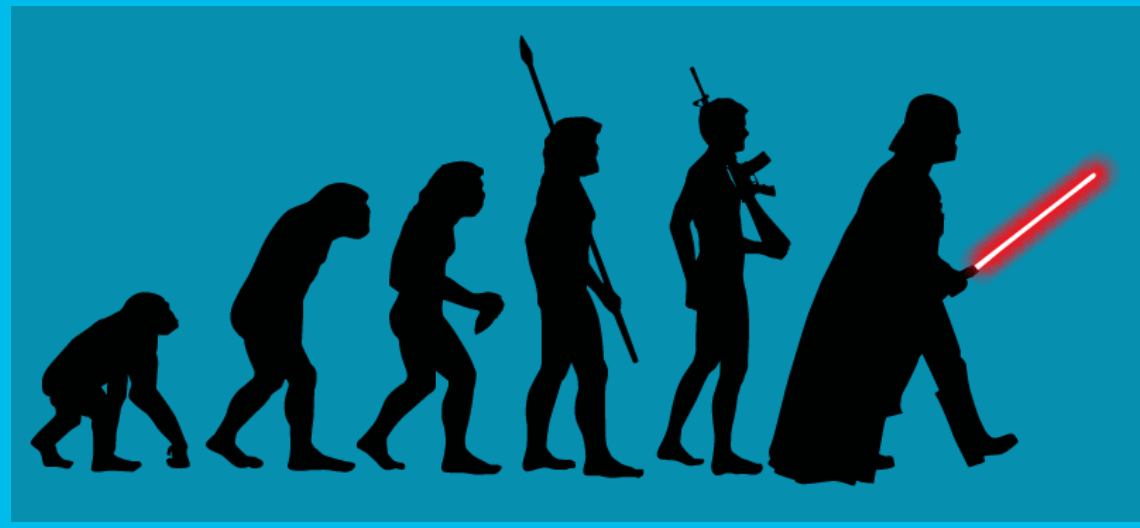
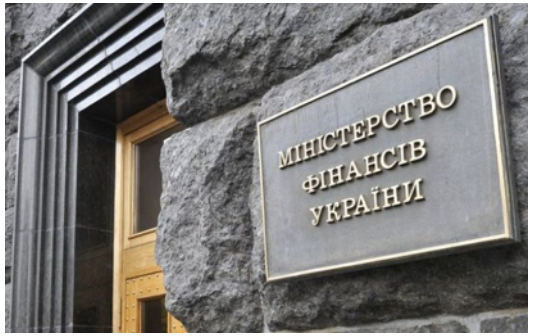
Архитектура обеспечения информационной безопасности. Подход Cisco

Павел Родионов
prodiono@cisco.com,

Состояние кибербезопасности



Атаки в Украине – декабрь 2016



АМПУ

ДЕРЖГЕОКАДАСТР
ДЕРЖАВНА СЛУЖБА УКРАЇНИ
З ПИТАНЬ ГЕОДЕЗІЇ, КАРТОГРАФІЇ ТА КАДАСТРУ

Сайт Міносвіти не працює через DDoS-атаки

Тривають роботи з відновлення роботи сайту.

Фото: autocentre.ua

Сайт Міністерства освіти і науки України не працює внаслідок **DDoS-атаки** на вихідних.

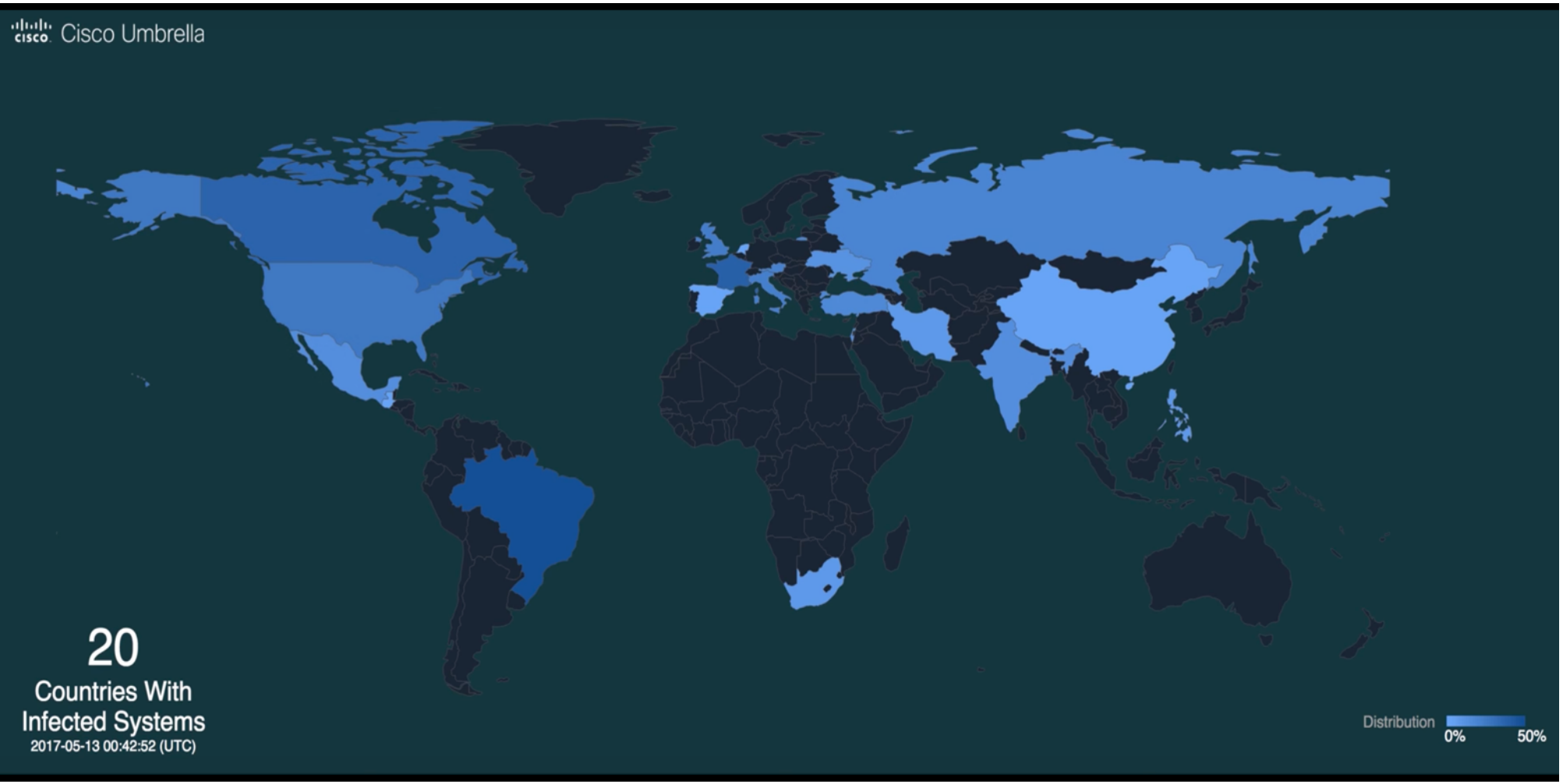
Про це повідомили в прес-службі відомства, передає **"Інтерфакс-Україна"**.

Як розповіли в Міносвіти, сама атака відбулася вихідних і в результаті сайт досі не працює.

Новый игрок. Скажи «привет» ‘WannaCry’

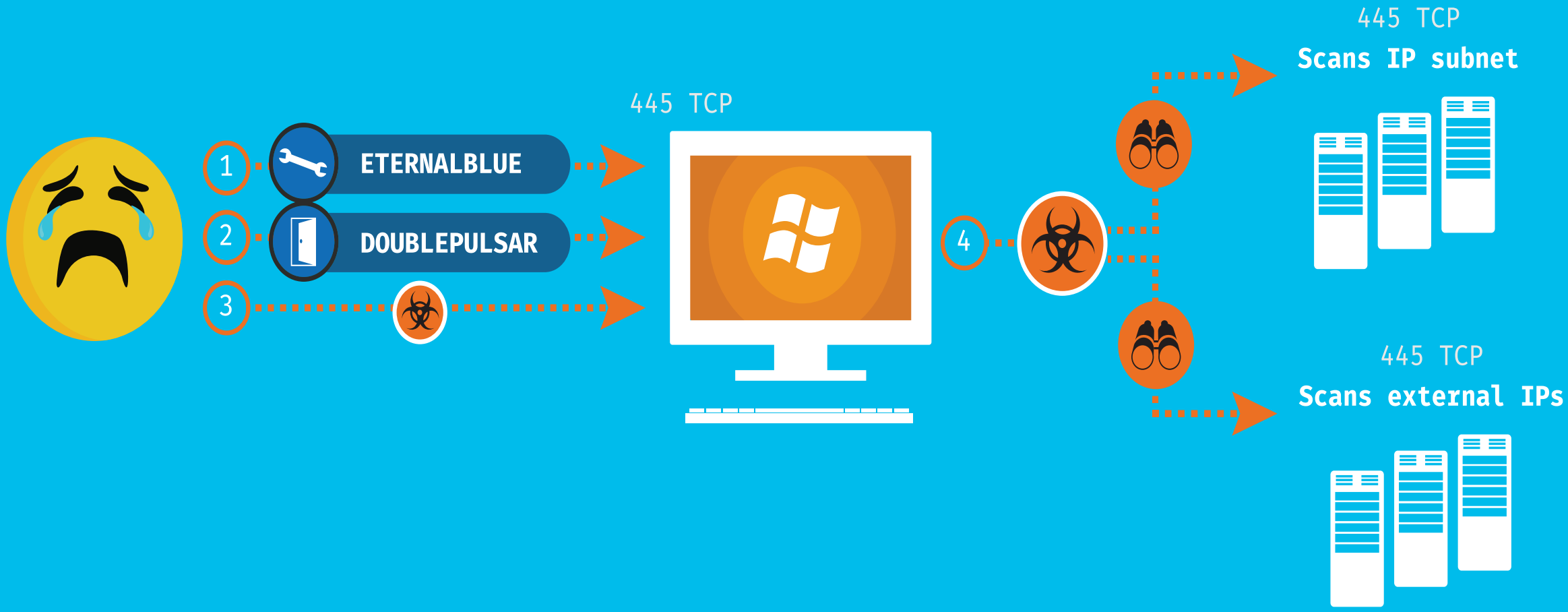
- Новый вариант вымогателя начал компрометировать системы 12 мая 2017
- Использовал уязвимости, которые были пропатчены с помощью MS17-010 в марте 2017

WannaCry шагает по планете – май 2017



[25855, 'RU']
[22986, 'CN']
[7614, 'TW']
[5966, 'UA']
[5054, 'US']
[3087, 'CA']
[2195, 'KR']
[1712, 'FR']
[1394, 'IN']
[1132, 'BR']
[943, 'HK']
[656, 'JP']
[651, 'GB']
[546, 'DE']
[518, 'PL']
[517, 'CL']
[480, 'MX']
[436, 'IT']
[430, 'VN']
[403, 'AM']
[397, 'KZ']
[363, 'RO']
[362, 'AR']
[337, 'MD']
[330, 'PH']
[277, 'TH']

Распространение WannaCry



SHODAN port:445 country:ua "SMB Version:1" !product:Samb Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

12,767

TOP COUNTRIES

Ukraine	12,767

TOP CITIES

Kiev	2,703
Dnepropetrovsk	1,301
Kharkiv	650
Lugansk	436
Kharkov	141

TOP ORGANIZATIONS

PJSC Ukrtelecom	802
Triolan	800
Kyivstar GSM	736
Private Stock company Sater	526
UMC	255

TOP OPERATING SYSTEMS

Windows 7 Ultimate 7601 Service Pack 1	3,220
Windows Server 2012 R2 Standard 9600	1,112
Windows 10 Pro 15063	929
Windows 7 Professional 7601 Service P...	512
Windows 8.1 Pro 9600	472

46.149.178.112

tun-46-149-178-112.kim.in.ua
Windows 10 Pro 15063
Kalush Information Network LTD
Added on 2017-11-13 21:08:57 GMT
Ukraine, Ivanofrankovsk
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthru,large-readx,large-writex,lwio,ext
```

91.243.214.165

Windows 7 Home Premium 7601 Service Pack 1
Intellect Dnepr Telecom LLC
Added on 2017-11-13 21:07:50 GMT
Ukraine, Dnepropetrovsk
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthru,large-readx,large-writex,lwio,ext
```

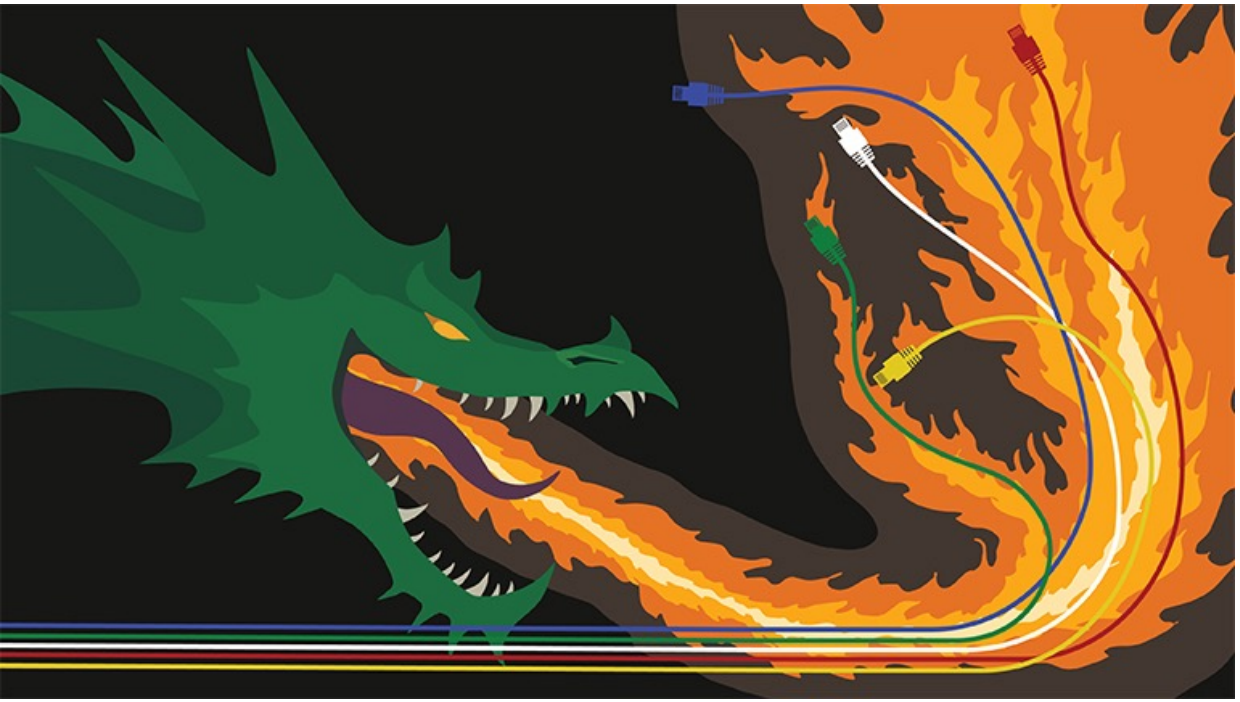
37.115.149.55

37-115-149-55.broadband.kyivstar.net
Windows 7 Ultimate 7601 Service Pack 1
Kyivstar GSM
Added on 2017-11-13 21:07:05 GMT
Ukraine, Chernihiv
Details

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthru,large-readx,large-writex,lwio,ext
```

Прошло полгода после WannaCry

Июнь 2017. Nyetya. Он же Petya-A. Он же Не-Петя

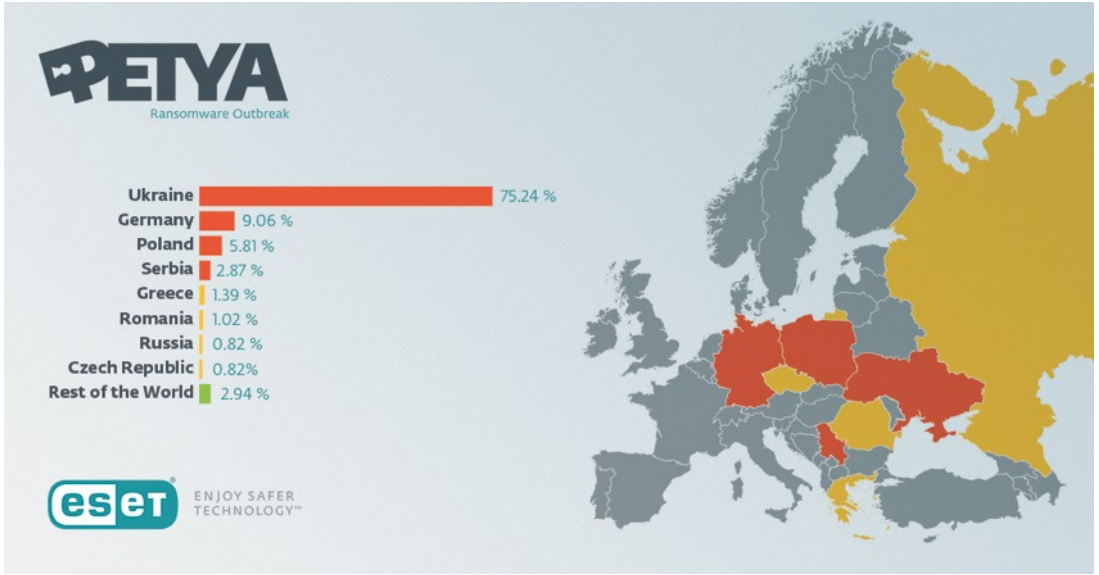


- Использовал доверенный канал бухгалтерского ПО для доставки в организации
- Использовал гибридную методологию распространения
- Шифровал файлы не с целью получения выкупа, а для нанесения урона

Расследование атаки от группы Cisco Talos – The MeDoc Connection

http://www.cisco.com/c/dam/global/ru_ua/solutions/security/ransomware/pdfs/cisco_blog_ransomware_attack_ua_upd4-graphics.pdf

Neytya/Petya: результаты атаки



- До 10% корпоративных компьютеров было поражено

  Дмитрий Шимкив

- Потери от Petya.A составили $850 млн

  Страховая компания Lloyd's

- 1/3 банков пострадало в ходе атаки

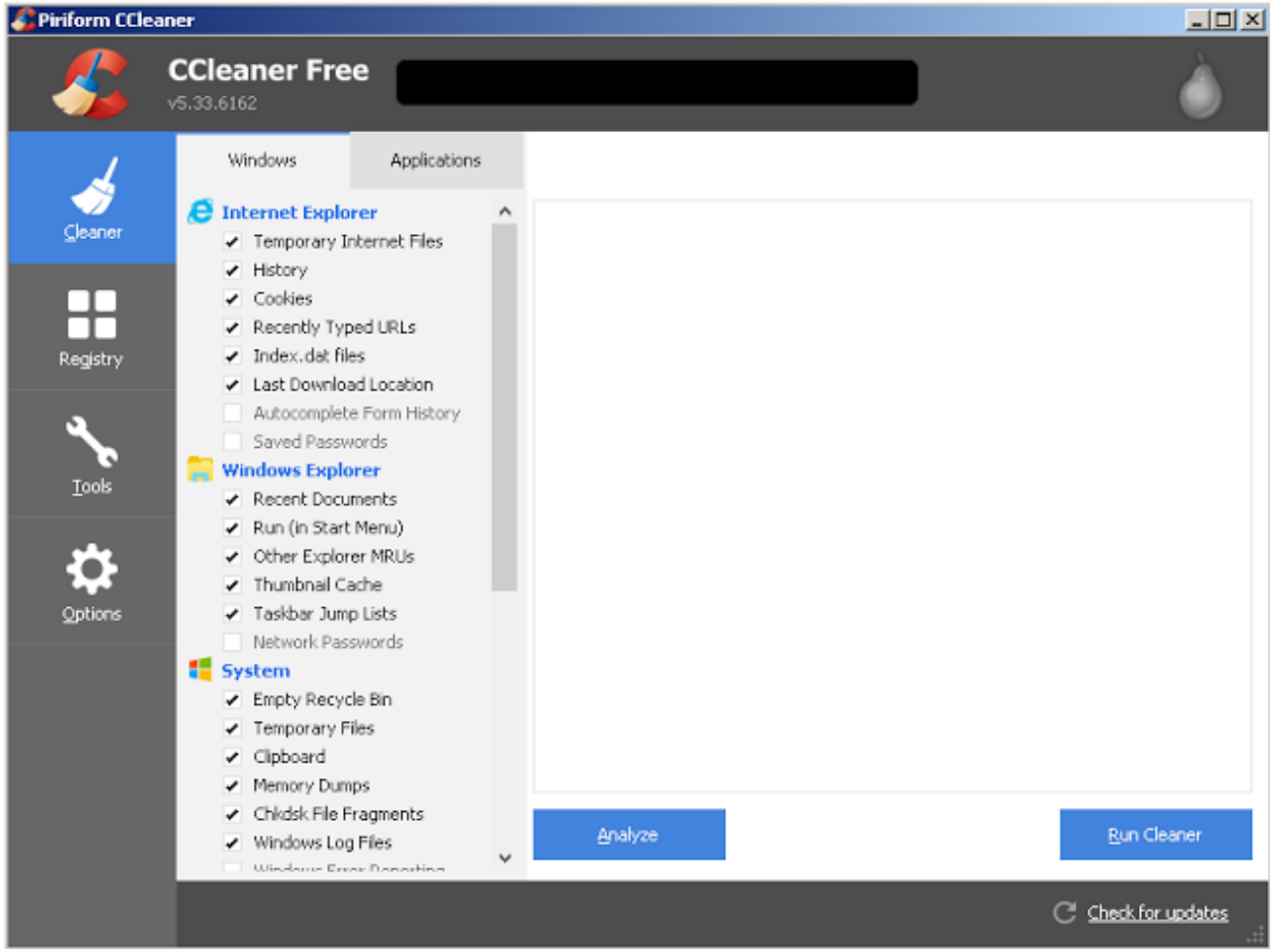
  Антон Кудин, Департамент безопасности НБУ

- Финансовые потери до 0.2 - 0.5% ВВП

  Экспертная оценка

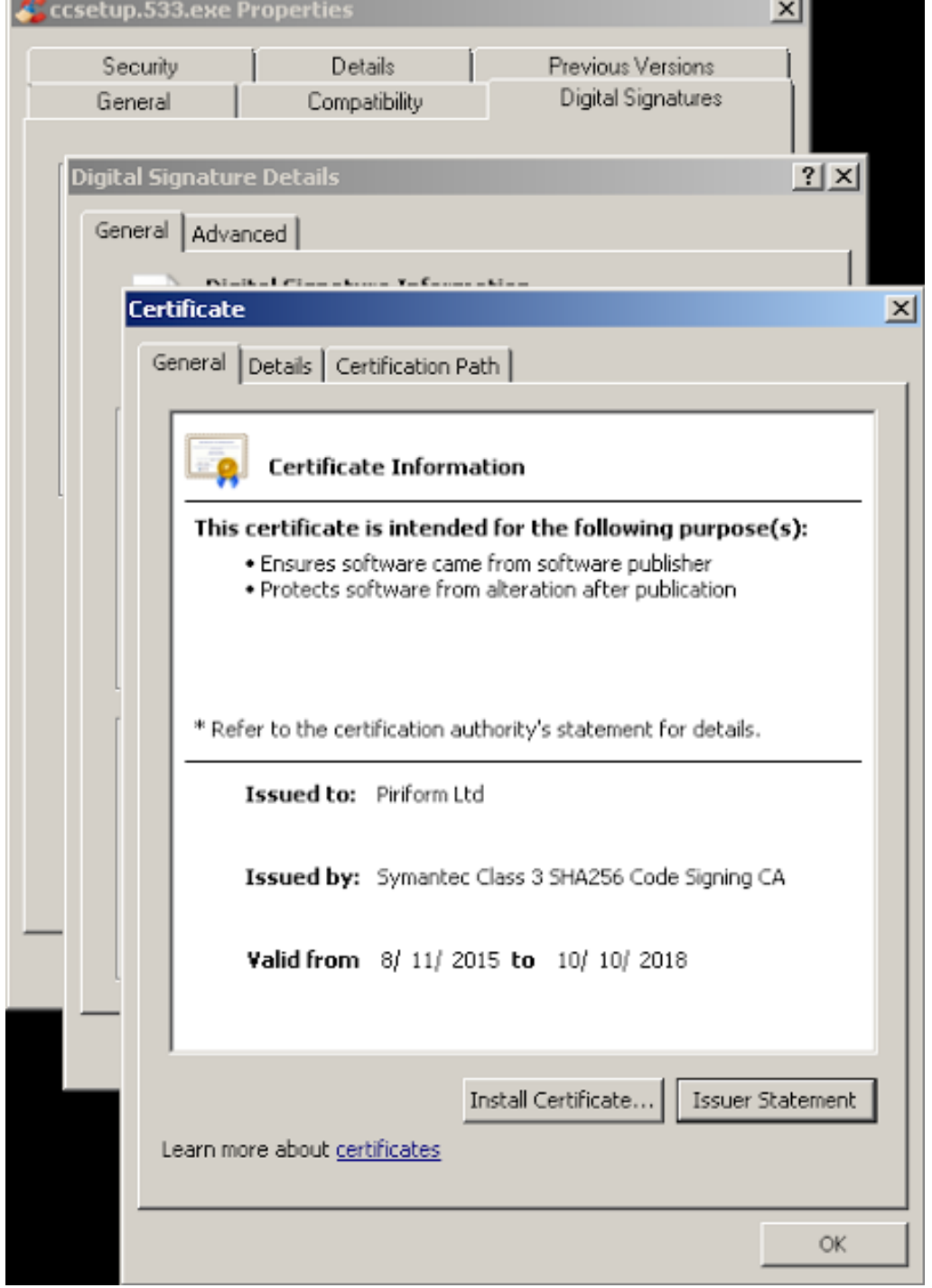
CCleaner

- Легитимное ПО с встроенным бэкдором
- Обнаружен Cisco при тестировании бета-версии системы защиты от malware



Особенности CCleaner

- Подписан легальным сертификатом



Цель атаки

- Направлен на крупные компании во всех странах
- Заразил несколько сот тысяч компьютеров
- Армейская дисциплинированность атакующих

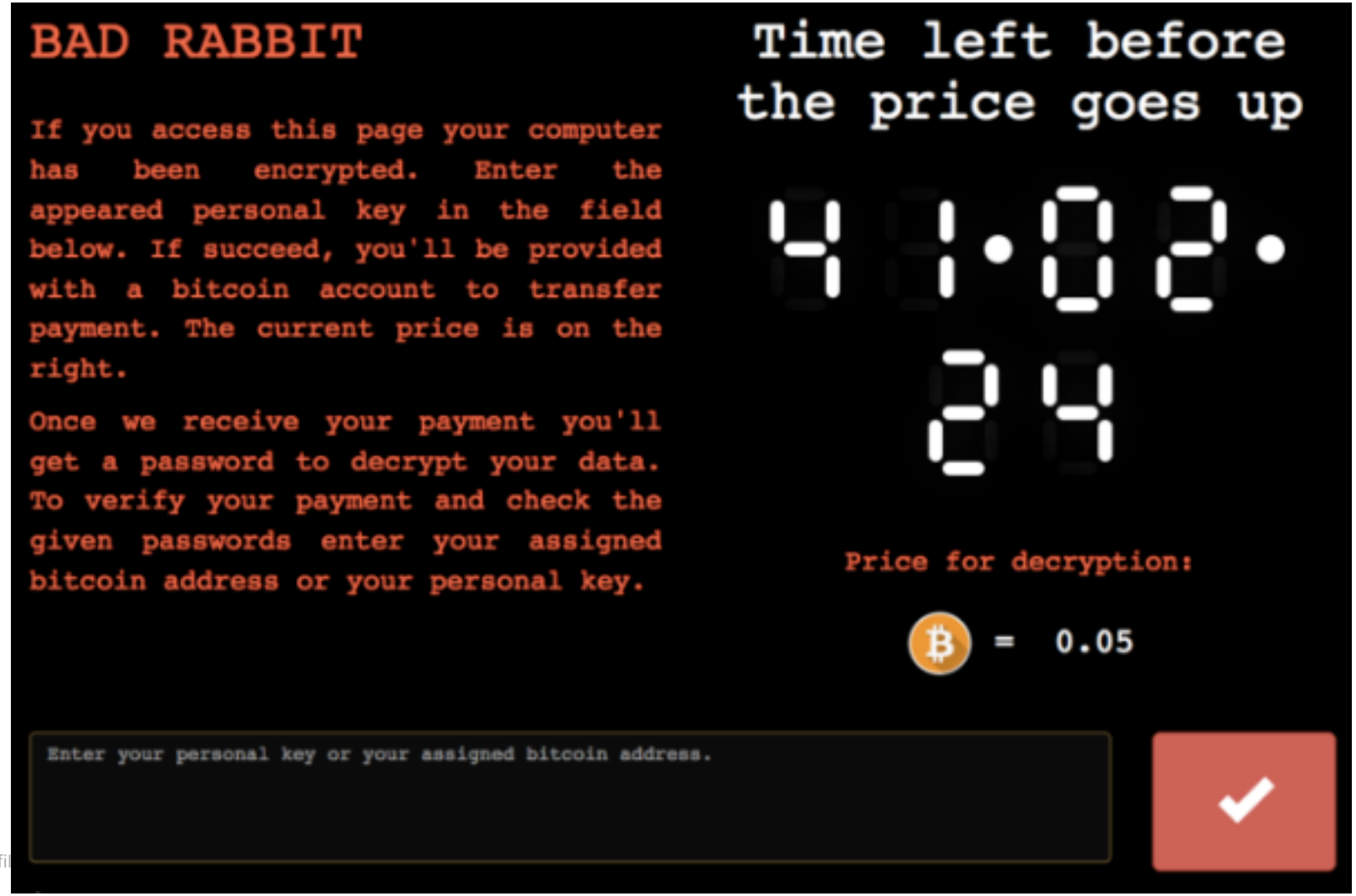
```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrdns.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

24 октября 2017
Следуй за «плохим кроликом»!



24 октября 2017
Следуй за «плохим кроликом»!

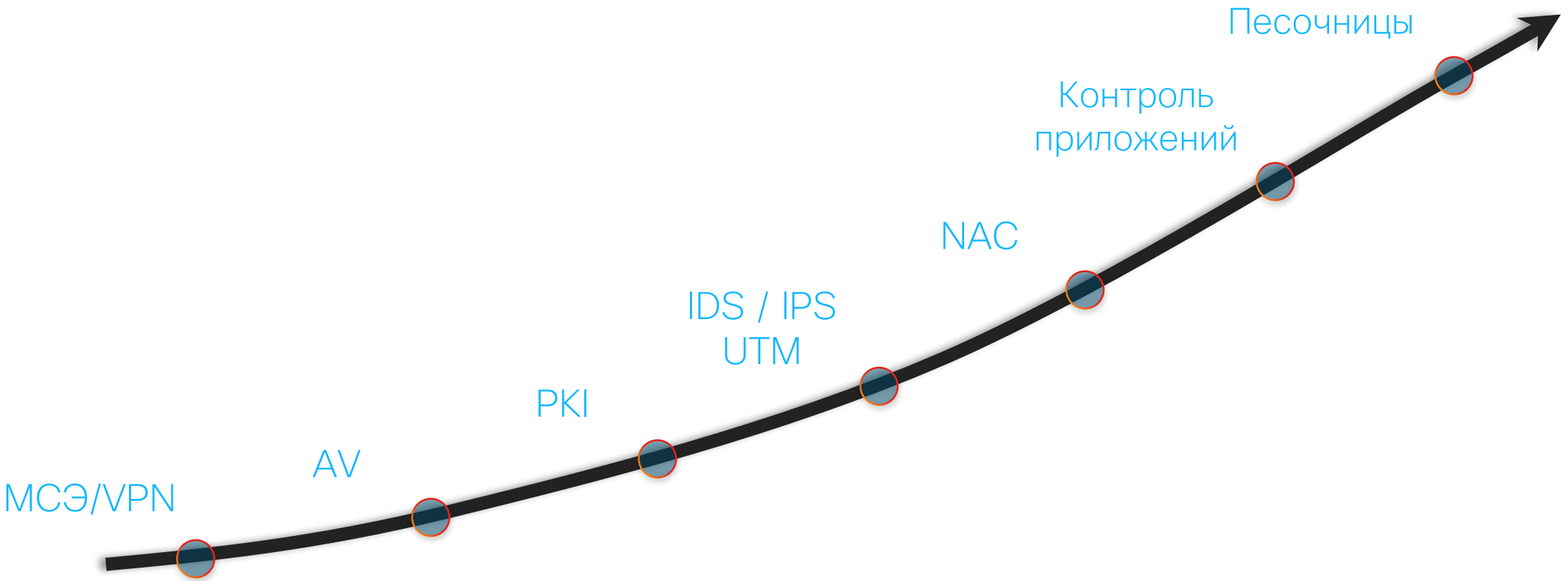
- BadRabbit -- массовая ransomware кампания
- Поражены организации в Украине, России, Болгарии, Турции
- Основной вектор заражения – поддельное обновление Adobe Flash
- Использует методы последовательного распространения из Petya/Nyetya

Как защититься?

Точечные средства защиты оказались неэффективными

Организации с архитектурой безопасностью обошлись минимальными потерями

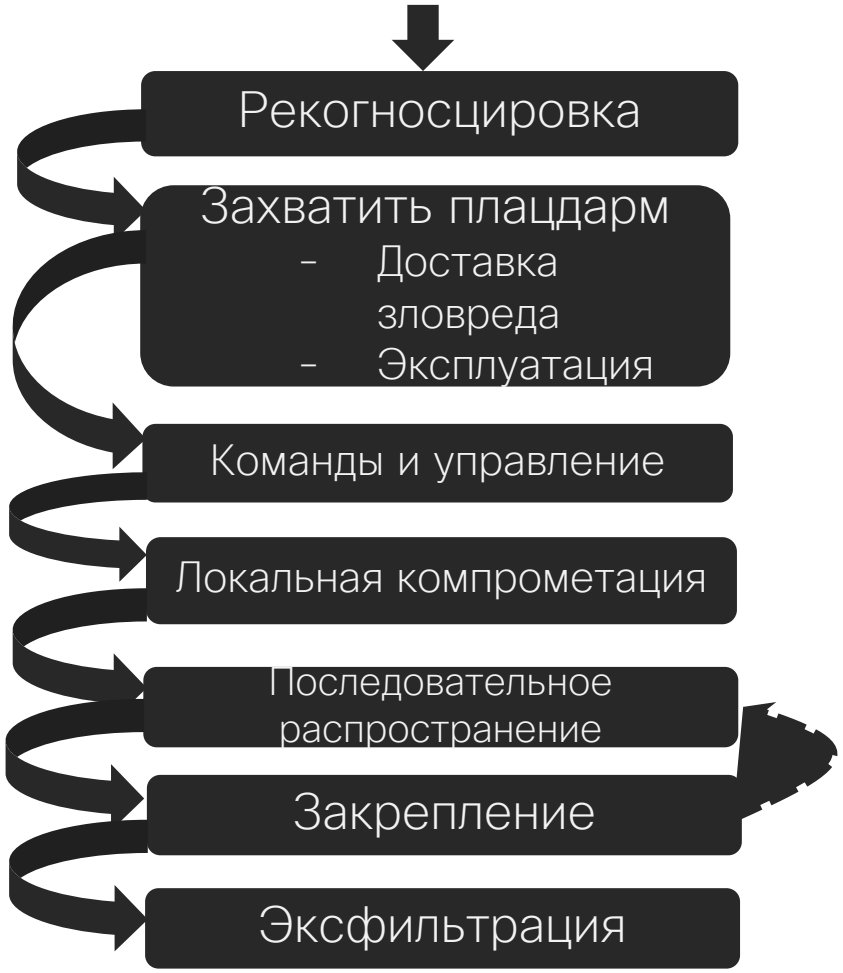
Серебряной пули не существует...



Ключевой пункт: защитить и обнаружить

- Сейчас большая часть трат IT безопасности приходится на ранние стадии последовательности атаки
- Нужен другой баланс
- “**Организации должны изменить пропорцию инвестиций от 90% на предотвращение и 10% обнаружения и реагирования на пропорцию. 60/40**

Петер Зондергард, Гартнер



Постулаты Cisco для разработки подхода

Осведомленность о проблемах безопасности

+

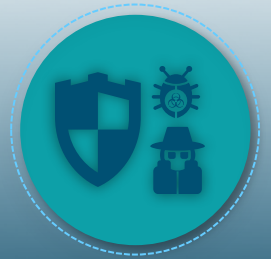
Реализуемость подхода

+

Нехватка персонала

Требуется изменение подхода к построению ИБ

Видимость



Знание угроз

Платформы

Консалтинг

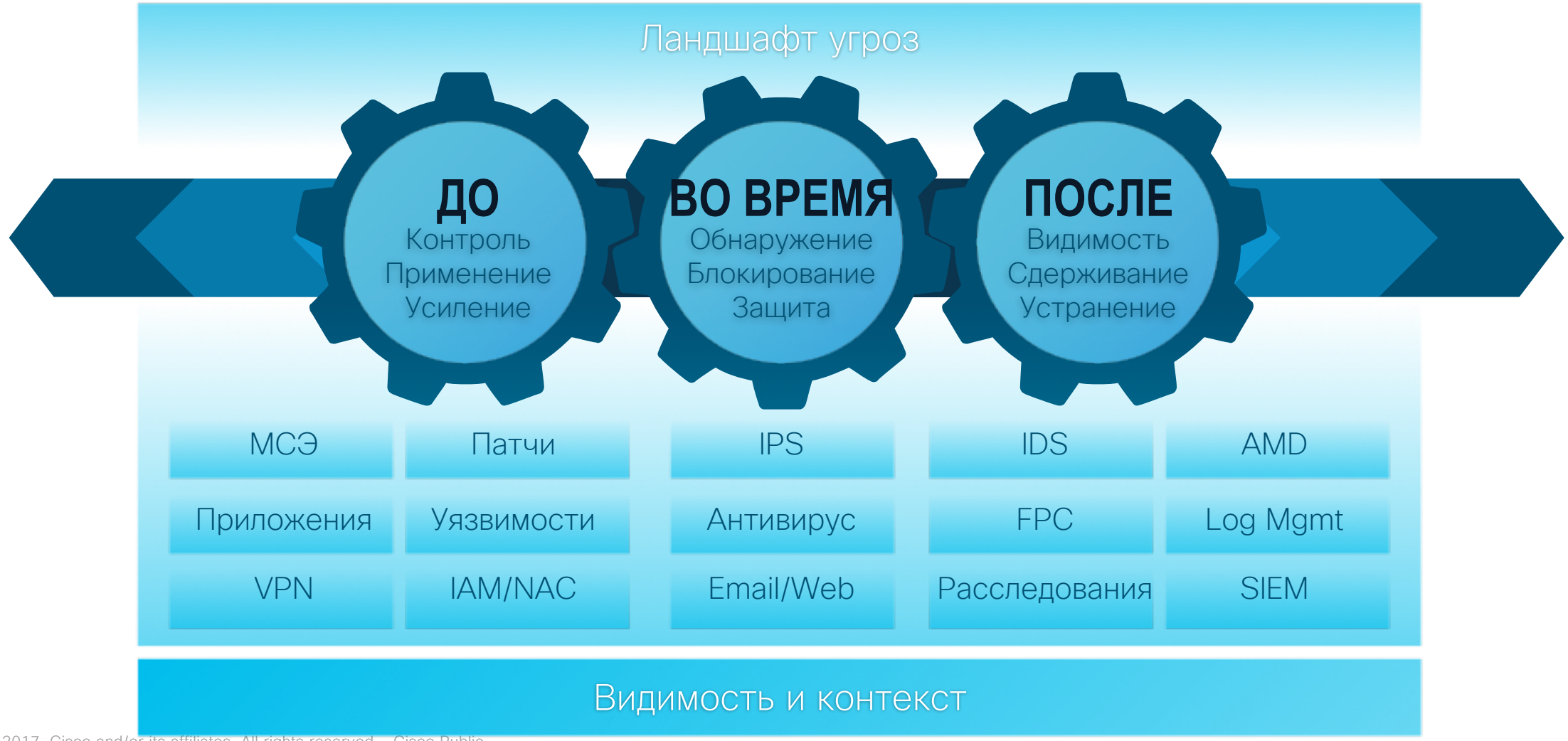
Интеграция

Управление

Портфолио Cisco учитывает данную модель

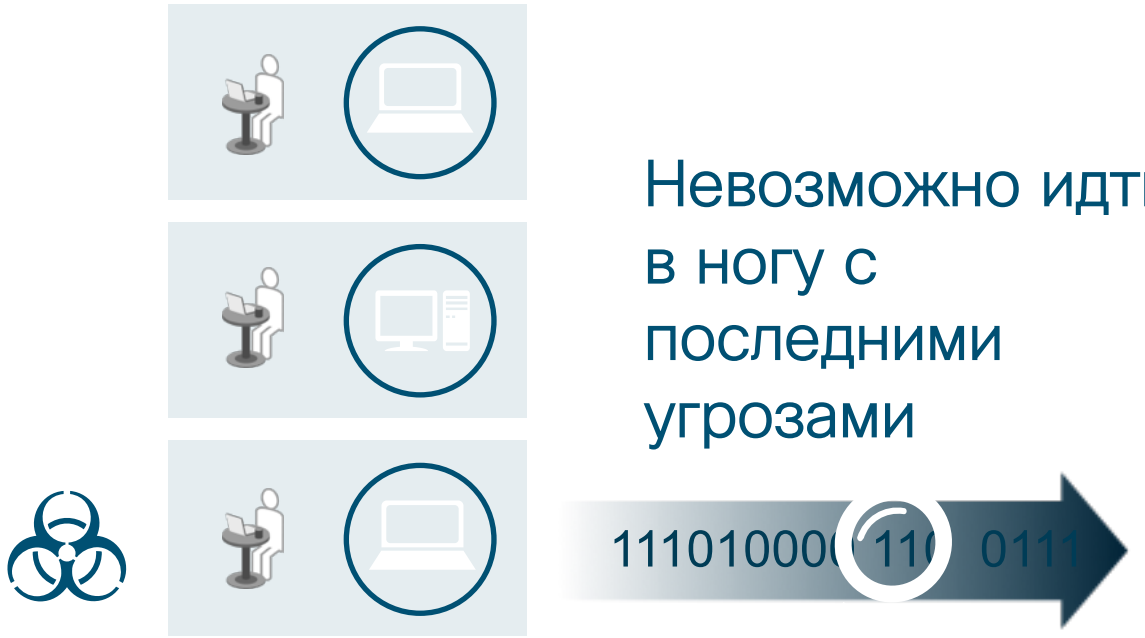
Новая модель должна быть реализована повсюду, а не только на периметре!

От модели к технологиям

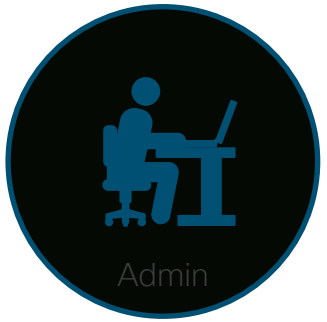


Фокус на угрозы

Проблемы с подходом «сделай сам»



Невозможно идти в ногу с последними угрозами



Базируется на правилах

- Зависимость от сложно создаваемых вручную правил
- Зависимость от человеческого фактора

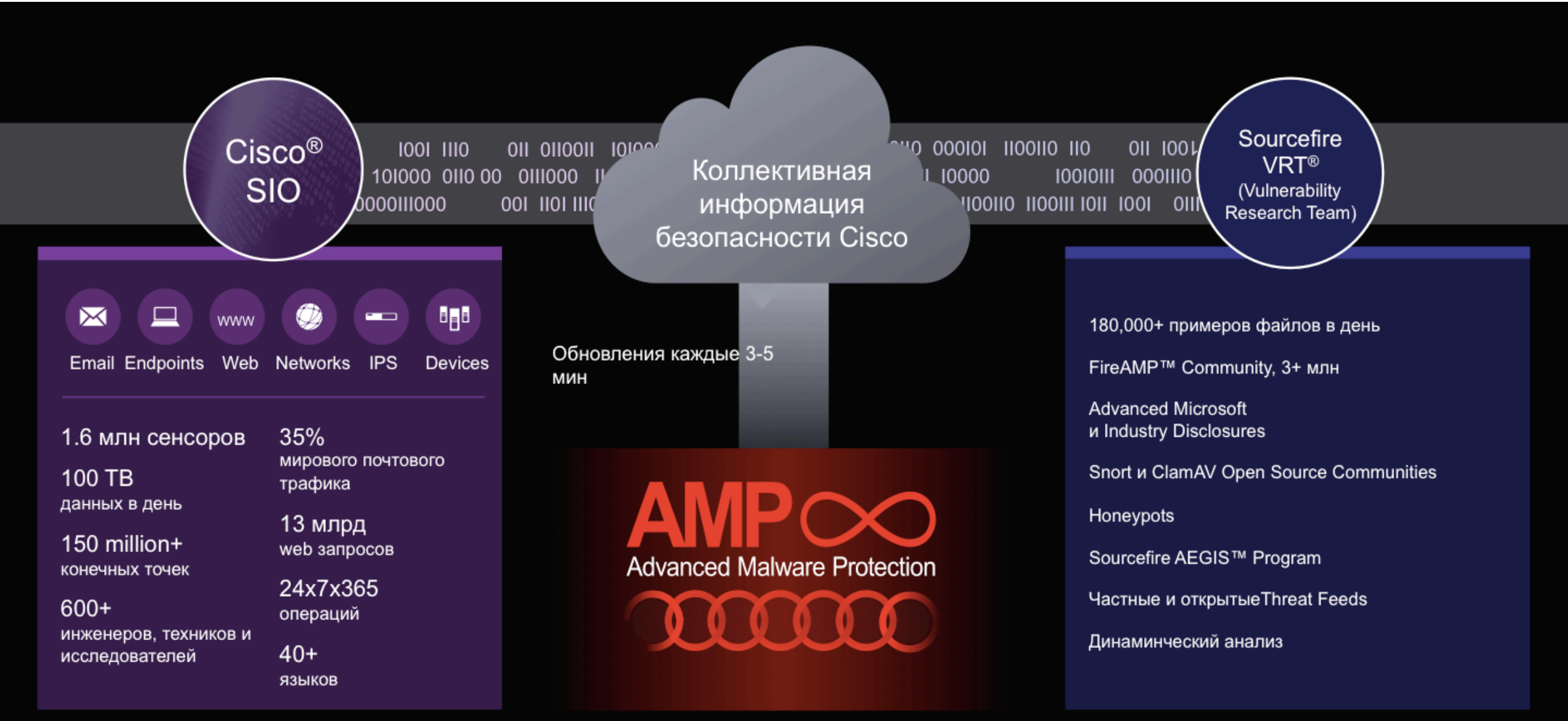
Зависимость от времени

- Занимает недели или месяцы на обнаружение
- Требует постоянного тюнинга

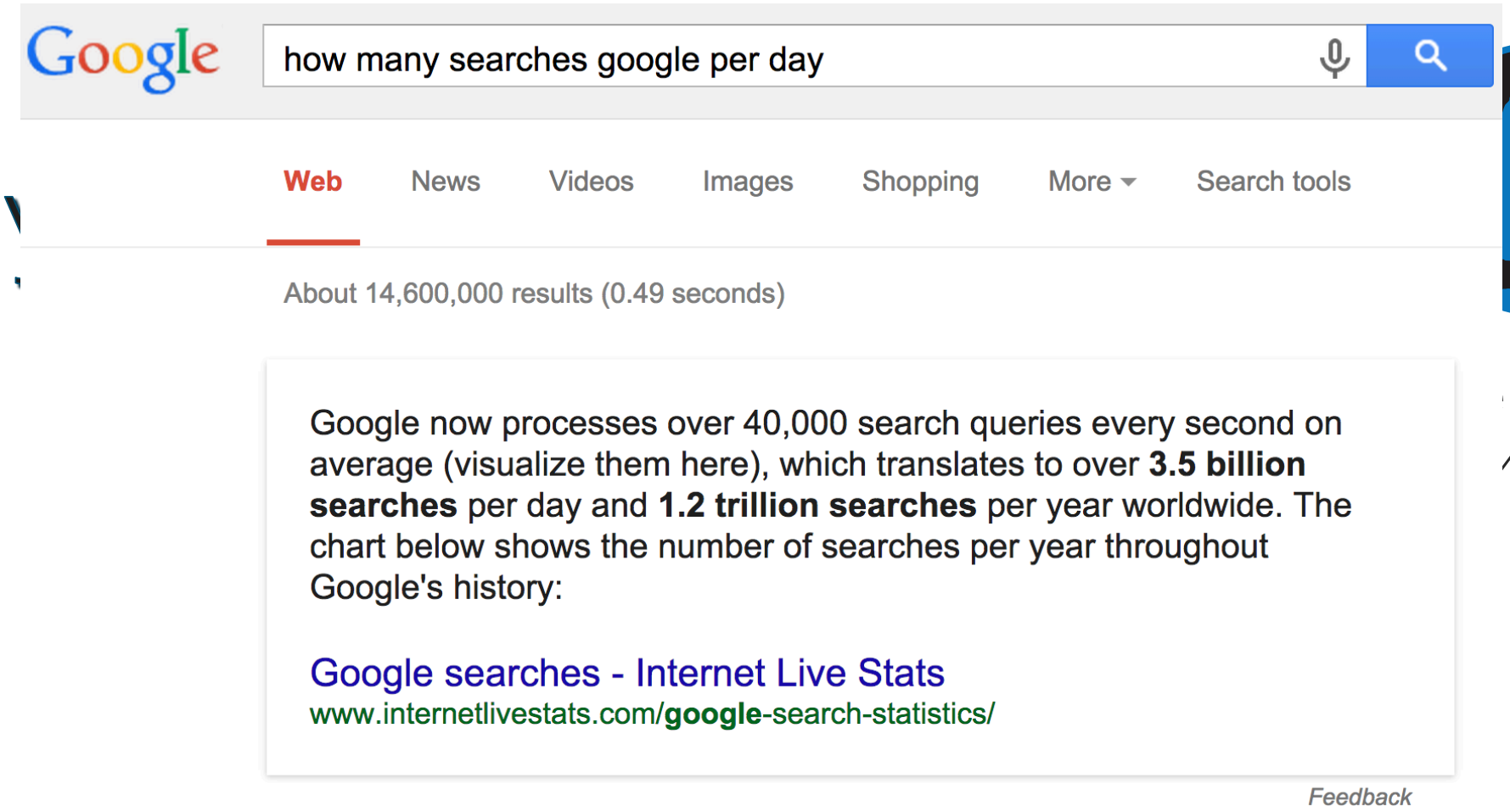
Очень сложно

- Часто требует квалифицированный персонал для управления и поддержки

Cisco SIO + Sourcefire VRT = Cisco Talos



Оцените масштаб охвата



проживает
ларда человек

Около 3-х угроз
на каждого
жителя Земли
приходится
ежедневно

5 департаментов

TALOS

90 МЛРД

DNS-запросов в день

18.5 МЛРД / 1,5 МЛН

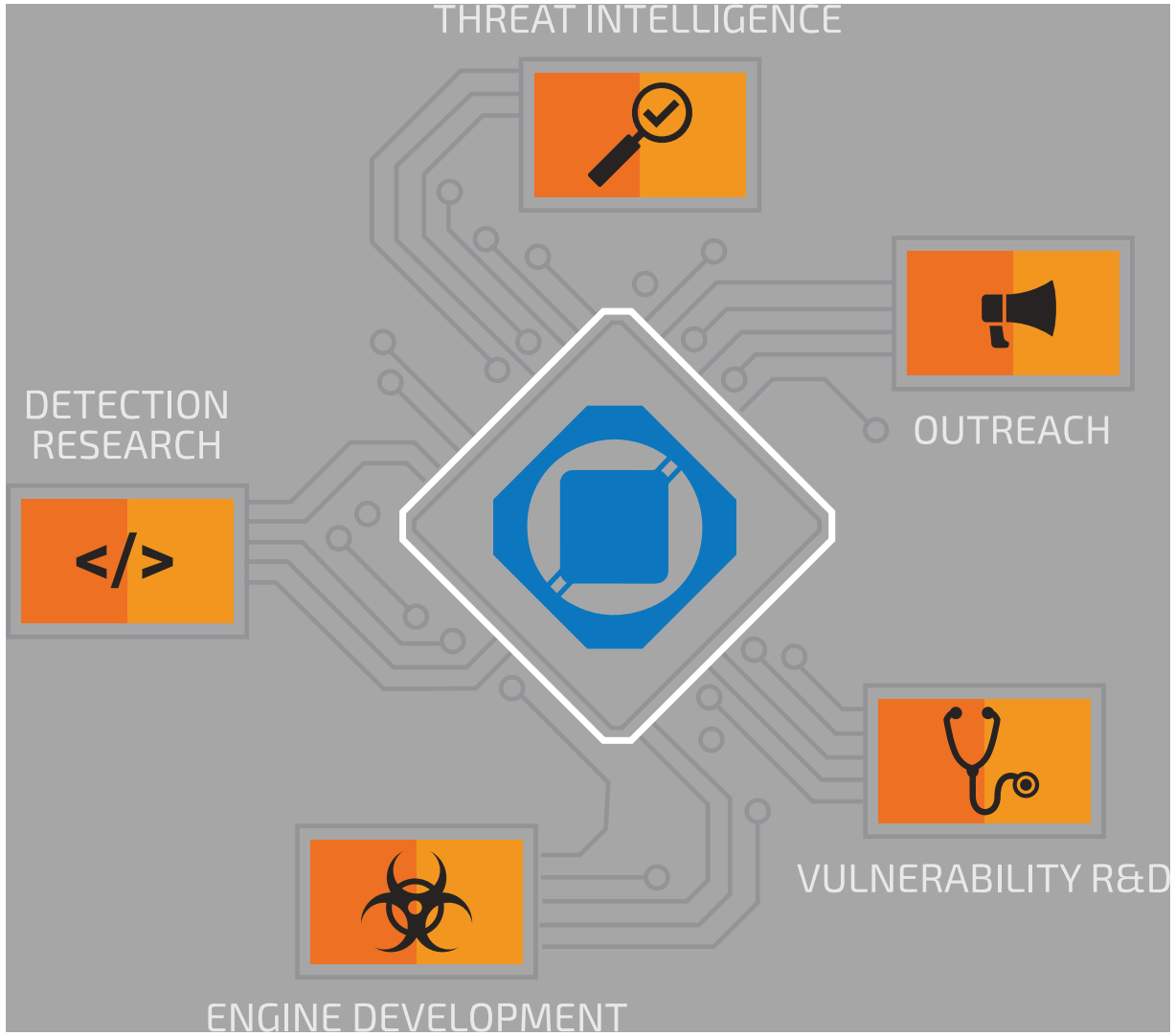
Файлов / семплов в день

16 МЛРД

Web-запросов в день

600 МЛРД

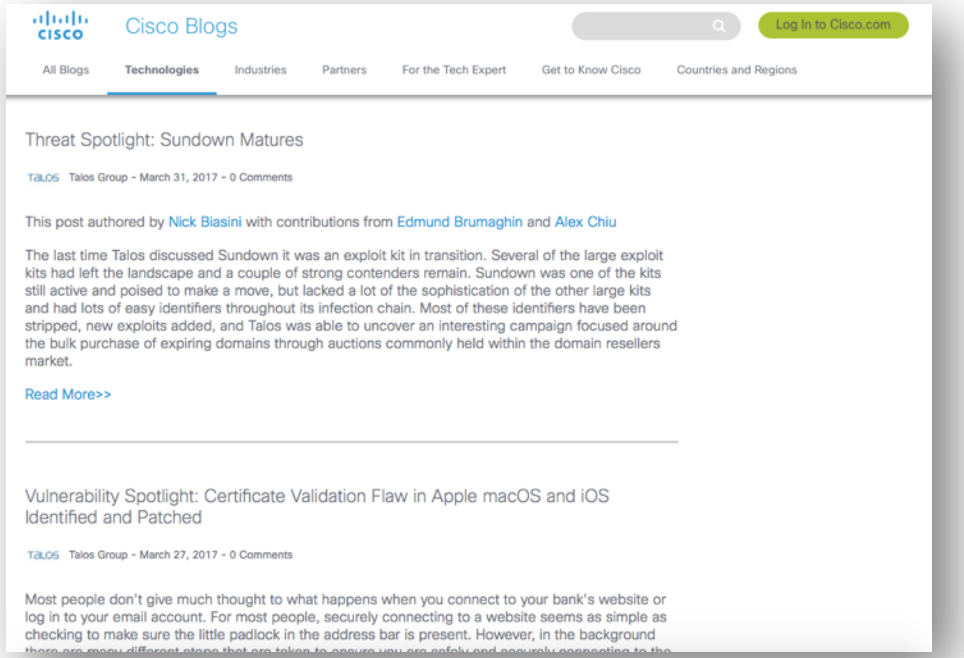
сообщений email в день



Мозг архитектуры безопасности Cisco

Где увидеть исследования Cisco Talos?

http://www.talosintelligence.com



http://blogs.cisco.com/talos

«Продукты» Cisco Talos

Разведка

ПК

Сеть

Облака

Email

Web

Open Source

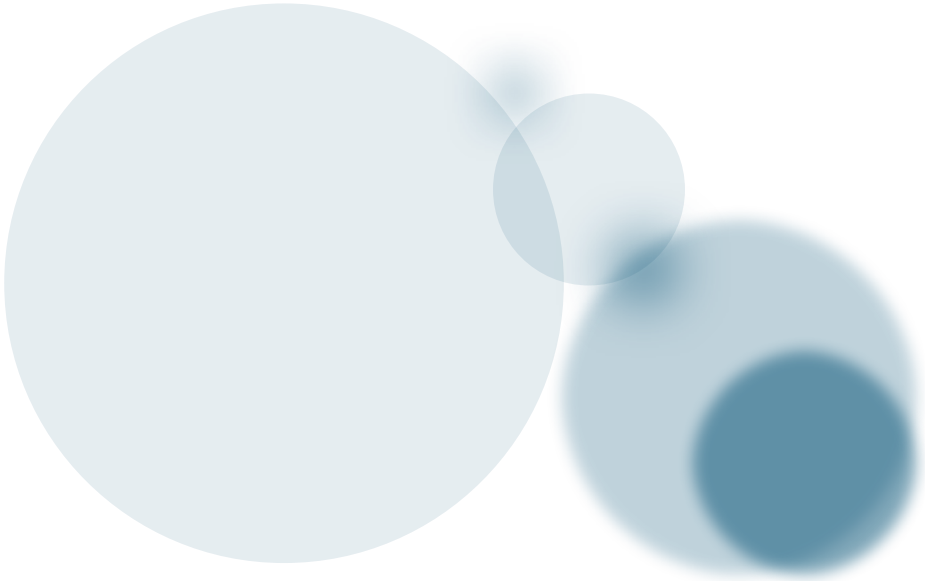
Услуги

ПРОДУКТЫ							
ThreatGrid	AMP ClamAV	FirePower/ASA ISR Meraki	CWS CES OpenDNS	ESA | ClamAV SpamCop SenderBase	WSA CWS	Snort Rules ClamAV Sigs ClamAV	ATA IR
СЕРВИСЫ ОБНАРУЖЕНИЯ							
Cloud & End Point IOCs	Cloud & End Point IOCs	Policy & Control	URL, Domain, IP Reputation	Email Reputation	URL, Domain, IP Reputation	Vulnerability Protection	Cloud & End Point IOCs
Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection
URL, Domain, IP Reputation	IP Reputation	URL, Domain, IP Reputation	AVC	URL, Domain, IP Reputation	AVC	Policy & Control	URL, Domain, IP Reputation
Network Protection		Vulnerability Protection		Phishing Protection			Vulnerability Protection
				Spoof & Spam Detection			Custom Protection

Решения Cisco: полнота охвата

Вопросы, на которые помогут ответить решения Cisco

- Что присутствует в инфраструктуре, в каком состоянии находятся эти платформы (и при необходимости ограничить доступ ненадлежащих устройств)
- Как обеспечить действительно гибкую контекстно-зависимую политику безопасности в рамках всей ИТ-инфраструктуры
- Кто и как _реально_ взаимодействует по моей сетевой инфраструктуре (работают ли политики)
- Комплекс вопросов и проблем, связанных с защитой периметра
- Что делать, если мы 8 часов назад пропустили в сеть файл, который, как оказалось, был вредоносным?
- Как моя инфраструктура выглядит для всего мира?
- Какие инциденты произошли в моей инфраструктуре?



Внутренняя инфраструктура

Сегментируйте сеть и контролируйте доступ

Сеть как защитная стена

Сегментация сети

для локализации атак

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

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

Контроль доступа

для выполнения политик

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

Физические и виртуальные разрешения и запреты (Access Control Lists)

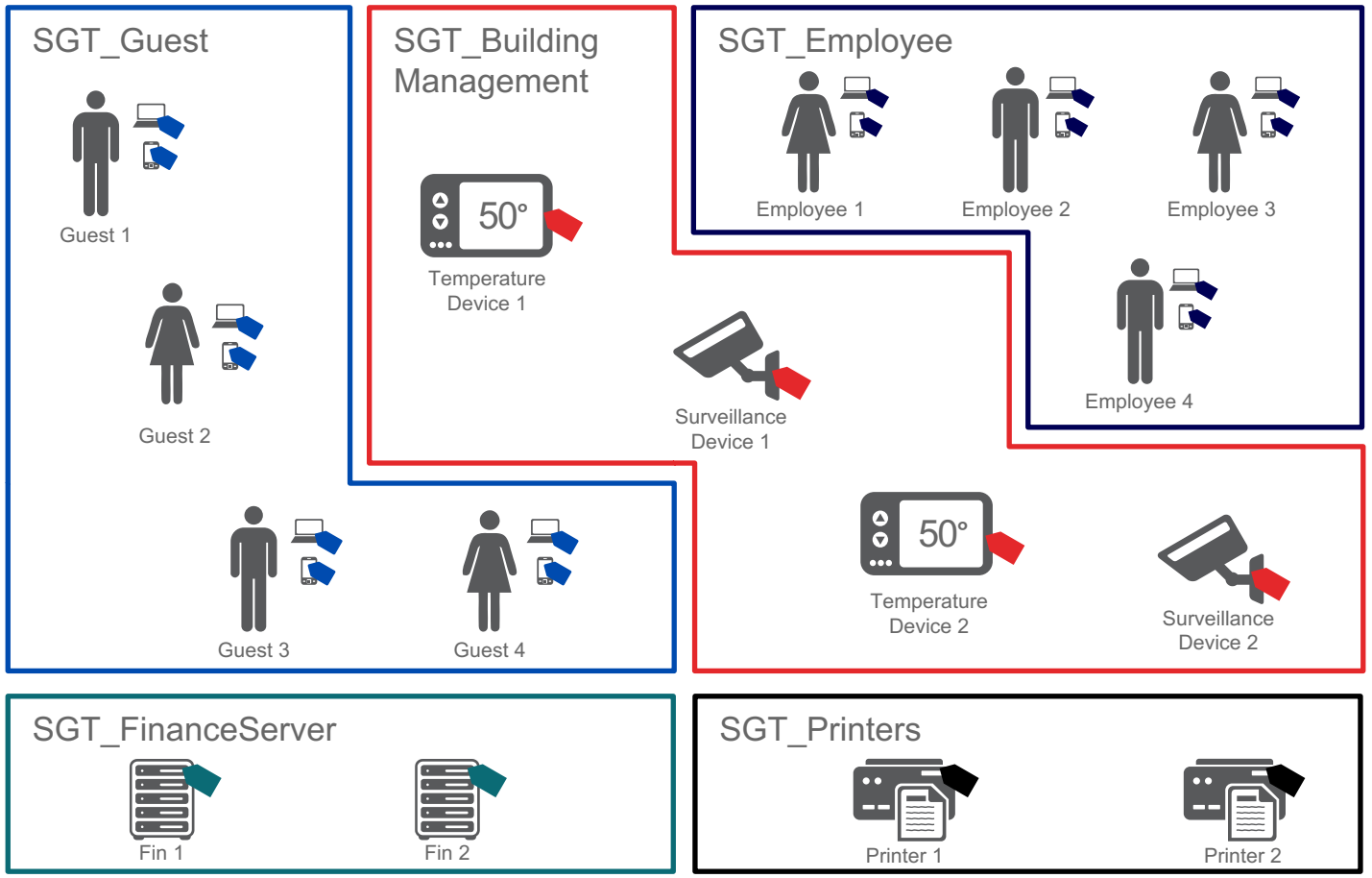
Единая политика для проводного/беспроводного/удаленного доступа (ISE, Unified Access Switches)

Платформа Cisco Identity Services Engine (ISE)

ISE – это централизованное решение, которое позволяет автоматизировать управление доступом к сетевым ресурсам с учетом контекста, «поделиться контекстом» с другими решениями и автоматизировать защиту

ISE обеспечивает **сегментацию** сети

- Для любых пользователей и устройств
- В качестве инструмента могут быть **любые сетевые устройства** (файерволы, коммутаторы, маршрутизаторы, WiFI…)



Cisco Platform Exchange Grid (pxGrid)

Повышение эффективности решений партнеров через обмен контекстом

Что более полезно с точки зрения безопасности?

“Адрес скомпрометированного устройства 192.168.100.123”

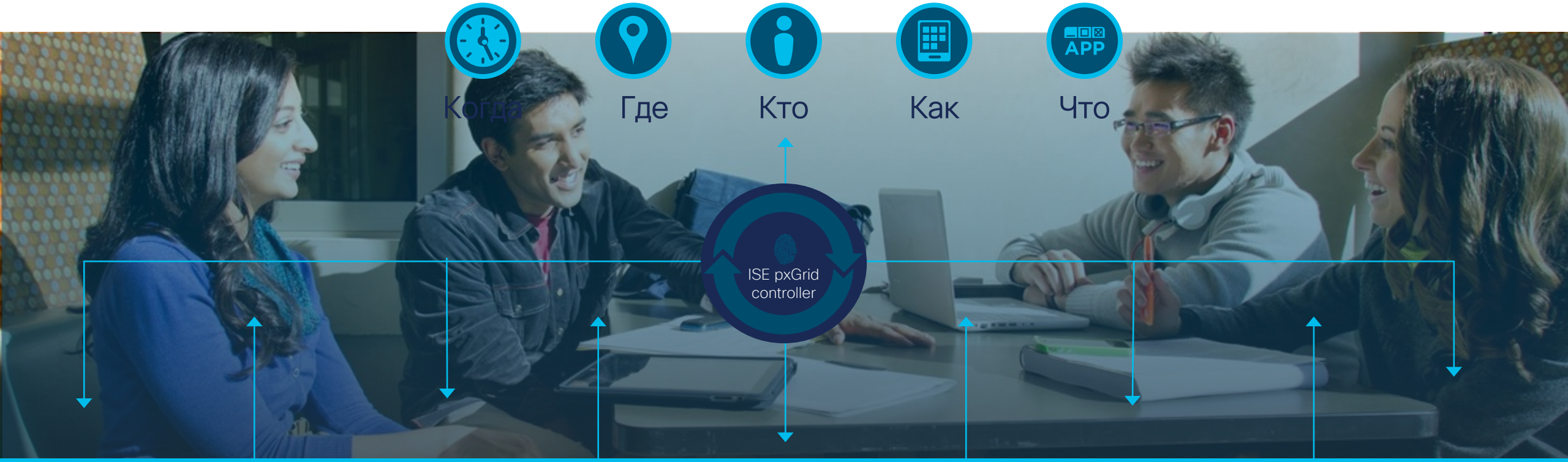
– ИЛИ –

“Скомпрометировано устройство iPad Васи в строении 1”

Cisco ISE собирает контекстуальные “big data” из множества источников в сети. С помощью Cisco pxGrid эта информация «делится» с решениями партнеров.

С контекстуальными данными ISE, решения партнеров могут более аккуратно и быстро идентифицировать, нейтрализовывать и реагировать на сетевые угрозы.

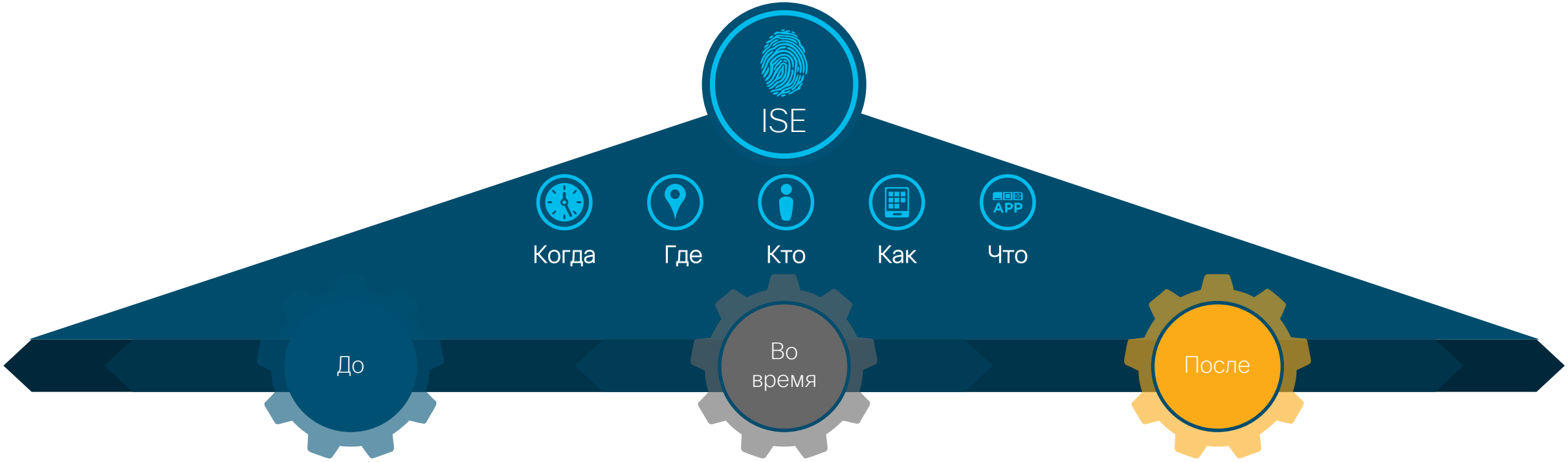
Легко интегрируется с партнерскими решениями



Lancope Network Performance + Security Monitoring™ | splunk> | EMULEX | Ping Identity | BAYSHORE INDUSTRIAL-STRENGTH CYBERSECURITY | tenable network security | Infoblox | cisco | Meraki | Check Point SOFTWARE TECHNOLOGIES LTD.

SIEM | EMM/MDM | Firewall | Vulnerability Assessment | Threat Defense | IoT | IAM/SSO | PCAP | Web Security | CASB | Performance Management

ISE это краеугольный камень ваших Cisco решений

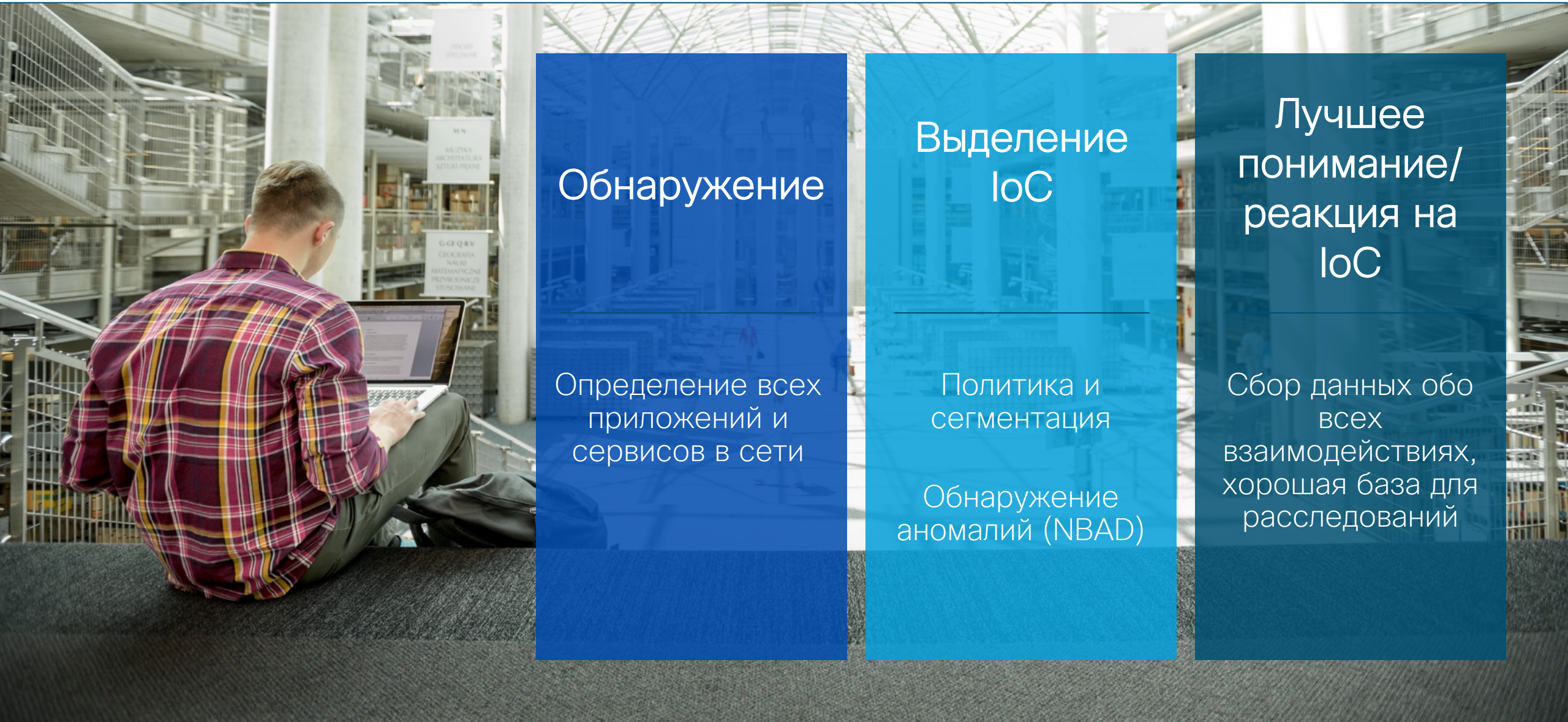


Система StealthWatch (сеть как сенсор)

Мониторинг на всех уровнях в реальном времени

- Аналитика с использованием данных, собираемых по всей сети
- Обнаружение ресурсов
- Профилирование сети
- Мониторинг выполнения политики безопасности
- Обнаружение аномалий
- Ускорение обработки инцидентов

Анализ NetFlow с помощью StealthWatch



Обнаружение

Определение всех приложений и сервисов в сети

Выделение IoC

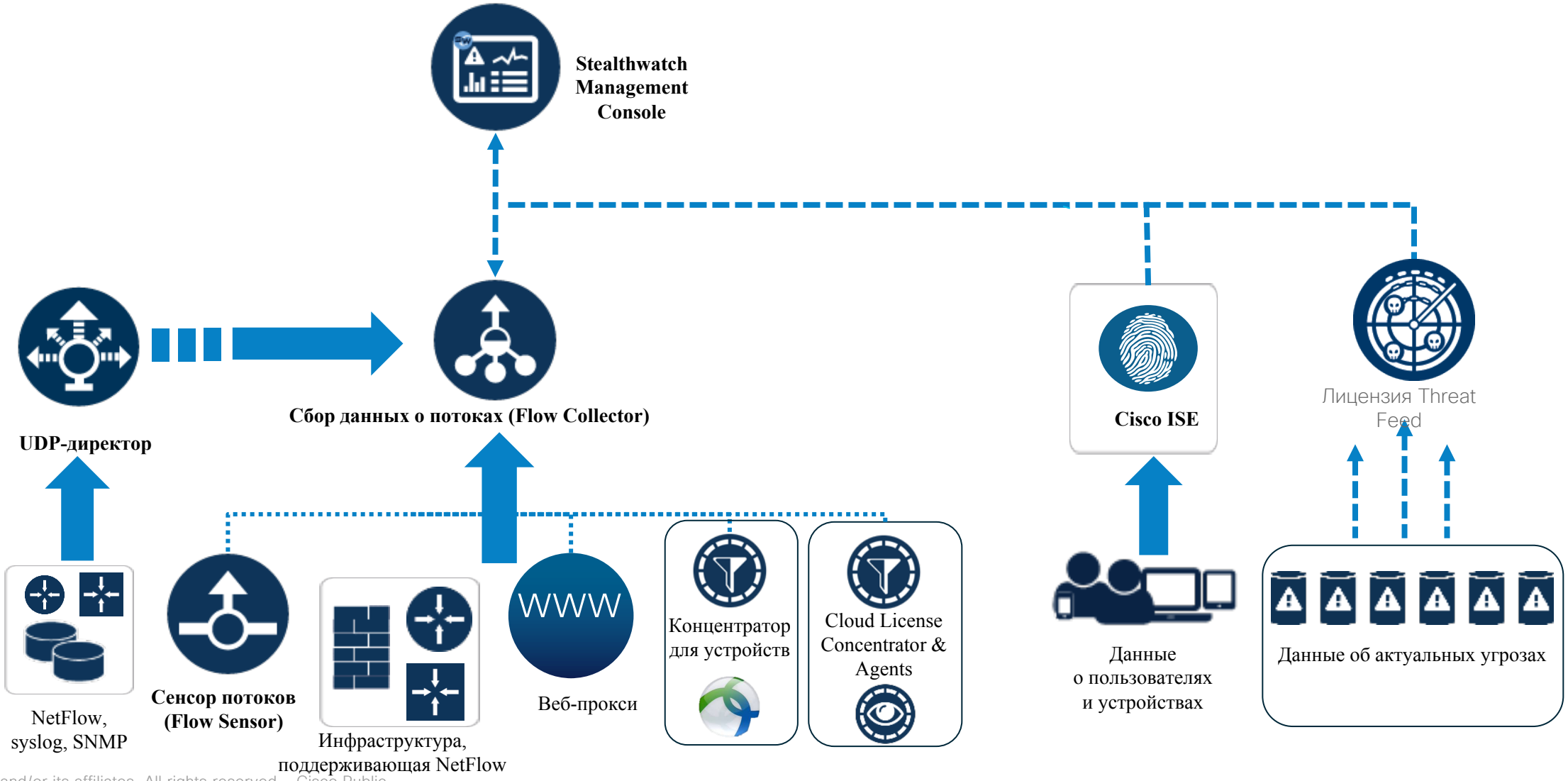
Политика и сегментация

Обнаружение аномалий (NBAD)

Лучшее понимание/ реакция на IoC

Сбор данных обо всех взаимодействиях, хорошая база для расследований

Компоненты системы Stealthwatch



AnyConnect – больше чем просто VPN

IPsec VPN

SSL / DTLS VPN

Оценка состояния

(HostScan/ISE)

Cloud Web Security/ OpenDNS

L2 саппликант (Win Only)

AMP Enabler

Модуль сетевой видимости

Базовый VPN

Расширенный VPN

Другие сервисы

Центральные устройства

Коммутаторы и контроллеры WLC

ISE/ACS

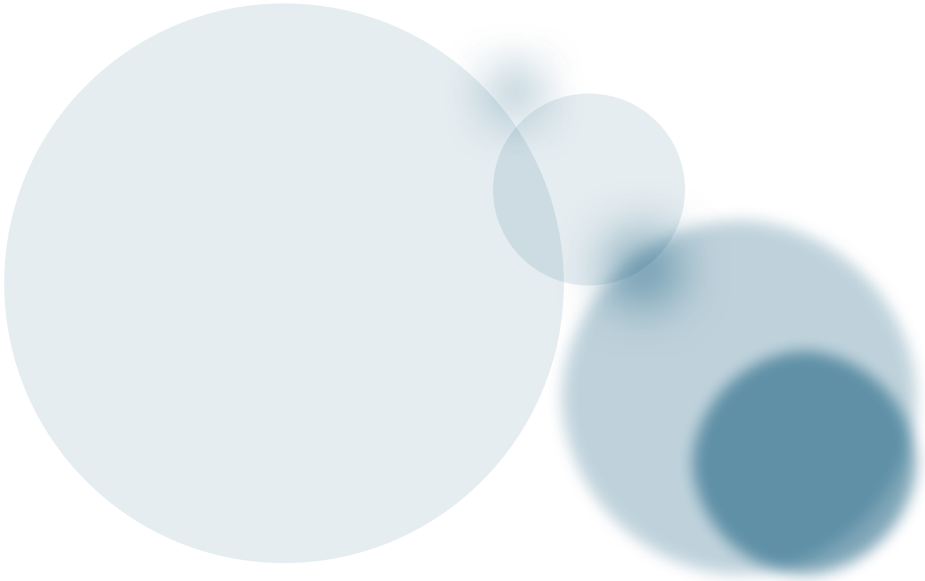
ASA

WSA

Cloud Web Security + AMP

ASR/ CSR

ISR

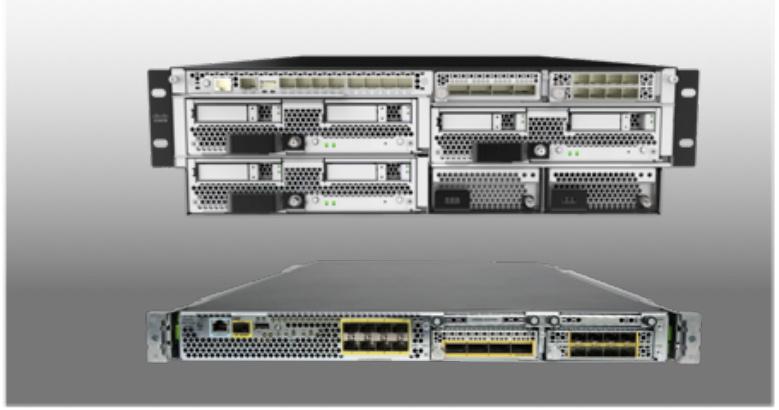


Периметр

Периметр: набор признанных решений

- Web Security Appliance – апробированная платформа очистки веб-трафика
- Email Security Appliance – признанный в отрасли анти-спам
  Помните про возможность перезаписи URL и отслеживания кликов!!!
  Помним про вычистку ящика в Office365 по данным AMP в ESA 10.0
- Cloud Web Security (exScanSafe)/Open DNS
- Cloud Email Security/….
- Современные межсетевые экраны/системы предотвращения вторжений
- Платформа Cisco AMP – не только периметр (включая ThreatGrid)

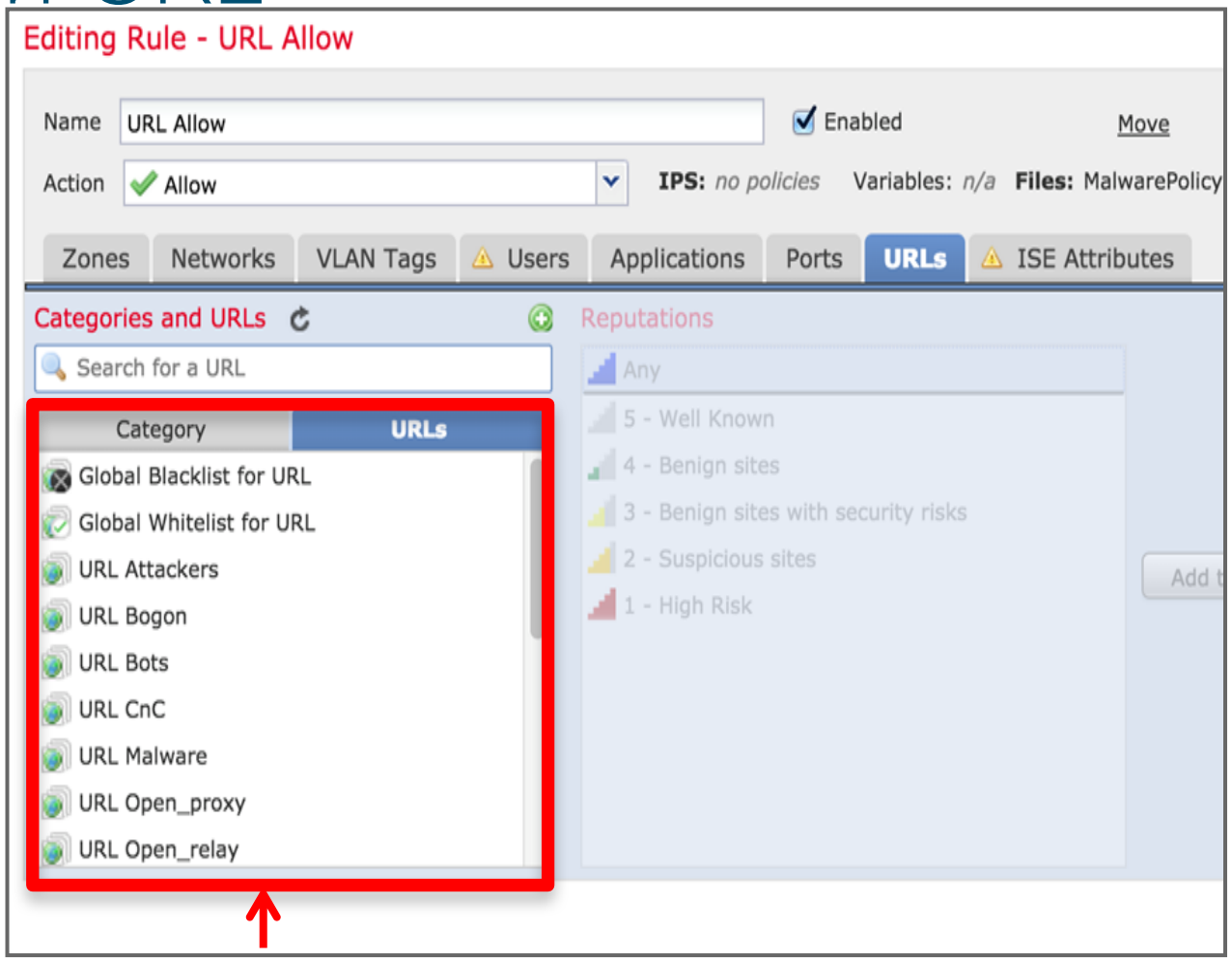
Платформы Cisco NGFW

Firepower Threat Defense для ASA 5500-X	Firepower серии 2100	Firepower серии 4100 и Firepower 9300
		
250 Мбит/с -> 1,75 Гбит/с (сервисы NGFW + IPS)	2 Гбит/с -> 8 Гбит/с (сервисы NGFW + IPS)	41xx = 10 Гбит/с -> 24 Гбит/с 93xx = 24 Гбит/с -> 53 Гбит/с

Все платформы NGFW управляются Firepower Management Center

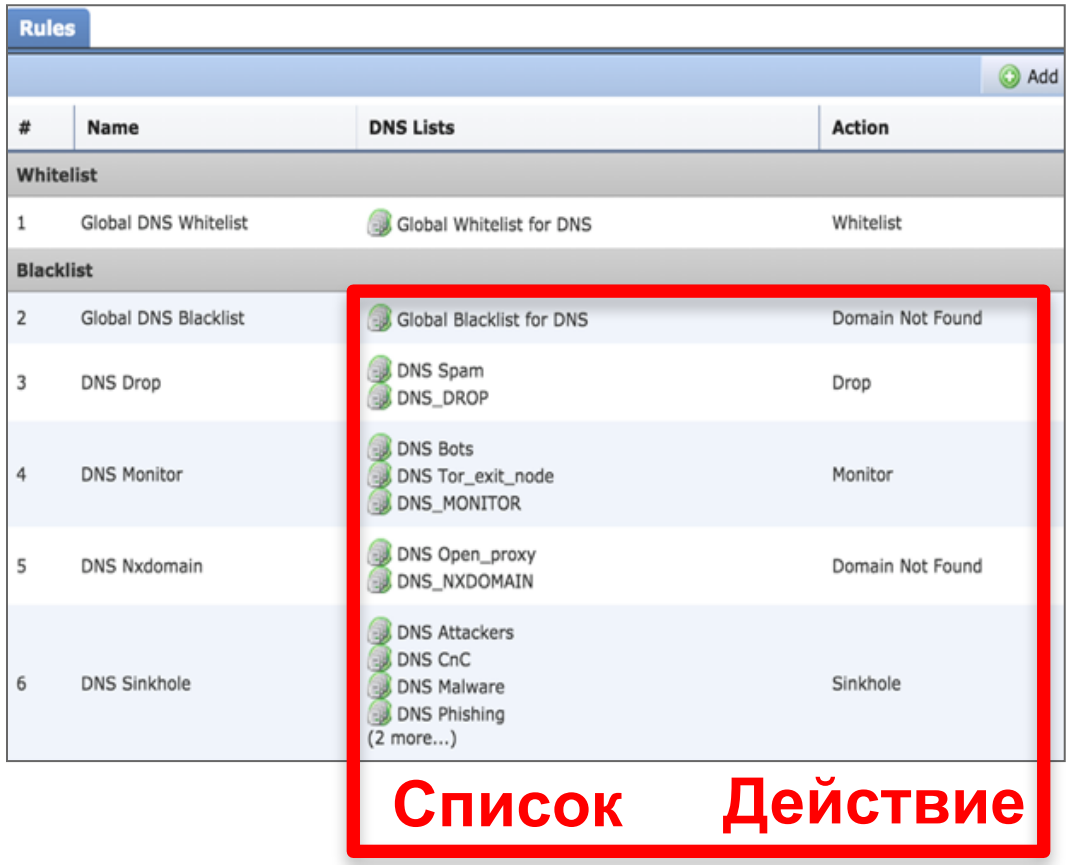
Аналитика безопасности URL

- Дополнение механизмов безопасности на базе IP
- Динамический фид TALOS, сторонние фиды и списки
- Различные категории: вредоносное ПО, фишинг, CnC,…
- Разные действия: Allow, Monitor, Block, Interactive Block,…
- Настройка политик с помощью правил доступа или черного списка
- Теги IoC для URL CnC и вредоносного ПО
- Новый виджет для URL SI
- Помещение URL-адреса в черный/белый список с помощью одного щелчка



Анализ DNS-трафика

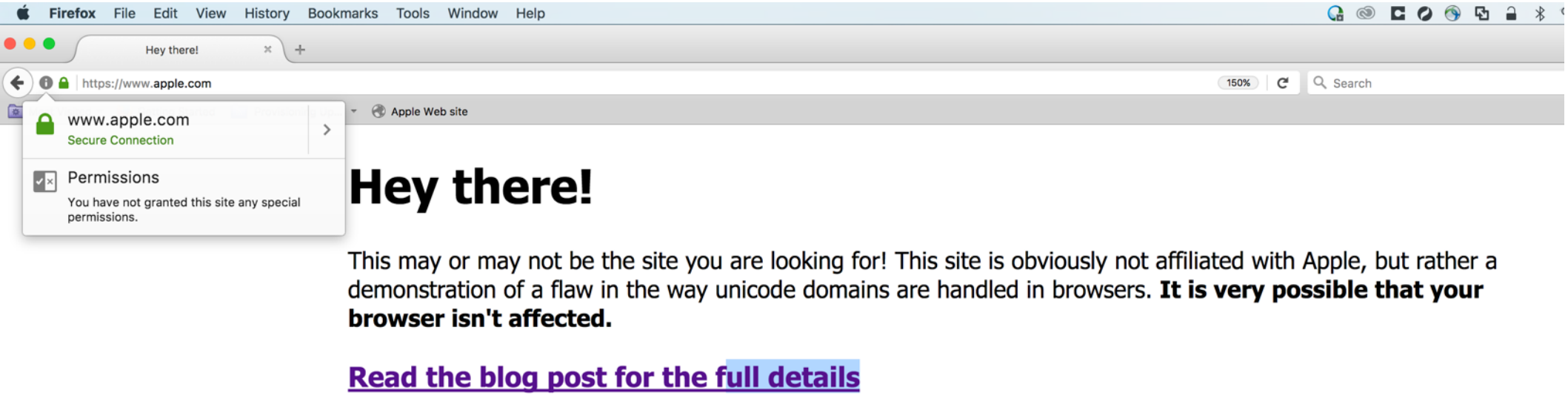
- Поддержка аналитики безопасности для доменов
- Решение вопросов, связанных с доменами fast-flux
- Предоставляемые Cisco и определяемые пользователем (либо выбранные внешние) фиды DNS: CnC, спам, вредоносное ПО, фишинг
- Разные действия: Block, Domain Not Found, Sinkhole, Monitor
- IoC дополнены данными, основанными на анализе DNS-трафика
- Новый виджет для SI DNS



А что вы привязались к DNS?

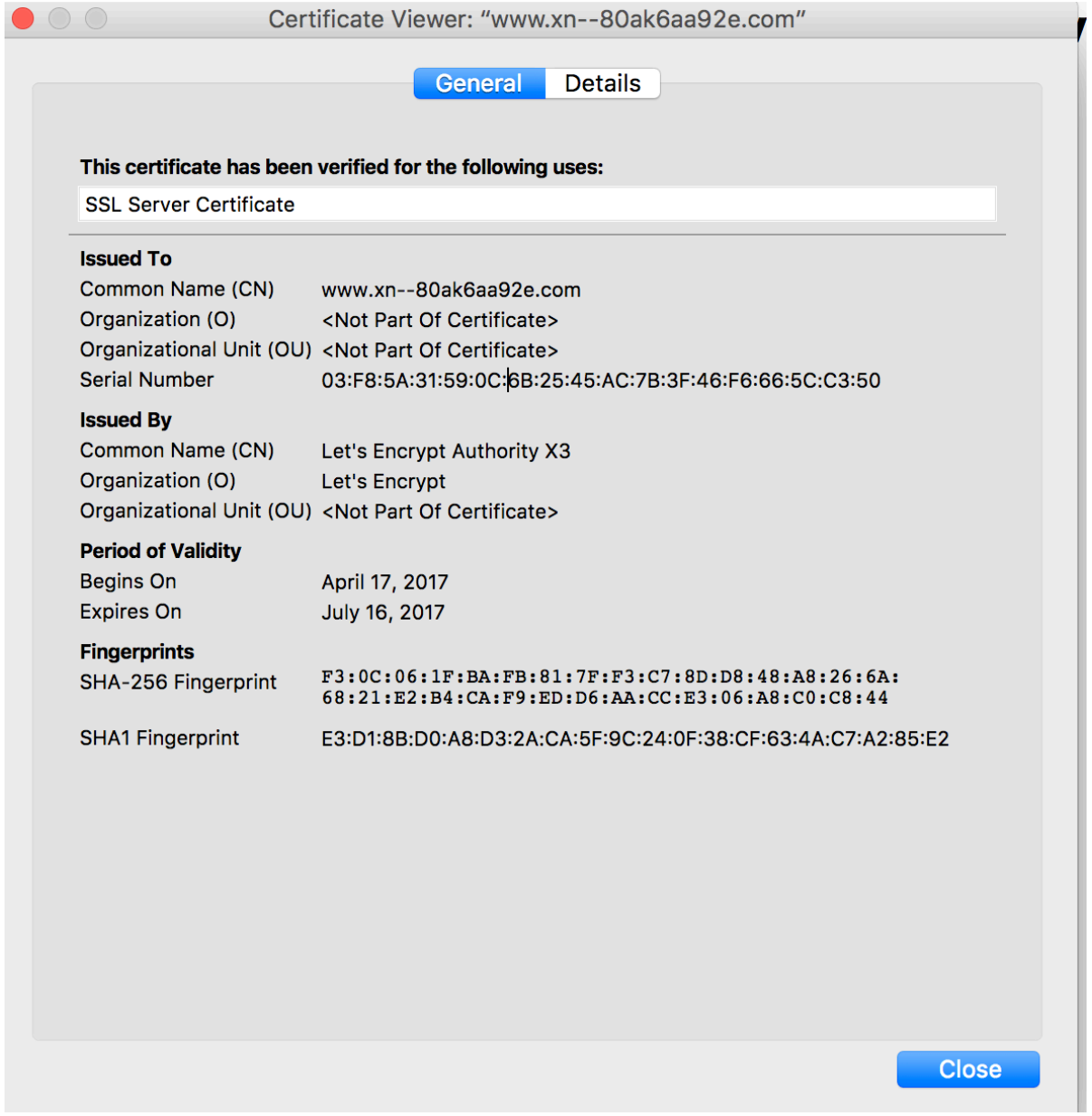
- Способ удобного взаимодействия с центрами управления
- Прекрасный вариант масштабирования инфраструктуры распространения вредоносного ПО
- Прекрасный вариант маскировки инфраструктуры распространения вредоносного ПО
- Недурной апробированный туннельный транспорт
- Ещё есть домены с опечатками …
- Ещё есть возможность автоматической генерации доменов
- **И это всё абсолютно справедливо**
- Но мы же помним «с системами работают начинающие, профессионалы работают с людьми».
- Давайте, посмотрим на маленький нюанс реализации… вы хотели посетить apple.com или apple.com?

Серьёзно, как это работает?



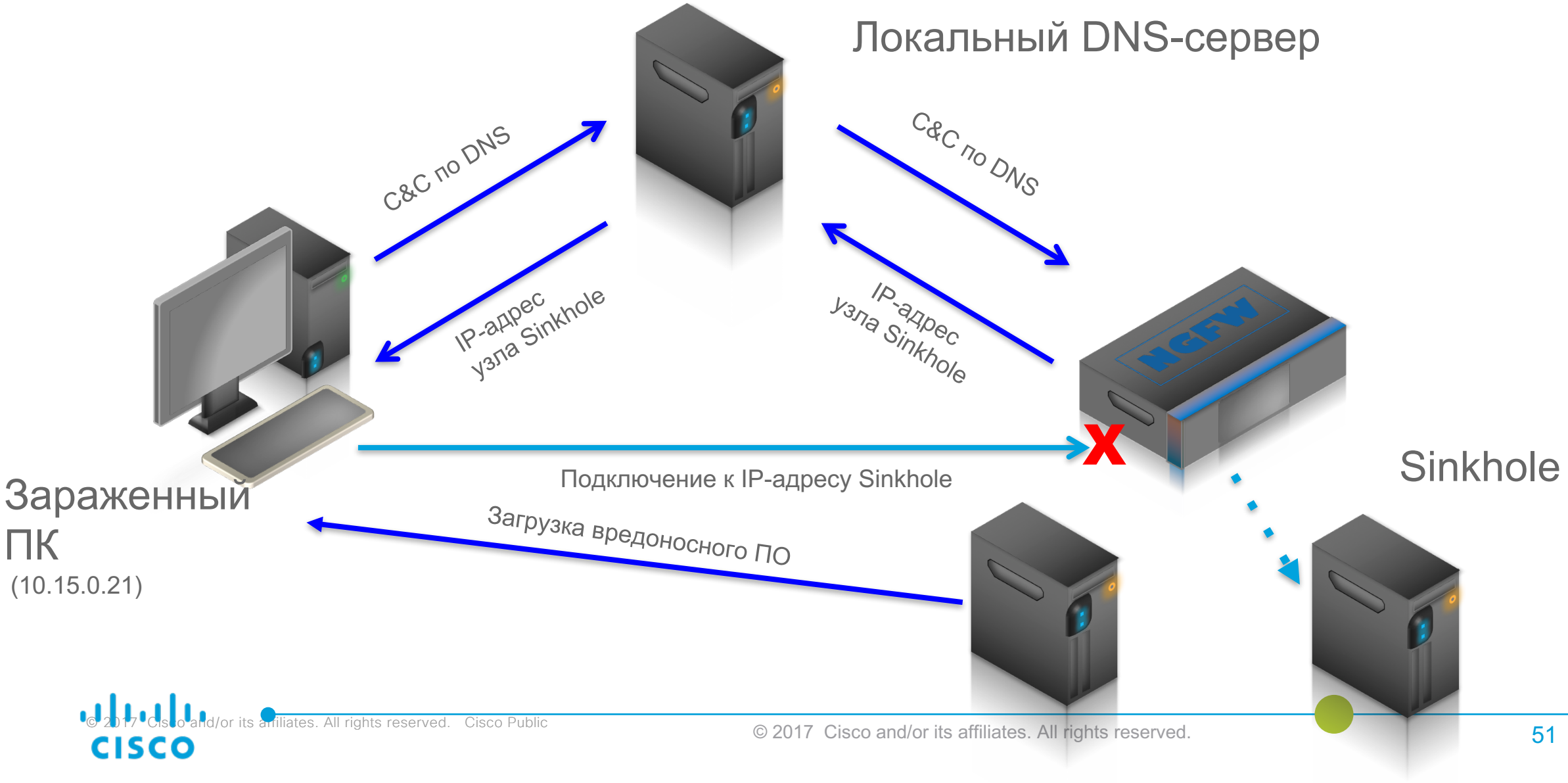
© 2017 Cisco and/or its affiliates. All rights reserved.

Всё для людей...

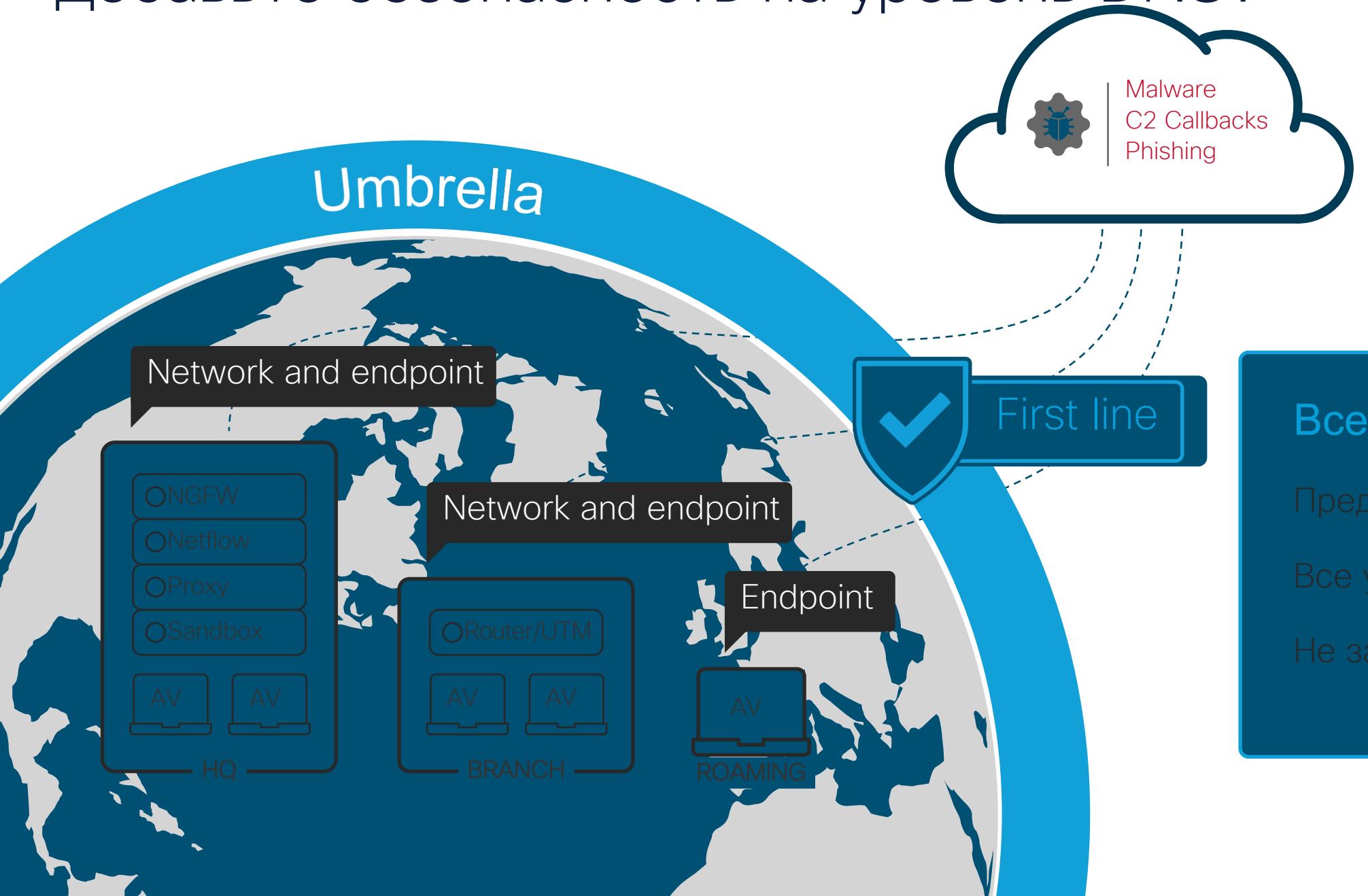


Действие DNS Sinkhole

Политика NGFW
DNS SI: серверы C&C
Действие: DNS Sinkhole
Создание событий SI и IoC



Добавьте безопасность на уровень DNS?



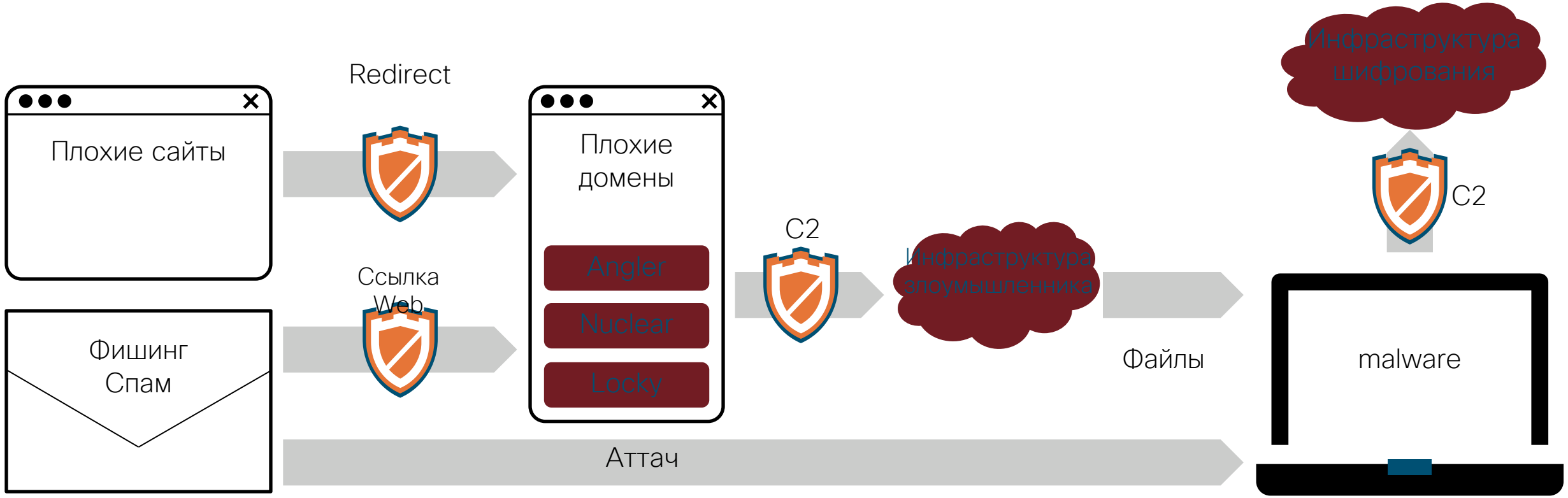
Все начинается с DNS

Предваряет IP подключение

Все устройства

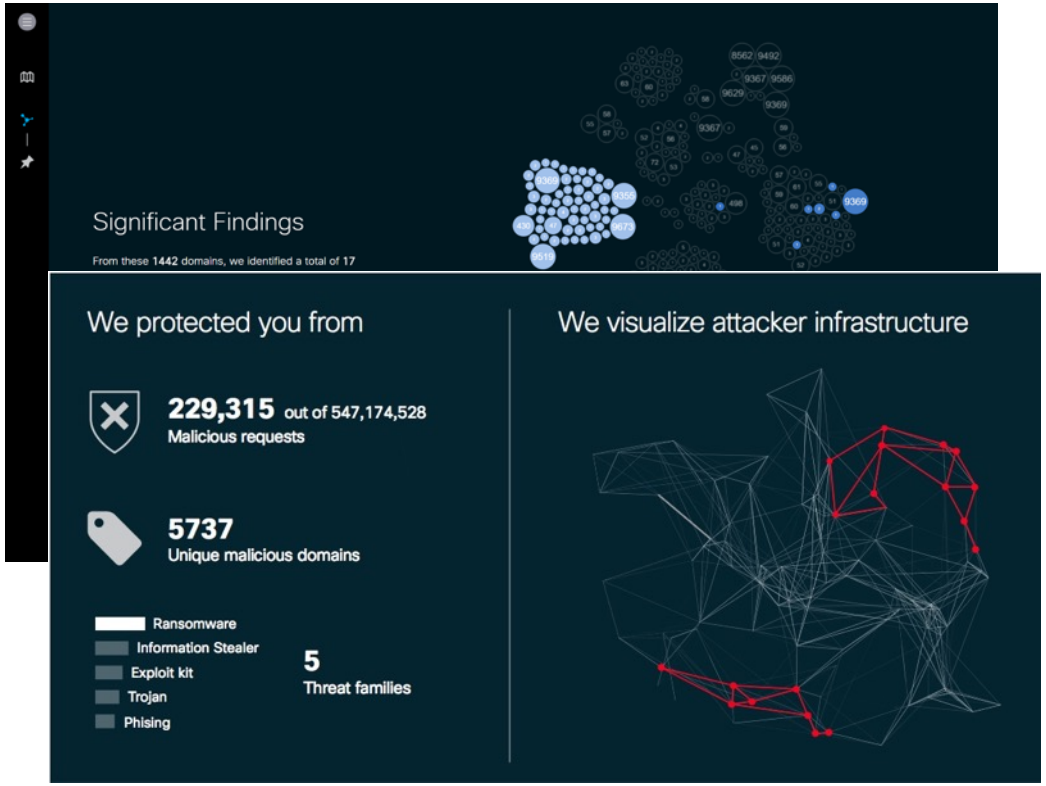
Не зависит от порта

OpenDNS/Umbrella предотвращает заражение и распространение вредоносного кода



Заблокировано Cisco Umbrella. (DNS безопасность)

Самая простая система безопасности в мире!



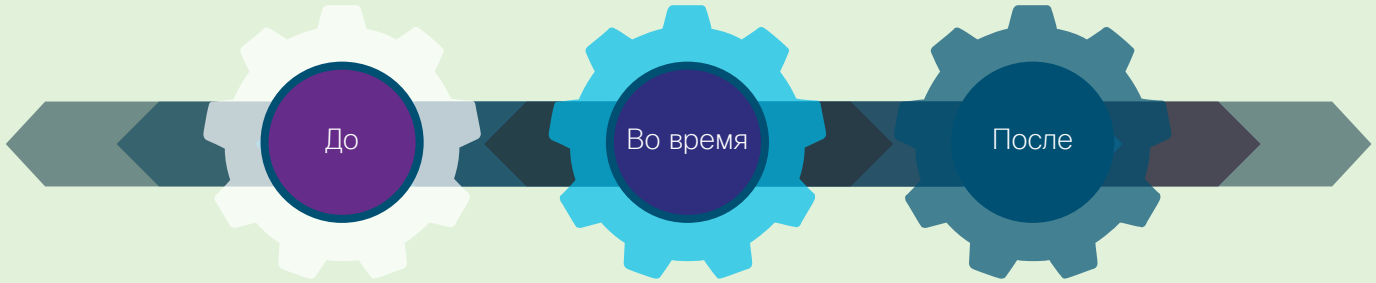
1. Добавьте в ваши DNS сервера Forwarders:
   - 208.67.222.222
   - 208.67.220.220
2. Зарегистрируйтесь
3. Добавьте адрес вашей сети для безопасности и мониторинга
4. Попросите сделать отчет
5. **Можете продолжать использовать сервис и после окончания тестирования/срока действия лицензии!**

- Есть бесплатная опция для домашнего использования

Платформа Cisco AMP

Cisco AMP предоставляет три выгоды

3 Защищает на всех этапах атаки



2 Защита на нескольких рубежах

Контент

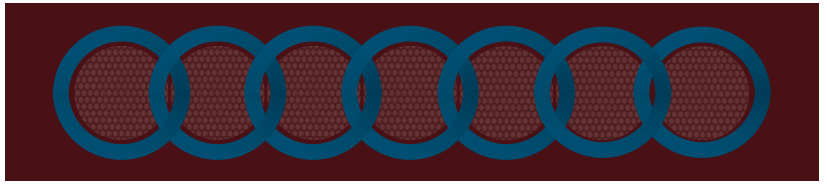
Сеть

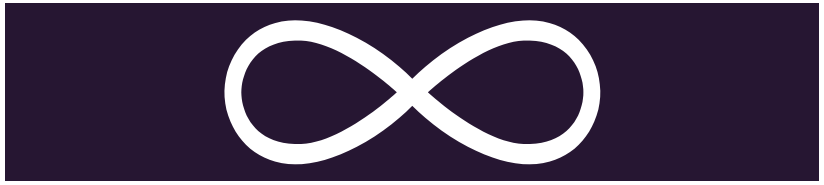
Хосты

1 Несколько методов обнаружения

Точечное обнаружение

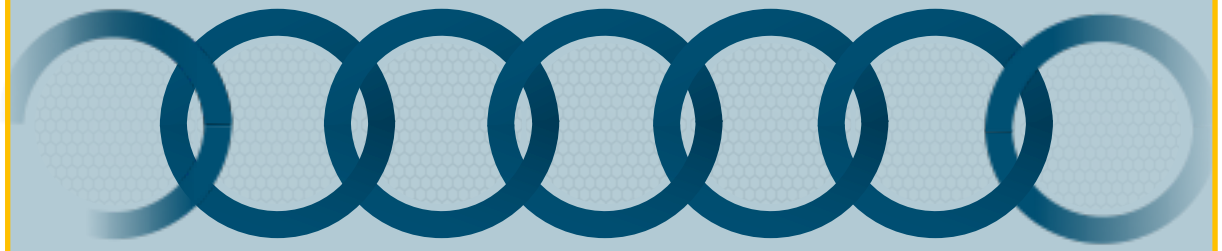
Cisco Talos





В Cisco AMP реализованы план А и план Б

Точечное обнаружение



Репутация и поведенческий анализ

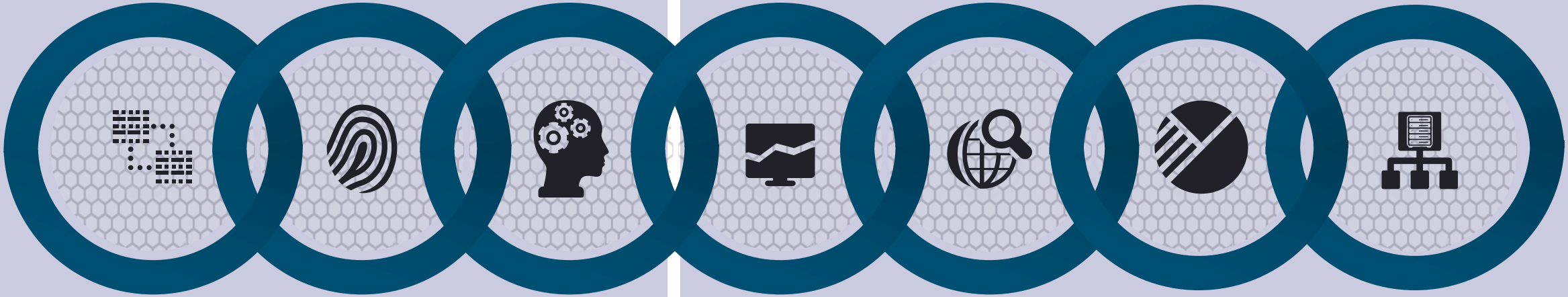
Ретроспективная безопасность

Постоянная защита

Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

Фильтрация по репутации

Поведенческое обнаружение



Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Признаки компрометации

Динамический анализ

Расширенная аналитика

Сопоставление потоков устройств

Cisco AMP – ретроспективная безопасность

Детальный анализ вредоносного ПО в AMP Threat Grid

Behavioral Indicators

Threat Score: 90

- Process Modified an Executable File — Severity: 95 Confidence: 95
- Process Created a File in the Windows Startup Folder — Severity: 80 Confidence: 50

A new file was added to the Windows StartUp folder to ensure that this file runs on system startup.
Please review the 'Disk Artifacts' section in order to view additional details about this file.

Categories persistence
Tags startup, file, folder, process, autorun

Report Error

Process ID	Process Name	Path
1100 (15e65a21af32dd3b5fe65da4807be21e.exe)	15e65a21af32dd3b5fe65da4807be21e.exe	\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe

- Process Modified File in a User Directory — Severity: 70 Confidence: 80
- Process Disabled Internet Explorer Proxy — Severity: 70 Confidence: 70
- Process Created an Executable in a User Directory — Severity: 60 Confidence: 95
- Potential Code Injection Detected — Severity: 50 Confidence: 50
- Dynamic DNS Domain Detected — Severity: 50 Confidence: 60
- PE Has Sections Marked Executable and Writable — Severity: 40 Confidence: 60
- Possible Fast Flux Domain Detected [Beta] — Severity: 35 Confidence: 20
- Outbound HTTP POST Communications — Severity: 25 Confidence: 25
- PE COFF Header Timestamp is Set to Date Prior to 1999 — Severity: 5 Confidence: 60
- PE Optional Header Linker Minor Version Abnormal — Severity: 5 Confidence: 60
- PE DOS Header Initial SP Value is Abnormal — Severity: 5 Confidence: 60
- PE COFF Header Timestamp is Not Set — Severity: 5 Confidence: 60

HTTP Traffic

- POST http://alexrpi.tk:80/solar/ — Server IP: 195.20.34.1 Server Port: 80 Resp. Content: text/html
- POST http://alexrpi.tk:80/solar/ — Server IP: 195.20.34.1 Server Port: 80 Resp. Content: text/html
- POST http://alexrpi.tk:80/solar/ — Server IP: 195.20.34.1 Server Port: 80 Resp. Content: text/html
- POST http://alexrpi.tk:80/solar/ — Server IP: 195.20.34.1 Server Port: 80 Resp. Content: text/html
- POST http://alexrpi.tk:80/solar/ — Server IP: 195.20.34.1 Server Port: 80 Resp. Content: text/html
  Method POST

Dest. Port
Transport ICMP
Timestamp +30.909s

IP Reverse Lookup igmp.mcast.net
IP ASN -

Processes

- Name: 15e65a21af32dd3b5fe65da4807be21e.exe
  PID: 1100 Children: 1 File Actions: 3 Registry Actions: 2 Analysis Reason:
- Name: lsass.exe
  PID: 1600 Children: 0 File Actions: 3 Registry Actions: 0 Analysis Reason:

Started At
Current Directory
Image Base Addr
Window Title
Shell Info
Desktop Info

DNS Traffic

- Query Type: A, Query Data: alexrpi.tk

TTL: - Timestamp: +101.195s

Query ID	28943
Timestamp	+101.195s
Type	A
Data	alexrpi.tk

Answers

Query ID	Timestamp
28943	+101.29s
28943	+101.29s

Nameserver Records

Data	Name
b	tk
c	tk
a.ns	tk

Registry Activity

- Created Keys

Created Key	PID	Access List	Option List
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\P3P\History	1148 (Explorer.EXE)	ENUMERATE_SUB_KEYS , CREATE_SUB_KEY	REG_OPTION_NON_VOLATILE

- Modified Keys
- Deleted Key Values

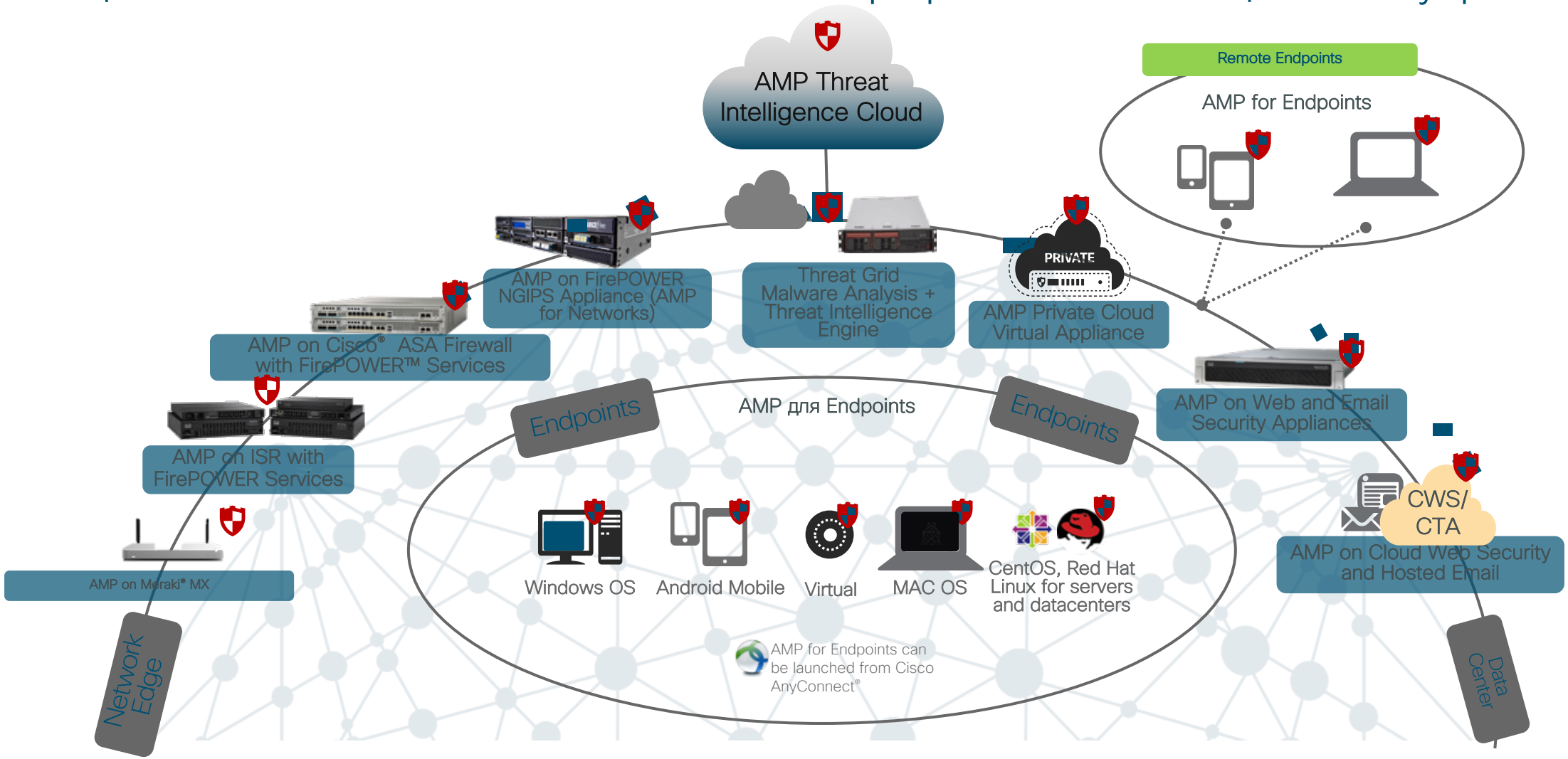
Filesystem Activity

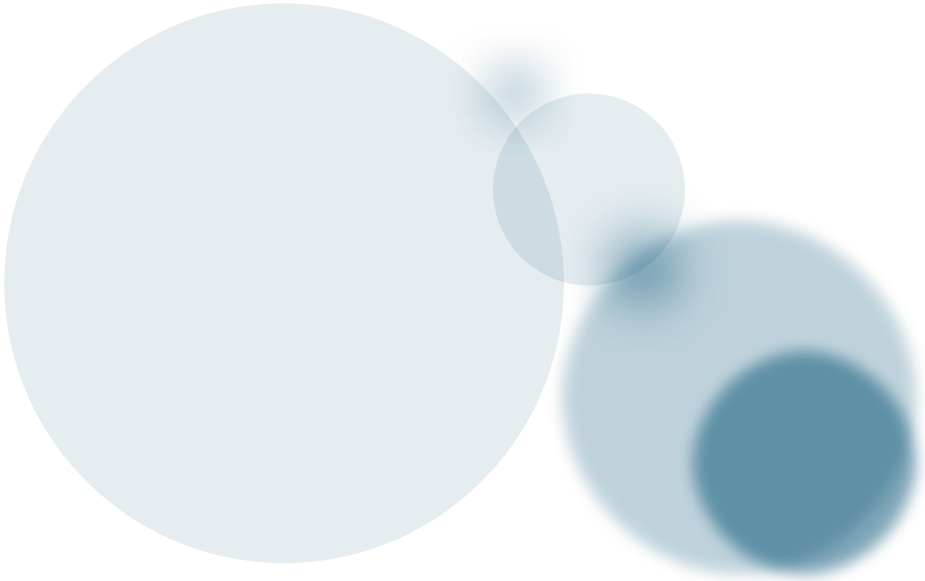
Files Created: 3 Files Read: 17 Files Modified: 5 Files Deleted: 0

Path	PID	Action
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\8HMRCBCR	1148 (Explorer.EXE)	Created

Архитектура «AMP везде»

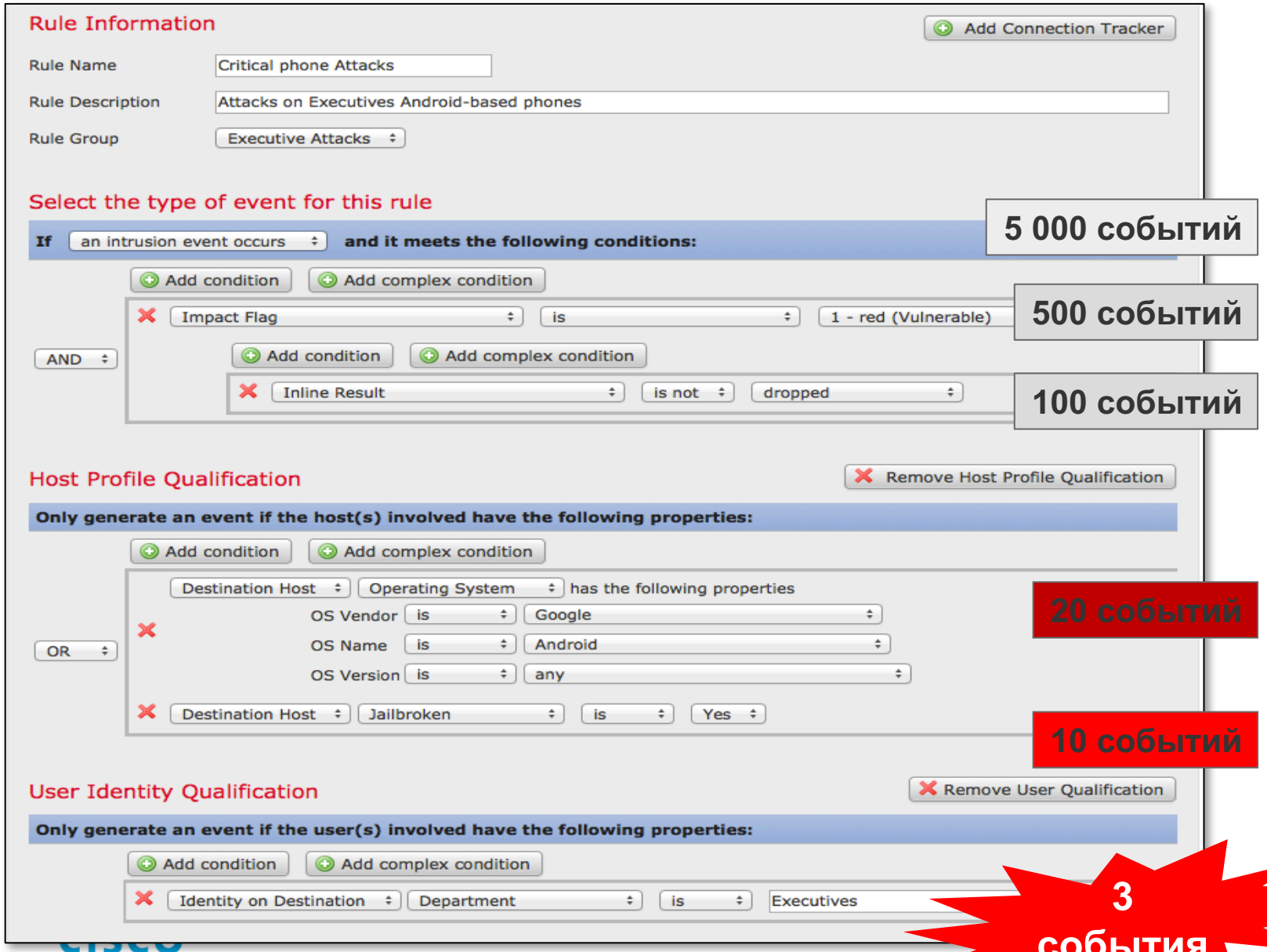
Защита AMP по всей сети как интегрированная защита от угроз.





АВТОМАТИЗАЦИЯ КРОМЕ pxGrid

Правила и политики корреляции в Firepower



5 000 событий

500 событий

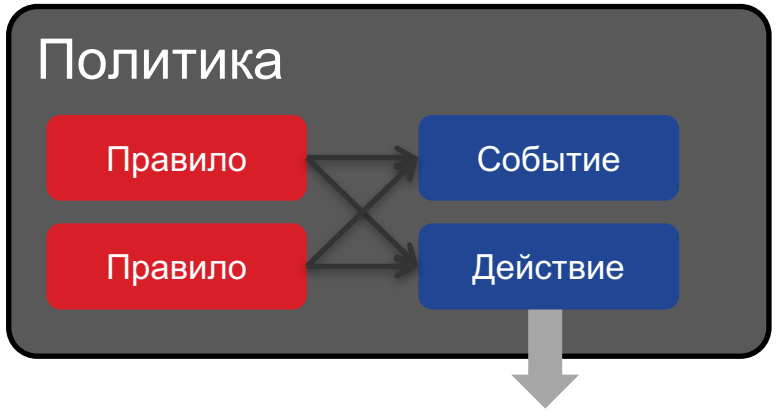
100 событий

20 событий

10 событий

3 события

Правила корреляции позволяют применять БУЛЕВУ алгебру к наборам данных в консоли Firepower. Правила можно связать с действиями: Email, Syslog, SNMP или нейтрализация.

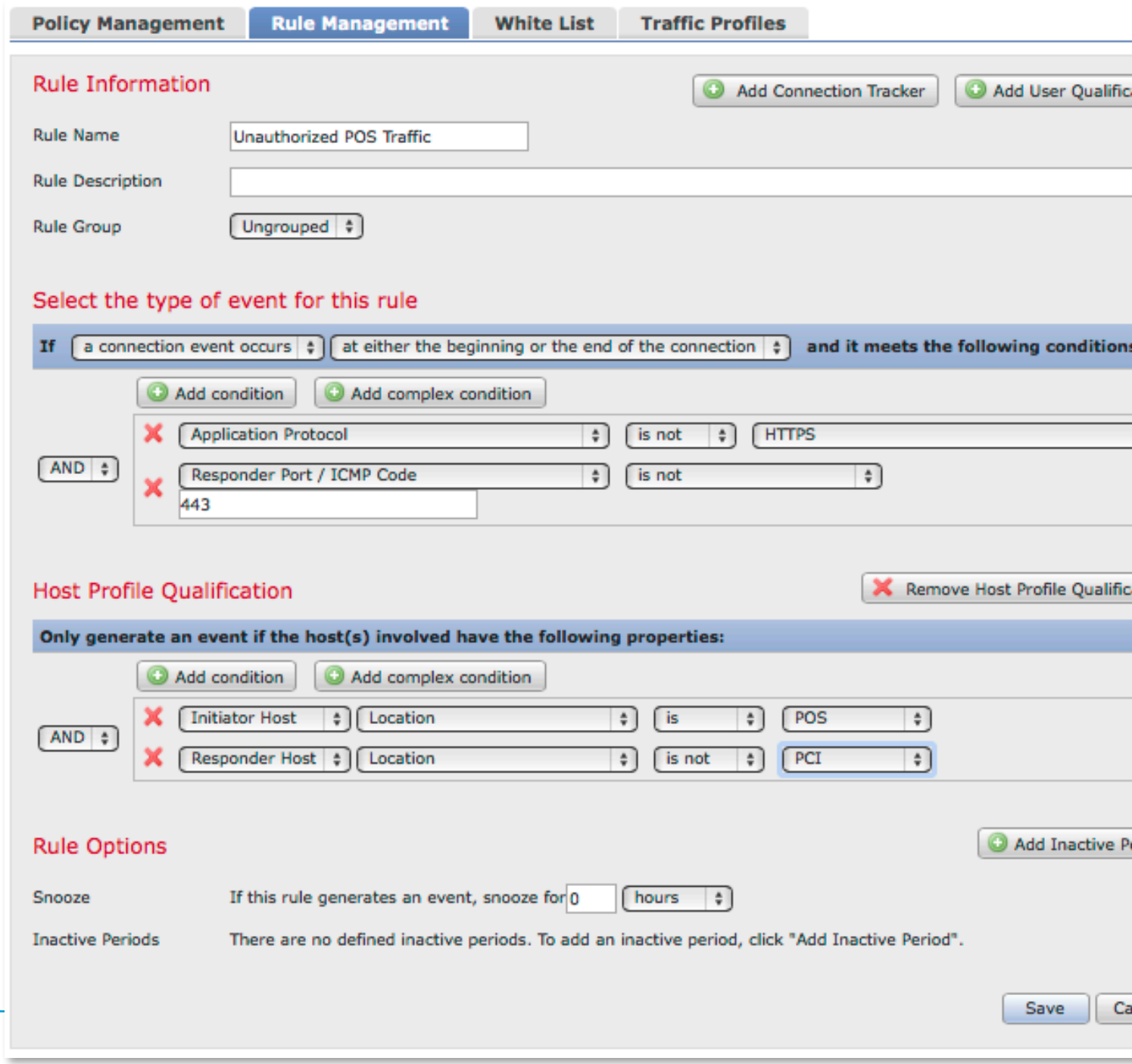


Email
Syslog
SNMP
Модуль нейтрализации

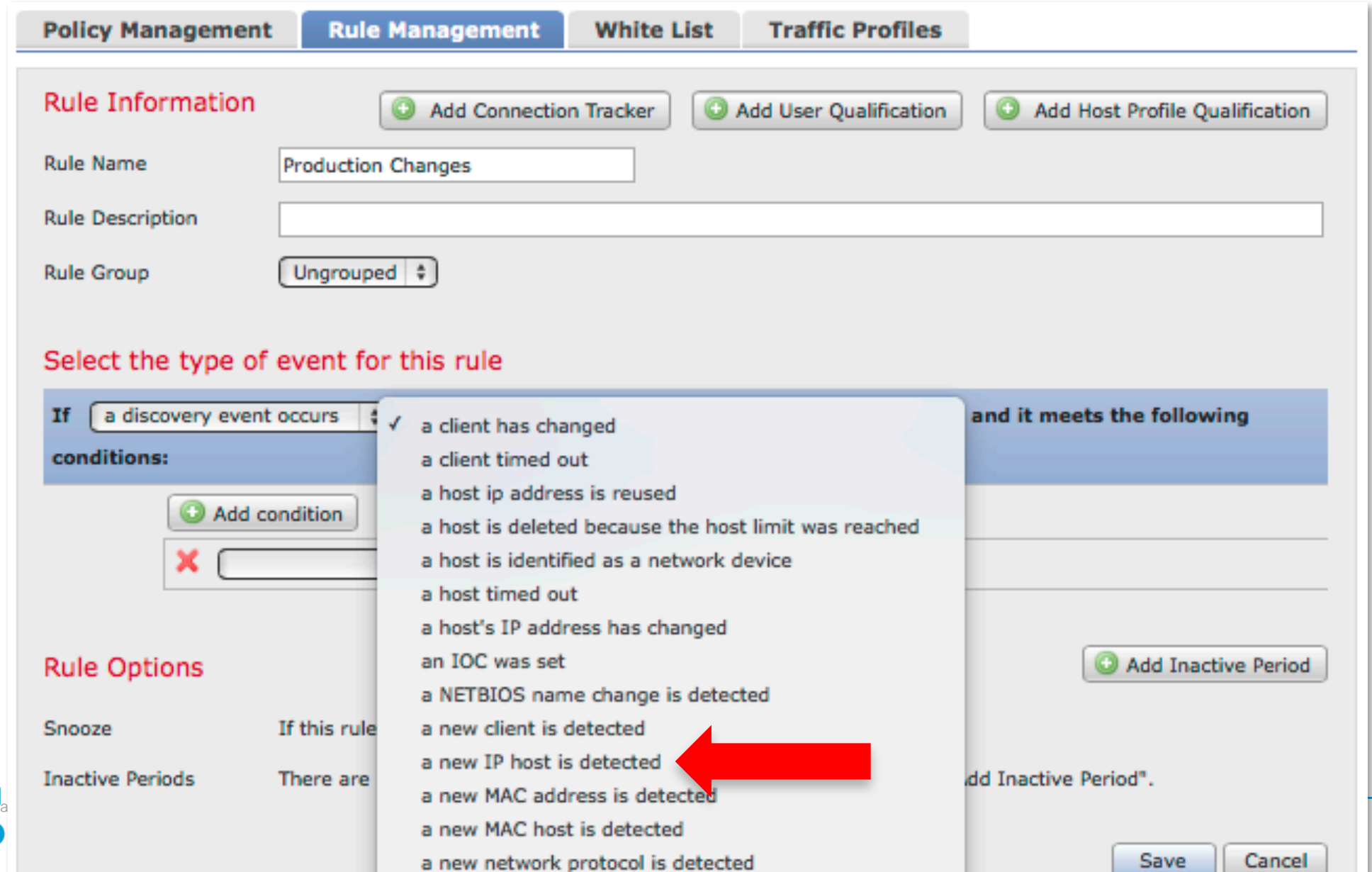
Пример правила

Мы хотим:

- Обеспечить только HTTPS-трафик по порту 443
- Трафик должен инициироваться хостом в заданном местоположении (атрибут хоста), и это POS
- HTTPS-трафик должен быть направлен в сеть PCI
- Иначе должно генерироваться событие.



Правила могут быть простыми



Правила должны формулироваться на основе логики

If “an Intrusion Event occurs”. . .

AND
- OR
  - Impact Flag is 3 - Yellow
  - Impact Flag is 4 - Blue
- OR
  - Source IP is in 192.168.0.0/16
  - Source IP is in 10.0.0.0/8
  - Source IP is in 172.16.0.0/12
- OR
  - Destination IP is not in 192.168.0.0/16
  - Destination IP is not in 10.0.0.0/8
  - Destination IP is not in 172.16.0.0/12

Скомпрометированный хост, вероятно, атакует внешние системы из вашей сети.

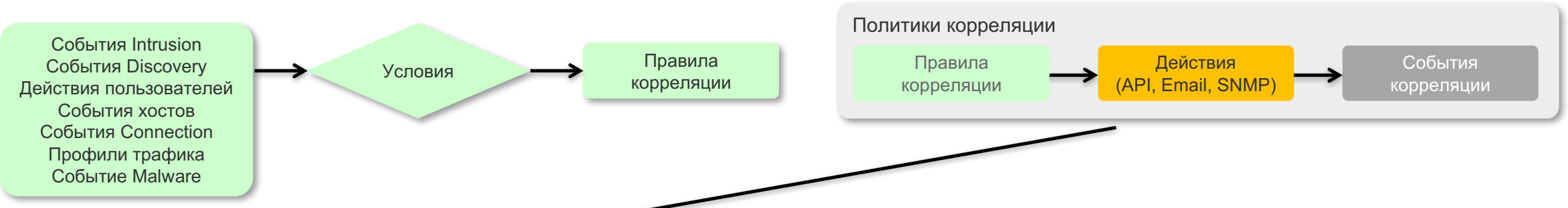
If “a Malware Event occurs”
“by retrospective network-based malware detection”

OR
- OR
  - Sending IP is in 192.168.0.0/16
  - Sending IP is in 10.0.0.0/8
  - Sending IP is in 172.16.0.0/12
- OR
  - Receiving IP is in 192.168.0.0/16
  - Receiving IP is in 10.0.0.0/8
  - Receiving IP is in 172.16.0.0/12

В вашей сети был файл, который недавно классифицирован как вредоносное ПО!

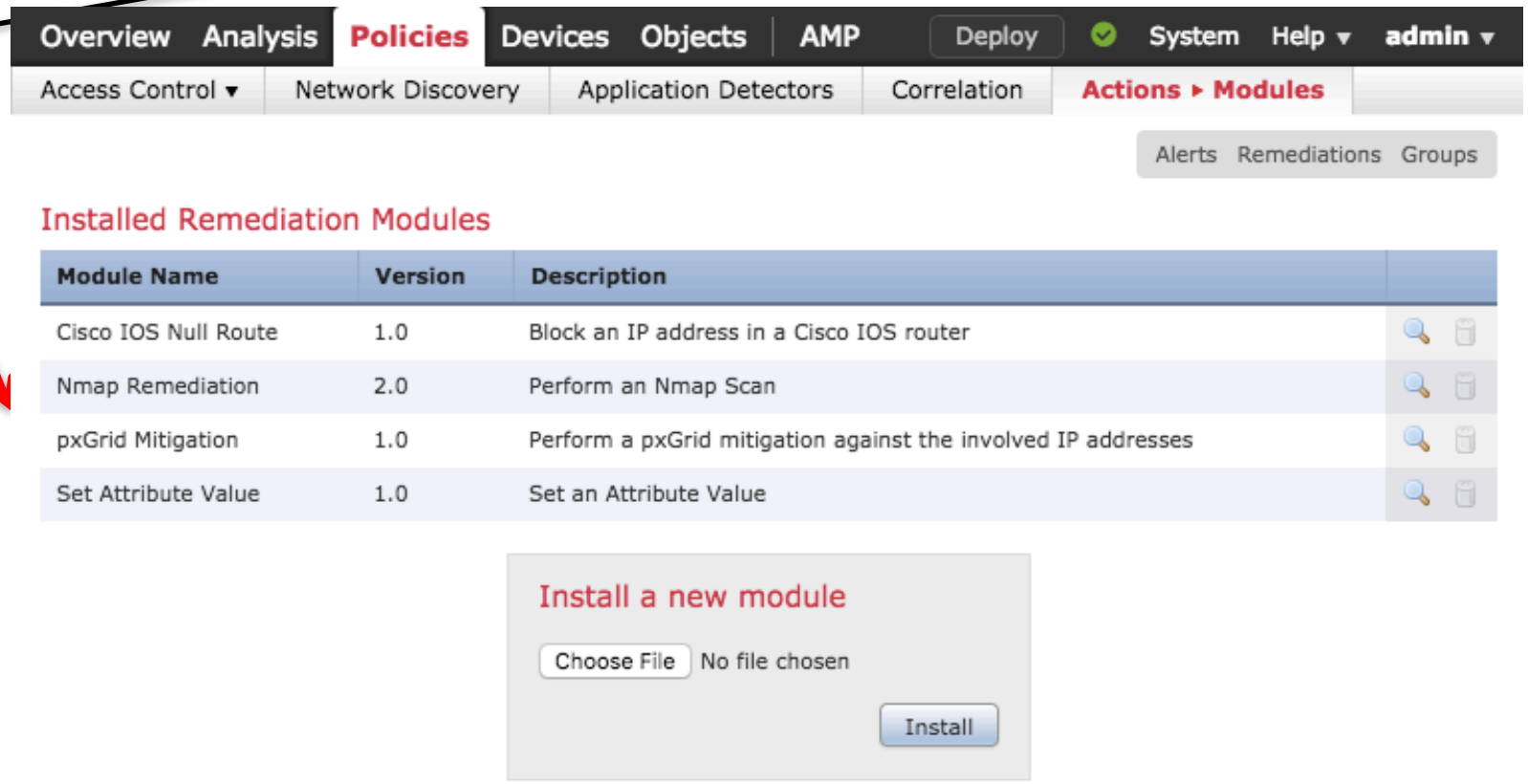
Пора что-то ДЕЛАТЬ!

Автоматизация нейтрализации



Примеры модулей нейтрализации

- Cisco ISE (pxGrid Mitigation)
- Установка атрибута хоста
- Скан Nmap
- Скрипты
- F5 iRules
- Netscaler
- …



О чем мы с вами не поговорили…

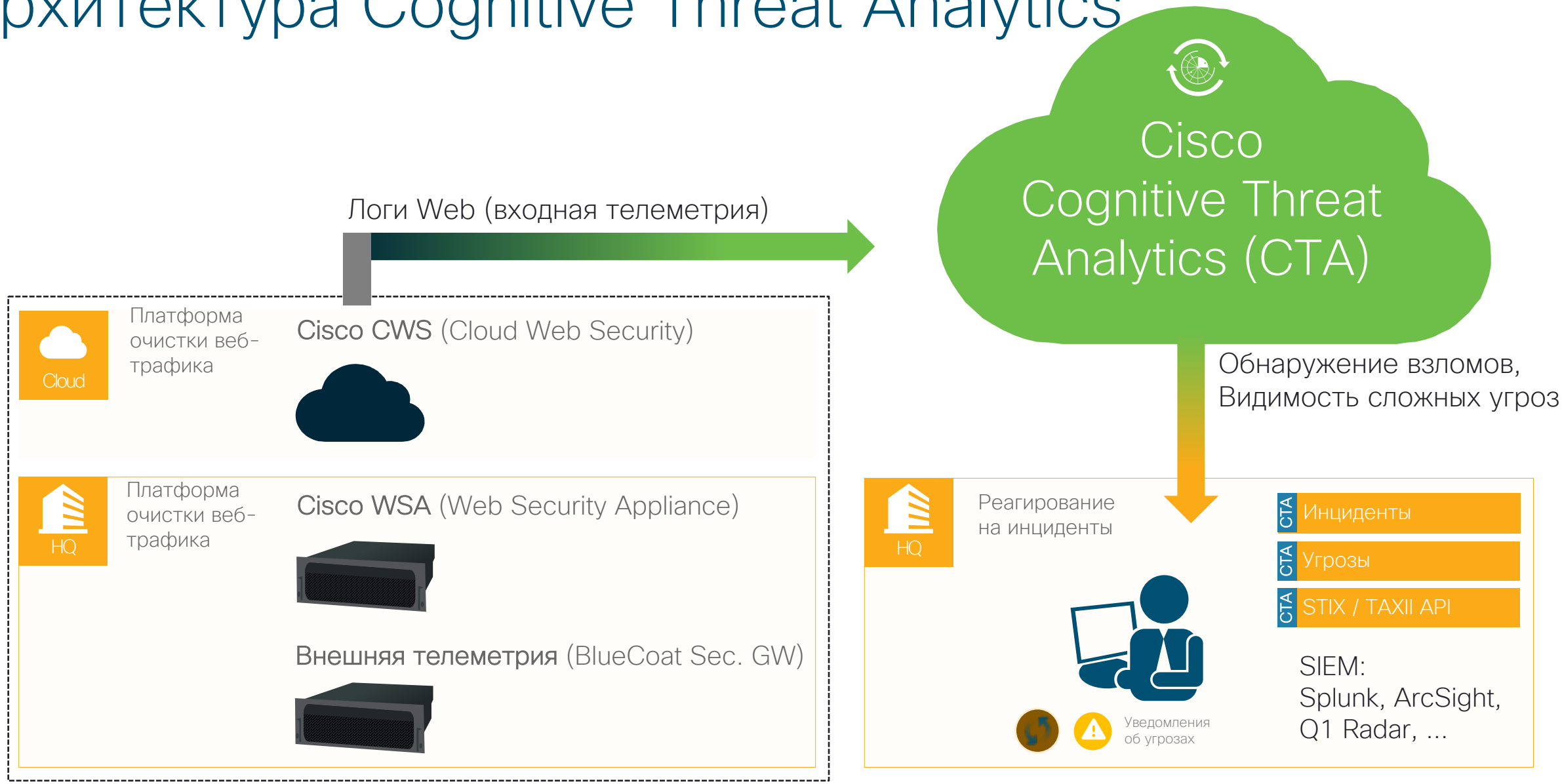
- https://developer.cisco.com/site/firepower/discover/overview/index.gsp
  - Database Access API
  - eStreamer API
  - Read / Write REST API
  - Host Input API
  - Remediation API

Интегрируйте (программным образом) межсетевые экраны и другие решения (например, Cisco ISE) в свою инфраструктуру управления безопасностью!

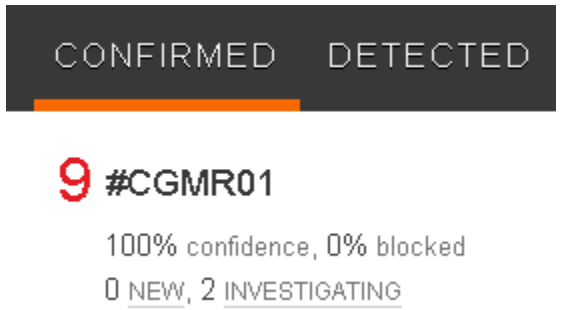
© 2017 Cisco and/or its affiliates. All rights reserved.

А что ещё для «после»

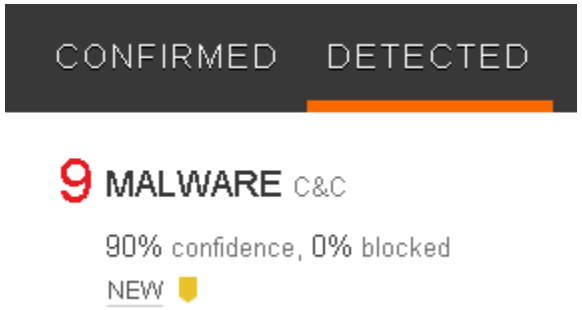
Архитектура Cognitive Threat Analytics



Процесс реагирования
Сила в интеграции с другими решениями Cisco



- Подтвержденные взломы:
- Автоматическое создание тикета, используя существующий SIEM для команды на очистку или переустановку ПК

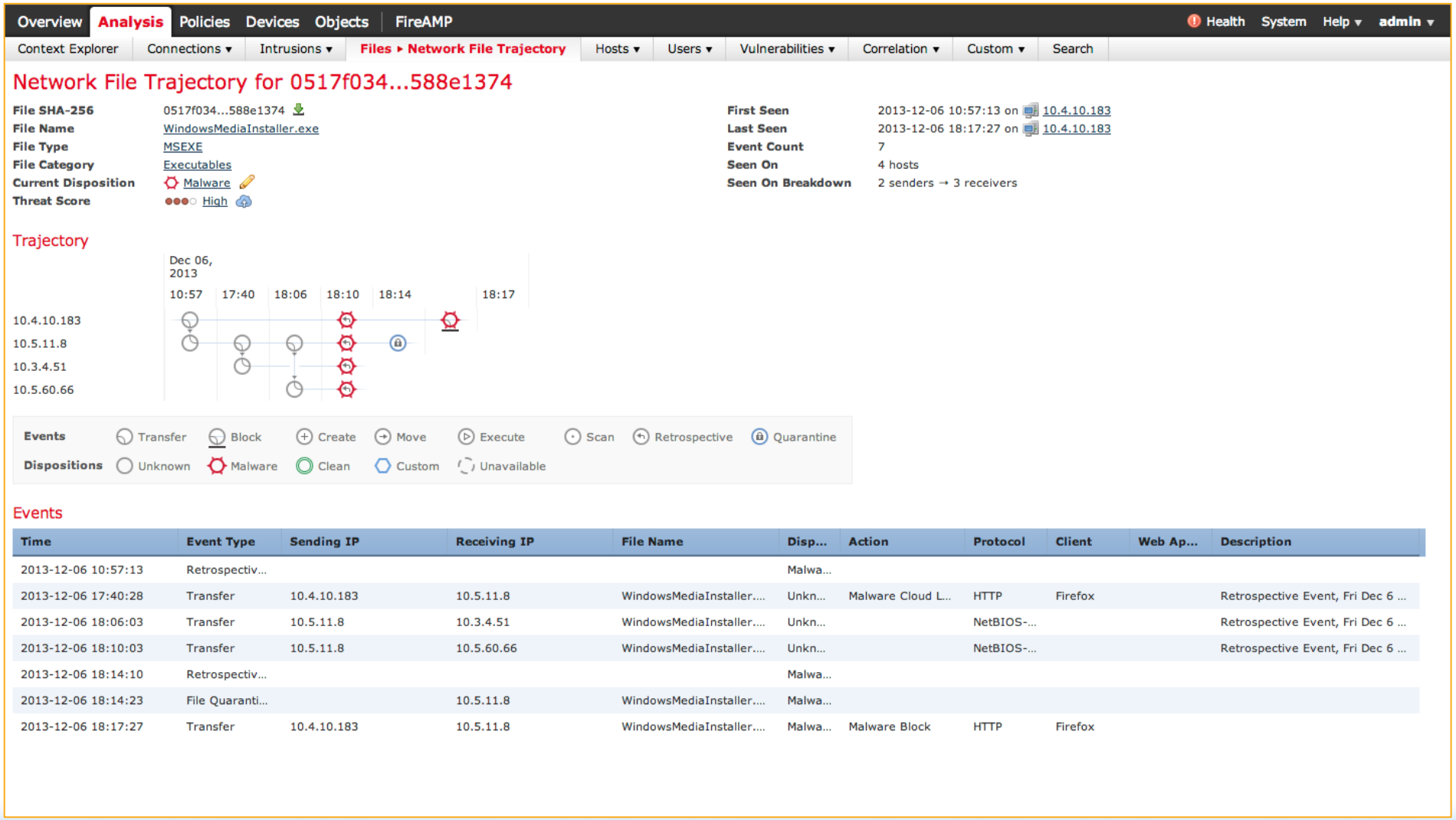


Подозреваемые взломы и целевые атаки:

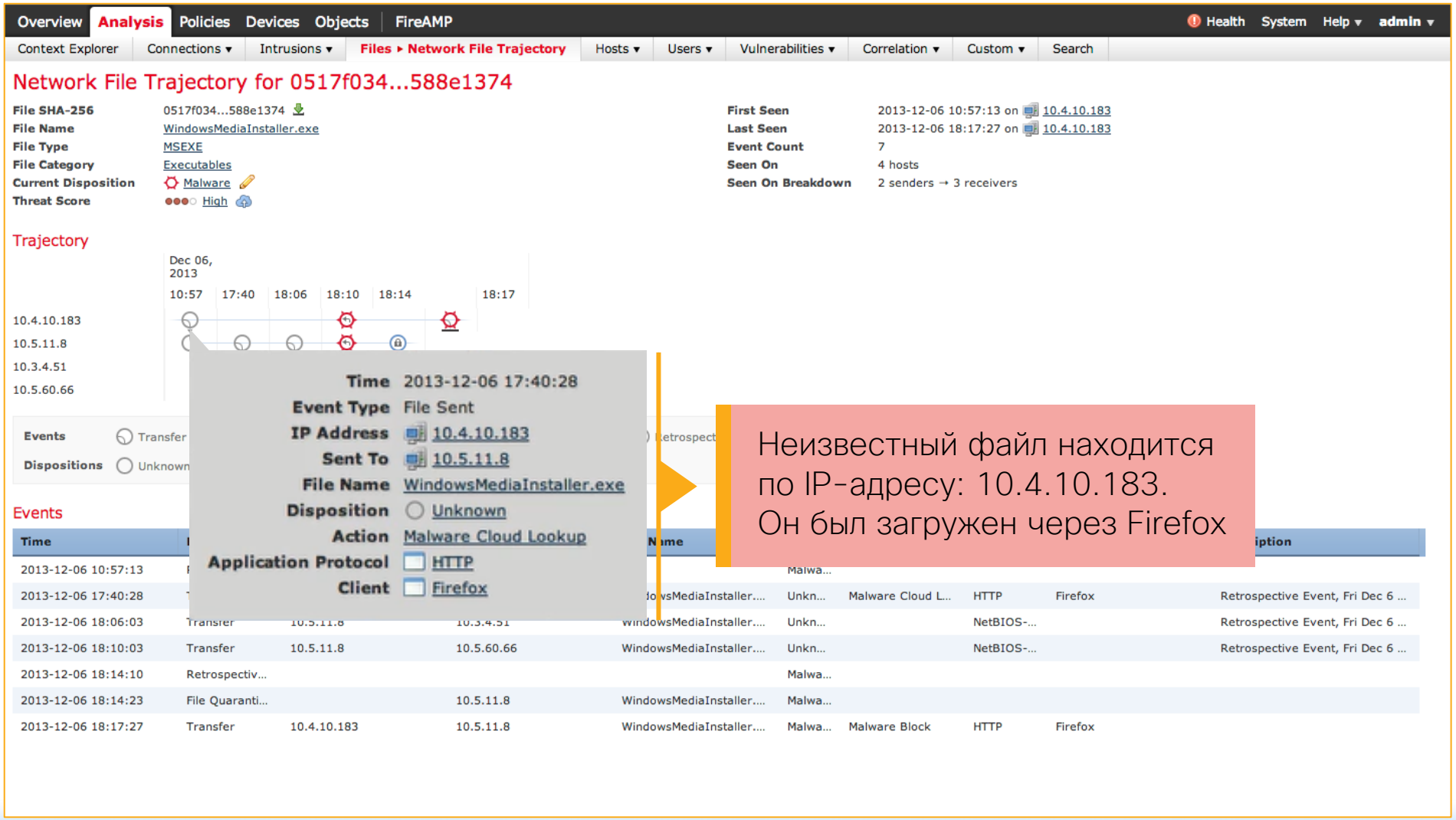
Комбинация высокого риска и высокой уверенности с подозреваемой утечкой данных может быть эскалирована на аналитиков 3-го уровня поддержки для ручного анализа

Ретроспектива с Cisco AMP

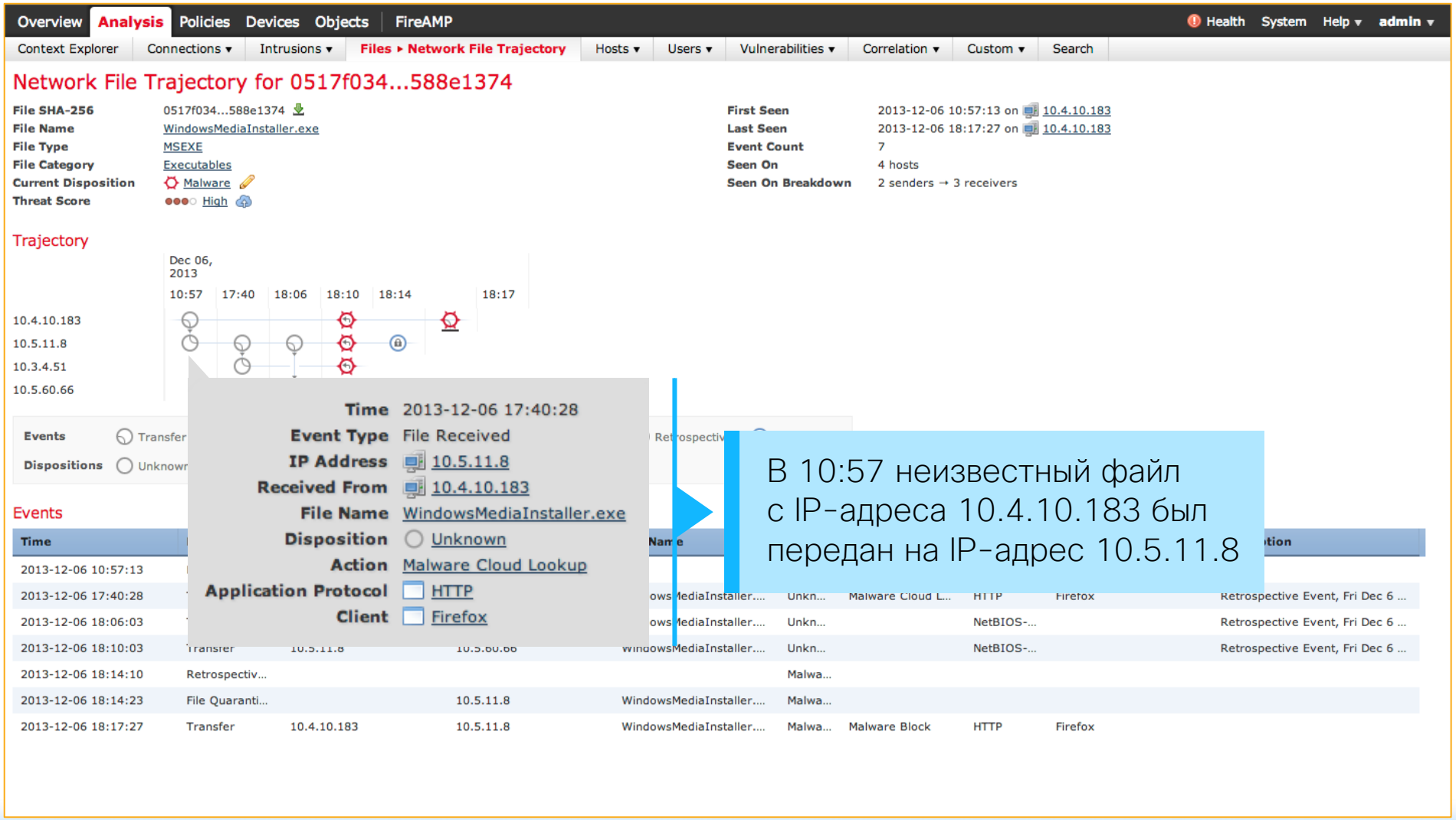
Пример траектории файла



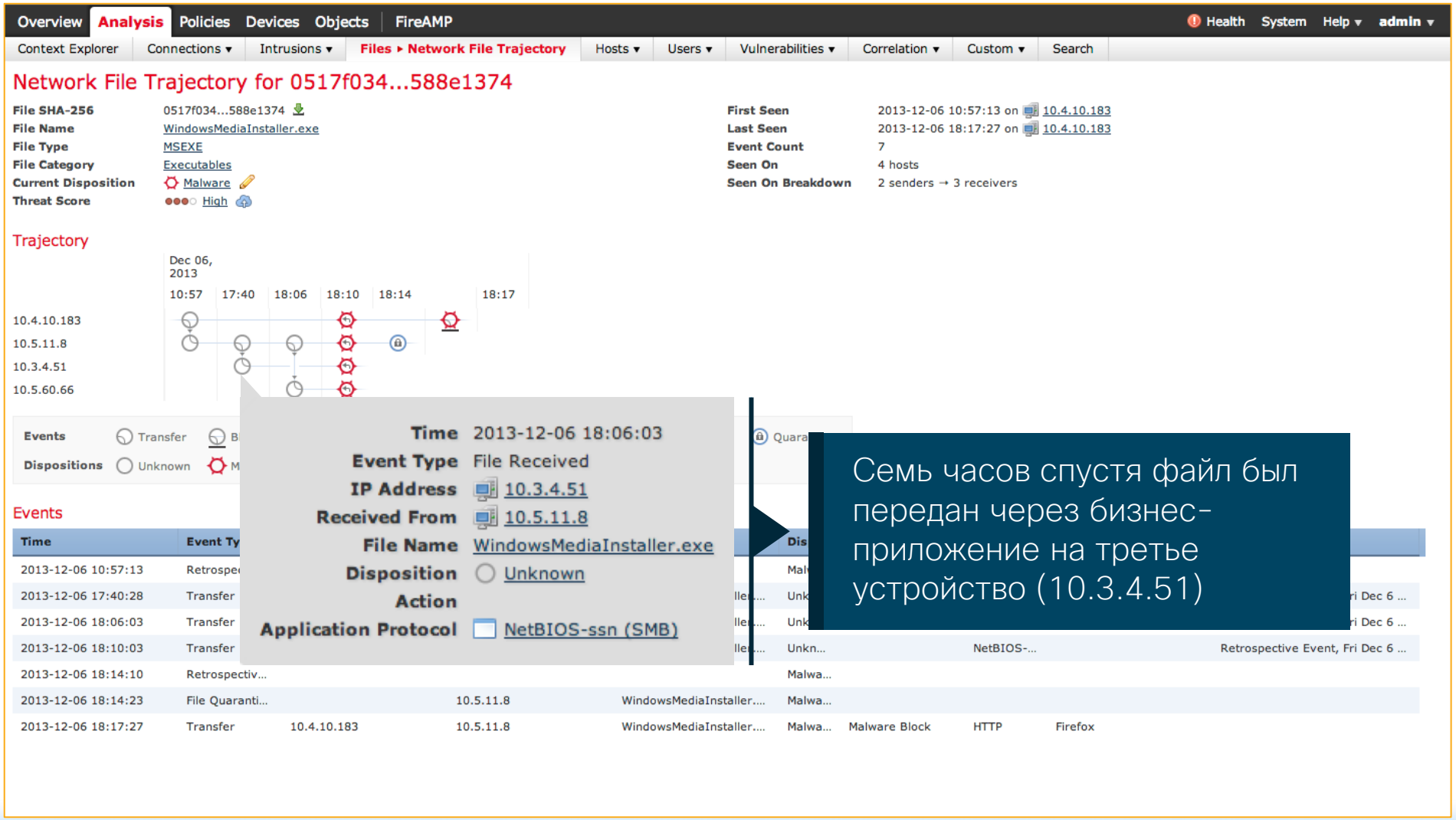
Пример траектории файла



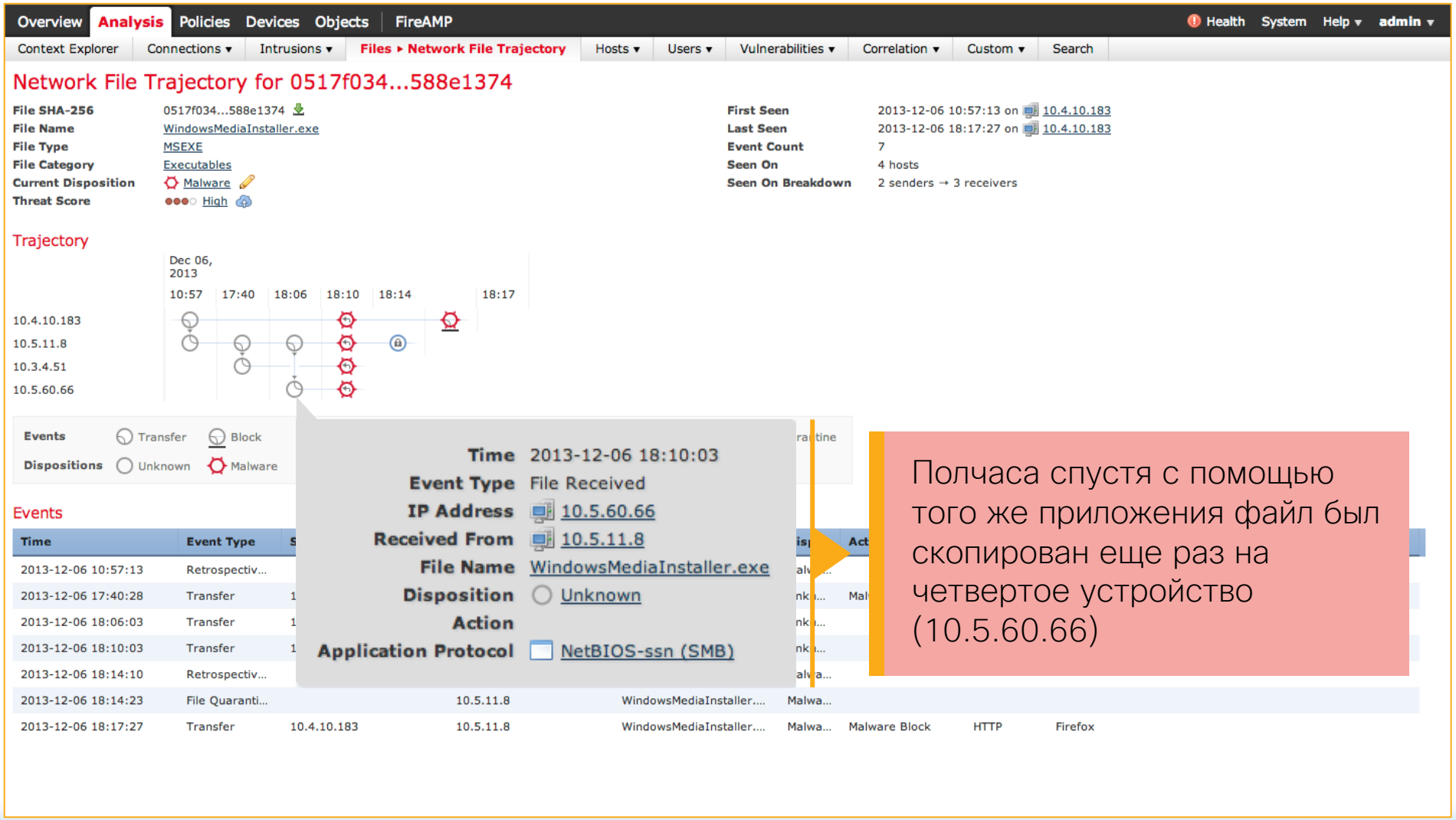
Пример траектории файла



Пример траектории файла

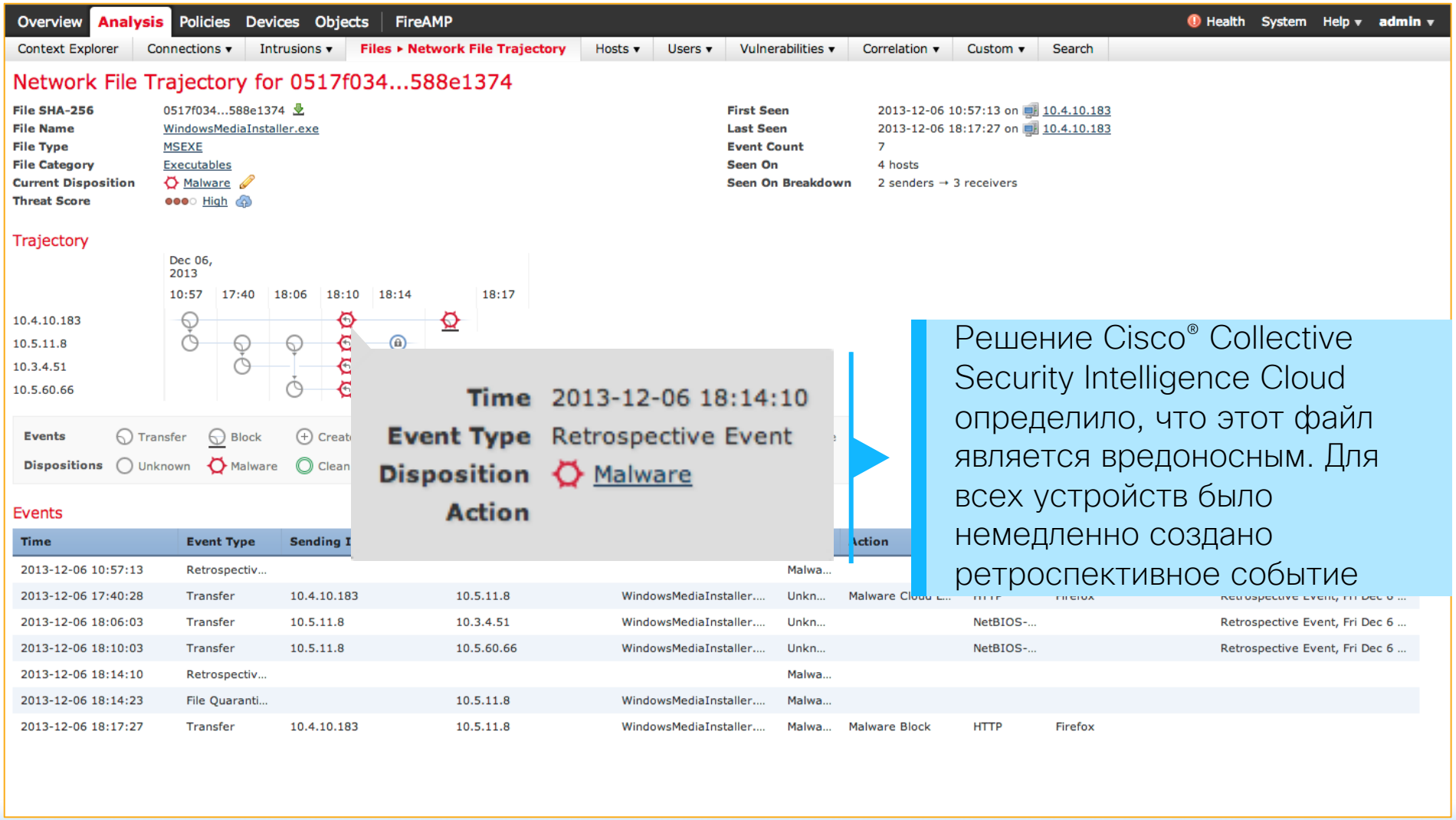


Пример траектории файла



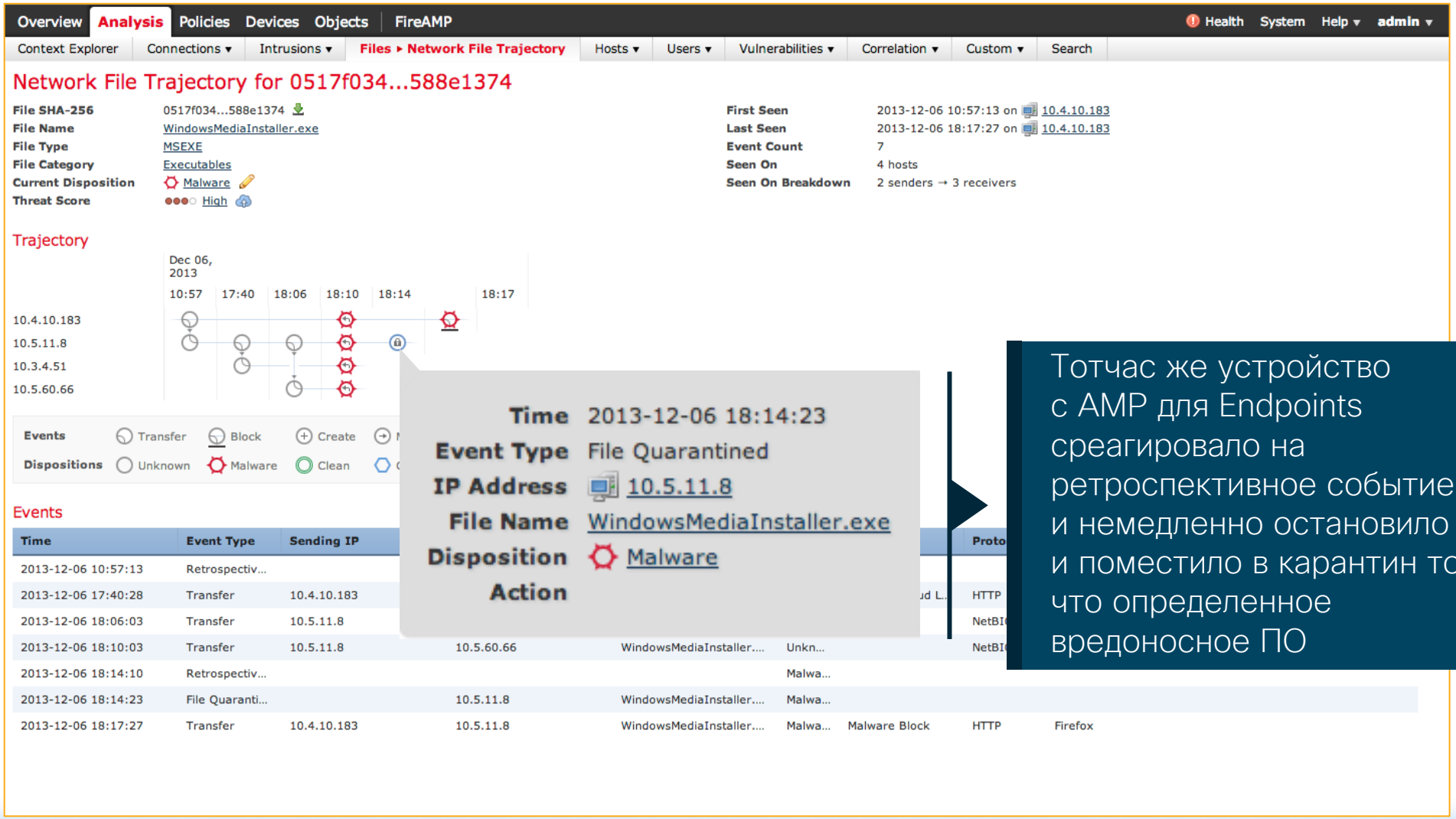
Полчаса спустя с помощью того же приложения файл был скопирован еще раз на четвертое устройство (10.5.60.66)

Пример траектории файла



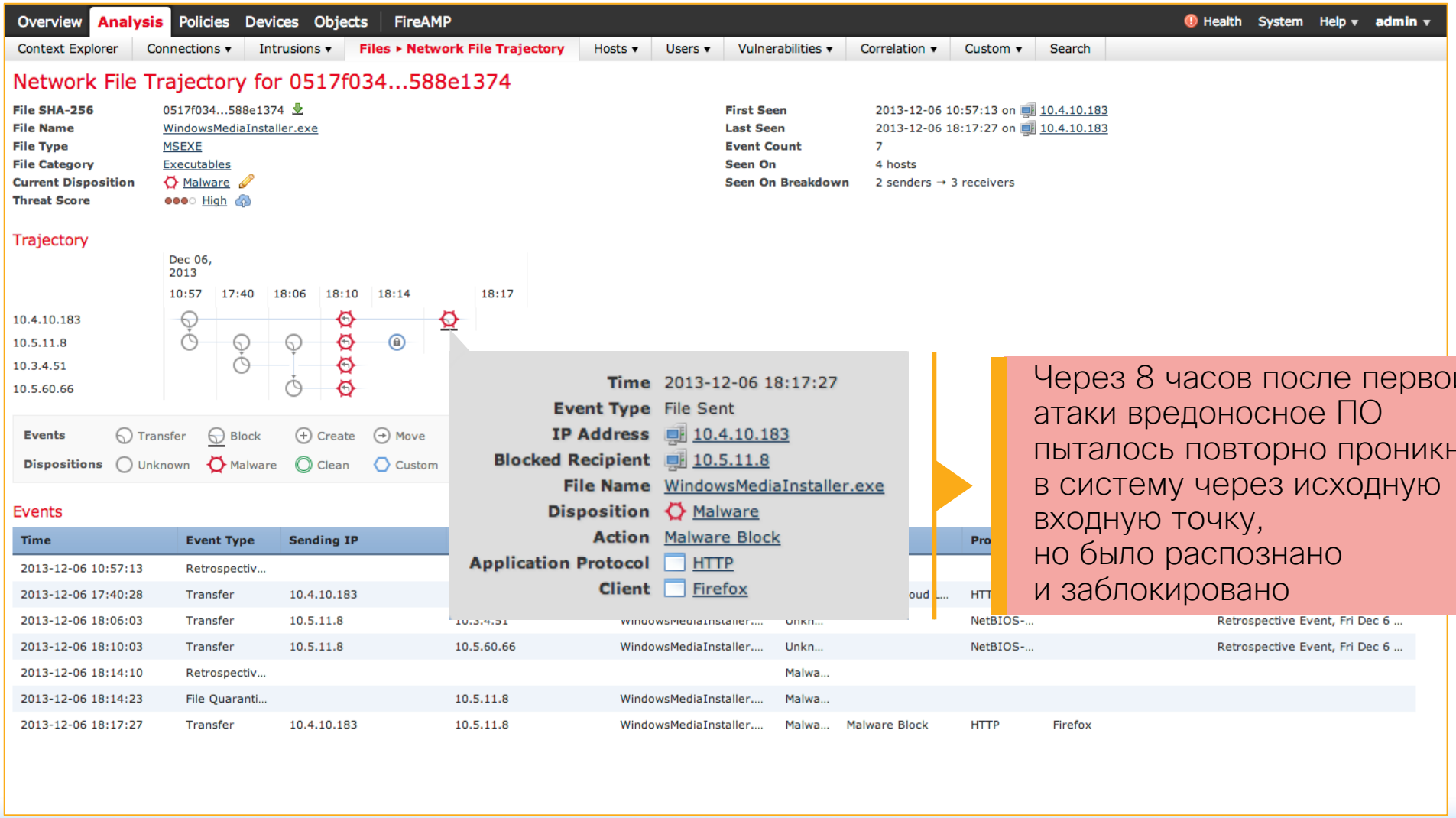
Решение Cisco® Collective Security Intelligence Cloud определило, что этот файл является вредоносным. Для всех устройств было немедленно создано ретроспективное событие

Пример траектории файла



Тотчас же устройство с AMP для Endpoints среагировало на ретроспективное событие и немедленно остановило ВПО и поместило в карантин только что определенное вредоносное ПО

Пример траектории файла



Через 8 часов после первой атаки вредоносное ПО пыталось повторно проникнуть в систему через исходную входную точку, но было распознано и заблокировано

Threat Centric NAC

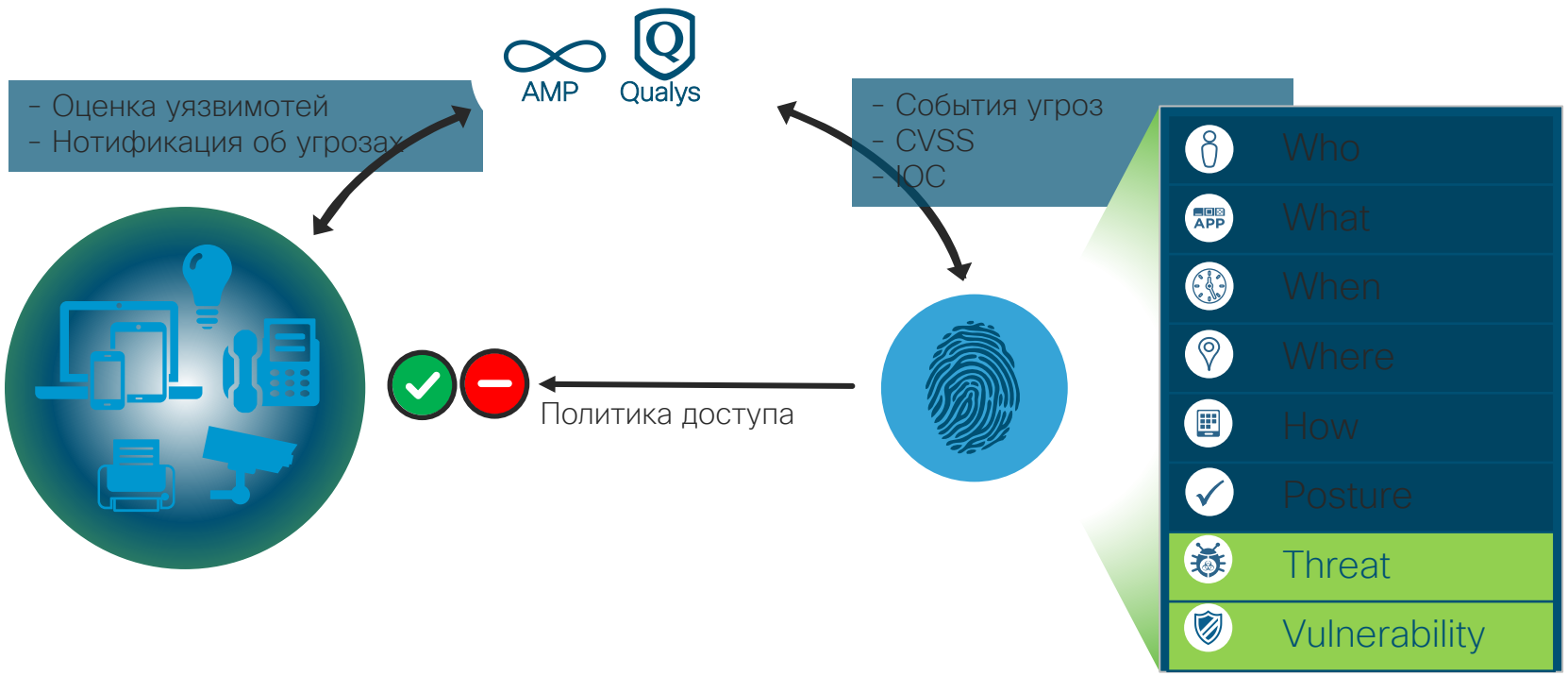
Cisco ISE защищает вашу сеть от брешей в данных с помощью сегментации скомпрометированных или уязвимых узлов

Оценка
Данные об уязвимостях

Расширенное управление
С помощью оценки уязвимостей и threat intelligence

Быстрое реагирование
с автоматизированными обновлениями в режиме реального времени на основании метрик угроз и данных об уязвимостях

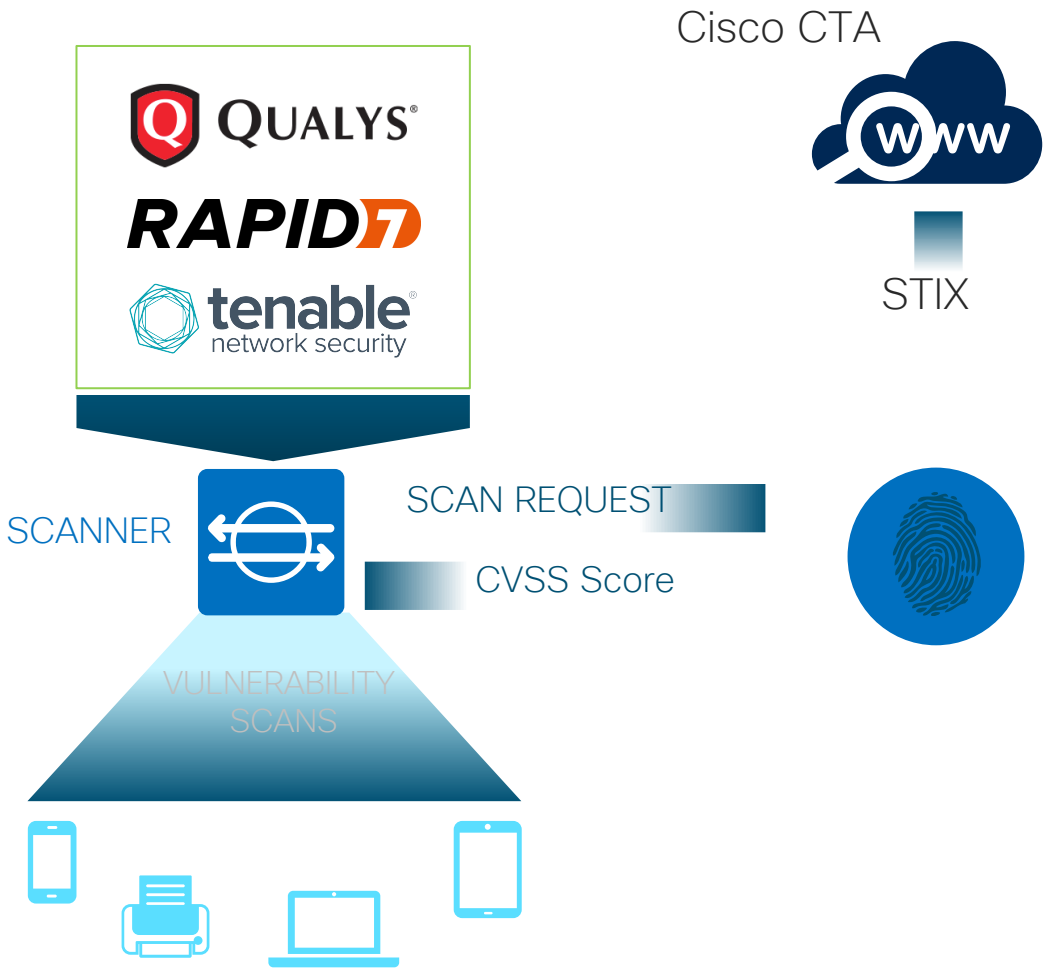
Создайте политики авторизации на основании анализа угроз и уязвимостей



Threat Centric NAC

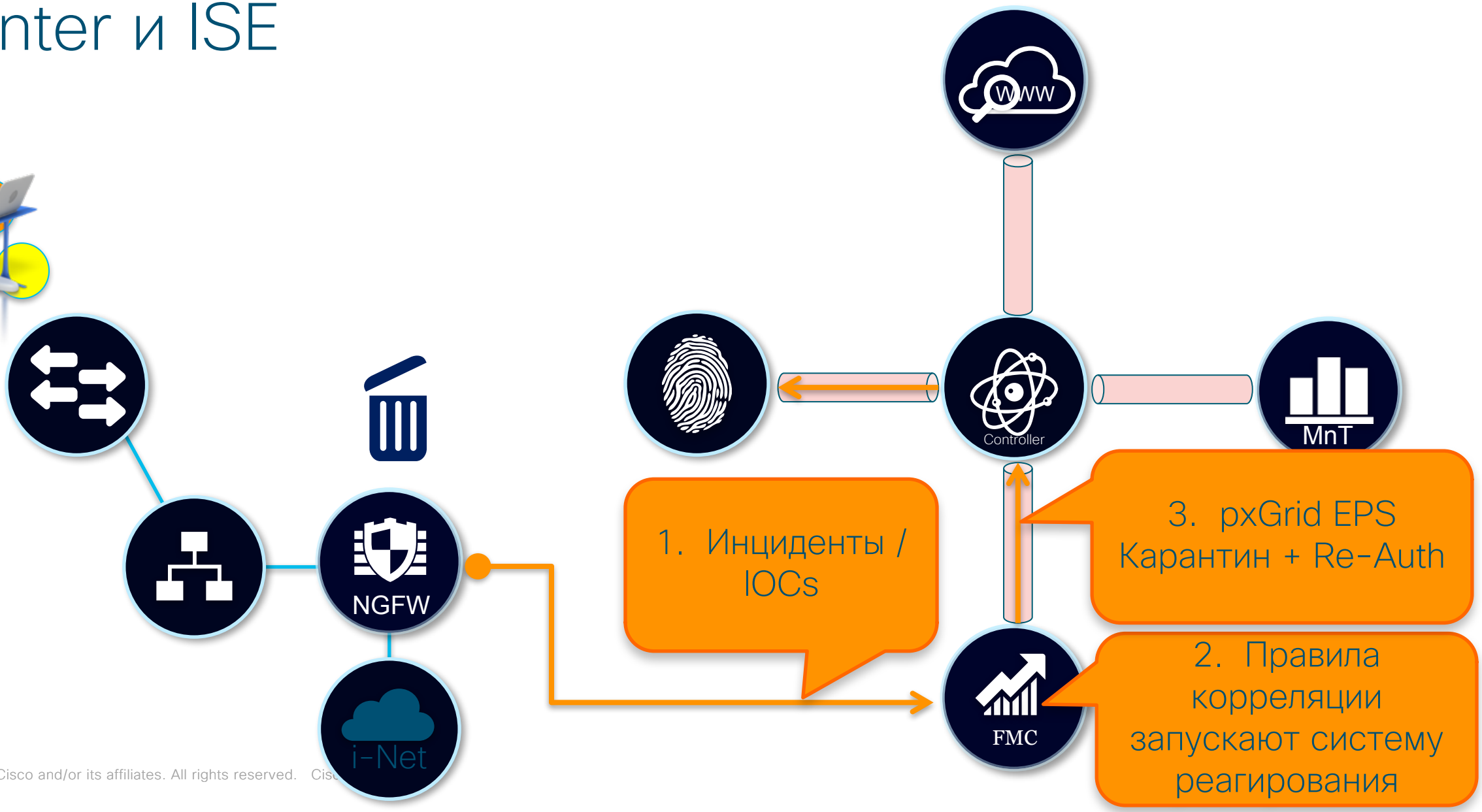
Выберите вендора для оценки уязвимостей

ISE 2.2

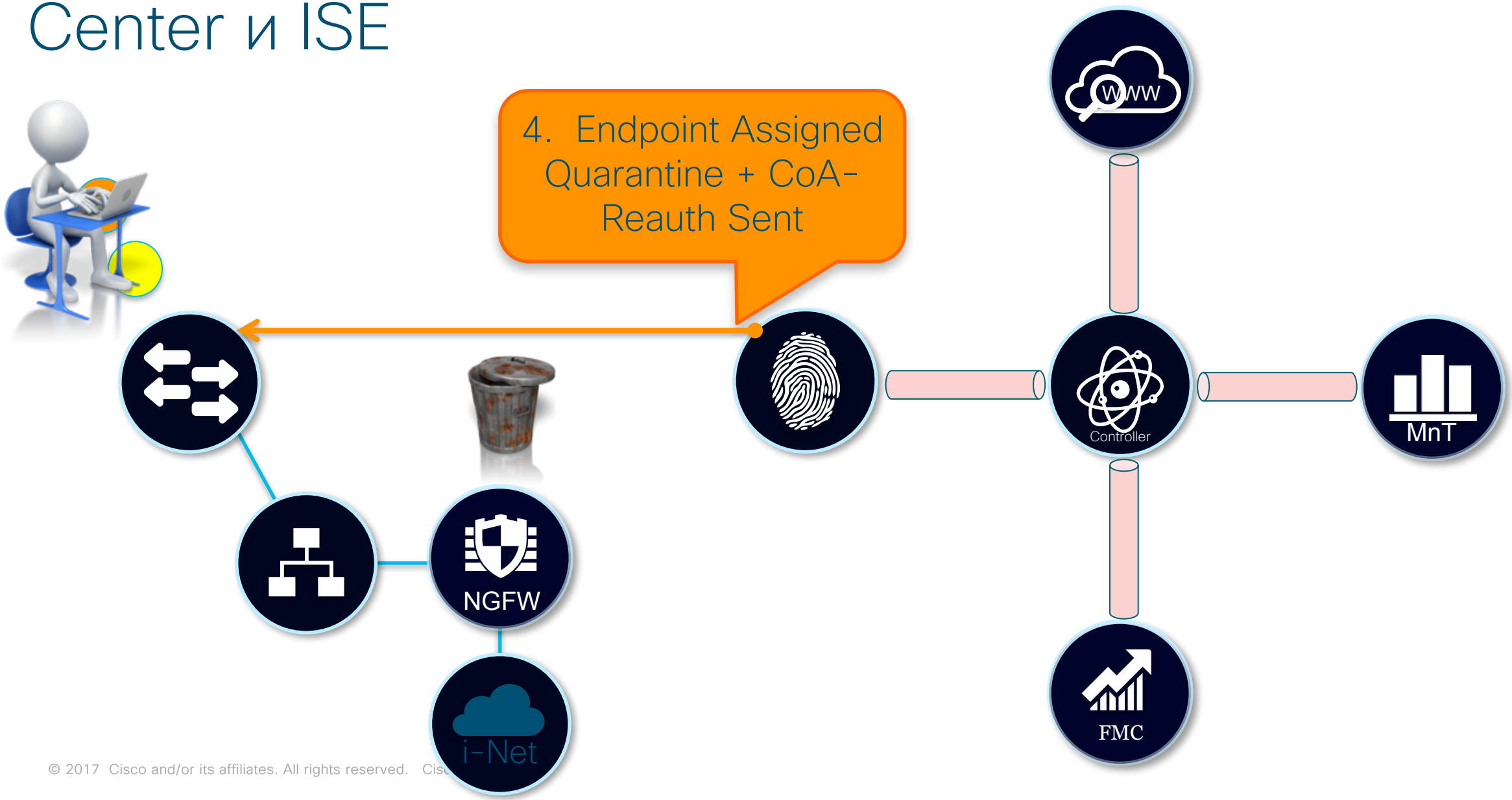


- В ISE 2.2, TC-NAC поддерживает Tenable, Cisco Threat Analytics (CTA) и Rapid7.
- Стандартный “listener” будет поддерживаться для анализа угроз с помощью STIX framework для автоматической отправки инфицированных узлов в карантин.

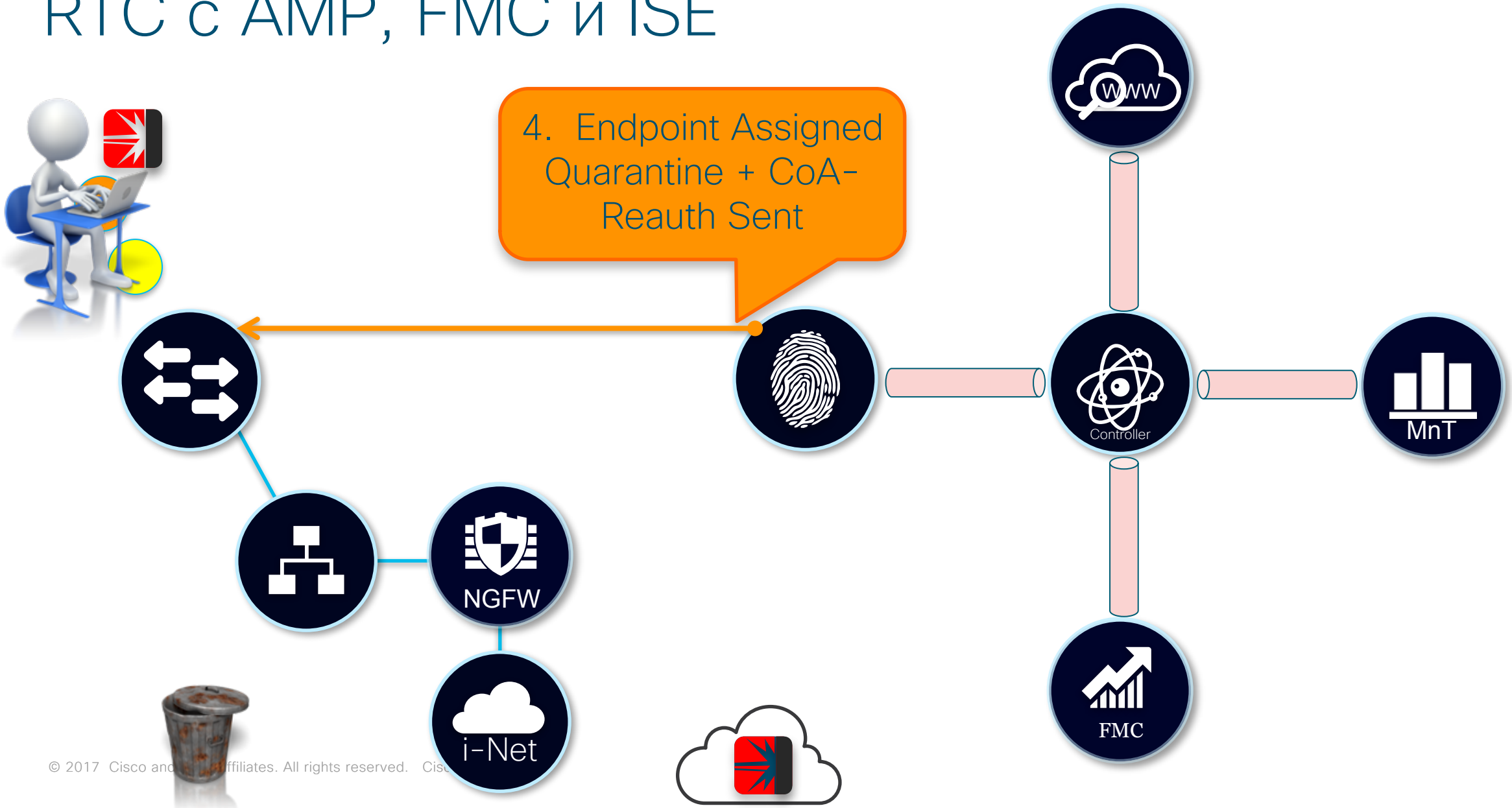
Rapid Threat Containment с Firepower Management Center и ISE



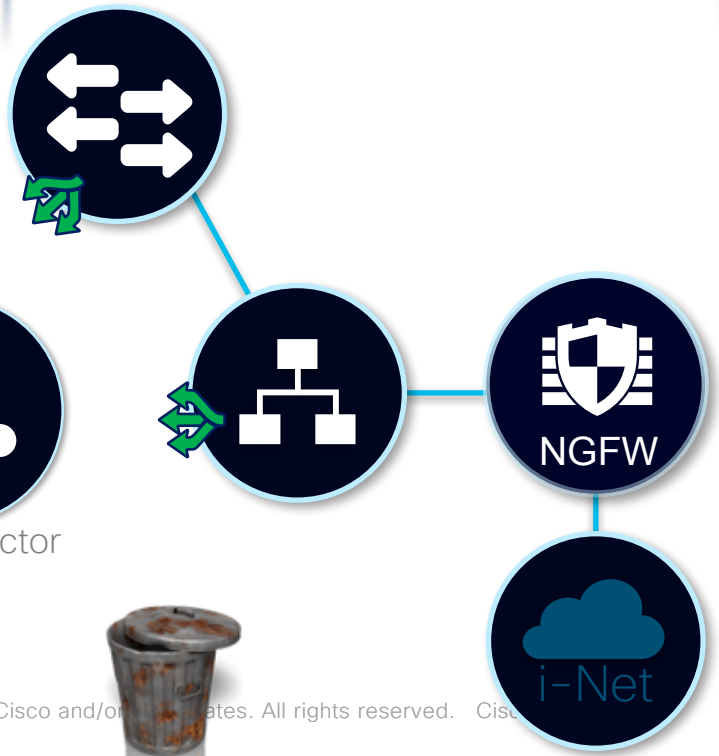
Rapid Threat Containment c Firepower Management Center и ISE



RTC с AMP, FMC и ISE



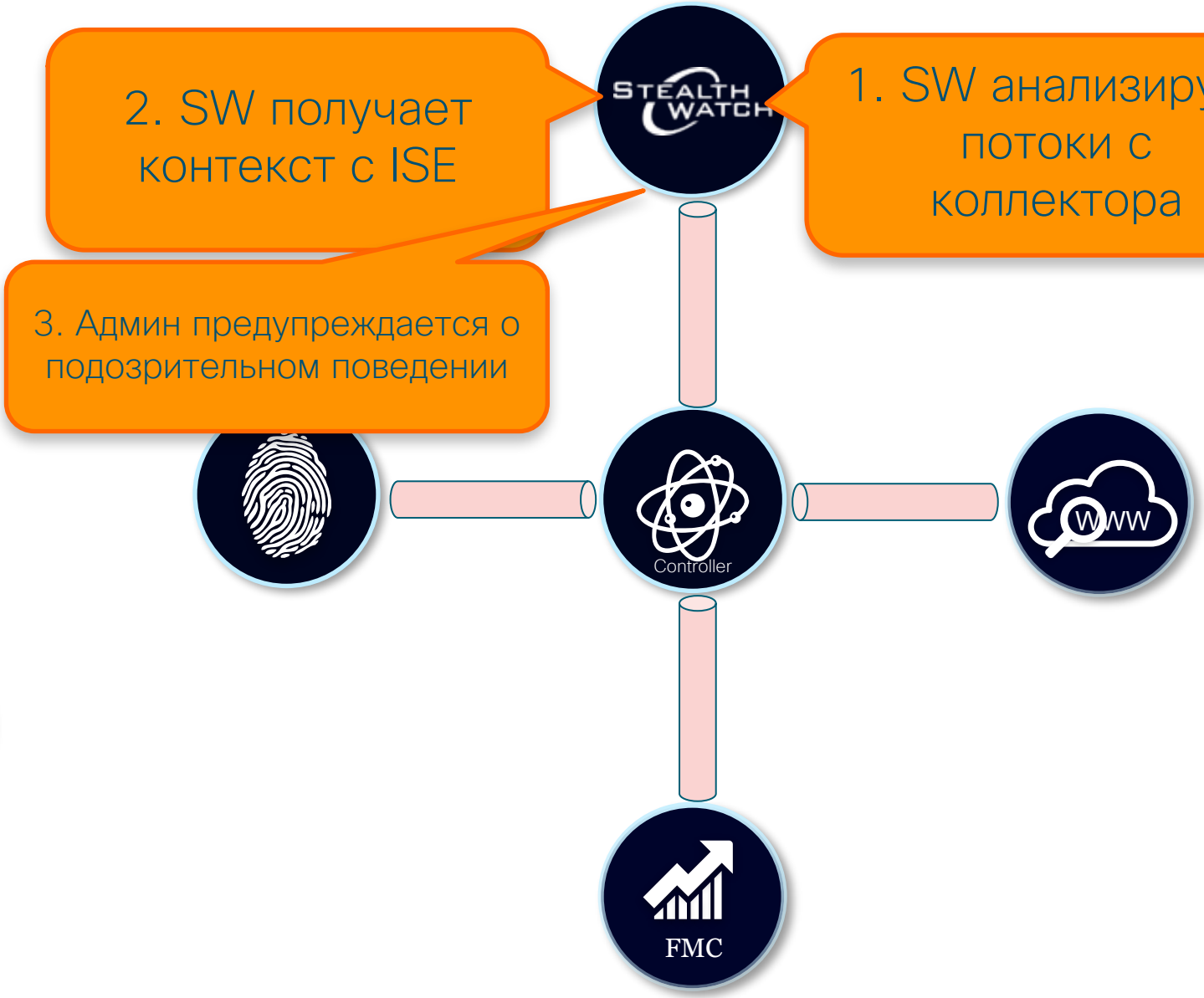
RTC с Stealthwatch & ISE



2. SW получает контекст с ISE

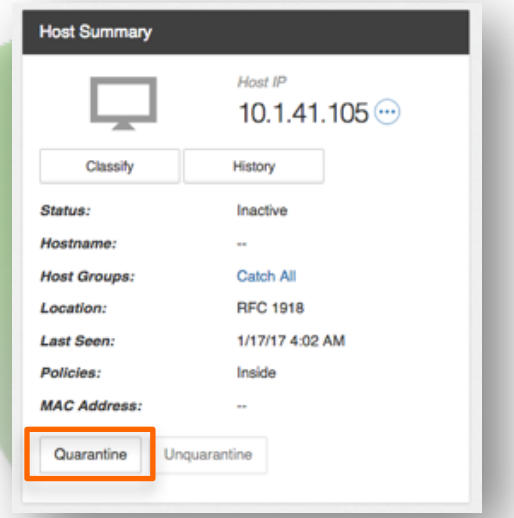
1. SW анализирует потоки с коллектора

3. Админ предупреждается о подозрительном поведении



RTC с Stealthwatch и ISE

4. Админ инициирует карантин



STEALTH WATCH

Controller

WWW

NGFW

Flow Collector

i-Net

FMC

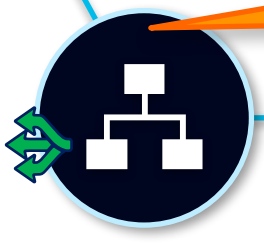
5. Endpoint Assigned Quarantine + CoA-Reauth Sent

RTC с Stealthwatch и ISE

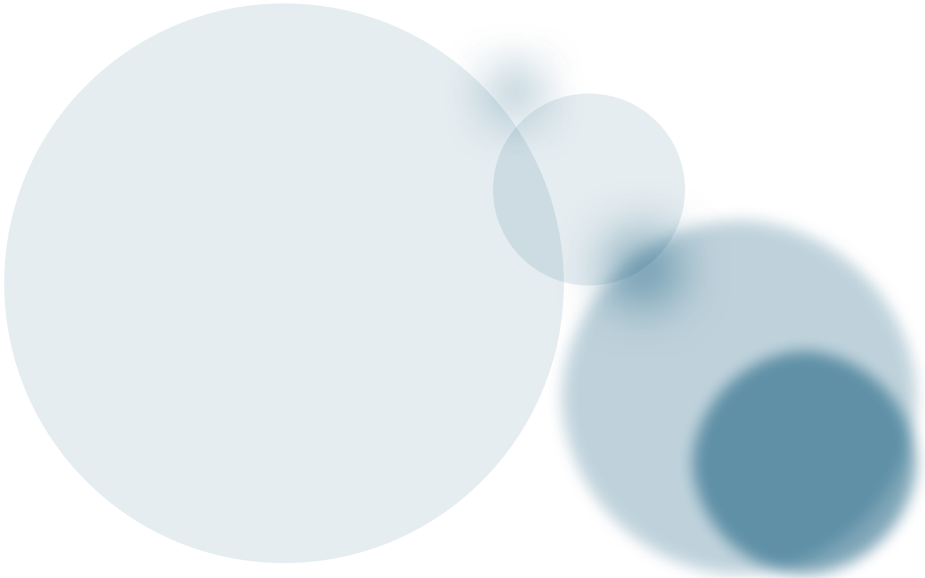
6. Применяются новые правила доступа

6a. Может запретить доступ

6b. Может фильтровать в сети (входящий)

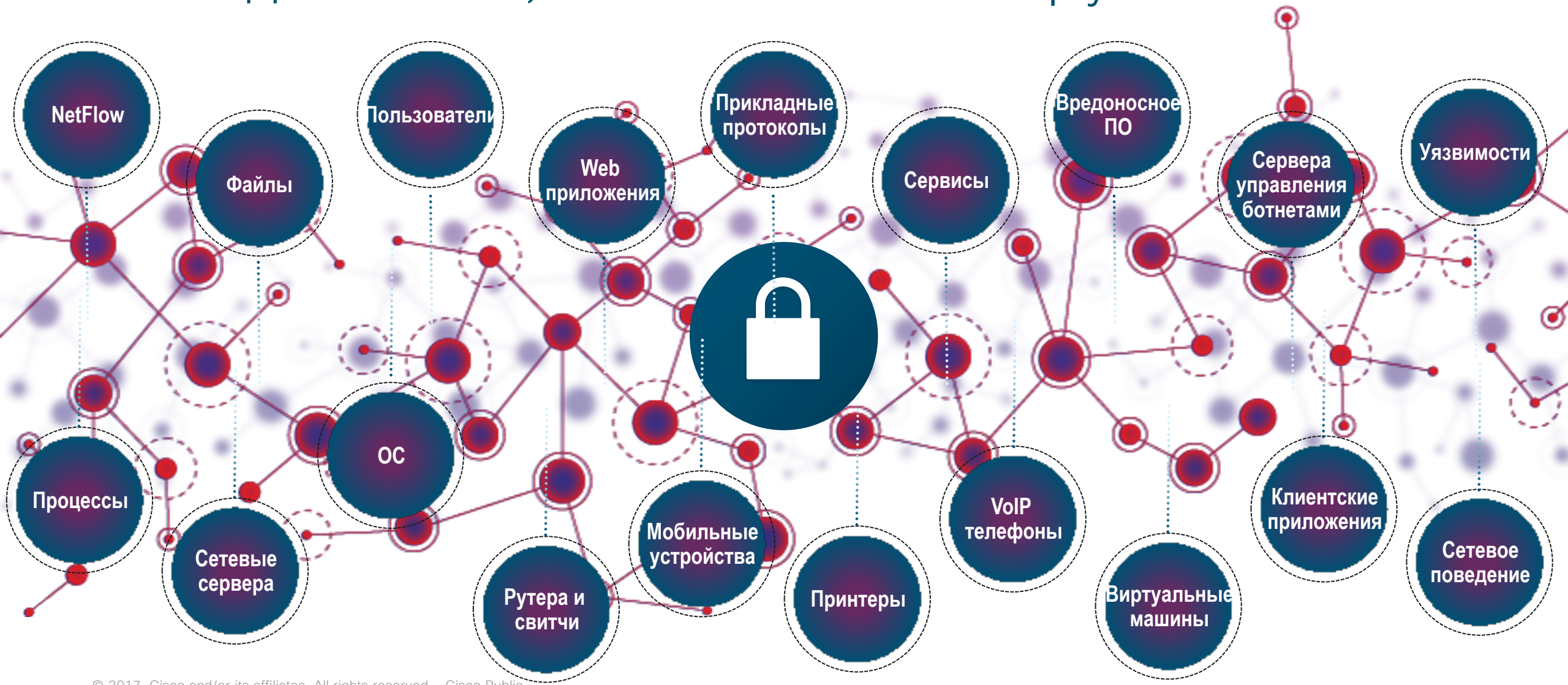


Flow Collector



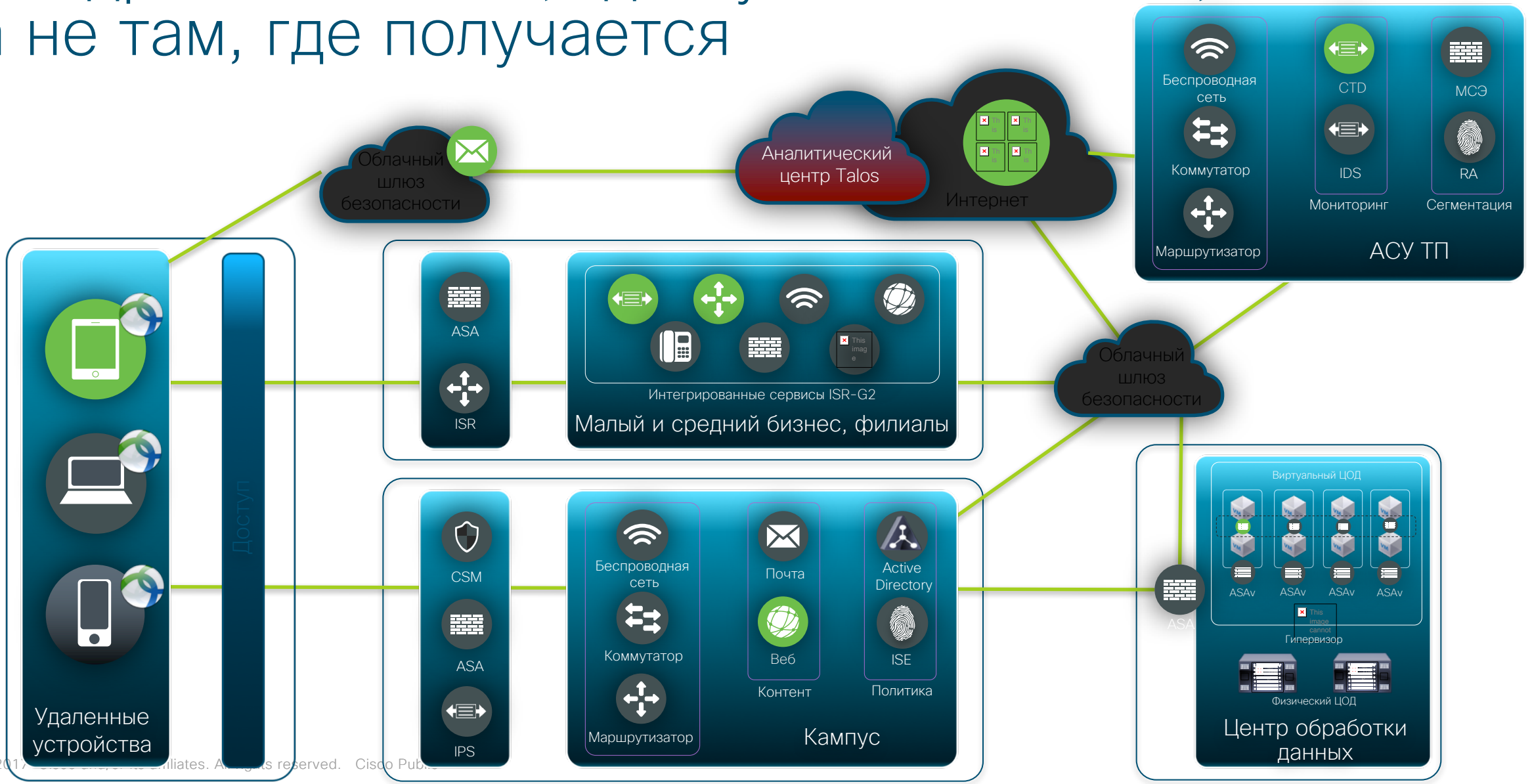
РЕЗЮМИРУЯ

Не видя ничего, ничего и не обнаружишь



Борьба с угрозами ДО, ВО ВРЕМЯ и ПОСЛЕ – ВЕЗДЕ

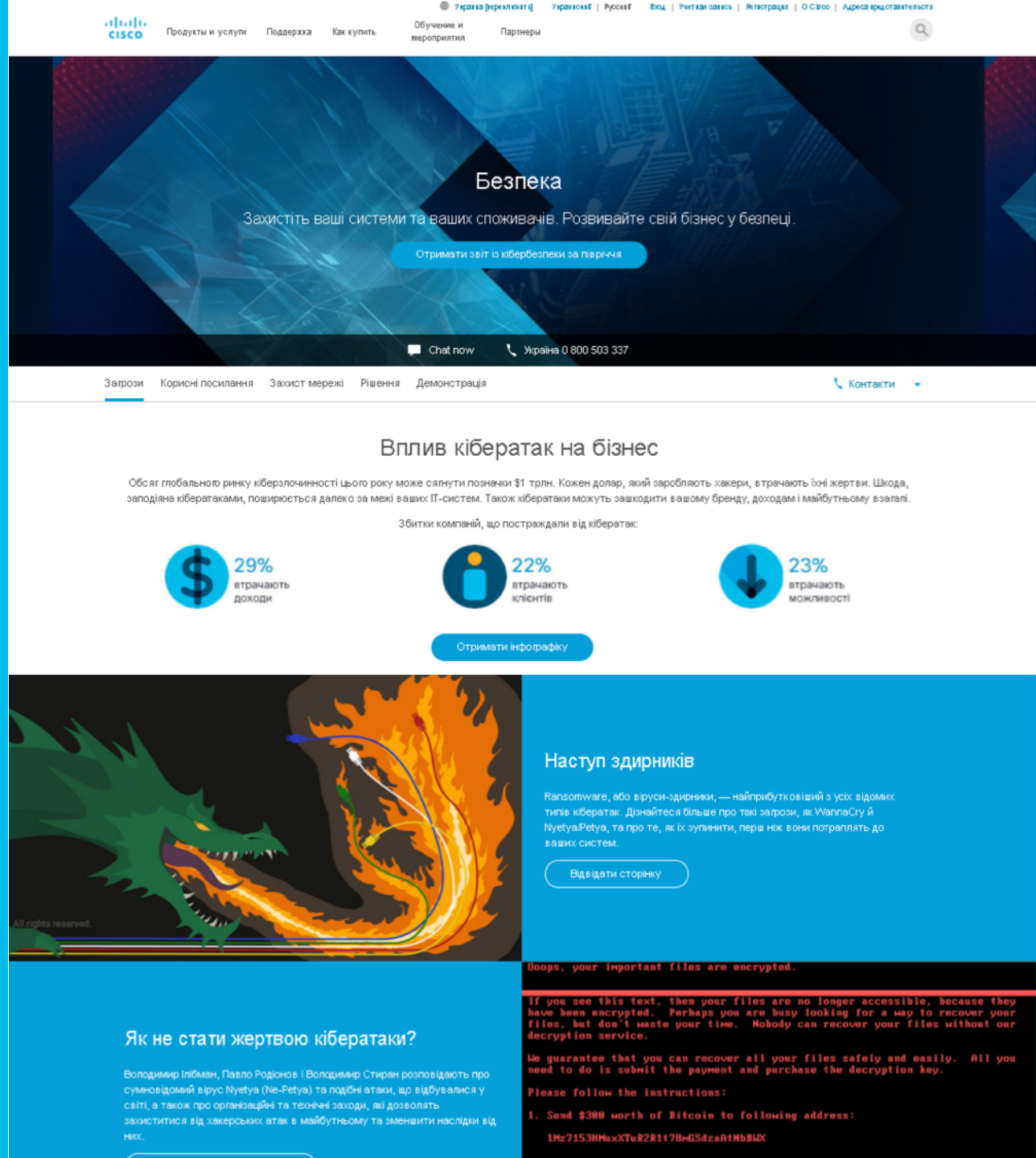
Внедрение ИБ там, где нужно БИЗНЕСУ, а не там, где получается



Security Hub

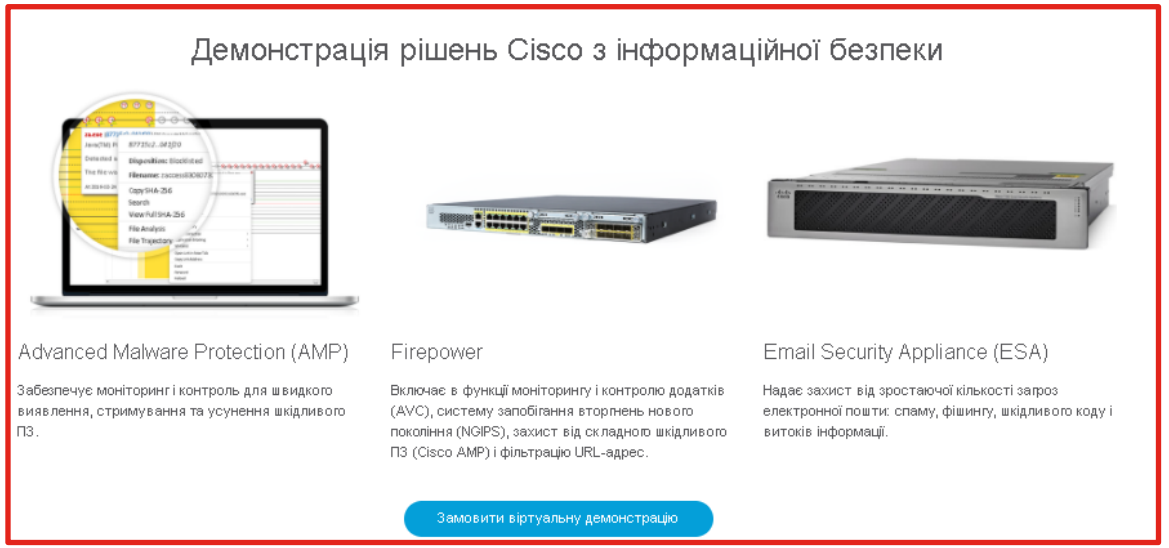
www.cs.co/security_hub

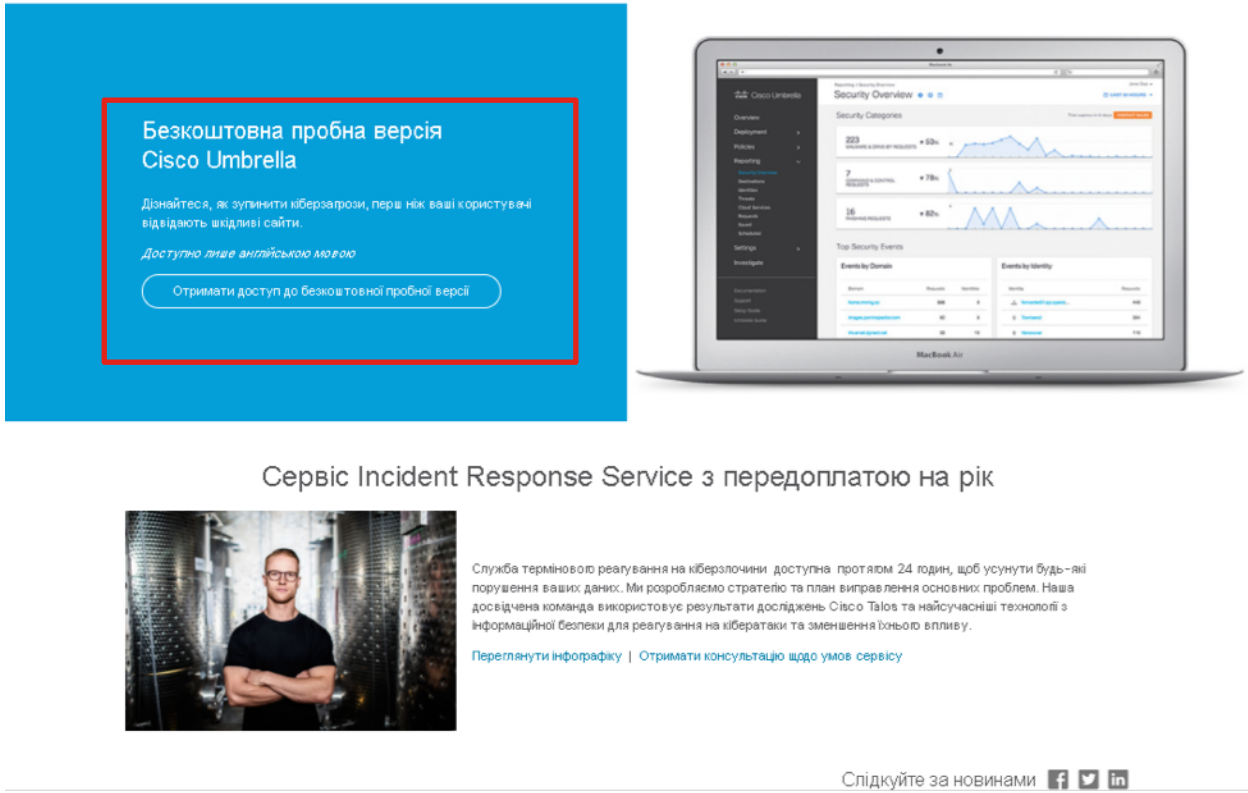
- Вебинары
- Статьи
- Отчеты
- Видео
- Брошюры
- Инфографика
- Решения
- Демонстрации
- Сервисы
- Trial
- ...



Security Hub
www.cs.co/security_hub

- Виртуальная демонстрация
  - ✓ AMP
  - ✓ Firepower
  - ✓ ESA
- Бесплатная пробная версия Cisco Umbrella






CISCO
TM