP, Xerox, Canon | ✓ | ✗ | ✗ |
| VoIP-телефоны | Avaya, Polycom | ✓ | ✗ | ✗ |
| Виртуальные машины | VMware, Xen, RHEV | ✓ | ✗ | ✗ |

Next-Gen FW (NGFW)

Стандартные возможности «предыдущего поколения»

Понимание приложений и их компонентов

Встроенный сетевой IPS

Интеграция с внешними сервисами, пример:

- Каталоги пользователей
- «Репутационные» сервисы

Next-Gen IPS (NGIPS)

Стандартные возможности «предыдущего поколения»

Понимание приложений

Понимание контекста и контента

Гибкий движок, оперативные обновления сигнатур

“NGIPS в будущем войдёт в NGFW, но сейчас большинство существующих NGFW обладают только базовым функционалом IPS”

Gartner[®]

Источник: “Defining Next-Generation Network Intrusion Prevention,” Gartner, October 7, 2011.
“Defining the Next-Generation Firewall,” Gartner, October 12, 2009

Ответ
предприятия



Антивирус
(Host-Based)

IDS/IPS
(Сетевой периметр)

Репутация (Global) и
песочница

Разведка и аналитика
(Облако)

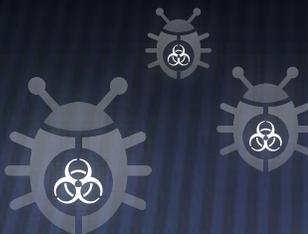
Угрозы

Черви и вирусы



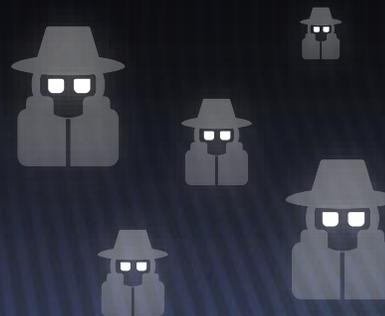
2000

Шпионское ПО
и руткит



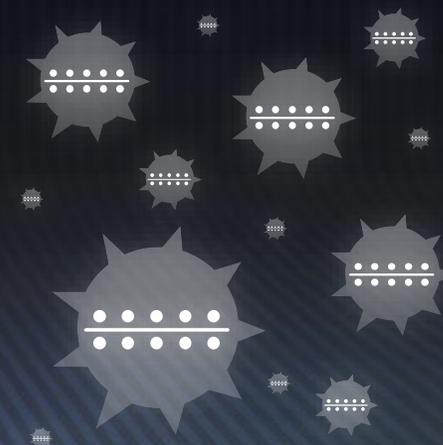
2005

APTс и
кибервойны



2010

Изменение
ландшафта угроз



завтра

ЭВОЛЮЦИЯ УГРОЗ