

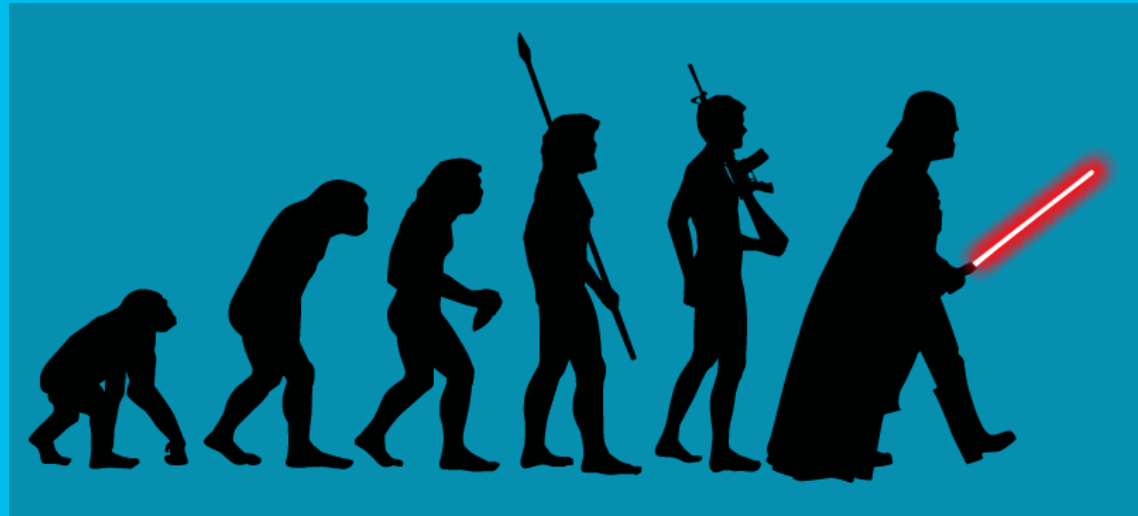


Архитектура обеспечения информационной безопасности. Подход Cisco

Павел Родионов

prodiono@cisco.com,

Состояние кибербезопасности



Атаки в Україні – декабрь 2016



Сайт Міносвіти не працює через DDoS-атаки

Тривають роботи з відновлення роботи сайту.



Фото: autocentre.ua

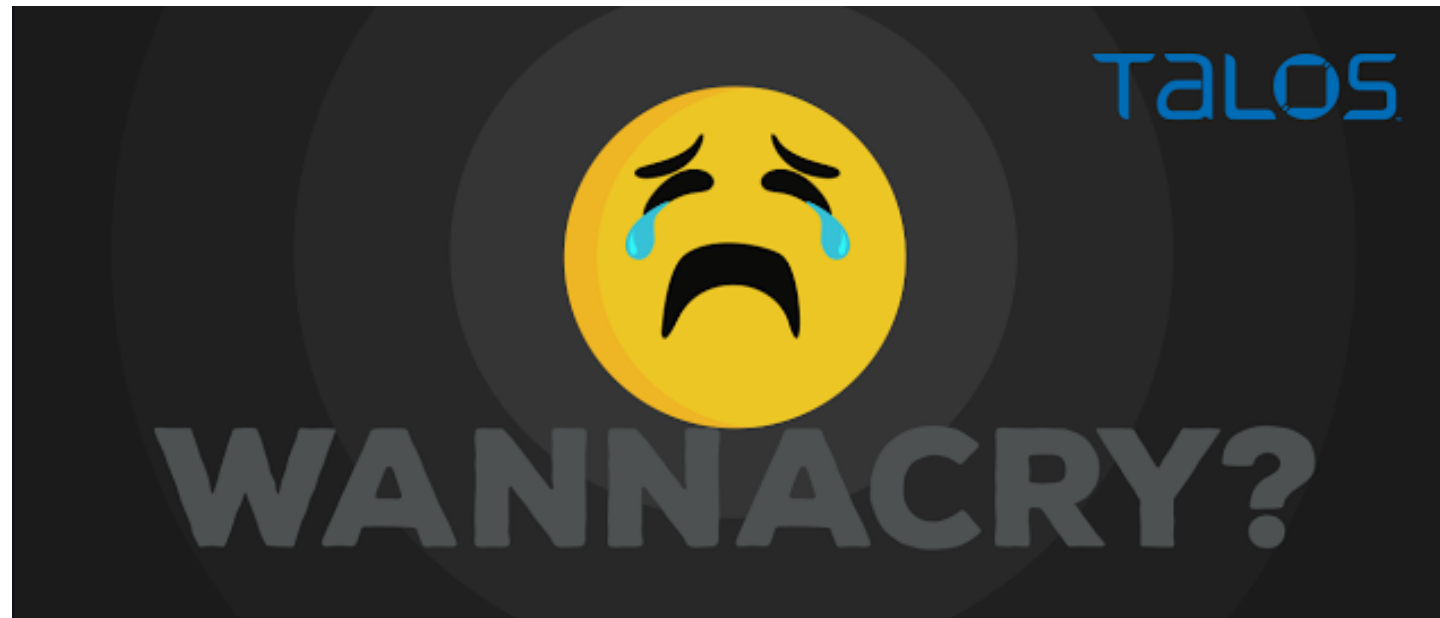
Сайт Міністерства освіти і науки України не працює внаслідок [DDoS-атаки](#) на вихідних.

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.

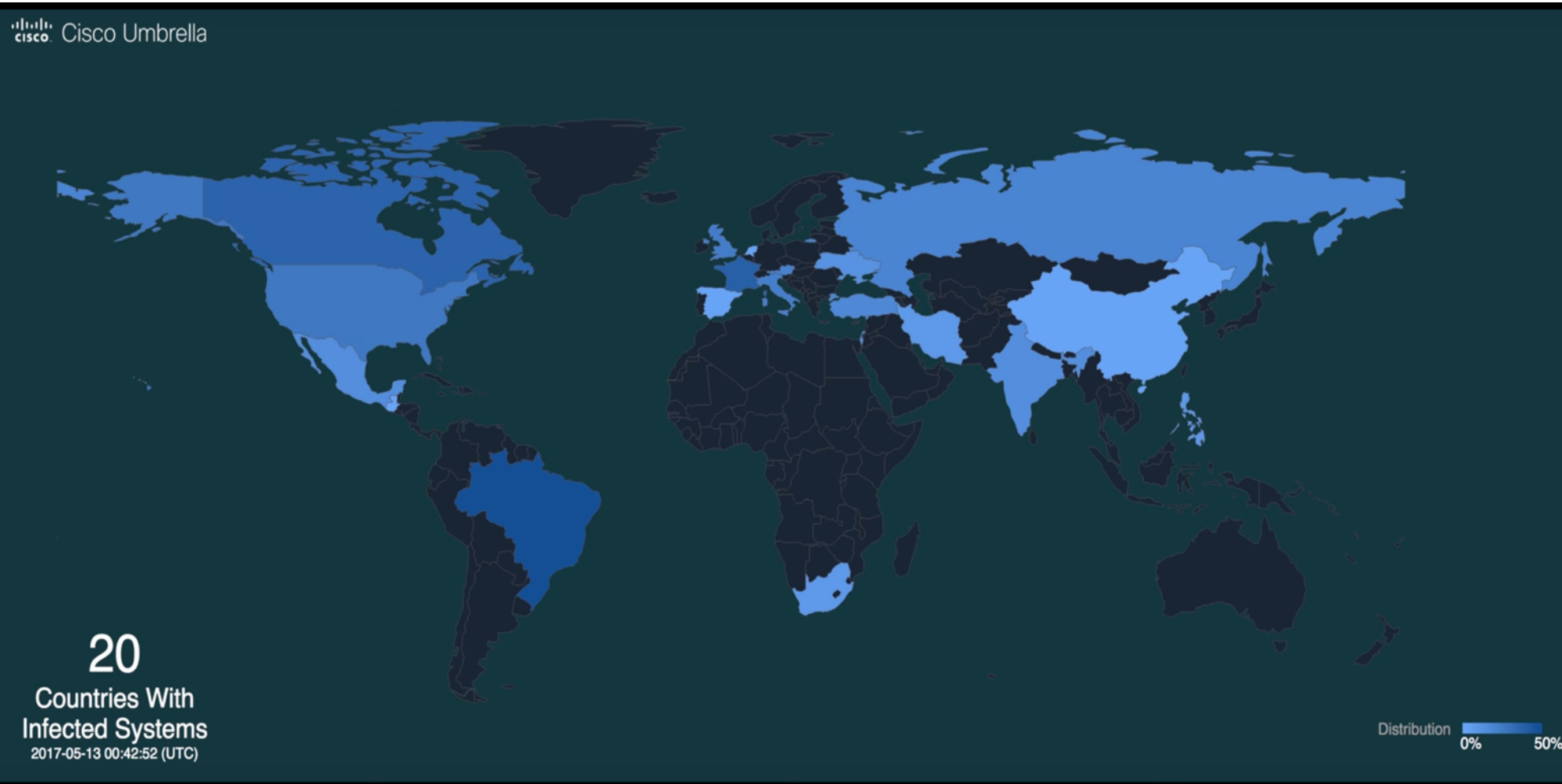
Новый игрок. Скажи «привет» ‘WannaCry’

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



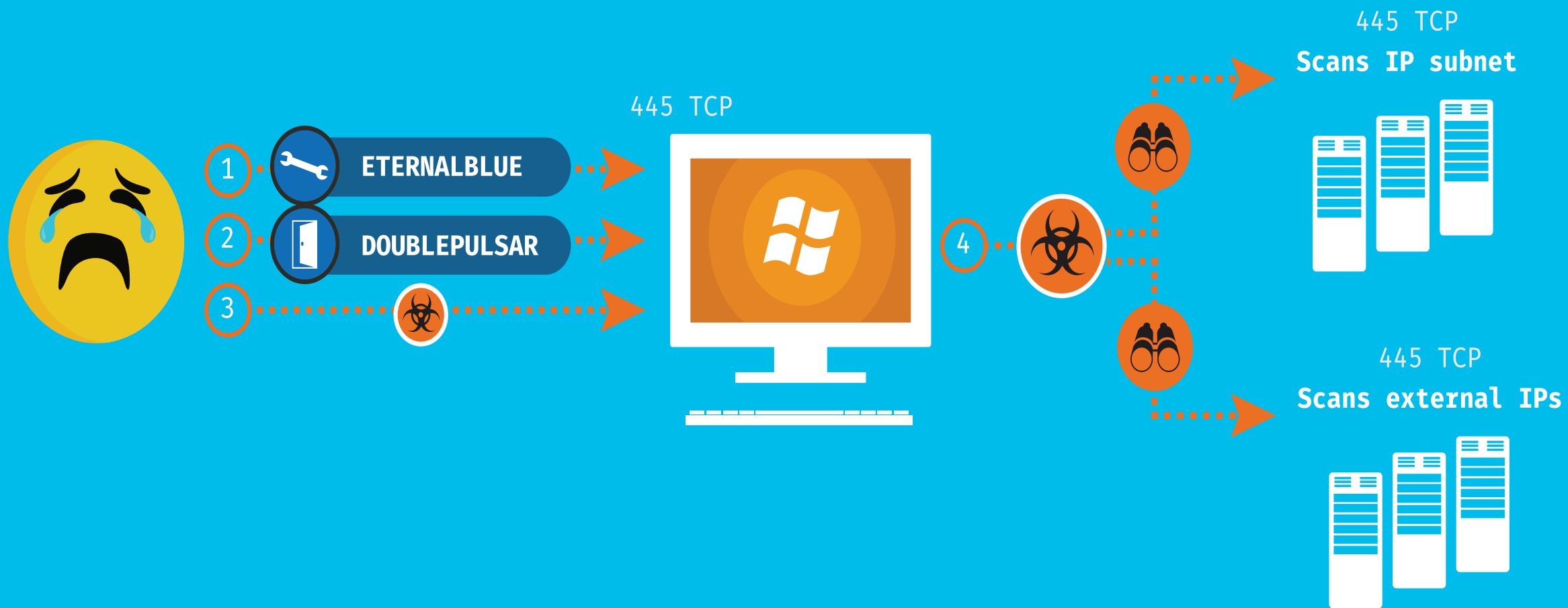
WannaCry шагает по планете – май 2017

Cisco Umbrella



[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



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

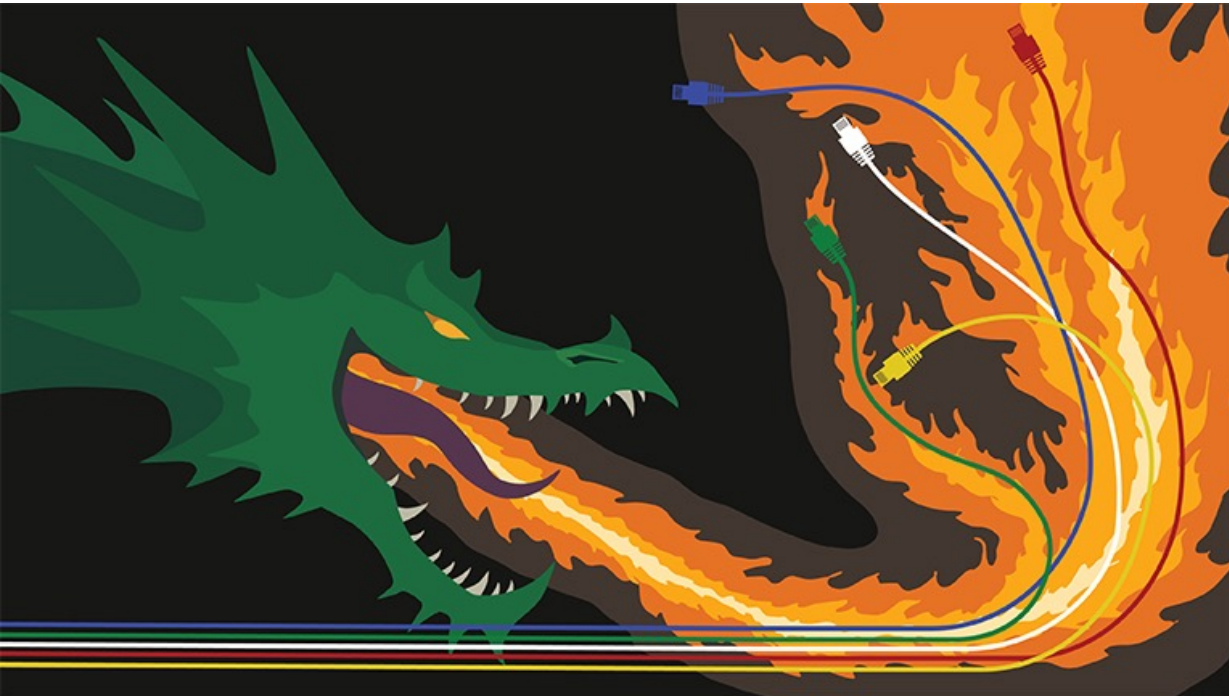
37-115-149-55.broadband.kyivstar.net
Windows 7 Ultimate 7601 Service Pack 1
Kyivstar GSM
 Added on 2017-11-13 21:07:05 GMT
 Ukraine, Chernihiv

[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

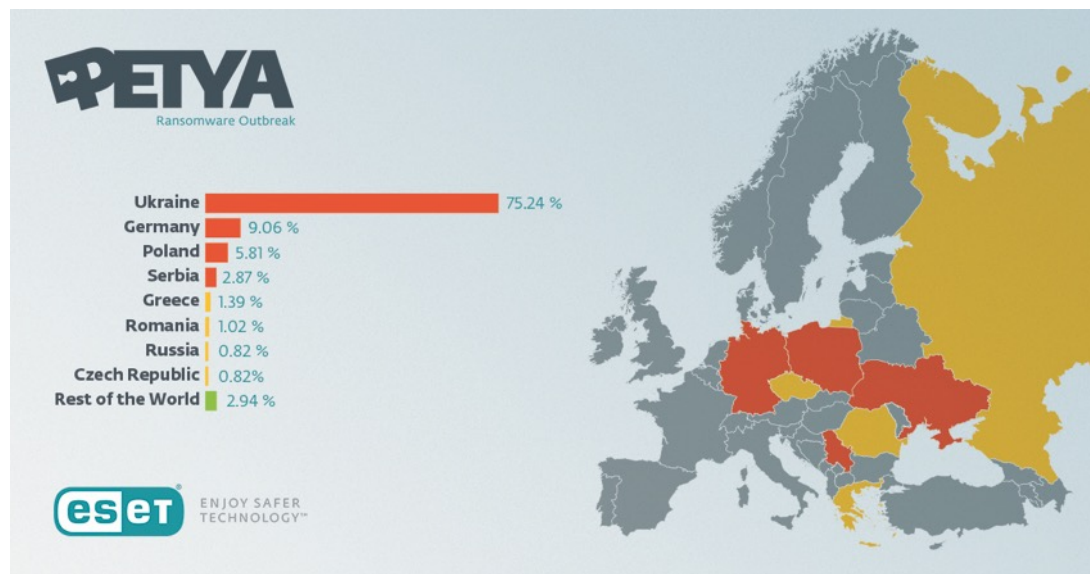


- Использовал доверенный канал бухгалтерского ПО для доставки в организации
- Использовал гибридную методологию распространения
- Шифровал файлы не с целью получения выкупа, а для нанесения урона

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

Neuyta/Petya: результаты атаки



- 1/3 банков пострадало в ходе атаки

Антон Кудин, Департамент безопасности НБУ

- До 10% корпоративных компьютеров было поражено
Дмитрий Шимкив

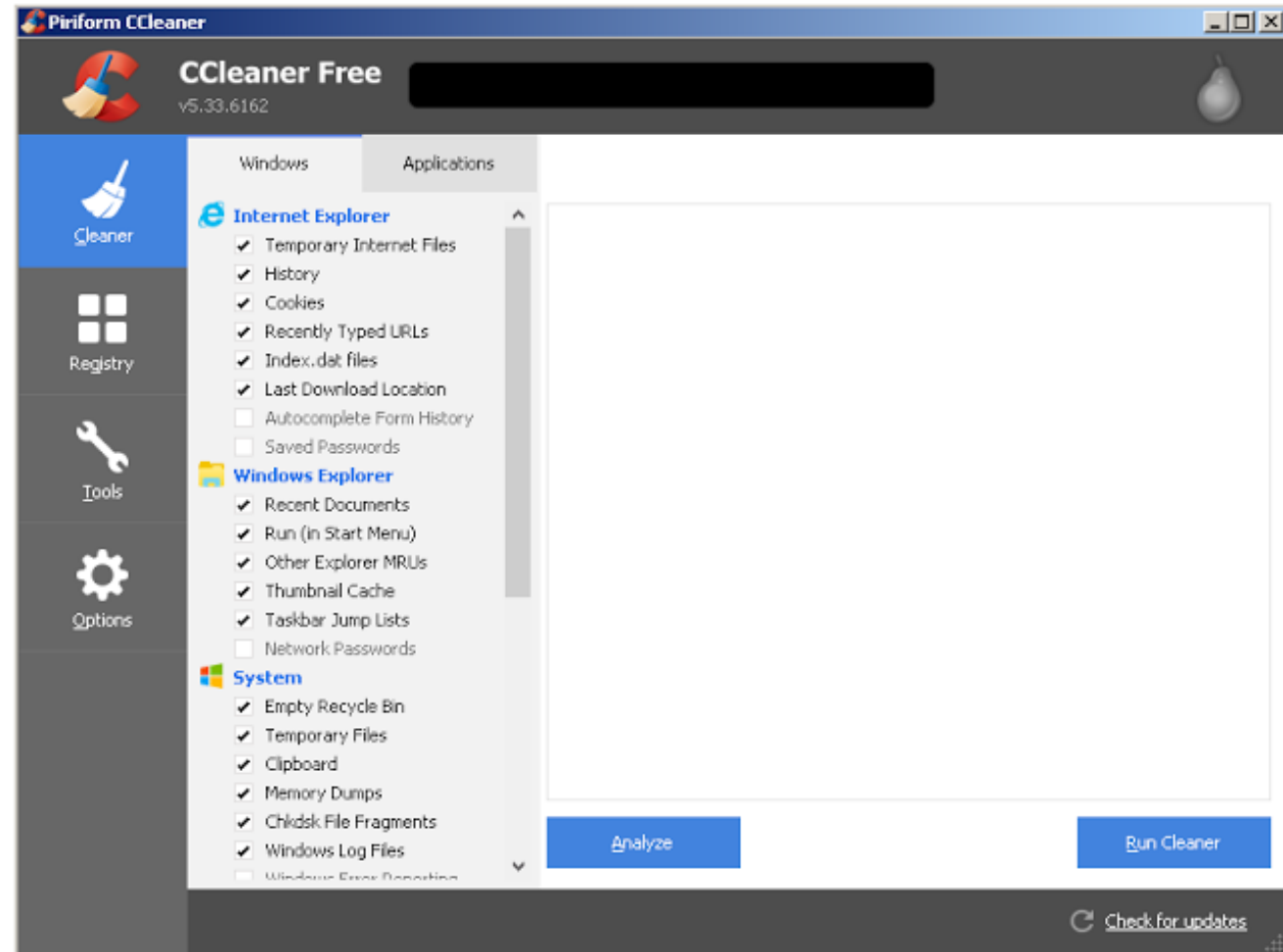
- Потери от Petya.A составили \$850 млн
Страховая компания Lloyd's

- Финансовые потери до 0.2 - 0.5% ВВП

Экспертная оценка

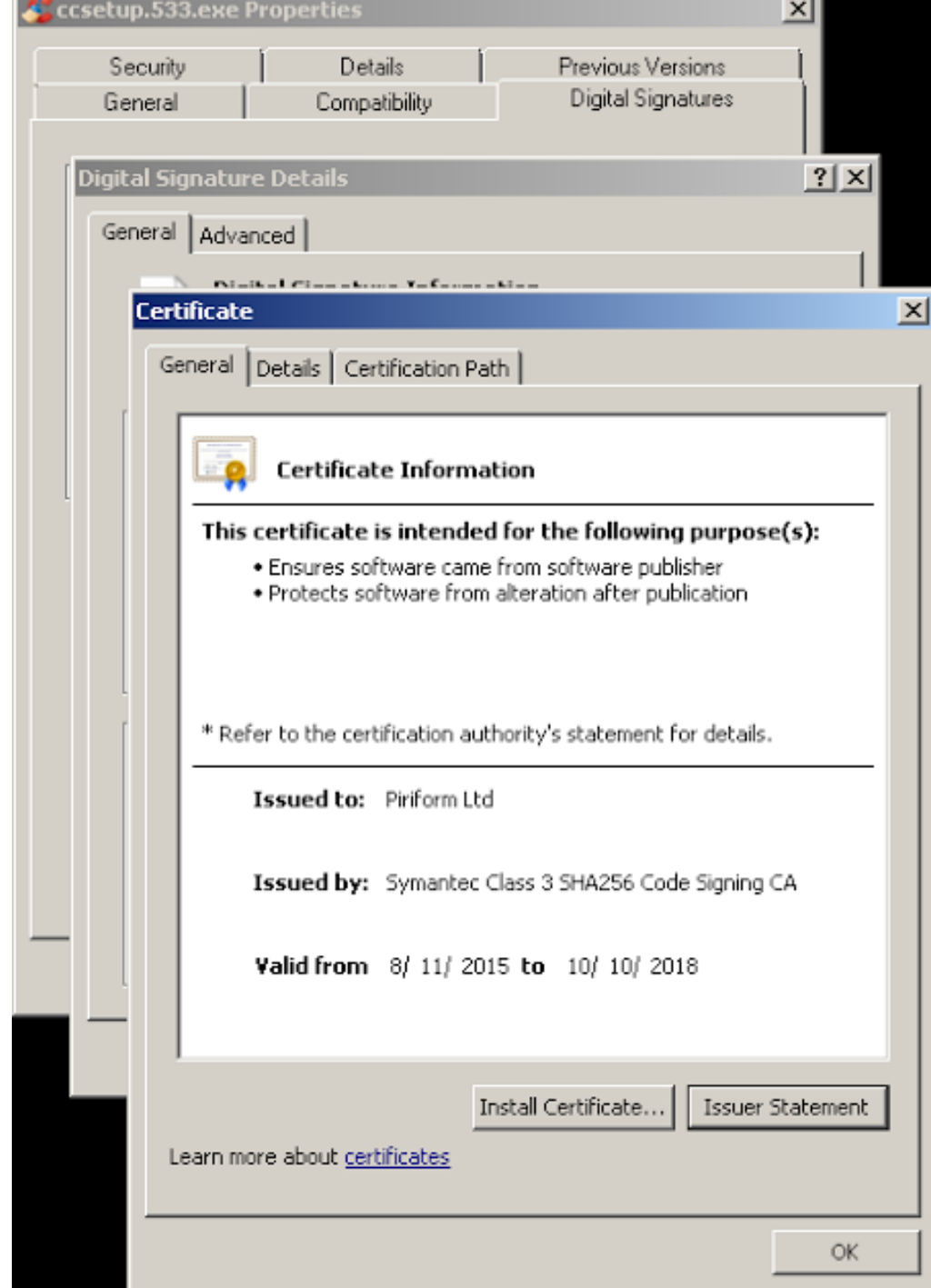
CCleaner

- 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»!

BAD RABBIT


If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.


Time left before the price goes up

41:02.
24

Price for decryption:

 = 0.05

Enter your personal key or your assigned bitcoin address.



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?

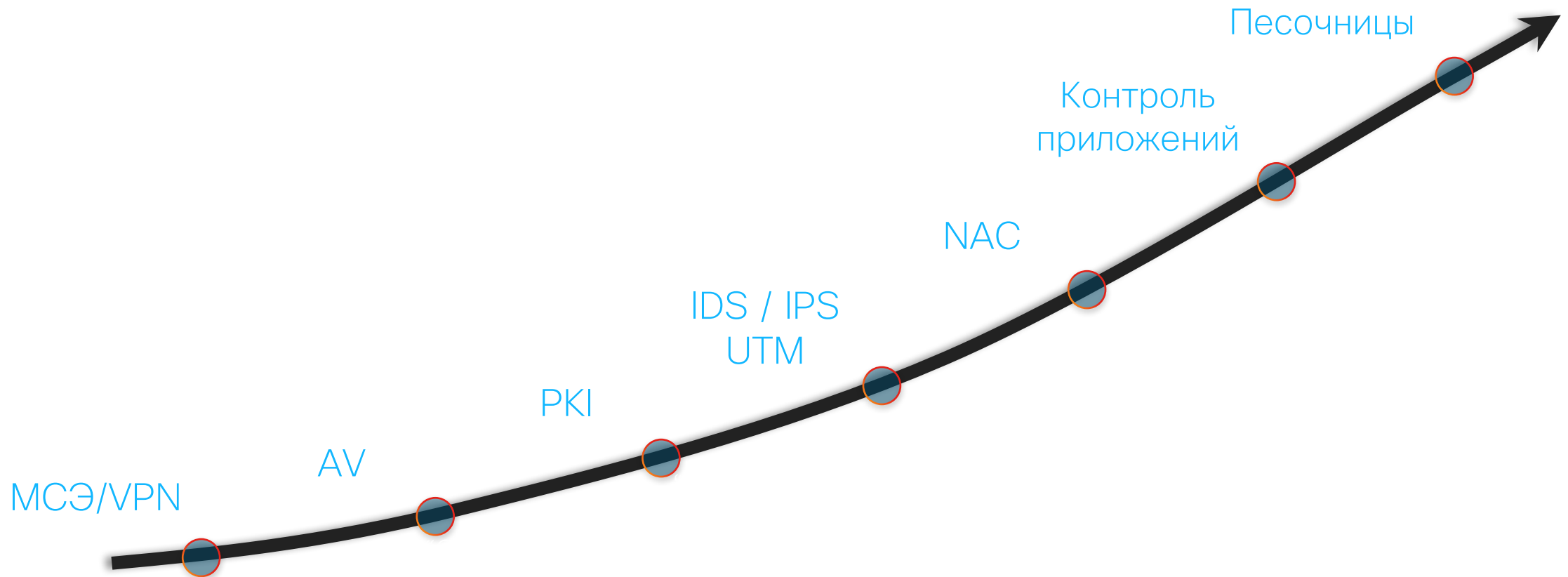


Точечные средства защиты оказались неэффективными



Организации с архитектурой безопасности 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



Ландшафт угроз

ДО

Контроль
Применение
Усиление

ВО ВРЕМЯ

Обнаружение
Блокирование
Защита

ПОСЛЕ

Видимость
Сдерживание
Устранение

Экономика

MCЭ

VPN

NGIPS / AMP

Advanced Malware Protection

NGFW

UTM

Web Security

Анализ поведения сети

NAC + Identity Services

Email Security

Реакция на инциденты

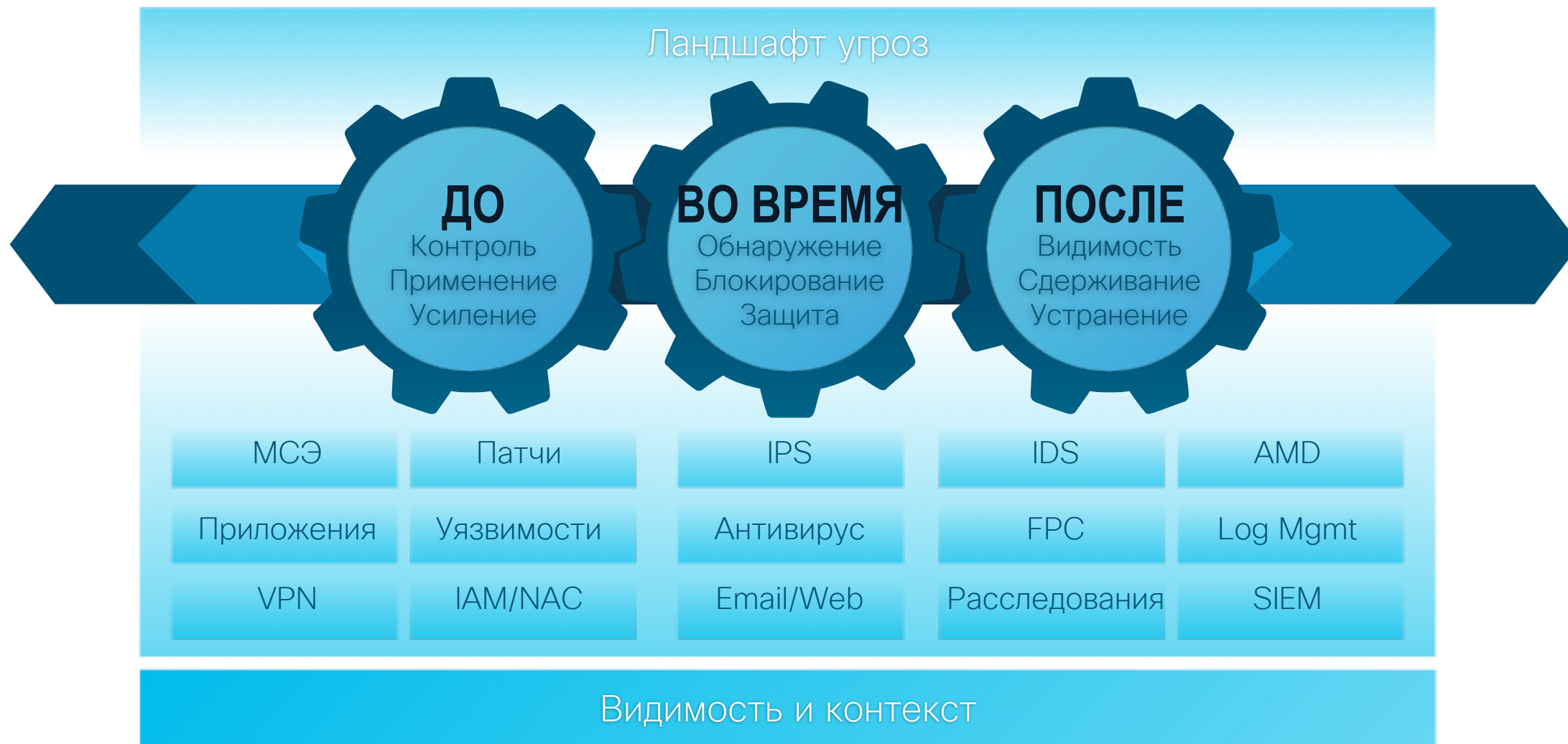
Соответствие
нормативным
требованиям

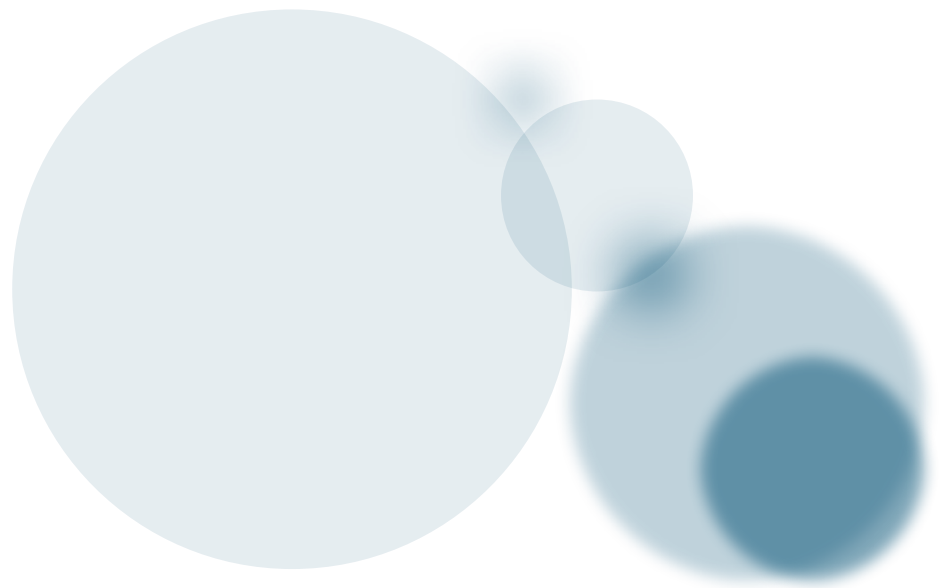
Видимость и контроль

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



От модели к технологиям





Фокус на угрозы

Проблемы с подходом «сделай сам»



Cisco SIO + Sourcefire VRT = Cisco Talos



1001 1110 011 0110011 101000
101000 0110 00 0111000 11
0000111000 001 1101 1110 1100110 11001110 1101 1001 0111



Коллективная информация безопасности Cisco

Обновления каждые 3-5 мин

Email Endpoints Web Networks IPS Devices

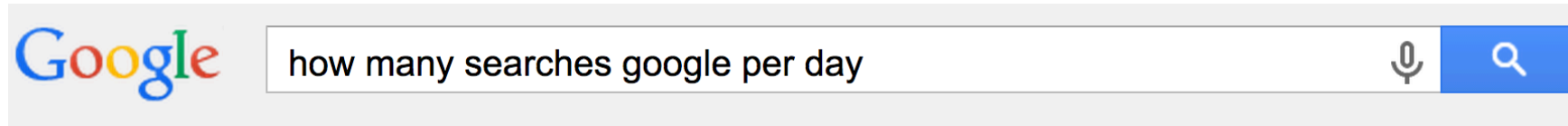
1.6 млн сенсоров
100 TB данных в день
150 million+ конечных точек
600+ инженеров, техников и исследователей

35% мирового почтового трафика
13 млрд web запросов
24x7x365 операций
40+ языков



180,000+ примеров файлов в день
FireAMP™ Community, 3+ млн
Advanced Microsoft и Industry Disclosures
Snort и ClamAV Open Source Communities
Honeypots
Sourcefire AEGIS™ Program
Частные и открытые Threat Feeds
Динамический анализ

Оцените масштаб охвата



Web News Videos Images Shopping More ▾ Search tools

About 14,600,000 results (0.49 seconds)

Google now processes over 40,000 search queries every second on average (visualize them here), which translates to over **3.5 billion searches** per day and **1.2 trillion searches** per year worldwide. The chart below shows the number of searches per year throughout Google's history:

[Google searches - Internet Live Stats](http://www.internetlivestats.com/google-search-statistics/)
www.internetlivestats.com/google-search-statistics/

Feedback



проживает
1арда 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



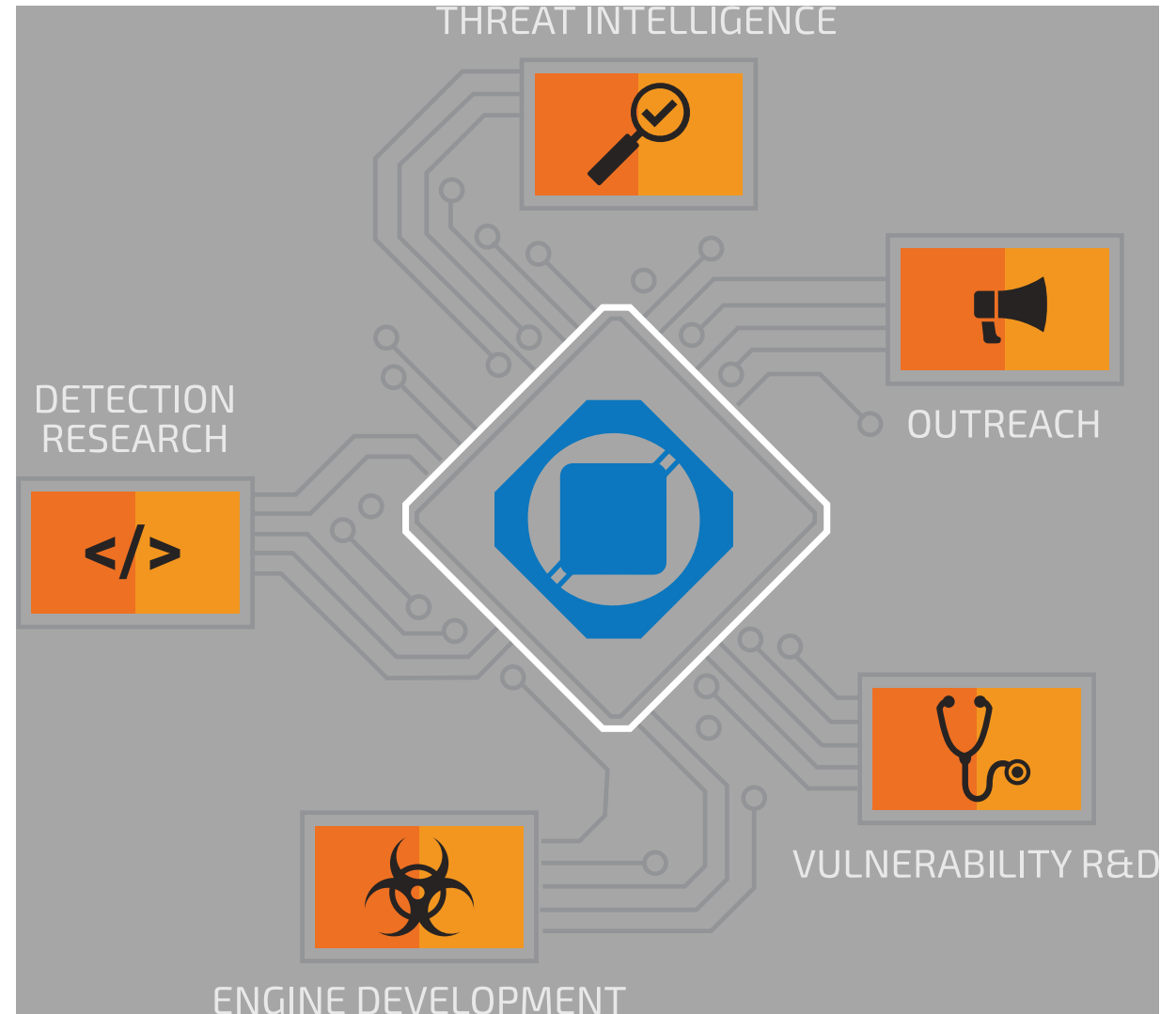
16 МЛРД

Web-запросов в день



600 МЛРД

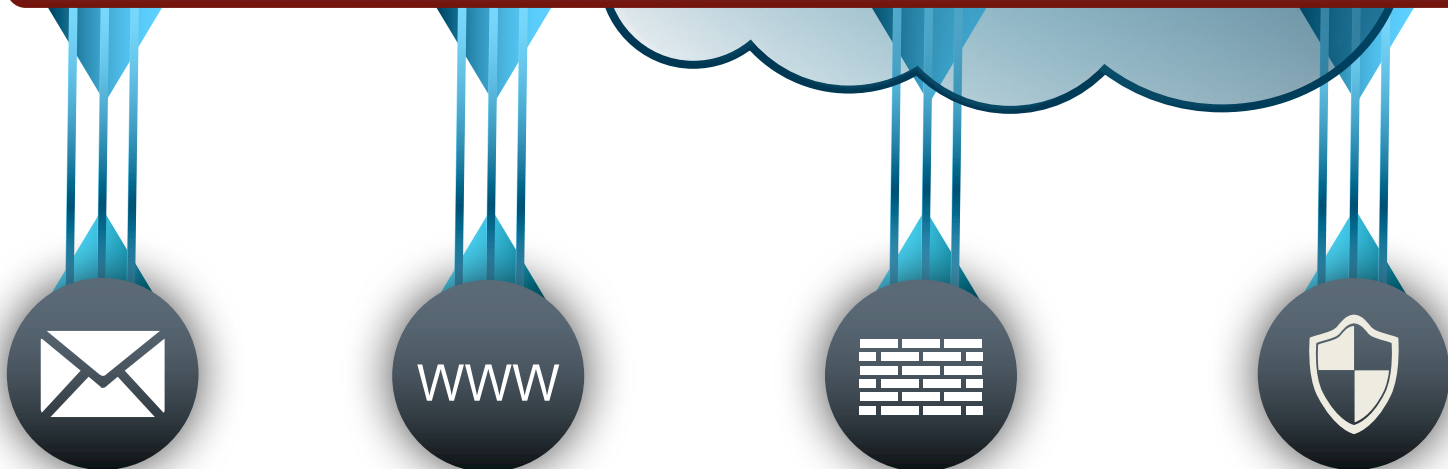
сообщений email в день



Мозг архитектуры безопасности Cisco

Репутация **Сигнатуры** Правила и логика для конкретных платформ

Cisco Talos



Действующее
соединение SMTP?
(ESA)

Ненадлежащий или
нежелательный
контент?
(ASA/WSA/CWS)

Место для
контроля и
управления?
(ASA/WSA)

Вредоносное
действие?
(ASA/IPS)



Черные списки
и репутация



Ловушки для
спама, ловушки
для хакеров,
интеллектуальные
анализаторы

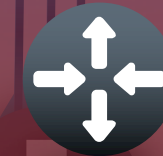


Регистрация
доменов

Сигнатуры



Проверка
контента



Партнерство
со сторонними
разработчиками



Исследование
угроз

Где увидеть исследования Cisco Talos?

The screenshot shows the Talos website homepage. The top navigation bar includes links for SOFTWARE, COMMUNITY, VULNERABILITY REPORTS, ADDITIONAL RESOURCES, TALOS, ABOUT TALOS, JOIN OUR TEAM, CONTACT US, and BLOG. The main content area features a large graphic with the text "We Keep Your Network Safe." and a sub-headline "TALOS BLOG". Below this, there is a featured article titled "INTRODUCING ROKRAT" dated APRIL 3, 2017 6:01 PM by PAUL RASCAGNERES. The article text states: "This blog was authored by Warren Mercer and Paul Rascagneres with contributions from Matthew Molyett." Below the article is an "EXECUTIVE SUMMARY" section that begins with "A few weeks ago, Talos published research on a Korean MailDoc. As we previously discussed this actor is quick to cover their tracks and very quickly cleaned up their compromised hosts. We believe the compromised infrastructure was live for a mere matter of hours during any campaign. We identified a new campaign, again leveraging a malicious Hangul Word Processor (HWP) document. After analyzing the final payload, we determined the winner was... a Remote Administration Tool, which we have named ROKRAT." At the bottom of the article, it says "Like in the p..."

<http://www.talosintelligence.com>

The screenshot shows the Cisco Blogs website. The top navigation bar includes the Cisco logo, "Cisco Blogs", a search bar, and a "Log In to Cisco.com" button. Below the navigation bar, there are several article listings. The first article is titled "Threat Spotlight: Sundown Matures" by TALOS Talos Group, dated March 31, 2017, with 0 Comments. The article text states: "This post authored by Nick Biasini with contributions from Edmund Brumaghin and Alex Chiu. The last time Talos discussed Sundown it was an exploit kit in transition. Several of the large exploit kits had left the landscape and a couple of strong contenders remain. Sundown was one of the kits still active and poised to make a move, but lacked a lot of the sophistication of the other large kits and had lots of easy identifiers throughout its infection chain. Most of these identifiers have been stripped, new exploits added, and Talos was able to uncover an interesting campaign focused around the bulk purchase of expiring domains through auctions commonly held within the domain resellers market." Below the article is a "Read More>>" link. The second article is titled "Vulnerability Spotlight: Certificate Validation Flaw in Apple macOS and iOS Identified and Patched" by TALOS Talos Group, dated March 27, 2017, with 0 Comments. The article text states: "Most people don't give much thought to what happens when you connect to your bank's website or log in to your email account. For most people, securely connecting to a website seems as simple as checking to make sure the little padlock in the address bar is present. However, in the background there are many different steps that are taken to ensure you are safely and securely connecting to the..."

<http://blogs.cisco.com/talos>

«Продукты» Cisco Talos



Разведка



ПК



Сеть



Облака



Email



Web



Open Source



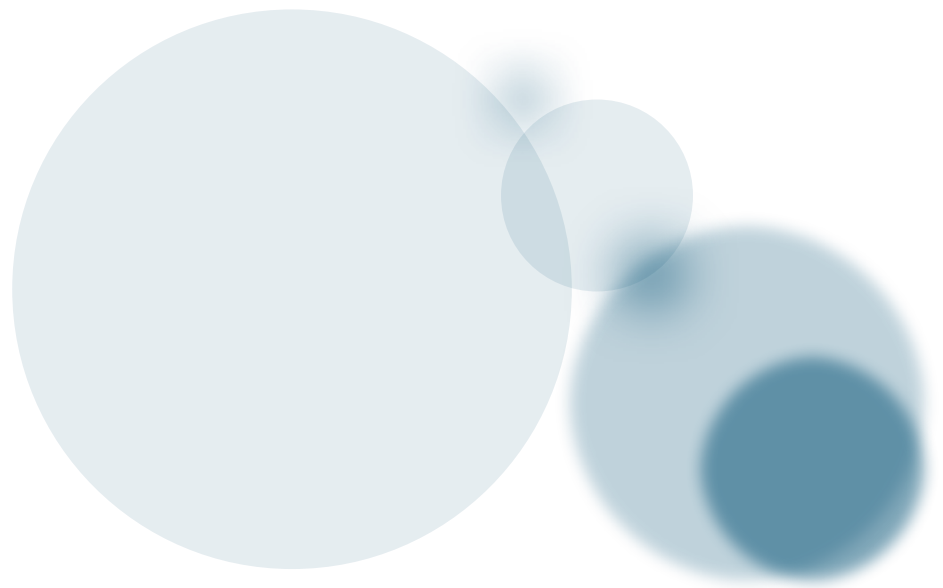
Услуги

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

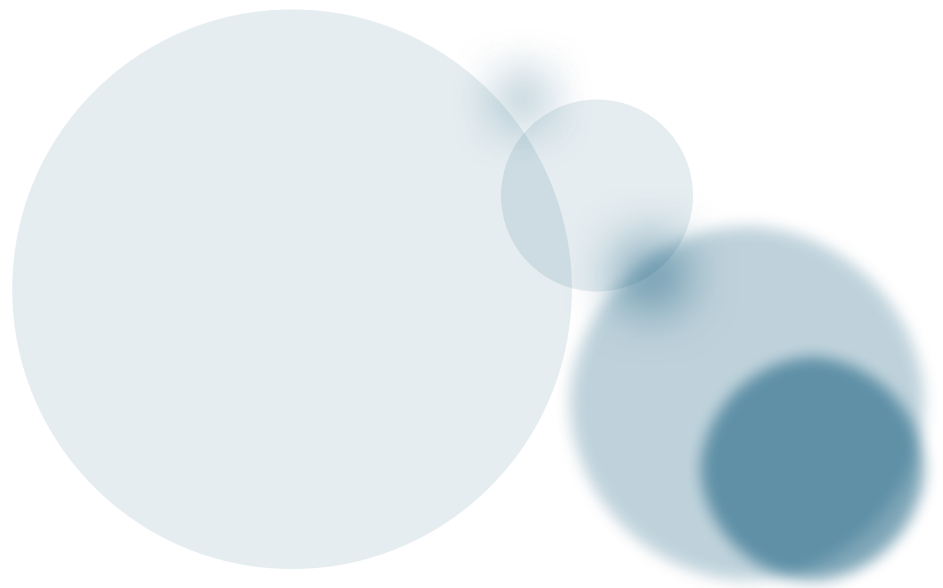
Cloud & End Point IOCs	Cloud & End Point IOCs	Policy & Control	URL, Domain, IP Reputation	Email Reputation	URL, Domain, IP Reputation	Vulnerability Protection	Cloud & End Point IOCs
Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware Protection	Malware 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)

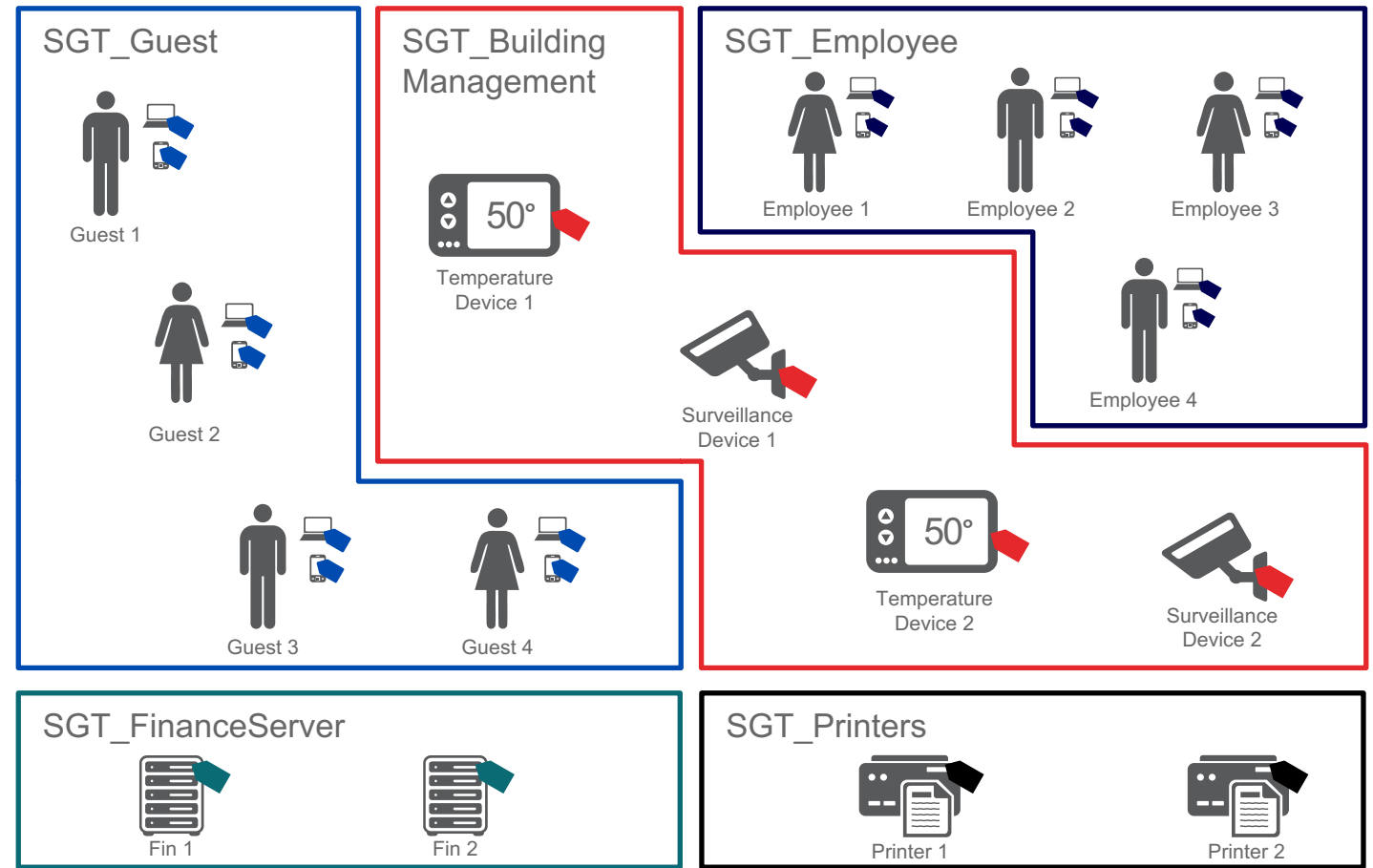
Платформа Cisco Identity Services Engine (ISE)

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?

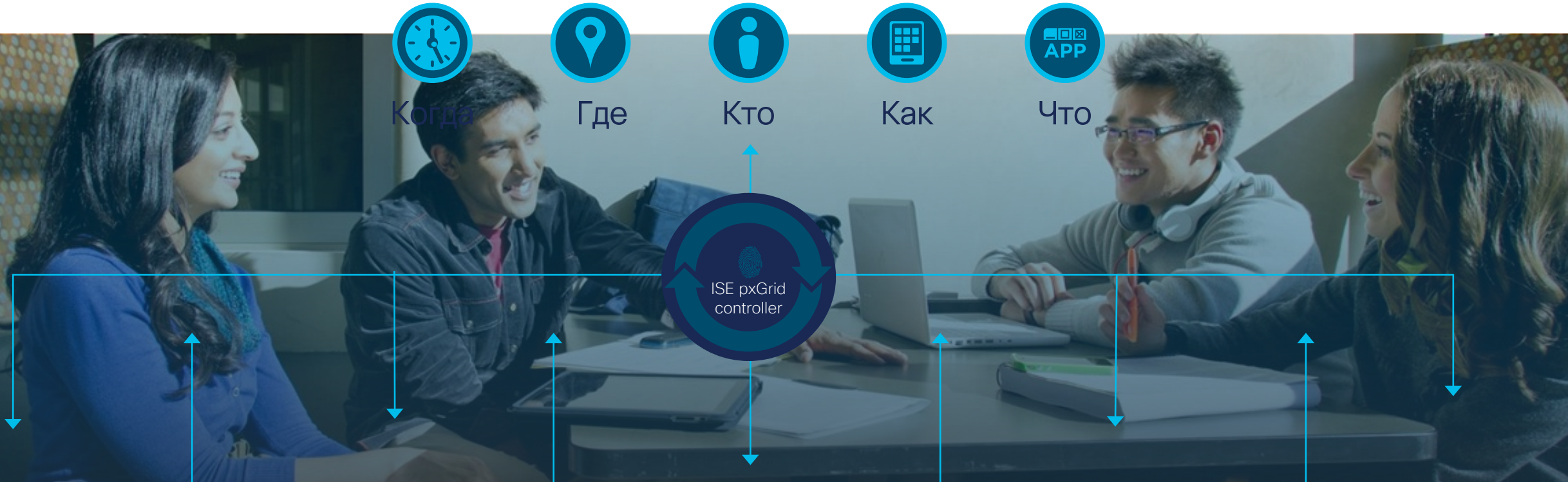
“Адрес скомпрометированного устройства 192.168.100.123”
– ИЛИ –

“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

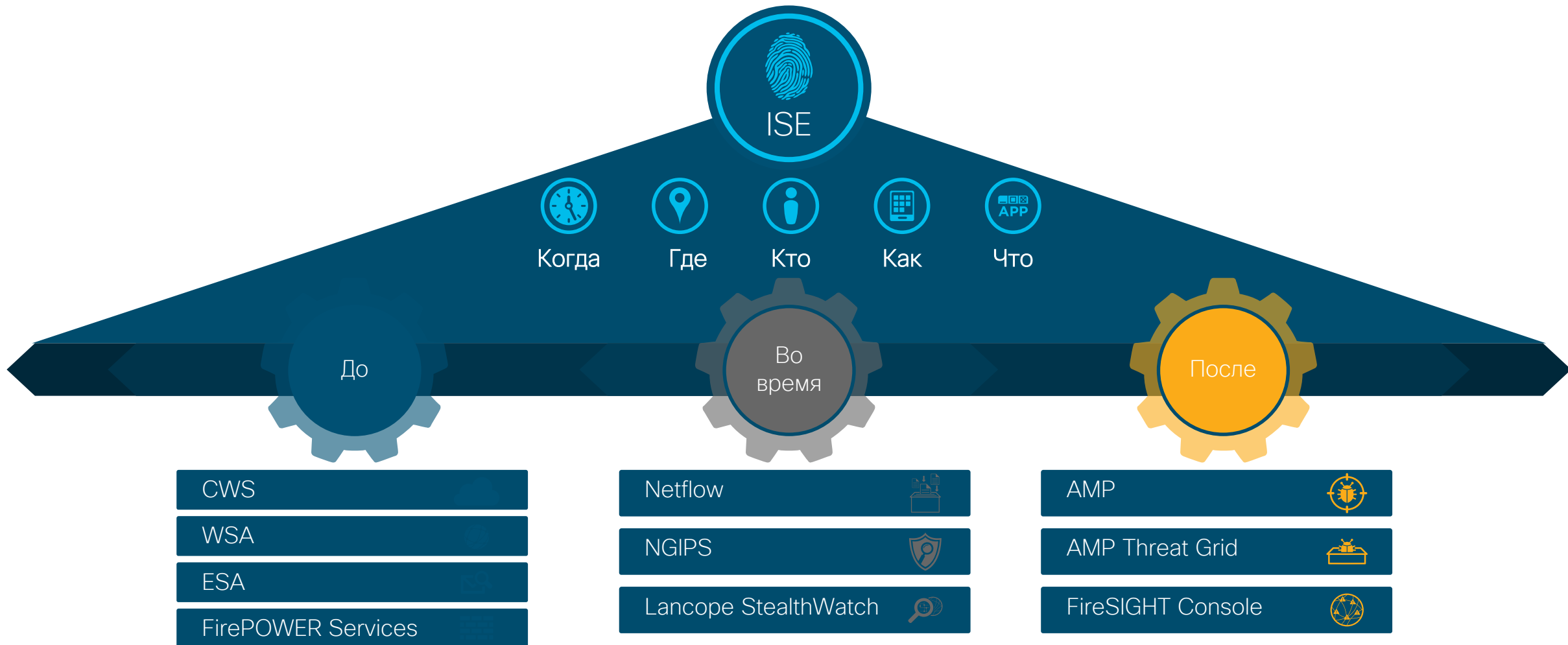
PCAP

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

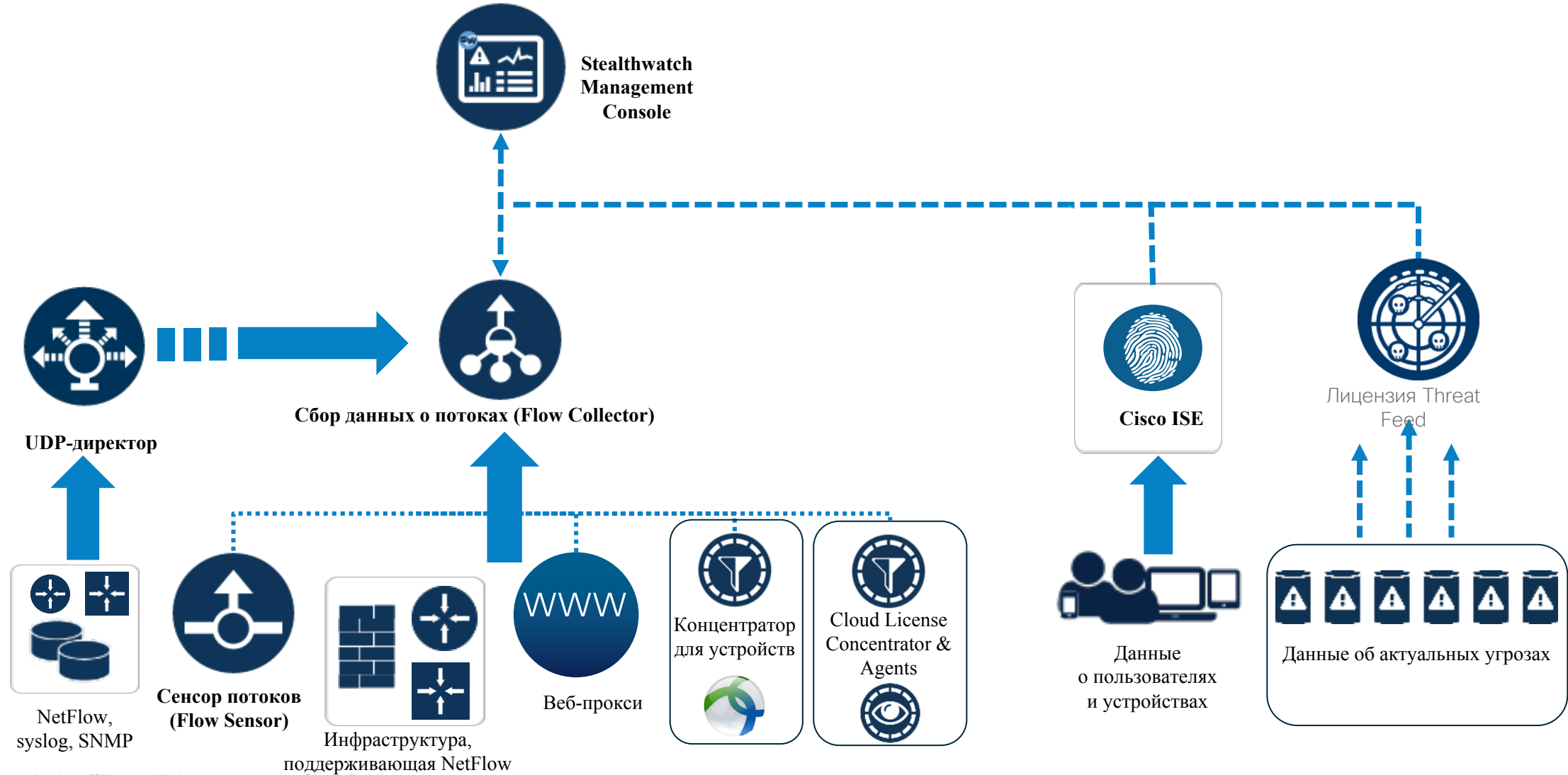
Политика и сегментация

Обнаружение аномалий (NBAD)

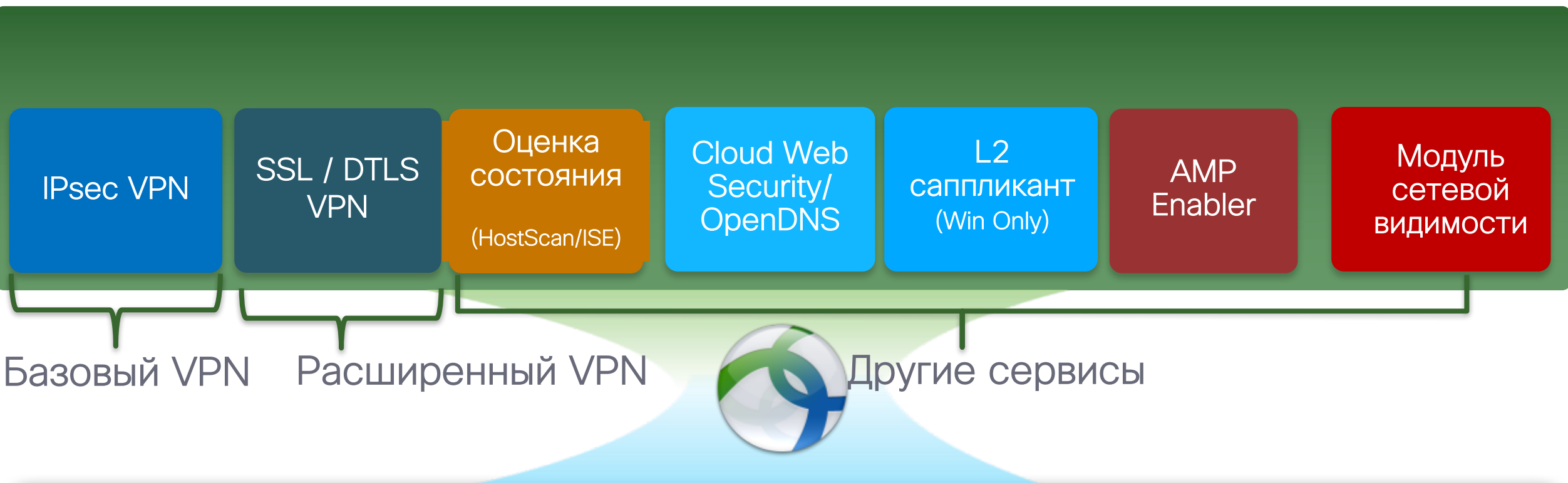
Лучшее понимание/ реакция на IoC

Сбор данных обо всех взаимодействиях, хорошая база для расследований

Компоненты системы Stealthwatch



AnyConnect – больше чем просто VPN



Центральные устройства



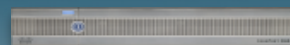
Коммутаторы и контроллеры WLC



ISE/ACS



ASA



WSA



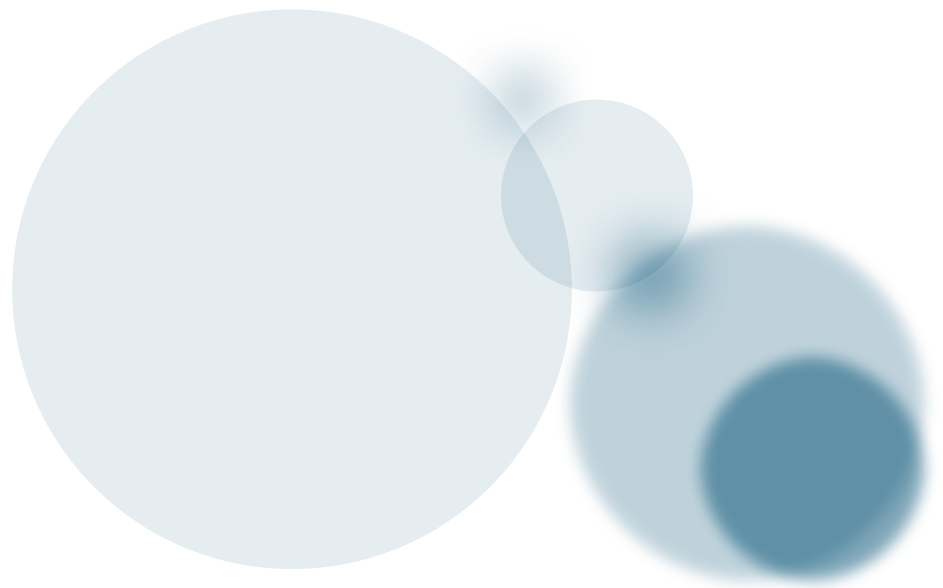
Cloud Web Security + AMP



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



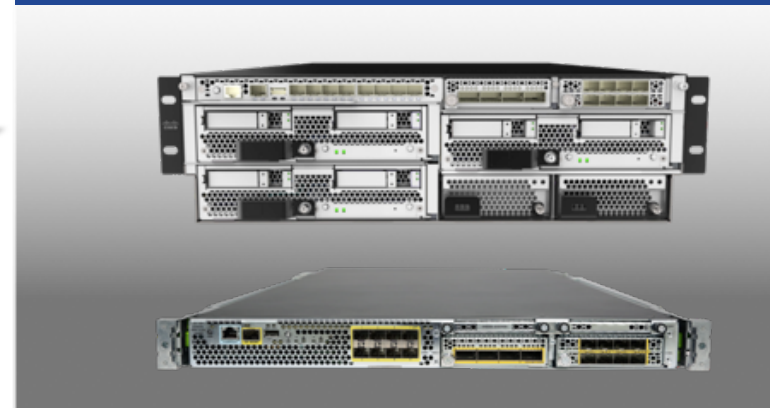
250 Мбит/с -> 1,75 Гбит/с
(сервисы NGFW + IPS)

Firepower серии 2100



2 Гбит/с -> 8 Гбит/с
(сервисы NGFW + IPS)

Firepower серии 4100
и Firepower 9300



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

Editing Rule - URL Allow

Name: URL Allow Enabled [Move](#)

Action: Allow **IPS:** no policies **Variables:** n/a **Files:** MalwarePolicy

Zones Networks VLAN Tags **Users** Applications Ports **URLs** ISE Attributes

Categories and URLs [Reputations](#)

Search for a URL

Category	URLs
<input checked="" type="checkbox"/> Global Blacklist for URL	
<input checked="" type="checkbox"/> Global Whitelist for URL	
<input type="checkbox"/> URL Attackers	
<input type="checkbox"/> URL Bogon	
<input type="checkbox"/> URL Bots	
<input type="checkbox"/> URL CnC	
<input type="checkbox"/> URL Malware	
<input type="checkbox"/> URL Open_proxy	
<input type="checkbox"/> URL Open_relay	

Reputations

- Any
- 5 - Well Known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High Risk

Add to

Категории
URL-SI

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

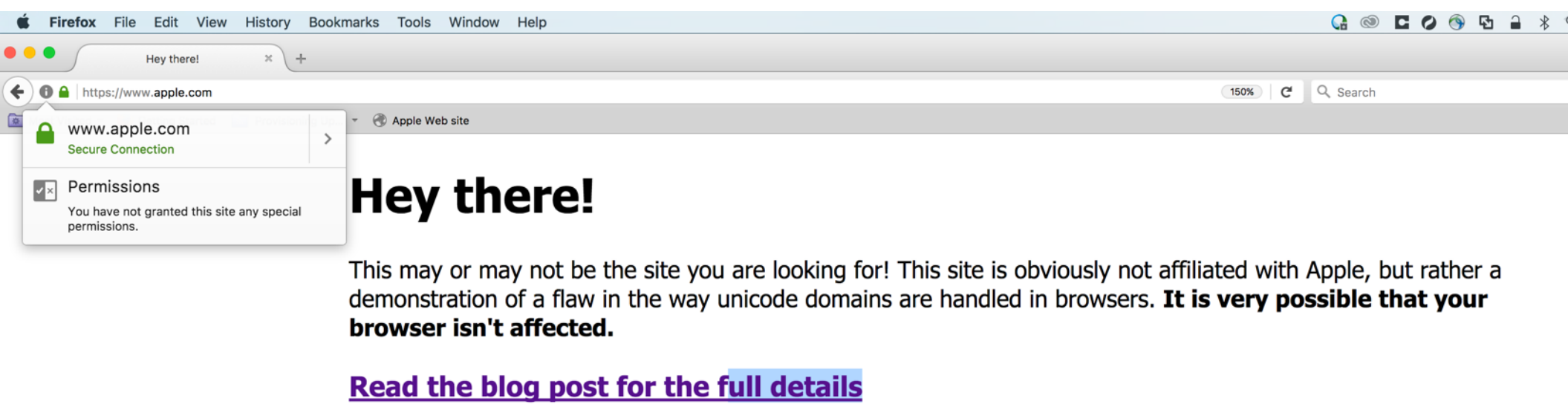
#	Name	DNS Lists	Action
Whitelist			
1	Global DNS Whitelist	Global Whitelist for DNS	Whitelist
Blacklist			
2	Global DNS Blacklist	Global Blacklist for DNS	Domain Not Found
3	DNS Drop	DNS Spam DNS_DROP	Drop
4	DNS Monitor	DNS Bots DNS Tor_exit_node DNS_MONITOR	Monitor
5	DNS Nxdomain	DNS Open_proxy DNS_NXDOMAIN	Domain Not Found
6	DNS Sinkhole	DNS Attackers DNS CnC DNS Malware DNS Phishing (2 more...)	Sinkhole

Список Действие

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?



The screenshot shows a Firefox browser window with the address bar displaying 'https://www.apple.com'. A security warning is visible in the address bar area, indicating a 'Secure Connection'. A permissions dialog box is open, showing 'Permissions' for the site, with a note that no special permissions have been granted. The main content of the page reads: 'Hey there! This may or may not be the site you are looking for! This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.** [Read the blog post for the full details](#)'



Всё для людей...

Certificate Viewer: "www.xn--80ak6aa92e.com"

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.xn--80ak6aa92e.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	03:F8:5A:31:59:0C:6B:25:45:AC:7B:3F:46:F6:66:5C:C3:50

Issued By

Common Name (CN)	Let's Encrypt Authority X3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	April 17, 2017
Expires On	July 16, 2017

Fingerprints

SHA-256 Fingerprint	F3:0C:06:1F:BA:FB:81:7F:F3:C7:8D:D8:48:A8:26:6A: 68:21:E2:B4:CA:F9:ED:D6:AA:CC:E3:06:A8:C0:C8:44
SHA1 Fingerprint	E3:D1:8B:D0:A8:D3:2A:CA:5F:9C:24:0F:38:CF:63:4A:C7:A2:85:E2

Close

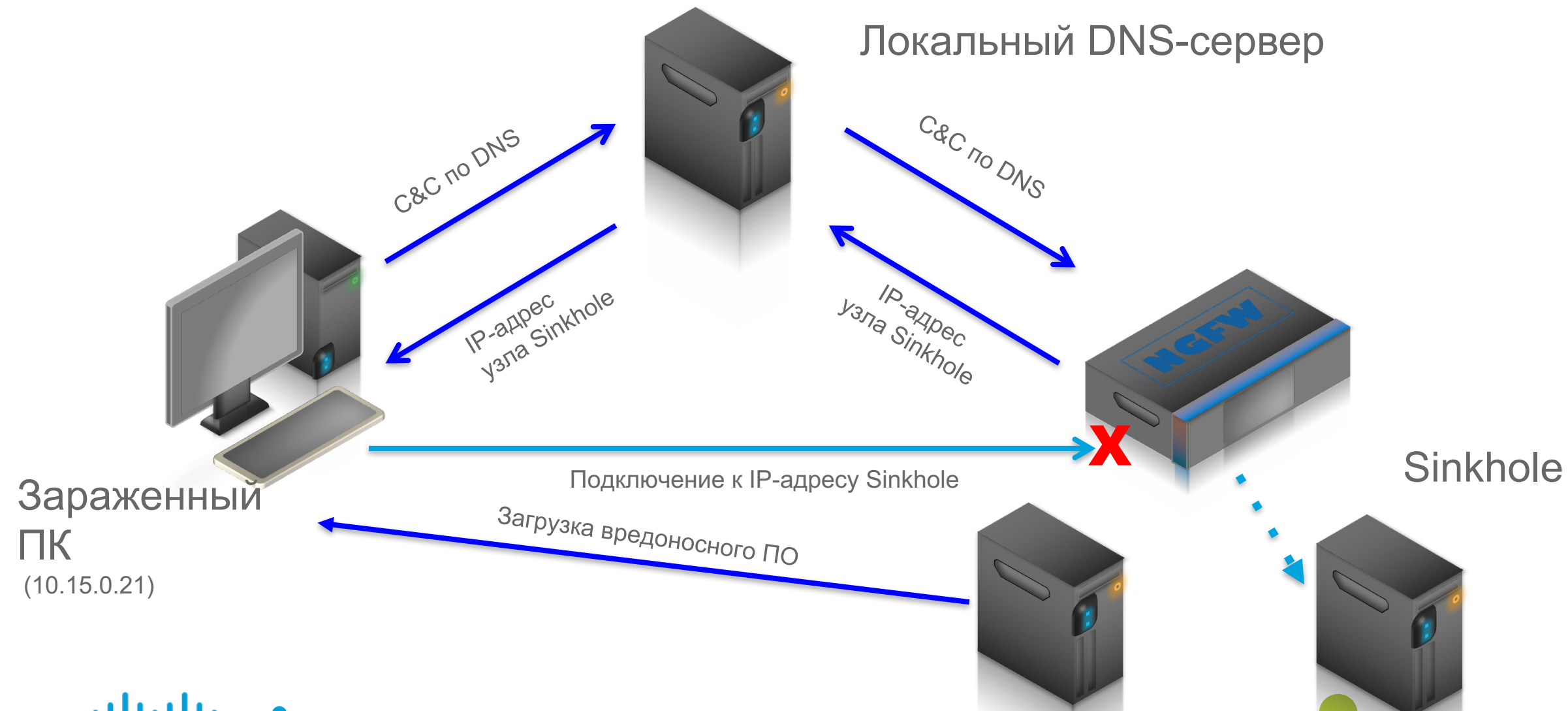
Действие DNS Sinkhole

Политика NGFW

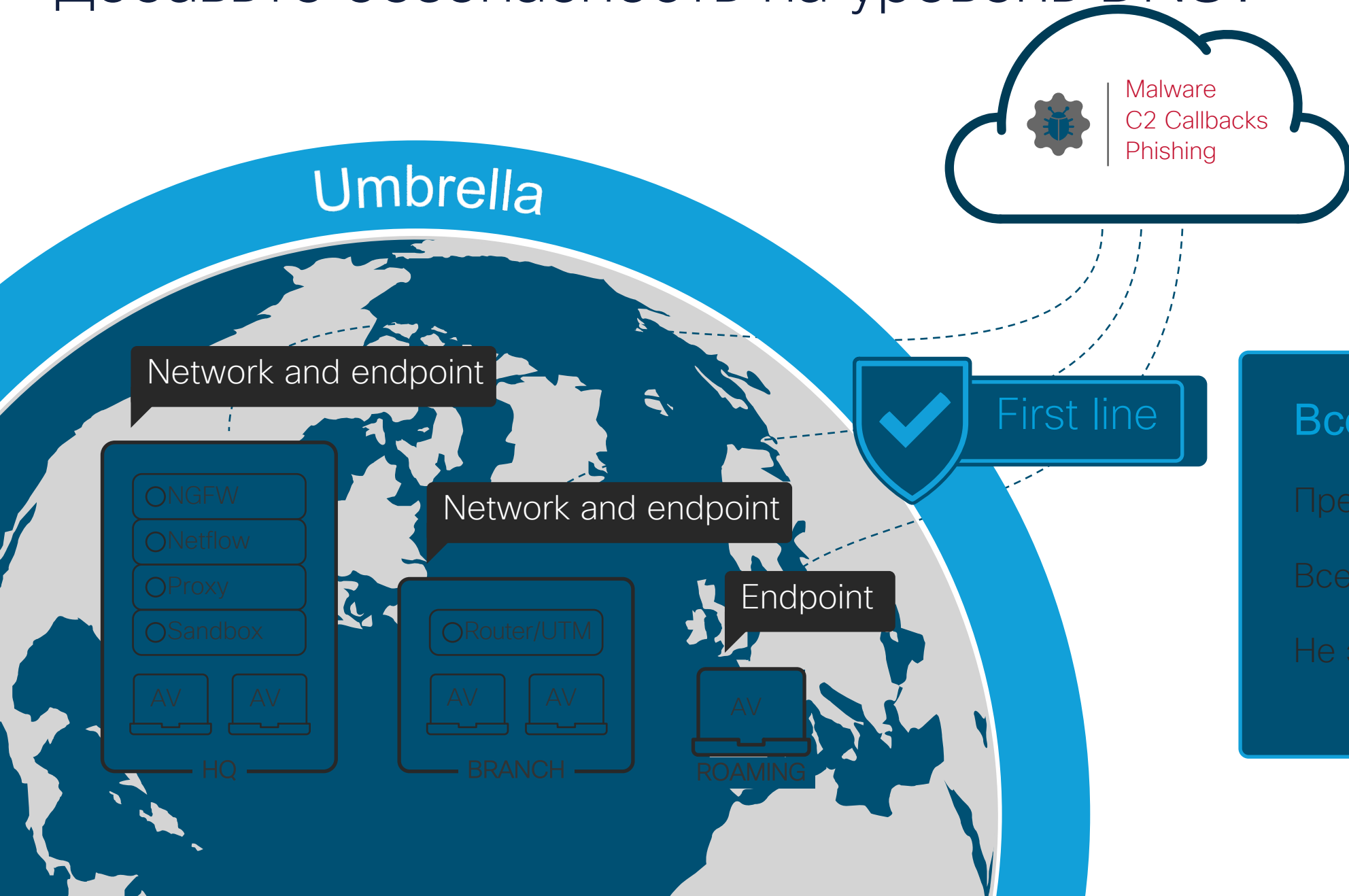
DNS SI: серверы C&C

Действие: DNS Sinkhole

Создание событий SI и IoC



Добавьте безопасность на уровень DNS?



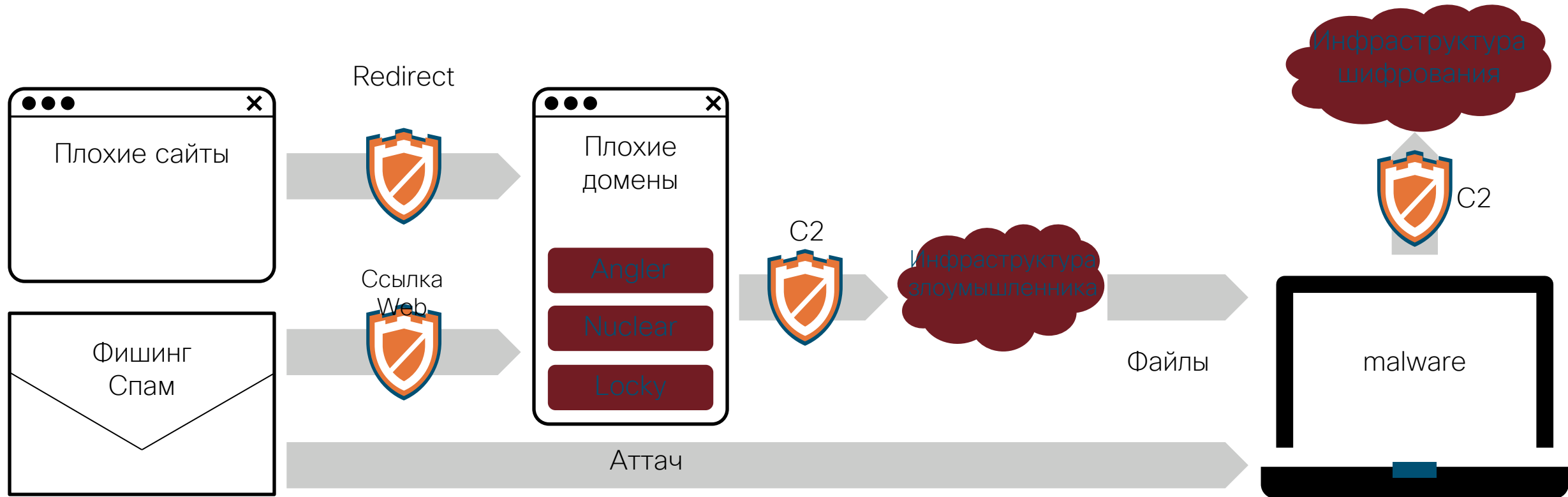
Все начинается с DNS

Предваряет IP подключение

Все устройства

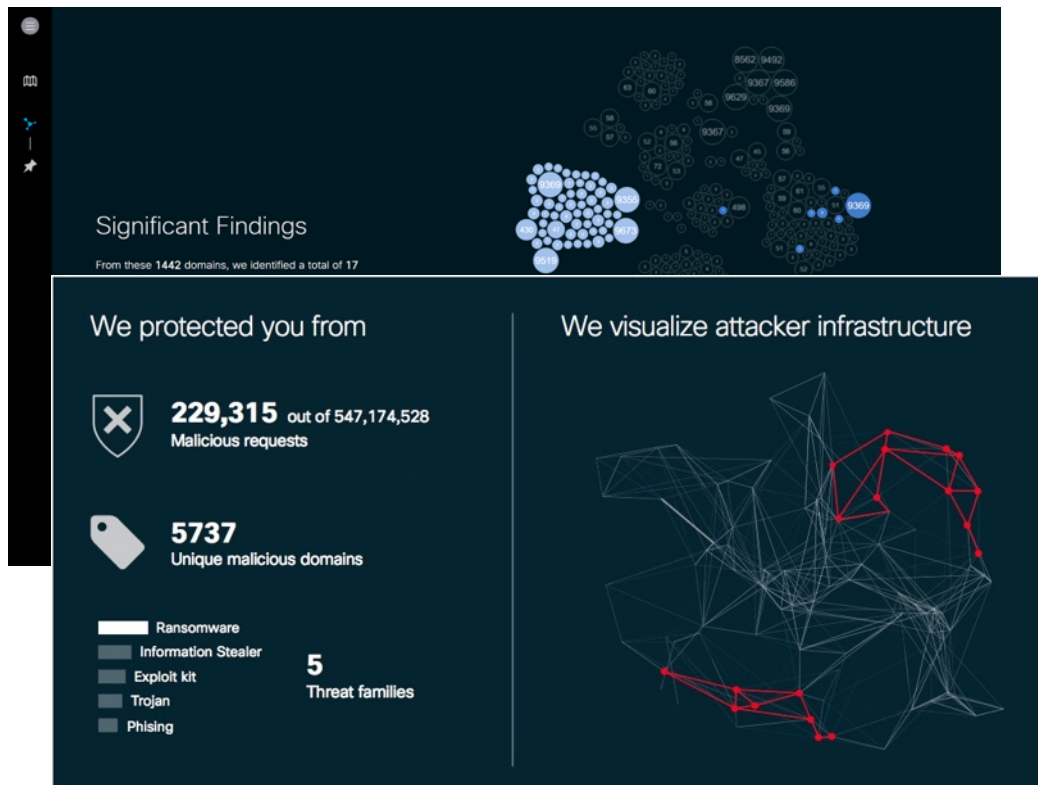
Не зависит от порта

OpenDNS/Umbrella предотвращает заражение и распространение вредоносного кода

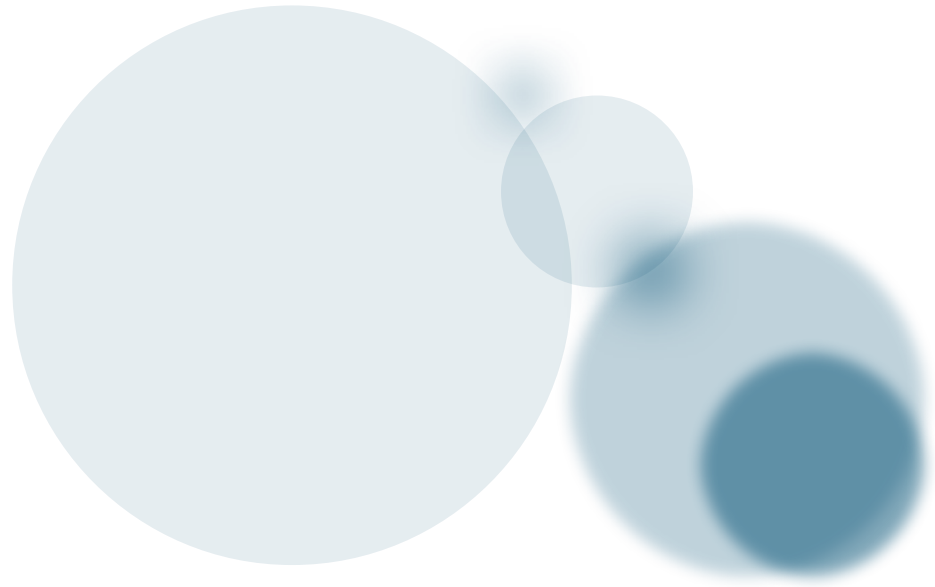


Заблокировано
Cisco Umbrella. (DNS
безопасность)

Самая простая система безопасности в мире!

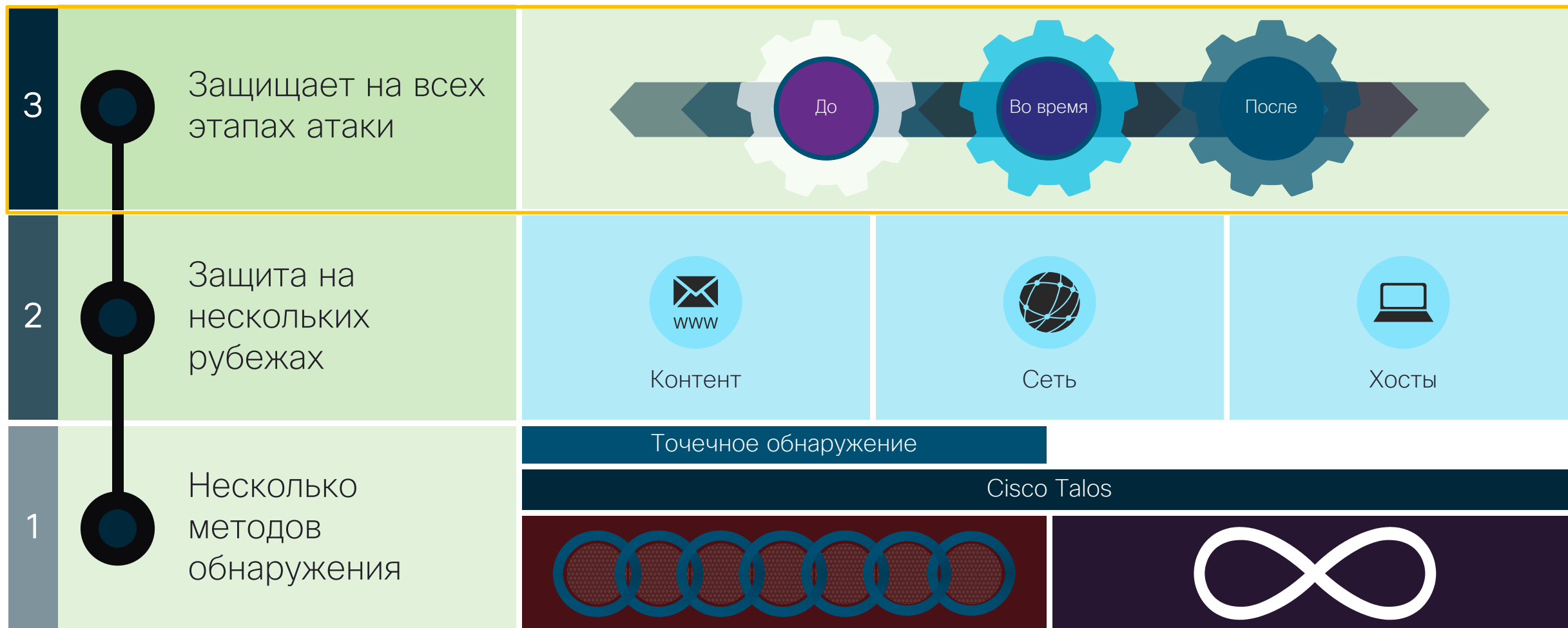


1. Добавьте в ваши DNS сервера Forwarders:
 - 208.67.222.222
 - 208.67.220.220
 2. Зарегистрируйтесь
 3. Добавьте адрес вашей сети для безопасности и мониторинга
 4. Попросите сделать отчет
 5. **Можете продолжать использовать сервис и после окончания тестирования/срока действия лицензии!**
- Есть бесплатная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



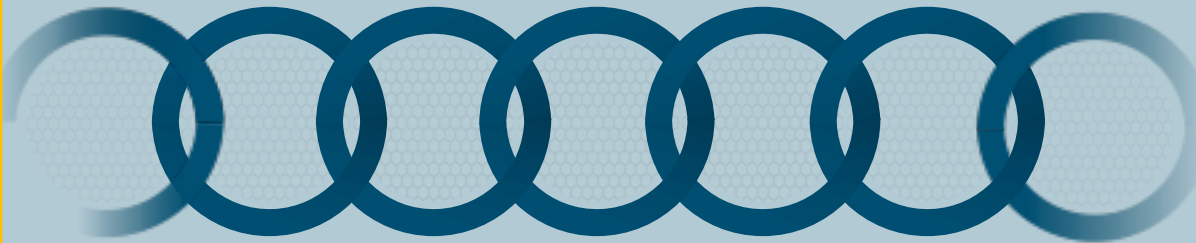
Платформа Cisco AMP

Cisco AMP предоставляет три выгоды



В Cisco AMP реализованы план А и план Б

Точечное обнаружение



Репутация и поведенческий анализ

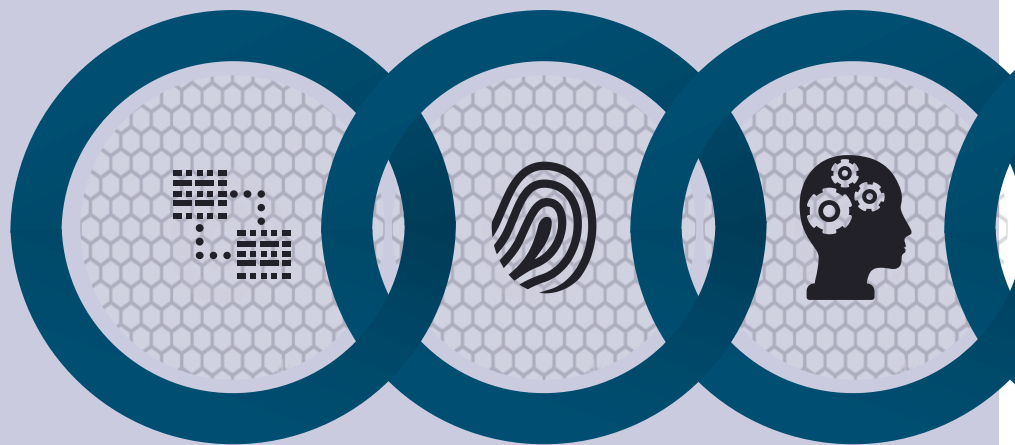
Ретроспективная безопасность



Постоянная защита

Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

Фильтрация по репутации

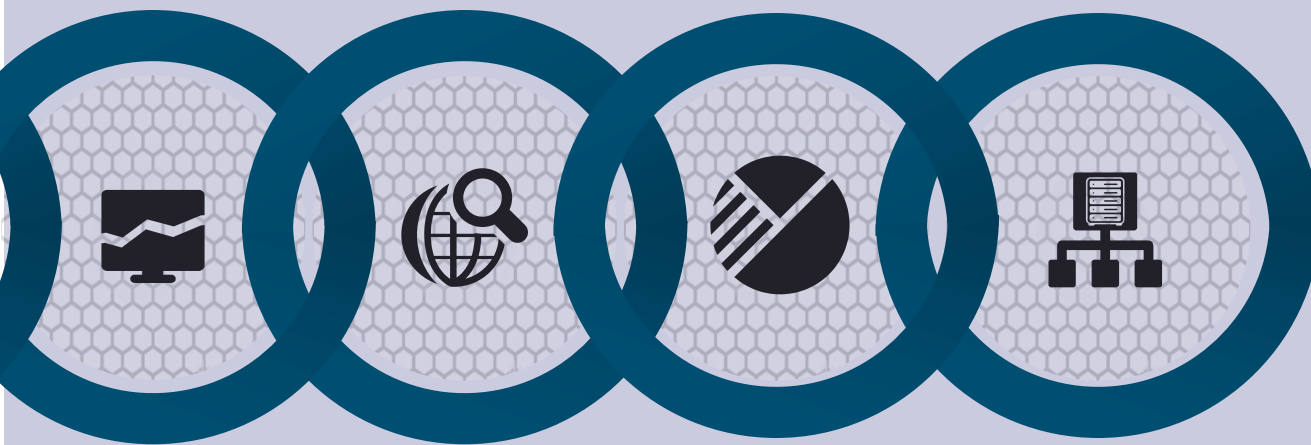


Идентичная
сигнатура

Нечеткие
идентифицирующие
метки

Машинное
обучение

Поведенческое обнаружение



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

Method	Server IP	Server Port	Resp. Content
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html
POST	195.20.34.1	80	text/html

DNS Traffic

Query Type: A, Query Data: alexrpi.tk

TTL: - Timestamp: +101.195s

Query ID	Timestamp	Type	Data
28943	+101.29s	A	alexrpi.tk
28943	+101.29s	A	alexrpi.tk

Nameserver Records

Data	Name
b	tk
c	tk
a.ns	tk
d	tk

IP Reverse Lookup	lgmp.mcast.net
IP ASN	-
IP Geo Location	-

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\IP3P\History	1148 (Explorer.EXE)	ENUMERATE_SUB_KEYS, CREATE_SUB_KEY	REG_OPTION_NON_VOLATILE

Modified Keys

Deleted Key Values

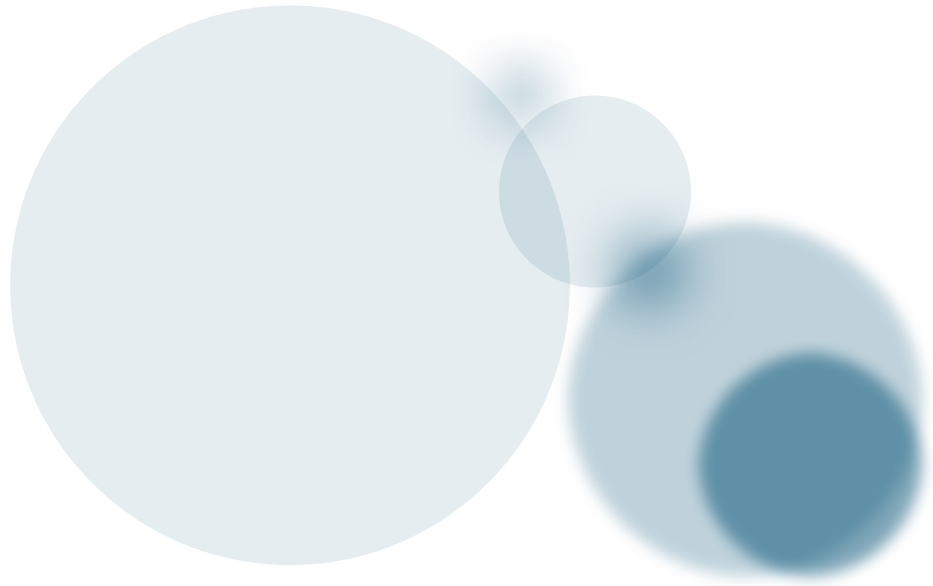
Filesystem Activity

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

Processes

Name: 15e65a21af32dd3b5fe65da4807be21e.exe	PID: 1100	Children: 1	File Actions: 3	Registry Actions: 2	Analysis Reason: Started At Current Directory Image Base Address Window Title Shell Info Desktop Info
Name: lsass.exe	PID: 1600	Children: 0	File Actions: 3	Registry Actions: 0	Analysis Reason: Started At Current Directory Image Base Address Window Title Shell Info Desktop Info

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



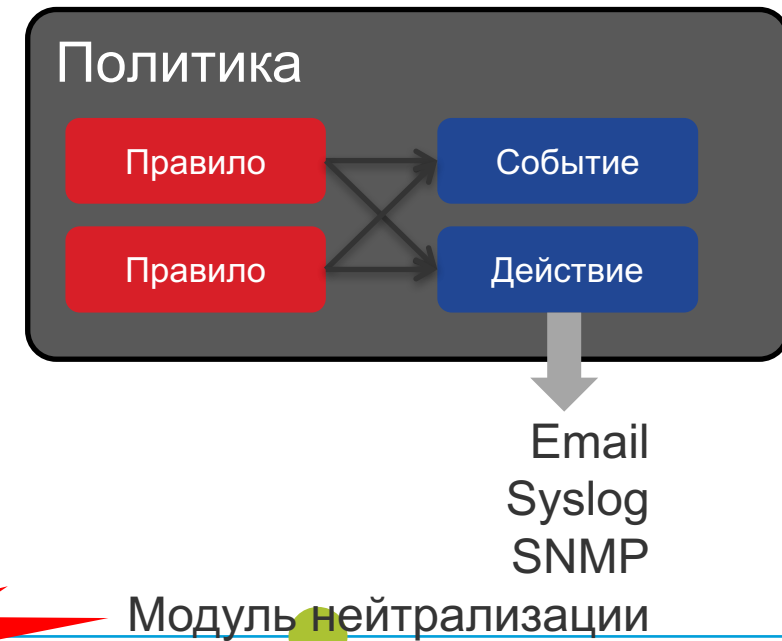
АВТОМАТИЗАЦИЯ КРОМЕ pxGrid

Правила и политики корреляции в Firepower

The screenshot shows the configuration of a rule named "Critical phone Attacks". The rule description is "Attacks on Executives Android-based phones" and it belongs to the "Executive Attacks" group. The rule is configured with the following conditions:

- Event Type:** "an intrusion event occurs" (5 000 событий)
- Conditions (AND):**
 - "Impact Flag" is "1 - red (Vulnerable)" (500 событий)
 - "Inline Result" is not "dropped" (100 событий)
- Host Profile Qualification (OR):**
 - "Destination Host" "Operating System" has the following properties:
 - OS Vendor is "Google" (20 событий)
 - OS Name is "Android" (20 событий)
 - OS Version is "any" (20 событий)
 - "Destination Host" "Jailbroken" is "Yes" (10 событий)
- User Identity Qualification:** "Identity on Destination" "Department" is "Executives" (3 события)

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



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.

The screenshot displays the Cisco Policy Manager interface for configuring a rule. The tabs at the top are 'Policy Management', 'Rule Management', 'White List', and 'Traffic Profiles'. The 'Rule Information' section shows the rule name 'Unauthorized POS Traffic' and the group 'Ungrouped'. The 'Select the type of event for this rule' section is set to 'If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions'. The conditions are: 'Application Protocol is not HTTPS' and 'Responder Port / ICMP Code is not 443'. The 'Host Profile Qualification' section is set to 'Only generate an event if the host(s) involved have the following properties: Initiator Host Location is POS and Responder Host Location is not PCI'. The 'Rule Options' section shows a snooze time of 0 hours and no inactive periods defined.

Policy Management | **Rule Management** | White List | Traffic Profiles

Rule Information

Rule Name: Unauthorized POS Traffic
Rule Description:
Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:

AND

- Application Protocol is not HTTPS
- Responder Port / ICMP Code is not 443

Host Profile Qualification

Only generate an event if the host(s) involved have the following properties:

AND

- Initiator Host Location is POS
- Responder Host Location is not PCI

Rule Options

Snooze: If this rule generates an event, snooze for 0 hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Правила могут быть простыми

The screenshot displays the Cisco Policy Management interface, specifically the Rule Management section. The main tabs are Policy Management, Rule Management (selected), White List, and Traffic Profiles. The Rule Information section shows the Rule Name as 'Production Changes', Rule Description as an empty field, and Rule Group as 'Ungrouped'. There are three buttons to add qualifications: Add Connection Tracker, Add User Qualification, and Add Host Profile Qualification. Below this, a section titled 'Select the type of event for this rule' shows a dropdown menu with 'a discovery event occurs' selected. A list of conditions is displayed, with 'a new IP host is detected' highlighted by a red arrow. The 'Rule Options' section includes 'Snooze' and 'Inactive Periods' fields. At the bottom right, there are 'Save' and 'Cancel' buttons.

Policy Management **Rule Management** White List Traffic Profiles

Rule Information

Rule Name:

Rule Description:

Rule Group:

Select the type of event for this rule

If and it meets the following

conditions:

- a client has changed
- a client timed out
- a host ip address is reused
- a host is deleted because the host limit was reached
- a host is identified as a network device
- a host timed out
- a host's IP address has changed
- an IOC was set
- a NETBIOS name change is detected
- a new client is detected
- a new IP host is detected
- a new MAC address is detected
- a new MAC host is detected
- a new network protocol is detected

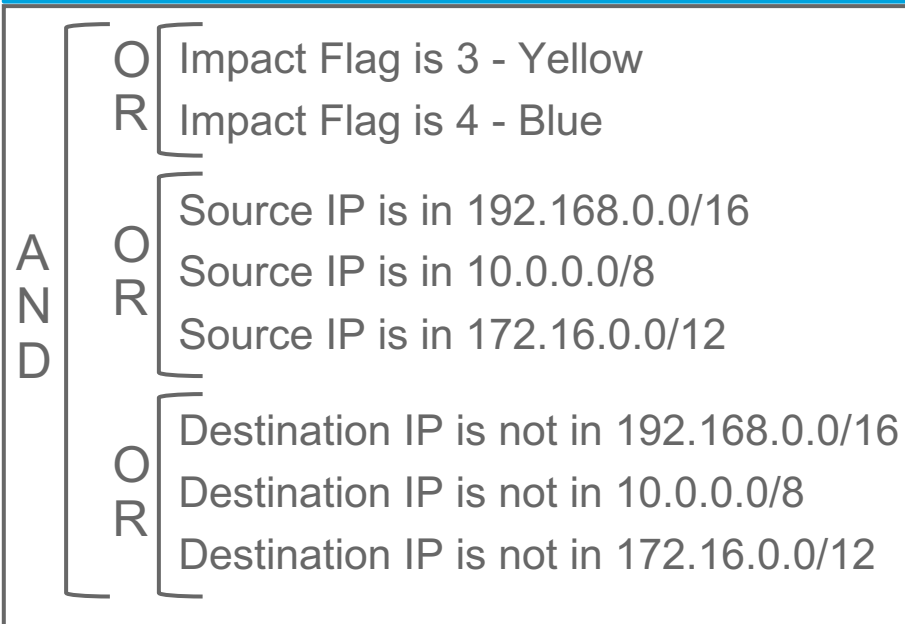
Rule Options

Snooze: If this rule

Inactive Periods: There are

Правила должны формулироваться на основе ЛОГИКИ

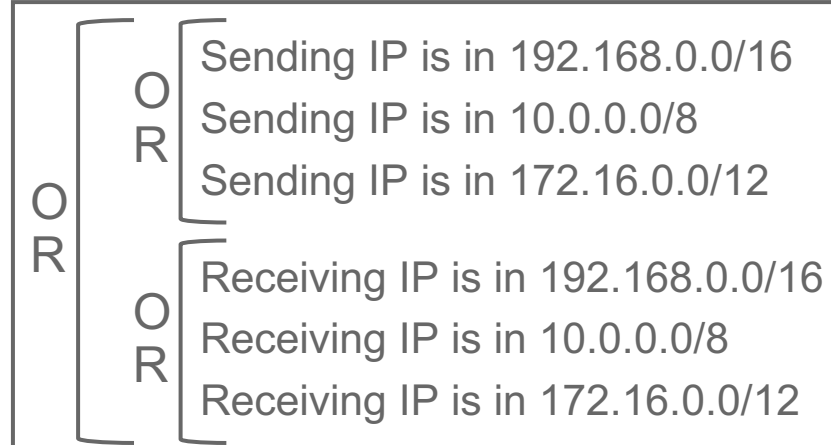
If “an Intrusion Event occurs” . . .



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

If “a Malware Event occurs”

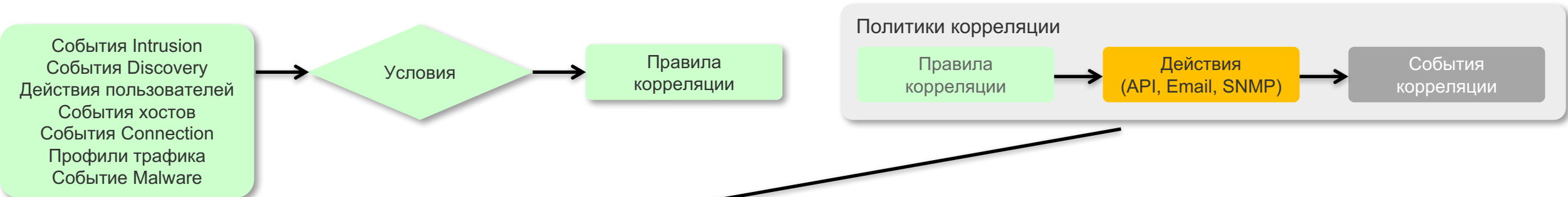
“by retrospective network-based malware detection”



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

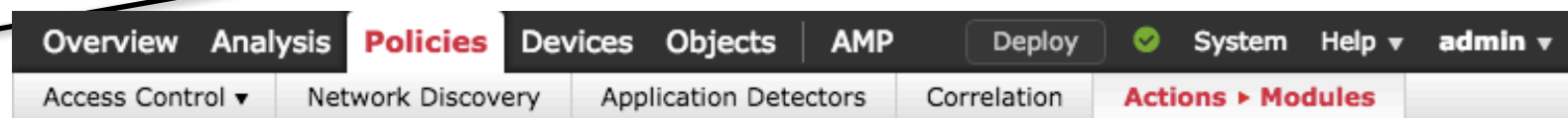
Пора что-то ДЕЛАТЬ!

Автоматизация нейтрализации











Примеры модулей нейтрализации

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



Installed Remediation Modules

Module Name	Version	Description	
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router	 
Nmap Remediation	2.0	Perform an Nmap Scan	 
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses	 
Set Attribute Value	1.0	Set an Attribute Value	 

Install a new module

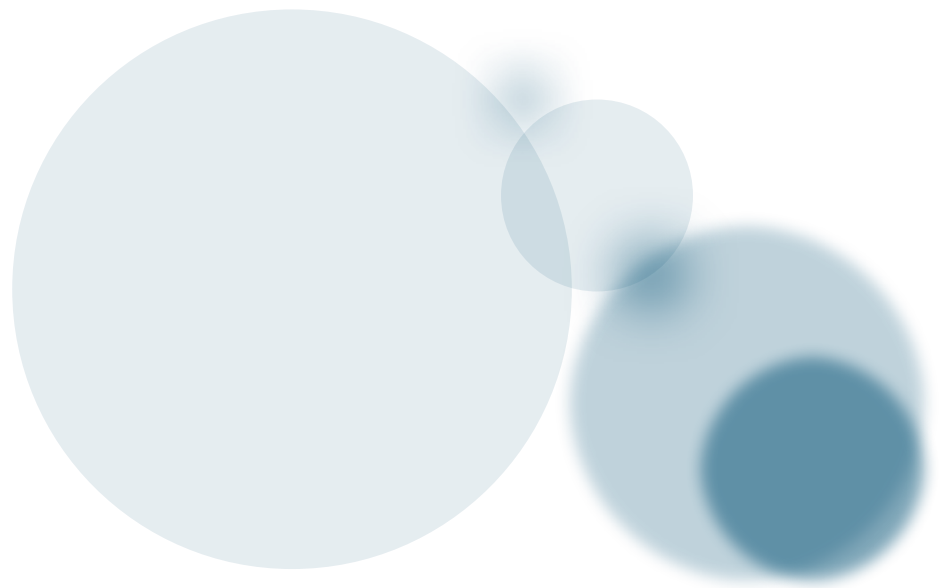
Choose File No file chosen

Install

О чем мы с вами не поговорили...

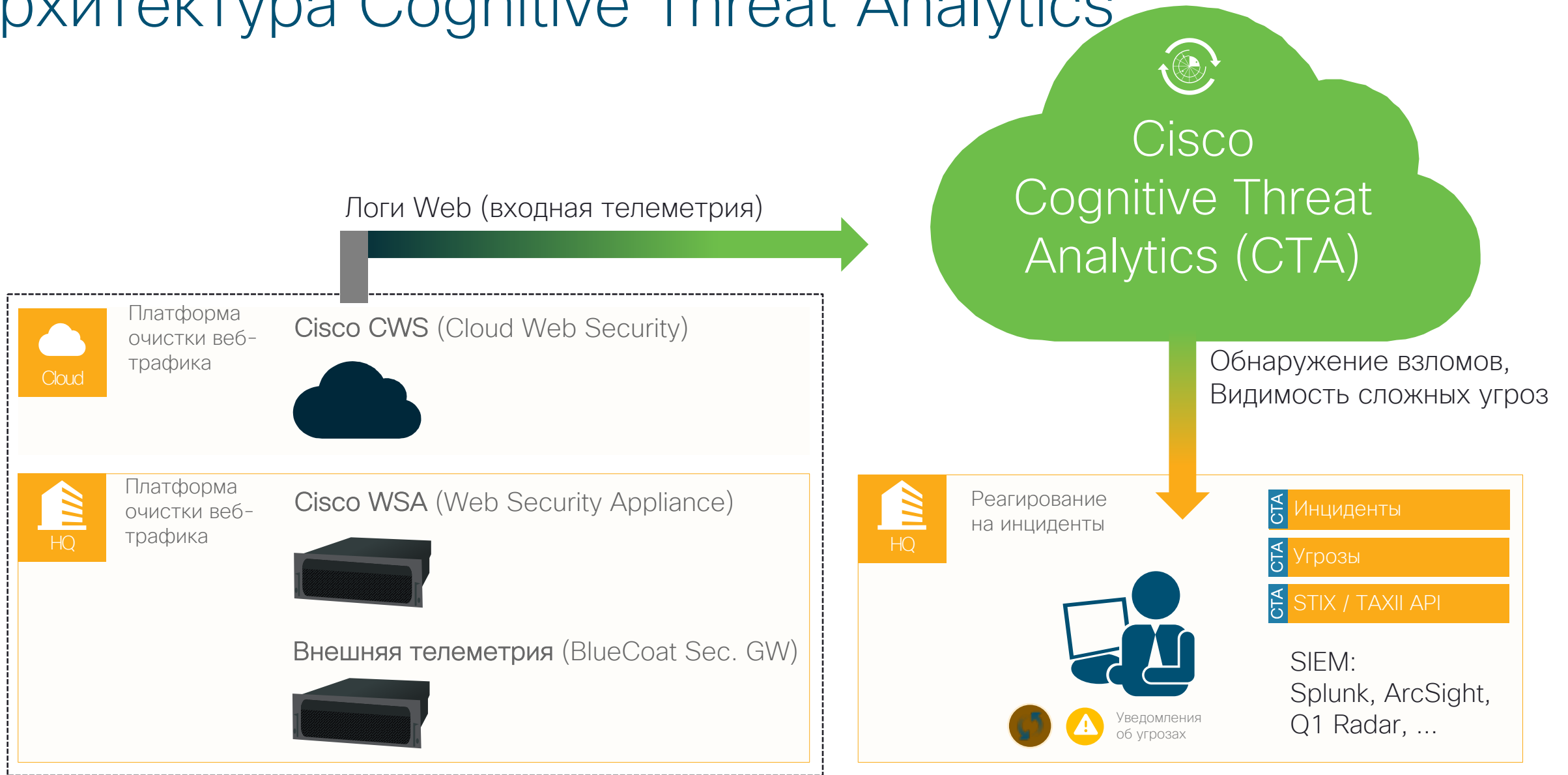
- <https://developer.cisco.com/site/firepower/discover/overview/index.gsp>
 - Database Access API
 - eStreamer API
 - Read / Write REST API
 - Host Input API
 - Remediation API

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



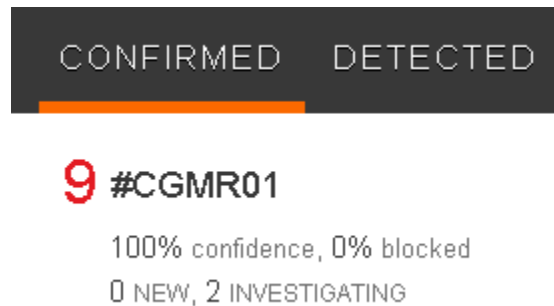
А что ещё для «после»

Архитектура Cognitive Threat Analytics

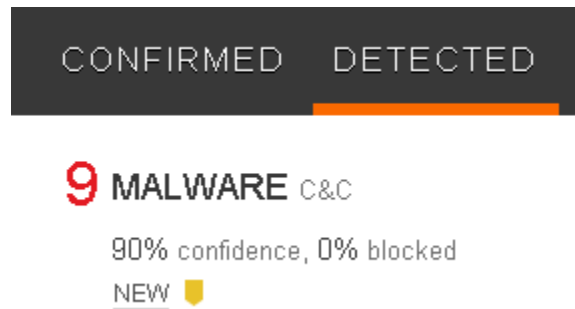


Процесс реагирования

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

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition Malware

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...					Malwa...				
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...					Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013
10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events Transfer Unknown

Events

Time	Source IP	Destination IP	File Name	Disposition	Action	Application Protocol	Client	Description
2013-12-06 10:57:13	10.4.10.183	10.5.11.8	WindowsMediaInstaller.exe	Malware	Malware Cloud Lookup	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 17:40:28	10.5.11.8	10.3.4.51	WindowsMediaInstaller.exe	Unknown				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	10.5.11.8	10.3.4.51	WindowsMediaInstaller.exe	Unknown				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	10.5.11.8	10.5.60.66	WindowsMediaInstaller.exe	Unknown				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	10.5.11.8	10.5.11.8	WindowsMediaInstaller.exe	Malware				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:23	10.5.11.8	10.5.11.8	WindowsMediaInstaller.exe	Malware				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:17:27	10.4.10.183	10.5.11.8	WindowsMediaInstaller.exe	Malware	Malware Block	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...

Event Details:

- Time: 2013-12-06 17:40:28
- Event Type: File Sent
- IP Address: [10.4.10.183](#)
- Sent To: [10.5.11.8](#)
- File Name: [WindowsMediaInstaller.exe](#)
- Disposition: Unknown
- Action: [Malware Cloud Lookup](#)
- Application Protocol: HTTP
- Client: Firefox

Неизвестный файл находится по IP-адресу: 10.4.10.183. Он был загружен через Firefox

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition ⚠ Malware
Threat Score ●●●○ High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013
10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events Transfer Retrospective
Dispositions Unknown

Events

Time	Source IP	Destination IP	File Name	Disposition	Action	Application Protocol	Client
2013-12-06 10:57:13							
2013-12-06 17:40:28	10.4.10.183	10.5.11.8	WindowsMediaInstaller.exe	Unknown	Malware Cloud Lookup	HTTP	Firefox
2013-12-06 18:06:03							
2013-12-06 18:10:03	10.5.11.8	10.5.60.66	WindowsMediaInstaller.exe	Unknown		NetBIOS-...	
2013-12-06 18:14:10							
2013-12-06 18:14:23		10.5.11.8	WindowsMediaInstaller.exe	Malware			
2013-12-06 18:17:27	10.4.10.183	10.5.11.8	WindowsMediaInstaller.exe	Malware	Malware Block	HTTP	Firefox

Callout Box:
Time: 2013-12-06 17:40:28
Event Type: File Received
IP Address: 10.5.11.8
Received From: 10.4.10.183
File Name: WindowsMediaInstaller.exe
Disposition: Unknown
Action: Malware Cloud Lookup
Application Protocol: HTTP
Client: Firefox

Annotation: В 10:57 неизвестный файл с IP-адреса 10.4.10.183 был передан на IP-адрес 10.5.11.8

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

10:57 17:40 18:06 18:10 18:14 18:17

Events Transfer Block

Dispositions Unknown Malware

Events

Time	Event Type
2013-12-06 10:57:13	Retrospective...
2013-12-06 17:40:28	Transfer
2013-12-06 18:06:03	Transfer
2013-12-06 18:10:03	Transfer
2013-12-06 18:14:10	Retrospective...
2013-12-06 18:14:23	File Quaranti...
2013-12-06 18:17:27	Transfer

Time 2013-12-06 18:06:03
Event Type File Received
IP Address [10.3.4.51](#)
Received From [10.5.11.8](#)
File Name [WindowsMediaInstaller.exe](#)
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

Семь часов спустя файл был передан через бизнес-приложение на третье устройство (10.3.4.51)

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

10:57 17:40 18:06 18:10 18:14 18:17

Events Transfer Block
Dispositions Unknown Malware

Events

Time	Event Type	Disposition
2013-12-06 10:57:13	Retrospectiv...	
2013-12-06 17:40:28	Transfer	1
2013-12-06 18:06:03	Transfer	1
2013-12-06 18:10:03	Transfer	1
2013-12-06 18:14:10	Retrospectiv...	
2013-12-06 18:14:23	File Quaranti...	
2013-12-06 18:17:27	Transfer	

Event Details:

- Time** 2013-12-06 18:10:03
- Event Type** File Received
- IP Address** [10.5.60.66](#)
- Received From** [10.5.11.8](#)
- File Name** [WindowsMediaInstaller.exe](#)
- Disposition** Unknown
- Action**
- Application Protocol** NetBIOS-ssn (SMB)

Event Log:

Time	Source IP	Destination IP	File Name	Disposition	Action	Protocol	Application
2013-12-06 18:17:27	10.4.10.183	10.5.11.8	WindowsMediaInstaller...	Malwa...	Malware Block	HTTP	Firefox

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

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type [MSEXE](#)
File Category [Executables](#)
Current Disposition [Malware](#)
Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013
10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events Transfer Block Create
Dispositions Unknown Malware Clean

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disposition	Action
2013-12-06 10:57:13	Retrospectiv...				Malwa...	
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud ... HTTP Firefox Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...	NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...	NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...	
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...	
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block HTTP Firefox

Time 2013-12-06 18:14:10
Event Type Retrospective Event
Disposition [Malware](#)
Action

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

Пример траектории файла

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events Transfer Block Create Delete

Dispositions Unknown Malware Clean Quarantined

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disposition	Action
2013-12-06 10:57:13	Retrospectiv...					
2013-12-06 17:40:28	Transfer	10.4.10.183				
2013-12-06 18:06:03	Transfer	10.5.11.8				
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller...	Unkn...	
2013-12-06 18:14:10	Retrospectiv...				Malwa...	
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller...	Malwa...	
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller...	Malwa...	Malware Block HTTP Firefox

Time 2013-12-06 18:14:23
Event Type File Quarantined
IP Address [10.5.11.8](#)
File Name [WindowsMediaInstaller.exe](#)
Disposition Malware
Action

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

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type MSEXE
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013
10:57 17:40 18:06 18:10 18:14 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events Transfer Block Create Move
Dispositions Unknown Malware Clean Custom

Events

Time	Event Type	Sending IP
2013-12-06 10:57:13	Retrospectiv...	
2013-12-06 17:40:28	Transfer	10.4.10.183
2013-12-06 18:06:03	Transfer	10.5.11.8
2013-12-06 18:10:03	Transfer	10.5.11.8
2013-12-06 18:14:10	Retrospectiv...	
2013-12-06 18:14:23	File Quaranti...	10.5.11.8
2013-12-06 18:17:27	Transfer	10.4.10.183




Event Details:

- Time** 2013-12-06 18:17:27
- Event Type** File Sent
- IP Address** [10.4.10.183](#)
- Blocked Recipient** [10.5.11.8](#)
- File Name** [WindowsMediaInstaller.exe](#)
- Disposition** Malware
- Action** Malware Block
- Application Protocol** HTTP
- Client** Firefox

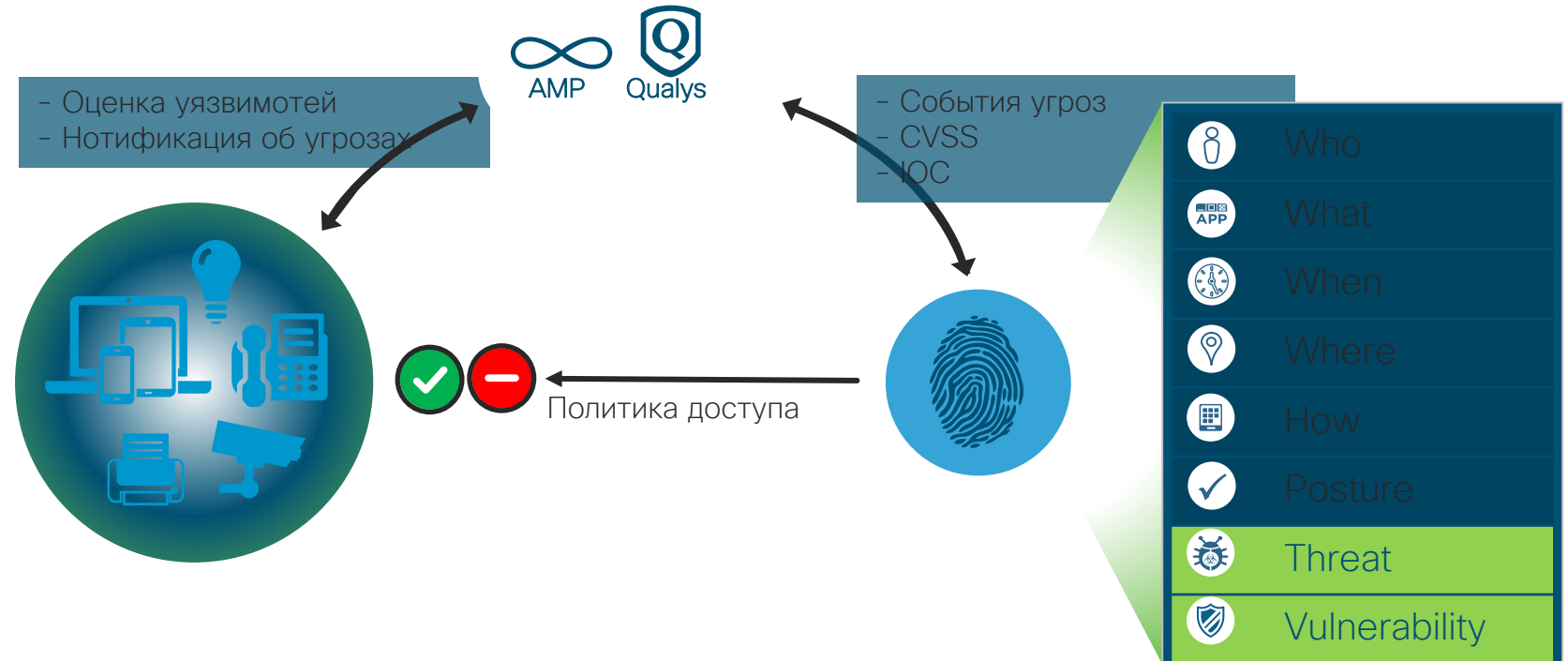
Через 8 часов после первой атаки вредоносное ПО пыталось повторно проникнуть в систему через исходную входную точку, но было распознано и заблокировано

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

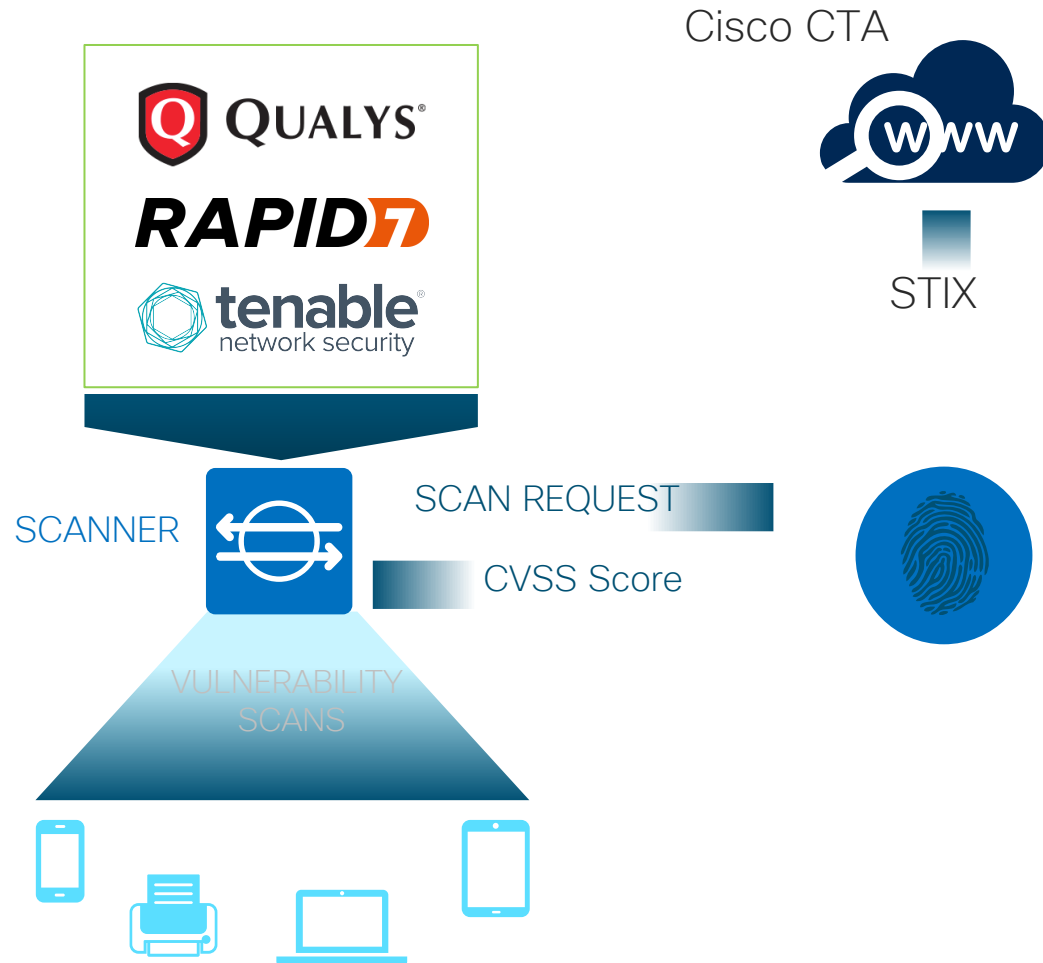
Создайте политики авторизации на основании анализа угроз и уязвимостей



Threat Centric NAC

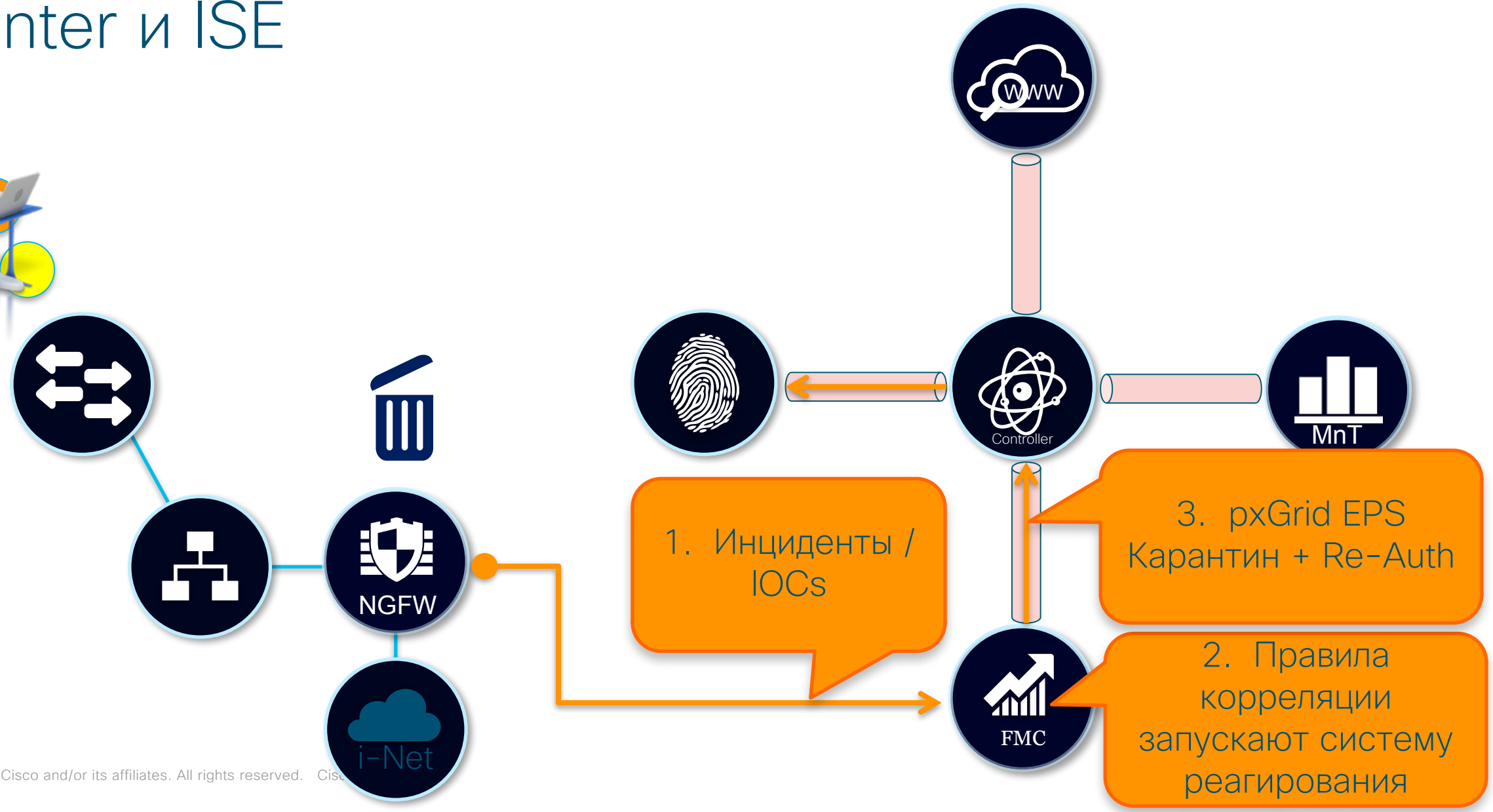
Выберите вендора для оценки уязвимостей

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.

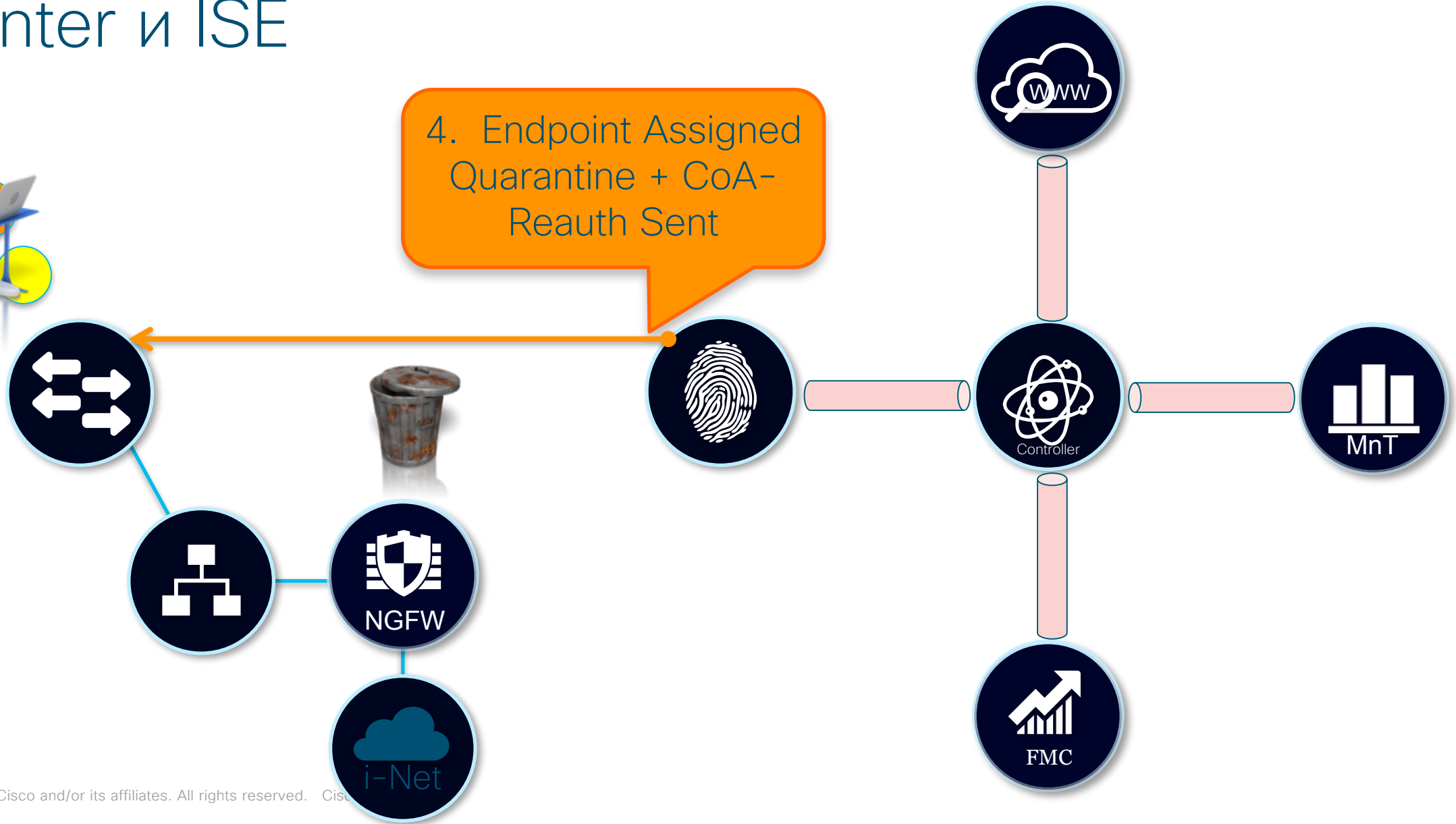
Rapid Threat Containment с Firepower Management Center и ISE



Rapid Threat Containment & Firepower Management Center & ISE



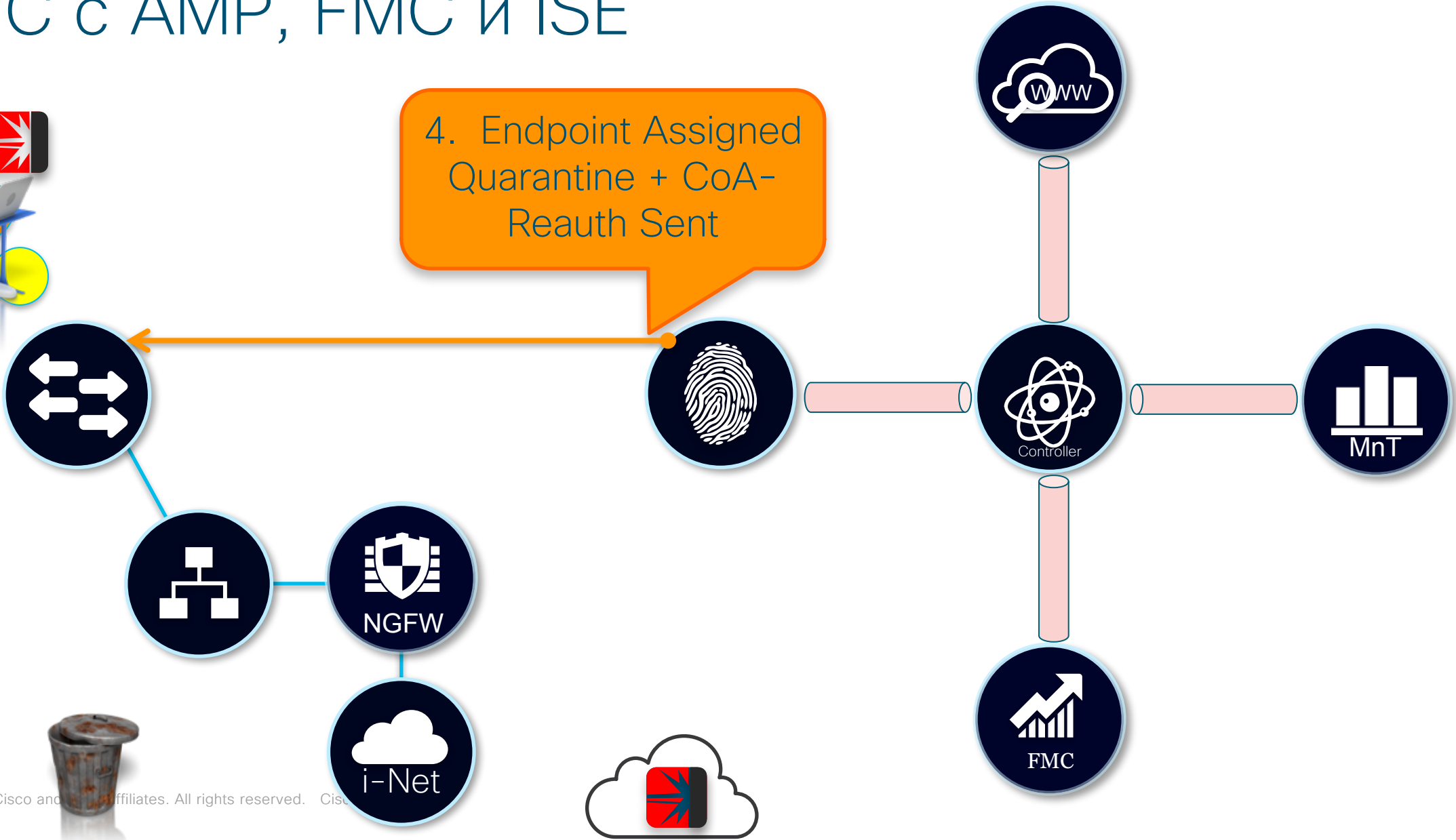
4. Endpoint Assigned Quarantine + CoA- Reauth Sent



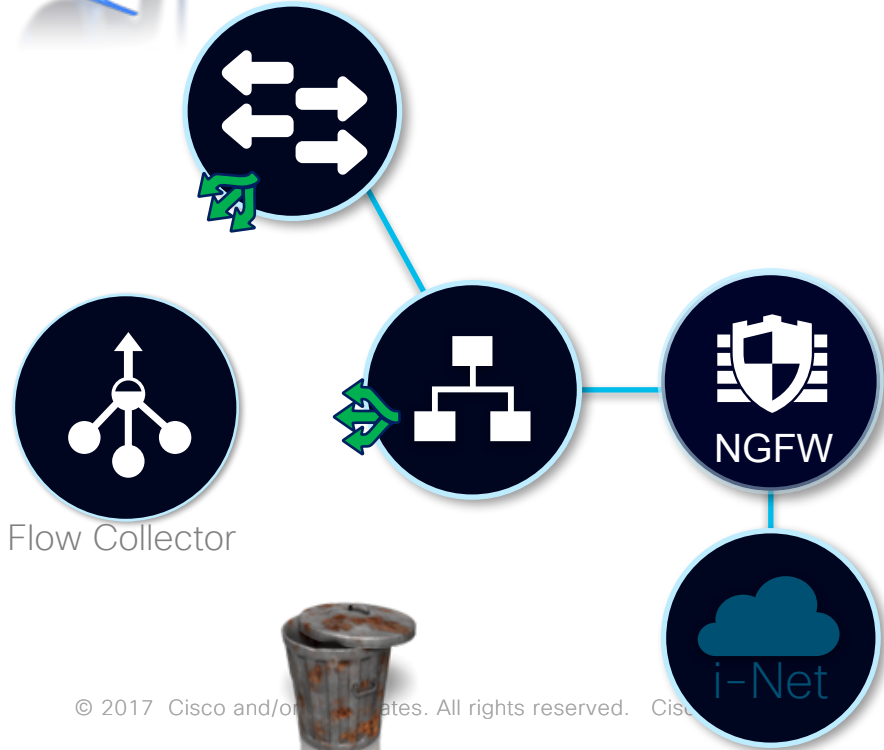
RTC с AMP, FMC и ISE



4. Endpoint Assigned Quarantine + CoA- Reauth Sent



RTC с Stealthwatch & ISE



RTC c Stealthwatch + ICF

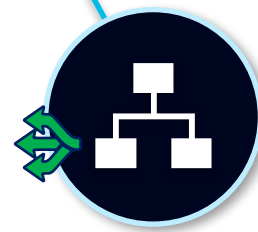
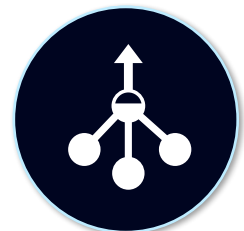
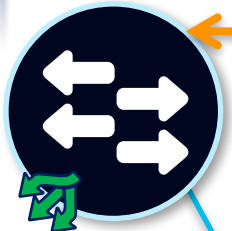


4. Админ инициирует карантин



Host Summary	
	Host IP: 10.1.41.105
<input type="button" value="Classify"/>	<input type="button" value="History"/>
Status:	Inactive
Hostname:	--
Host Groups:	Catch All
Location:	RFC 1918
Last Seen:	1/17/17 4:02 AM
Policies:	Inside
MAC Address:	--
<input type="button" value="Quarantine"/> <input type="button" value="Unquarantine"/>	

5. Endpoint Assigned Quarantine + CoA- Reauth Sent



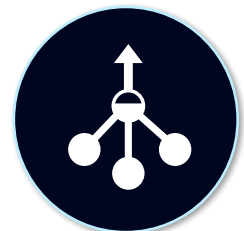
RTC с Stealthwatch и ISE



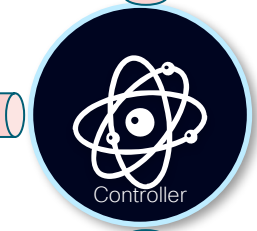
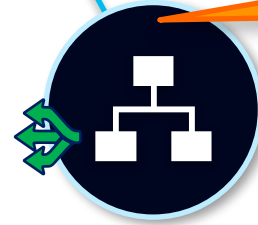
6. Применяются новые правила доступа

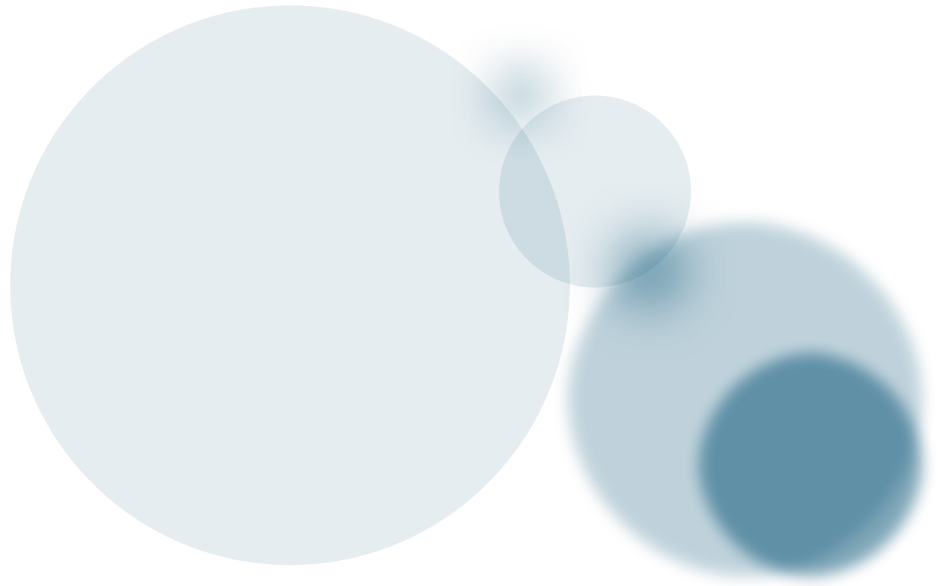
6a. Может запретить доступ

6b. Может фильтровать в сети (входящий)



Flow Collector





РЕЗЮМИРУЯ

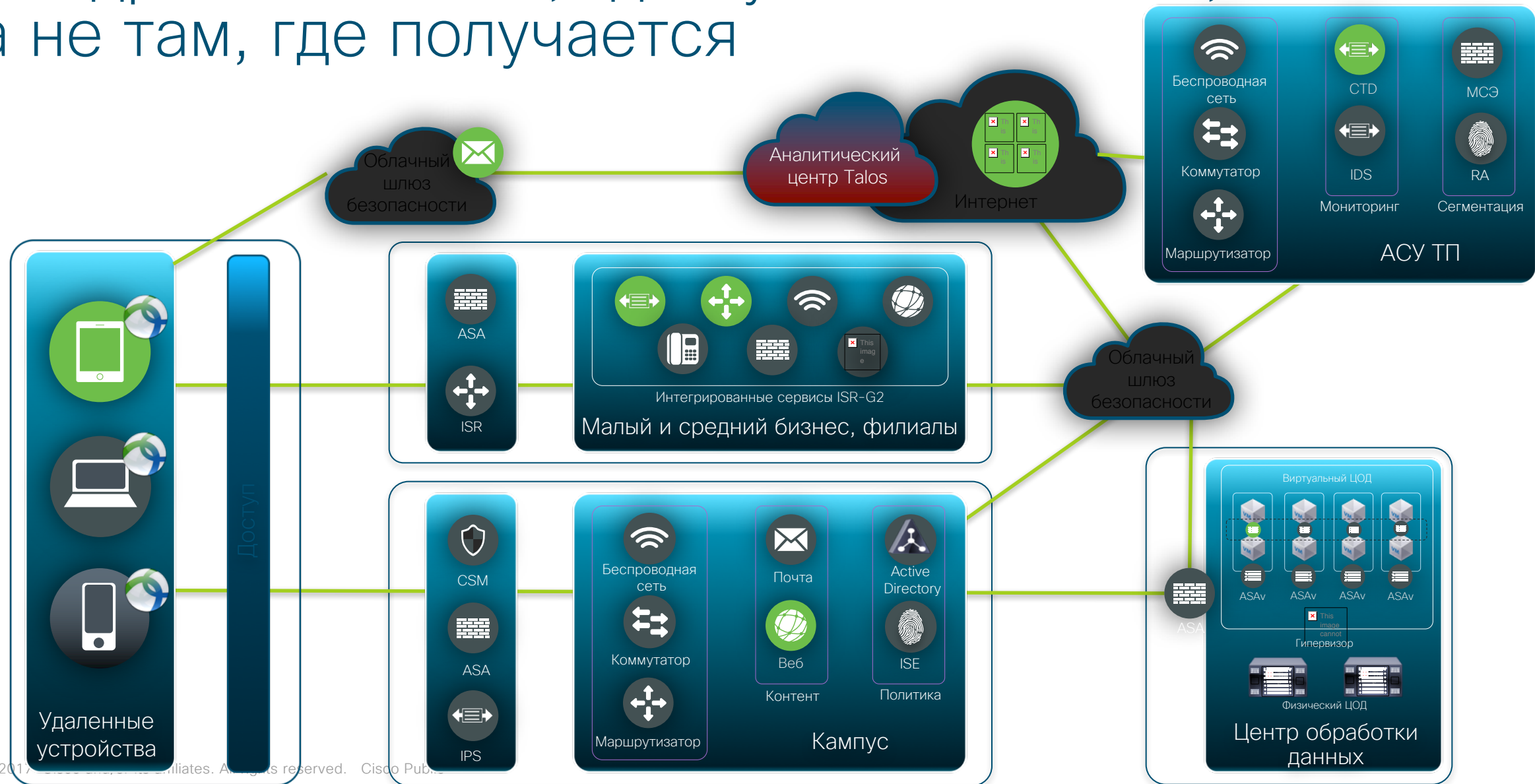
Не видя ничего, ничего и не обнаружишь



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

- Виртуальна демонстрація
 - ✓ AMP
 - ✓ Firepower
 - ✓ ESA
- Бесплатная пробная версия Cisco Umbrella

Демонстрація рішень Cisco з інформаційної безпеки



Advanced Malware Protection (AMP)

Забезпечує моніторинг і контроль для швидкого виявлення, стримування та усунення шкідливого ПЗ.



Firepower

Включає в функції моніторингу і контролю додатків (AVC), систему запобігання вторгнень нового покоління (NGIPS), захист від складного шкідливого ПЗ (Cisco AMP) і фільтрацію URL-адрес.



Email Security Appliance (ESA)

Надає захист від зростаючої кількості загроз електронної пошти: спаму, фішингу, шкідливого коду і витоків інформації.

[Замовити віртуальну демонстрацію](#)

Безкоштовна пробна версія Cisco Umbrella

Дізнайтеся, як зупинити кіберзагрози, перш ніж ваші користувачі відвідують шкідливі сайти.

Доступно лише англійською мовою

[Отримати доступ до безкоштовної пробної версії](#)



Сервіс Incident Response Service з передоплатою на рік



Служба терміново реагування на кіберзлочини доступна протягом 24 годин, щоб усунути будь-які порушення ваших даних. Ми розробляємо стратегію та план виправлення основних проблем. Наша досвідчена команда використовує результати досліджень Cisco Talos та найсучасніші технології з інформаційної безпеки для реагування на кібератаки та зменшення їхнього впливу.

[Переглянути інфографіку](#) | [Отримати консультацію щодо умов сервісу](#)




CISCO™