



Перспективные решения Cisco в области информационной безопасности

Василий Томилин

Инженер-консультант

security-request@cisco.com, vtomilin@cisco.com

Предпосылки и план разговора

- Наверное, вы (как-то) представляете себе набор решений Cisco #поИБ
- Возможно, вы слышали о Before/During/After
- Вероятно, вы слышали про открытость и интеграцию, всяческие интерфейсы и т.п. (хотя я напомню)
- Что мы уже сделали – вехи?
- Несколько продуктов, на которых я бы хотел сконцентрировать ваше внимание
- Что мы будем делать?

Ландшафт угроз



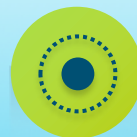
Сеть



Оконечные
устройства



Мобильные
устройства



Виртуальные
машины



Облако



В определенный
момент



Непрерывно

Какие решения по ИБ есть у Cisco?

МСЭ и NGFW

- Cisco ASA / ASA-SM
- Cisco IOS Firewall
- Cisco ASAv
- Cisco FirePOWER
- FTD/FTDv

IPS и NGIPS

- Cisco FirePOWER
- Cisco ASA with FirePOWER
- Cisco FirePOWER for ISR
- Cisco wIPS
- Cisco vNGIPS

Advanced Malware Protection

- AMP для Endpoint
- AMP для Network
- AMP для Content
- Threat Grid

Интернет-безопасность

- Cisco WSA / vWSA
- Cisco Umbrella
- Threat Awareness Service

Безопасность электронной почты

- Cisco ESA / vESA
- Cisco Cloud Email Security

NAC + Identity Services

- Cisco ISE / vISE

VPN

- Cisco AnyConnect
- Cisco ASA
- Cisco ISR / RVPN

UTM

- Meraki MX
- ASA with FirePOWER
- Firepower

Объективный контроль

- Cisco Stealthwatch

Сегментация/доступ

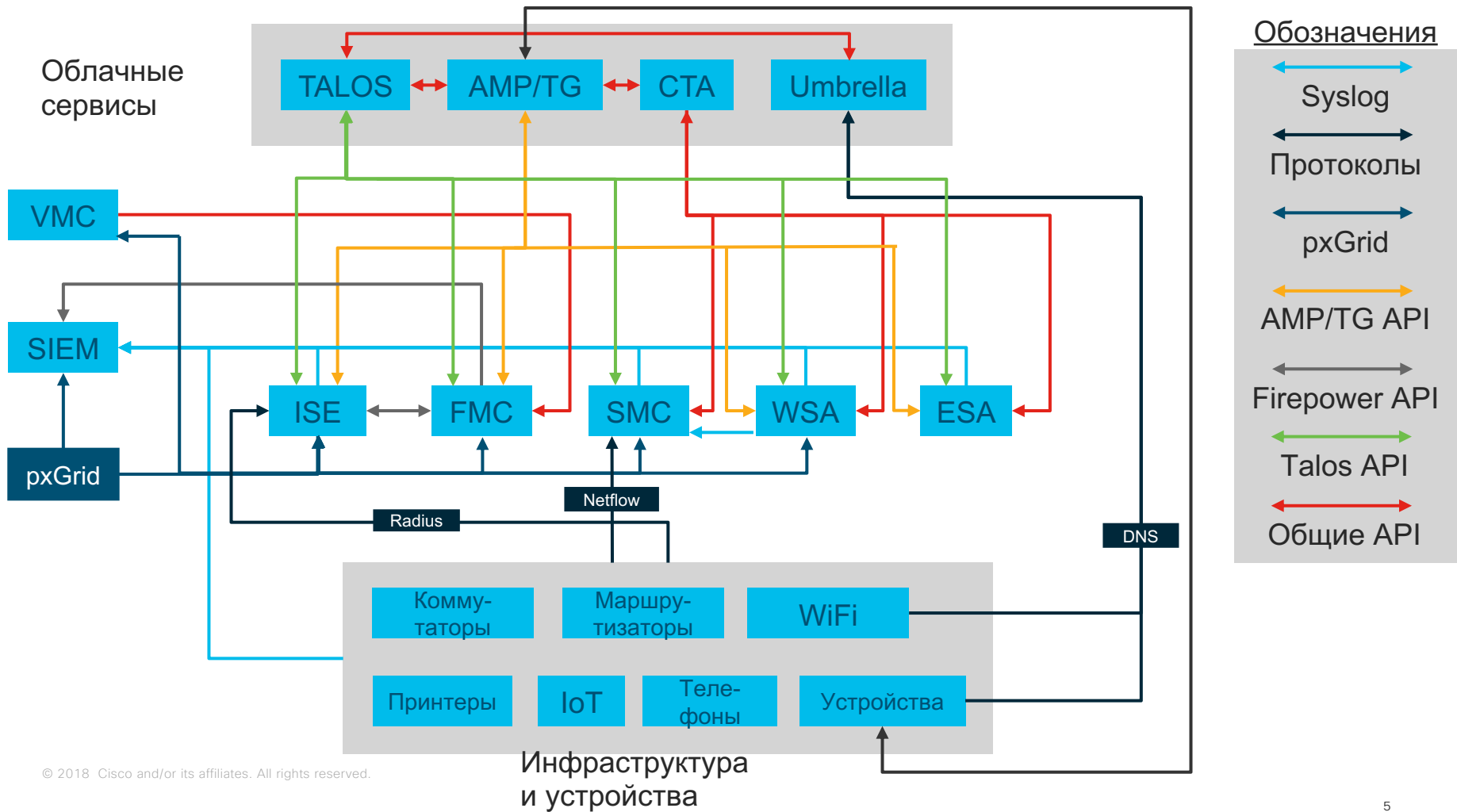
- Cisco TrustSec
- Cisco ISE

Защита ЦОД

- Cisco ASA / 1000v / ASAv / FTDv
- Cisco TrustSec

Контроль приложений

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



Cisco Security 2019

- Cisco Threat Intelligence
- Cisco Threat Response
- Cisco Platform Exchange



Интегрированная архитектура

Да, всего много... а что списано?

<https://www.cisco.com/c/en/us/products/eos-eol-listing.html>

Быстрая проверка, по каким продуктам
(и их версиям) объявлено окончание
продаж и поддержки

End-of-Sale and End-of-Life Products

These products are no longer being sold and might not be supported.
Click on the product link, when available, for more information.

Please see the [End-of-Life Policy](#) for more details.

Products End-of-Sale and End-of-Life RSS

Analytics and Automation Software

[Cisco ServiceGrid](#)

Application Networking Services

[Cisco ACE 4700 Series Application Control Engine Appliances](#)

[Cisco ACE 4710 Application Control Engine](#)

[Cisco ACE GSS 4400 Series Global Site Selector Appliances](#)

[Cisco GSS 4492R Global Site Selector](#)

А как нарисовать схему умному заказчику?

<https://www.cisco.com/go/visio>

Ресурс, позволяющий найти иконки продуктов Cisco для использования их в MS Visio



Products & Services /

Visio Stencils

You will need Microsoft Visio Standard or Professional in order to view and use these stencils correctly. The files listed for download on this page are .vss (Visio stencil) files within .zip files. Some of the .zip files contain Microsoft PowerPoint files in addition to Visio files. The PowerPoint files contain .emf (enhanced metafile) vector images derived from the Visio drawings. These may be copied and pasted into PowerPoint and other applications without requiring Visio.

If you are a Mac user, the stencils will also work with recent versions of OmniGraffle (by Omni Group), a Visio-like application for the Apple Mac platform.

- [Documentation: FAQ and User's Guide](#)
- [Documentation: Stencil Index and Table of Contents](#)
- All Visio Products: This file is no longer available due to the growth in the file size with the ongoing addition of new Visio stencil files. Please download Visio stencils from the individual links below which are the latest versions.
- [Link to Cisco Network Topology Icons](#)
- [Cisco Design Zone: Use our documentation for faster, more reliable and predictable deployment.](#)

View Documents by Topic

Choose a Topic



Application Networking Services

[Application Control Engine-ACE XML Gateway](#) (ZIP - 105 KB) 11/Jun/2008

Все для интеграции: Cisco DevNet

- [Developer.cisco.com](https://developer.cisco.com) – единая точка входа.
Множество API для решения самых разных задач.
- [Learninglabs.cisco.com](https://learninglabs.cisco.com) – практические лабораторные работы для освоения представленного материала (уроки для инженеров)

Мы запустили модуль по безопасности

DevNet Express for Security

This track contains the modules and labs taught at a DevNet Express event: where you listen, learn, and then put your new knowledge into practice. Learn about automation, operational scripting, and DevOps integration points on top of your security infrastructure. Looking to dive into the world of programming your enterprise security and automating your security workflows? Curious about the APIs available for Cisco Umbrella, Firepower, Advanced Malware Protection, and Threat Grid? Well, then this DevNet learning track is for you.

Beta



 10 Modules

 37 Learning Labs

 14 Hours 30 Minutes

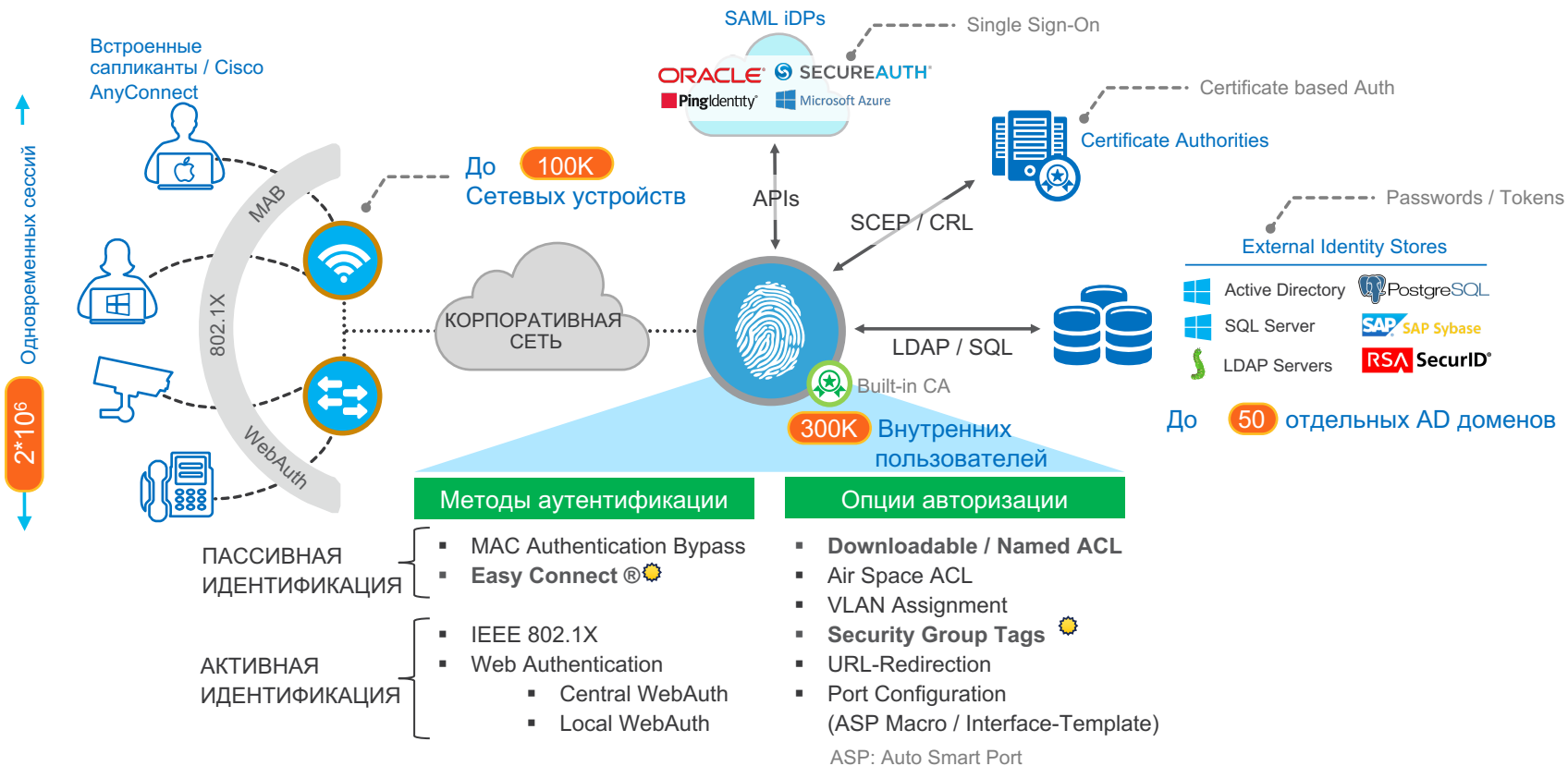
Choose a module to start learning

Мы продолжаем развитие

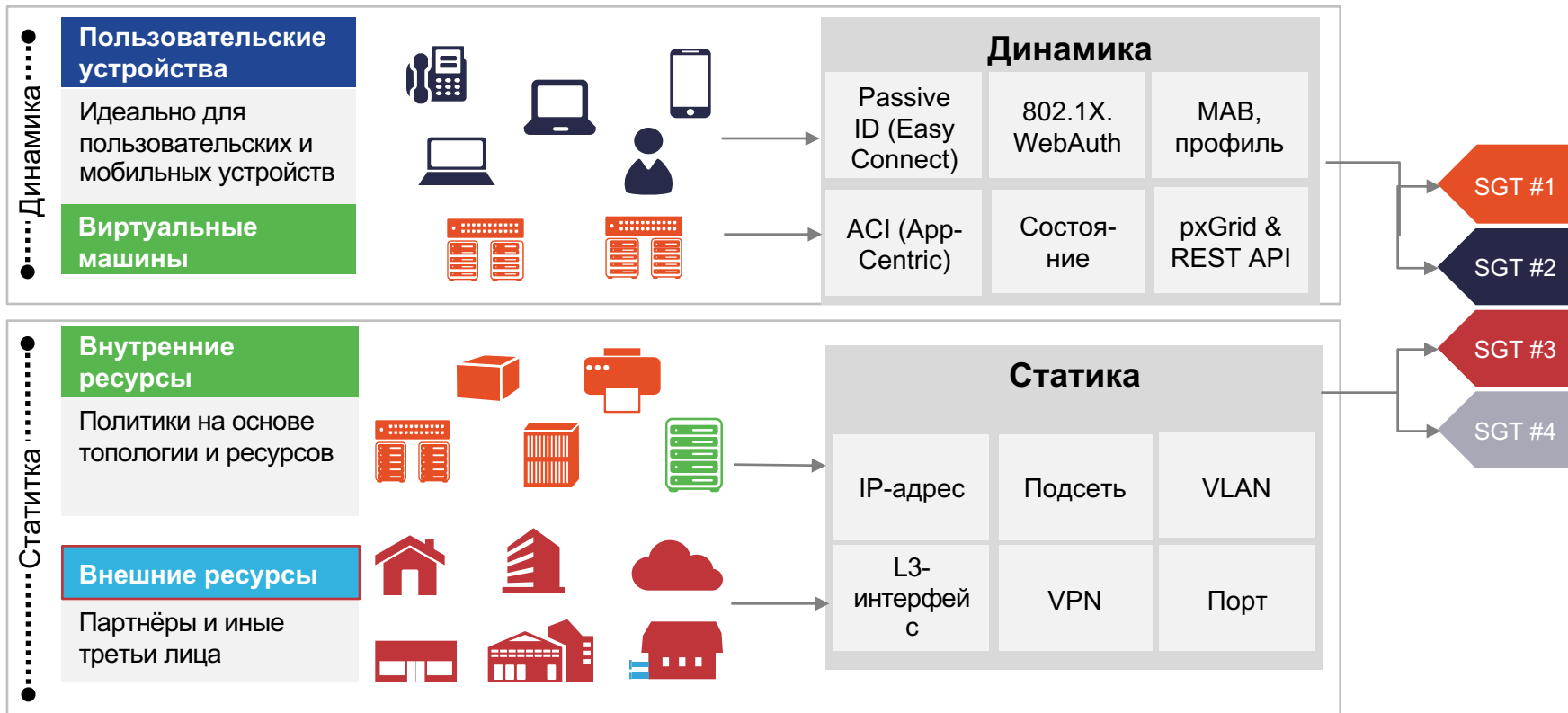
Вы помните про Cisco ISE? Теперь уже 2.6

- Расширение максимального развертывания до **$2 * 10^6$** активных одновременных подключений
- Расширение поддержки IPv6 на management
- Поддержка идентификации рабочих станций по UDID, а не MAC-адресу с AnyConnect 4.7 (уже выпущен и работает) – специально для «коворкинга» и «нового стиля работы»
- Более гибкие возможности Grace Period и настраиваемые уведомления (для Posture) с AnyConnect 4.7
- Проверка внесения изменений в инфраструктуру и отчеты после изменения политик TrustSec
- Аутентификация в AD логинов по CLI и REST API
- Поддержка Manufacturer Usage Descriptor (MUD) для создания профилей и автоматического создания устройств IoT

Cisco ISE: поддержка безопасного доступа



Гибкие методы классификации



Будем внимательны с маркетингом: SGACL – это не permit all/deny all

TrustSec

Overview Authentication Policy Authorization Policy Components Policy SXP Reports Settings

Egress Policy

Matrix

Source Tree

Destination Tree

Network Device Authorization

Permit_Email_Traffic

Access control policy to permit Email service

IPv4 IPv6 Agnostic

```
permit tcp dst eq 110
permit tcp dst eq 143
permit tcp dst eq 25
permit tcp dst eq 465
permit tcp dst eq 585
permit tcp dst eq 993
permit tcp dst eq 995
deny all log
```

Egress Policy (Matrix View)

Edit Add Clear Mapping Push Monitor All - Off Import Export View Show CustomView-1

Destination	Mail_Servers 120/0078	PCI_Devices 100/0064	Web_Servers 110/006E	Employee_FullAc... 10/000A	Contractors 30/001E
Source					
Contractors 30/001E	Permit_Email_Traffic	Deny IP		Cisco_Jabber_Access	
Employee_BYOD 20/0014	Permit_Email_Traffic	Deny IP		Malware_Control_ACL	
Employee_FullAc... 10/000A		Deny IP		Malware_Control_ACL	Cisco_Jabber_Access
PCI_Devices 100/0064	Deny IP		Deny IP	Deny IP	Deny IP

Default Enabled SGACLs : Permit IP Description : Default egress rule



Почему заказчики покупают ISE?



 Видимость устройств	Cisco ISE смотрит глубоко на всю сеть и предоставляет непревзойденную видимость того кто и что соединяется к ресурсам.
 Контроль доступа	Целостный контроль доступа в проводной, беспроводной и VPN сети.. 802.1X, MAC, WEB-Аутентификация и Easy-connect для контроля доступа
 Гостевой доступ	Полностью настраиваемые мобильный и десктоп гостевые порталы с простым визуальным Wizard'ом для простого управления гостевым доступом
 BYOD доступ	Упрощенное управление BYOD в строенным CA сервером и поддержкой сторонних MDM интеграций для саморегистрации собственных устройств
 Сегментация	Политика топологически-независимой сегментации для сдерживания сетевых угроз с использованием Cisco TrustSec
 Контроль угроз	Обмен контекстом с партнерской экосистемой для улучшения их эффективности и уменьшения времени реагирования на инцидент
 Доступ администратора	Cisco ISE поддерживает протокол TACACS+ для контроля и аудита конфигурационных изменений на сетевых устройствах.

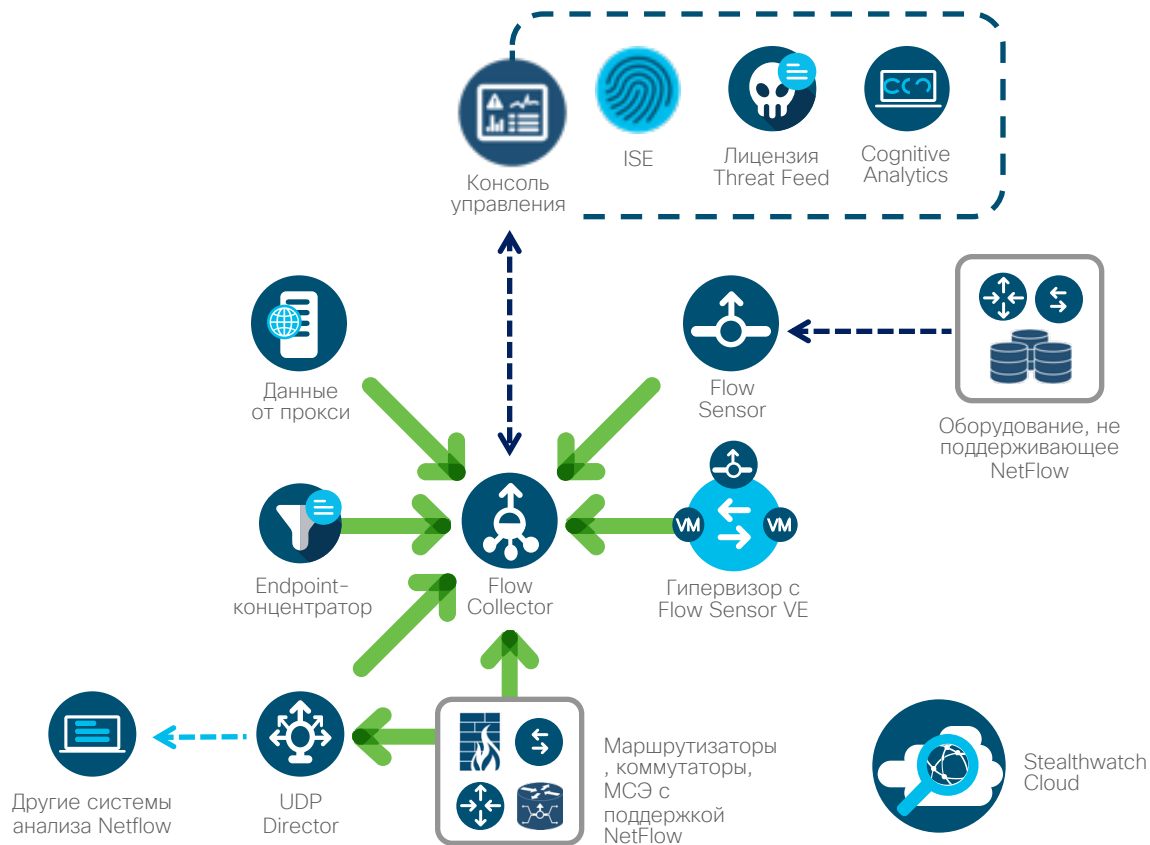
Вы помните про Cisco Stealthwatch? Уже 7.0

- Существенное расширение функционала веб-интерфейса
- Концепция App-ов
- Модификация API (только REST)
- И многое другое



Система Cisco Stealthwatch

Всеобъемлющий
мониторинг
безопасности и
работы сети



Обзор преимуществ системы StealthWatch

Угрозы

- Мы обнаруживаем больше, потому что видим больше
- Угрозы в сети – это реальность; верить нельзя никому (Stealthwatch можно)
- Использование существующей сетевой инфраструктуры для обнаружения и анализа современных угроз

Лучшее решение в своем классе

- Суть: многоуровневые машинное обучение, моделирование, статистический анализ
- Единственное решение класса NTA, реализующее ETA
- Полная интеграция с другими компонентами подсистемы обеспечения ИБ для ускорения обнаружения и оперативной реакции

Полная видимость

- Полная видимость – основа для обнаружения потенциальных инцидентов
- Намного больше, чем классический NetFlow
- Критически важна для внедрения и контроля сегментации

Новые возможности и особенности Stealthwatch



Улучшение управления

Security policy manager
Host Group manager
User manager



Упрощение управления

Appliance manager
Update manager
Stealthwatch Apps



Расширение аналитики

Обновления ядра
машинного обучения
(Cognitive Intelligence)



Нейтрализация с учётом контекста

Модернизация
интеграции
с ISE
(EPS->ANC)

Усовершенствования Policy Manager

- Существенная переработка управления политикой безопасности (чтобы тревоги соответствовали вашей логике)
- Политики Stealthwatch всех трех типов (core, custom и relationship) управляются централизованно с помощью веб-интерфейса
- Простота создания, правки и удаления событий
- Просмотр «эффективной политики» для хоста одним щелчком, простота «проваливания» в тревогу, чтобы настроить параметры события

Управление политикой - Core Events



1. Подробные сведения о тревогах, изменение политик на основании как поведенческих, так и «пороговых» моделей
2. Простота поиска политик, установленных для хоста или группы хостов
3. Просмотр, создание, изменение политик по умолчанию, определение политик для ролей и хостов
4. Фильтрация Core Events по многим параметрам

Policy Management

Search for a host or select a host group **2** Search

Custom Events (2) Relationship Events (352) **Core Events (654)** [Create New Policy](#)

EVENT	EVENT TY...	POLICY NAME	POLICY TYPE	HOSTS	WHEN HOST IS SOURCE	WHEN HOST IS TARGET
<i>Ex. Anomaly</i>	<i>Ex. C...</i>	<i>Ex. Outside Hosts</i>	<i>Ex. Role</i>	<i>Ex. Network Scanners</i>	<i>Ex. On + Alarm</i>	<i>Ex. On + Alarm</i>
Talks to Phantoms	Security	10.201.3.78	Host	10.201.3.78	On + Alarm	On
Talks to Phantoms	Security	Outside Hosts	Default	Outside Hosts	On	On
Talks to Phantoms	Security	Inside Hosts	Default	Inside Hosts	On	On
Target Data Hoarding	Security	10.201.0.23	Host	10.201.0.23	On	On + Alarm
Target Data Hoarding	Security	10.201.0.55	Host	10.201.0.55	On	On + Alarm
Target Data Hoarding	Security	Firewalls, Proxies, & NAT Devices	Role	NAT Gateway, Proxy	Off	Off
Target Data Hoarding	Security	Outside Hosts	Default	Outside Hosts	On	On
Target Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On	On + Alarm

4

3

1

Description

Behavioral and Threshold Threshold Only

One or more hosts have downloaded an unusual amount of data from the target host.

Tolerance / 100

Never trigger alarm when less than: downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: downloaded payload bytes in 24 hrs

Управление политикой – Custom Events

Configure

Policy
Management

Custom Events

1. Множество параметров для выбора
2. Возможность выбора полей Encrypted Traffic Analytics (ETA) для упрощения криптоаудита
3. Автоматически генерируемое простое, понятное и наглядное изложение правила

Примечание: Custom event'ы в веб-интерфейсе заменяют политики изоляции хостов в Java-клиенте

Policy Management | Custom Security Event

NAME *

Engineering Comms to Compliance via TLS 1.0

DESCRIPTION

Prohibited comm type to Compliance

When any host within *Engineering* communicates with any host within *Compliance Systems*; using *TLS 1.0 encryption*, an alarm is raised.

FIND ⓘ

SUBJECT HOST GROUPS ⓘ

Engineering ×

⊗ AND

PEER HOST GROUPS ⓘ

Compliance Systems ×

⊗ AND

ENCRYPTION TLS/SSL VERSION ⓘ

TLS 1.0 ×

⊗

Search for a rule type

Peer TrustSec IDs
Subject TrustSec Names
Peer TrustSec Names
Subject Applications
Peer Applications
Subject File Hashes
Peer File Hashes

[View All](#)

Управление политикой - Relationship Events



1. События «relationship» позволяют контролировать соблюдение политики группами хостов
2. Просмотр и изменение политик на основании поведенческих и «пороговых» метрик
3. Простота поиска политик, заданных для хоста или группы хостов
4. Фильтрация Relationship-событий по многим параметрам

Policy Management

Search for a host or select a host group 3

Custom Events (6) **Relationship Events (11)** Core Events (654) 1 [Create New Policy](#)

EVENT	POLICY NAME	MAP	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS
Ex. Relationship High Traffic	Confidential Systems <-> Out...	Filter Map	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"
Relationship High Total Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers ↔ Outside Hosts	All Services	All Applications
Description		<input checked="" type="radio"/> Behavioral and Threshold		Tolerance <input type="text" value="50"/> / 100	
This event indicates that the total traffic between the two host groups in the relationship exceeds the threshold. The alarm is raised if the alarm condition exists for longer than a user-specified duration.		<input type="radio"/> Threshold Only		Never trigger alarm when less than: <input type="text" value="953.67 M"/> bytes in 24 hours	
				Always trigger alarm when greater than: <input type="text" value="93.13 G"/> bytes in 24 hours	
				Trigger alarm when duration greater than: <input type="text" value="5"/> minutes	
Relationship High Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers ↔ Outside Hosts	All Services	All Applications
Relationship ICMP Flood	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers ↔ Outside Hosts	All Services	All Applications
Relationship Low Traffic	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers ↔ Outside Hosts	All Services	All Applications
Relationship Max Flows	Confidential Systems <-> Outside Hosts	Functional Map	Confidential Servers ↔ Outside Hosts	All Services	All Applications

Усовершенствования User Manager и Host Group Manager

- Добавление пользователей Stealthwatch и настройка их доступа к данным в соответствии с их ролями
- Классификация хостов в Host Groups для повышения эффективности обнаружения аномалий и угроз в соответствии с логикой работы организации

Управление группами хостов

Configure

Host Group Management

Host Group Management ⓘ

[Review Suggested Classification \(BETA\)](#)

Edit

- ▼ stealthwatch.com ⓘ
 - ▼ Inside Hosts ⓘ
 - Catch All ⓘ
 - Blackhole ⓘ
 - ▼ Business Units ⓘ
 - Contracts ⓘ
 - Development ⓘ
 - Engineering ⓘ
 - Executives ⓘ
 - ✓ Finance ⓘ
 - Human Resources ⓘ
 - Operations ⓘ
 - QA ⓘ
 - Sales and Marketing ⓘ
 - By Function ⓘ
 - By Location ⓘ
 - Cloud Hosts ⓘ
 - Compliance Systems ⓘ
 - Outside Hosts ⓘ

Finance Host Group ID: 137

HOST GROUP NAME *

Finance

PARENT HOST GROUP

Inside Hosts → Business Units

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES ⓘ

ex. 192.168.10.10, 192.168.10, 192.168.10-100, 192.168.10.0/24

[Import IP Addresses and Ranges](#)

ADVANCED OPTIONS ⓘ

- Enable baselining for hosts in this group
- Disable security events using excluded services
- Disable flood alarms and security events when a host in this group is the target
- Trap hosts that scan unused addresses in this group
- Send flows to Cognitive Threat Analytics

[Import All](#)

[Export All](#)

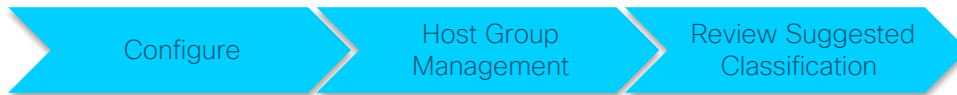
Cancel

Save



Stealthwatch Host Classifier

(ограниченная доступность, бета)



1. Автоматическое распределение хостов по 11 группам
2. Обучение алгоритма классификации по реакции пользователя
3. Анализ выполняется полностью локально, данные не отправляются в облако

Stealthwatch Host Classifier (BETA)

Classification Searches

SUGGESTED (100) Confirmed (0) Excluded (0)

Manually Confirm Automatically Confirm

Confirm that these hosts belong to the *Web Servers* host group, or exclude from future suggestions for this search.

#	IP ADDRESS	HOST NAME	CURRENT HOST GROUPS	LAST TIME MATCH	ACTIONS
1	10.201.0.23		Atlanta, Datacenter, Terminal Servers	8/8/2018	⋮
2	209.182.185.26	mail2.lancope.com	Datacenter	8/8/2018	⋮
3	10.192.102.12		Catch All	8/8/2018	⋮
4	10.192.101.13		Compliance Systems	8/8/2018	⋮
5	209.182.177.5	alp03-thor.lancope.com	Datacenter	8/8/2018	⋮
6	10.192.102.32		Catch All	8/8/2018	⋮
7	10.10.30.23		End User Devices, Domain Controllers, New ...	8/8/2018	⋮
8	10.192.103.22		Catch All	8/8/2018	⋮
9	10.192.102.11		Catch All	8/8/2018	⋮
10	209.182.184.1	lchqer01.lancope.com	Datacenter	8/8/2018	⋮

Управление пользователями

Global
Settings










User Management

User Management

Users

Data Roles

Create 

USER NAME	FULL NAME	MASTER ADMIN 	CONFIG MANAGER 	ANALYST 	POWER ANALYST 	DATA ROLE	STATUS	ACTIONS
<input type="text" value="Ex. jsmith"/>	<input type="text" value="Ex. 'John Smith'"/>					<input type="text" value="Ex. 'All Data(Read & Write)'"/>	<input type="text" value="Ex. On"/>	
admin	Admin User	✓				All Data (Read & Write)	<input checked="" type="checkbox"/> On 	
bbayles	Bo Bayles				✓	All Data (Read & Write)	<input checked="" type="checkbox"/> On 	
lahoskin	Lance Hoskins		✓	✓	✓	All Data (Read & Write)	<input checked="" type="checkbox"/> On 	
showadmin	Beta Admin	✓				All Data (Read & Write)	<input checked="" type="checkbox"/> On 	
swdemo	SW Analyst			✓		All Data (Read Only)	<input checked="" type="checkbox"/> On 	

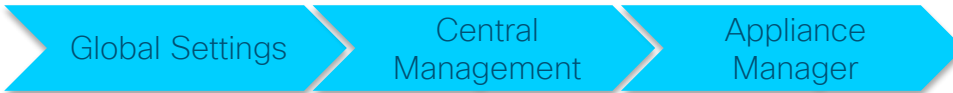
10  items per page

1 - 5 of 5 items   / 1  

Централизованное управление устройствами и обновлениями

- Поддержание системы в актуальном состоянии не должно отвлекать вас от обеспечения ИБ!
- Предприняты меры для упрощения управления и обновления компонентов платформы Stealthwatch (SMC, Flow Collector, ...).

Appliance Manager



Stealthwatch Central Management

Appliance Manager

Update Manager

App Manager

Inventory

2 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	Up to date	BetaFCNF01	Flow Collector FCNFVE-VMware-564d4655aaa46cd6-772d71786fdb8f3f	10.1...	⋮
Up	Up to date	BetaSMC01	SMC SMCVE-VMware-564dbb024469ba8c-acfc70615ef732b8	10.1...	⋮

- Edit Appliance Configuration
- View Appliance Statistics
- Manage Licenses
- Support
- Reboot Appliance
- Shut Down Appliance
- Remove This Appliance

Update Manager

Global Settings

Central Management

Update Manager



Stealthwatch Central Management

Appliance Manager

Update Manager

App Manager



Update Manager

Update Information ⓘ

Use the Update Manager page to apply software upgrades, updates, and patches. The SMC and Flow Collector must be on for at least 1 hour but no more than 1 week to be updated. For best results, perform the update procedures on each appliance in the following order:

- 1 All UDP Directors (also known as FlowReplicators) ⓘ
- 2 Flow Collector 5000 Series Databases
- 3 Flow Collector 5000 Series Engines
- 4 All other Flow Collectors

- 5 Endpoint Concentrator ⓘ
- 6 Secondary Stealthwatch Management Console
- 7 Primary Stealthwatch Management Console
- 8 All Flow Sensors

Upload

Upload one file at a time.

For important instructions, download the Stealthwatch Update Guide from the [Download & License Center](#).

System Updates ⓘ

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	BetaSMC01	10.192.102.21	29 days ago ⓘ	7.0.0 2018.07.08.0734-0	-		⋮
Flow Collector	BetaFCNF01	10.192.102.22	29 days ago ⓘ	7.0.0 2018.07.08.0732-0	7.0.0 2018.07.08.0732-0	Waiting to Install	⋮

Stealthwatch Apps

- Как быстро модифицировать функционал, не обновляя систему? Конечно, аппы!
- Два аппа первой волны:
 - [Stealthwatch Visibility Assessment](#)
 - упрощение пилотов, создание «отчётов для руководства» в существующих развёртываниях Stealthwatch
 - [Stealthwatch Host Classifier](#)
 - экономия времени и сил (и простота масштабирования) за счет динамического обнаружения и классификации основных ресурсов в сети (текущий статус: beta)

Stealthwatch Apps

Global Settings

Central Management

App Manager



Stealthwatch Central Management

Appliance Manager

Update Manager

App Manager



App Manager

Install App

Use the App Manager page to install Stealthwatch apps. Apps are available from the [Download & License Center](#).

Select a file to upload and install:

Browse

No file selected

A file must begin with "app". Upload one file at a time.

Пример аппа

Apps

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
Visibility Dashboard		9999.99.99	UpToDate	-	Uninstall

Отдельные «аппы», которые можно устанавливать и обновлять независимо от платформы Stealthwatch

Stealthwatch Visibility Assessment

Dashboard

Visibility Assessment

Cisco Stealthwatch

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy



Desktop Client



Network Visibility Dashboard (updated 5 min ago)

Internal Network
Scanners

25

Remote Access
Breach

03

Possible Malware

03

Internal Protocol
Servers

04

DNS Risks

11

Internal Monitored Network

1k

Hosts communicating within your network



6.64 TB

Internal traffic occurring on your network

2.22 TB

Traffic exchanged between your network and the internet

7.13 TB

Encrypted Traffic exchanged between your network and the internet

Traffic to High Risk Countries

447 GB

Traffic to or from high risk countries

High risk countries without traffic

High risk countries with traffic



- Теперь апп Stealthwatch **Visibility Assessment** выглядит так
- Наглядное представление ситуации как в рамках пилота, так и в процессе эксплуатации
- Вы сразу видите признаки «интересных» действий, включая:
 - взаимодействие по telnet
 - обмен по SMB
 - «незапланированные» DNS- и DHCP-серверы
 - хосты, использующие протоколы удаленного доступа

Turn on comment mode to collaborate on this prototype

0 Comments

OFF

Интеграция с Identity Services Engine (ISE)

- Stealthwatch интегрируется с ISE для получения дополнительных данных о пользователях и контексте взаимодействия
- Теперь мы можем осуществлять более тонкую нейтрализацию с помощью ANC-политик ISE
- Естественно, метки SGT также могут сослужить большую пользу

Усовершенствования интеграции с ISE

- ① Быстрая нейтрализация с помощью ANC-политик ISE – например, от уровня угрозы

Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 10.90.90.101

ISE	Username	MAC	ANC Policy
CiscoISE	dusti	1c:4d:70:e2:ea:9d	No policy appl... No policy applied ANC_Shutdown ANC_Suspicious ANC_NO_WEB ANC_Quarantine



Host Summary

Host IP: 10.90.90.101

Flows | Classify | History

Status: Active

Hostname: --

Host Groups: End User Devices, Main Campus Building 2

Location: RFC 1918

First Seen: 6/29/18 5:57 PM

Last Seen: 7/24/18 6:02 PM

Policies: Client IP Policy, Inside

MAC Address: 00:50:56:b6:37:1d (VMware, Inc.)

ISE ANC Policy: ANC_Suspicious Edit

- ② Метки SGT, которые считываются с ISE, теперь можно использовать в CSE совместно с IP-адресами (может быть полезно и при SDA)

- ③ Усовершенствования производительности и поддержка нескольких кластеров ISE

When any host within *Compliance Systems*; as a user with a TrustSec ID of 7 communicates with any host within *Outside Hosts*, an alarm is raised.

FIND

SUBJECT HOST GROUPS: Compliance Systems

PEER HOST GROUPS: Outside Hosts

SUBJECT TRUSTSEC IDS: 7

Классический периметр

Периметр: набор апробированных 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)

На чем фокусироваться?

Совсем новое

Duo MFA

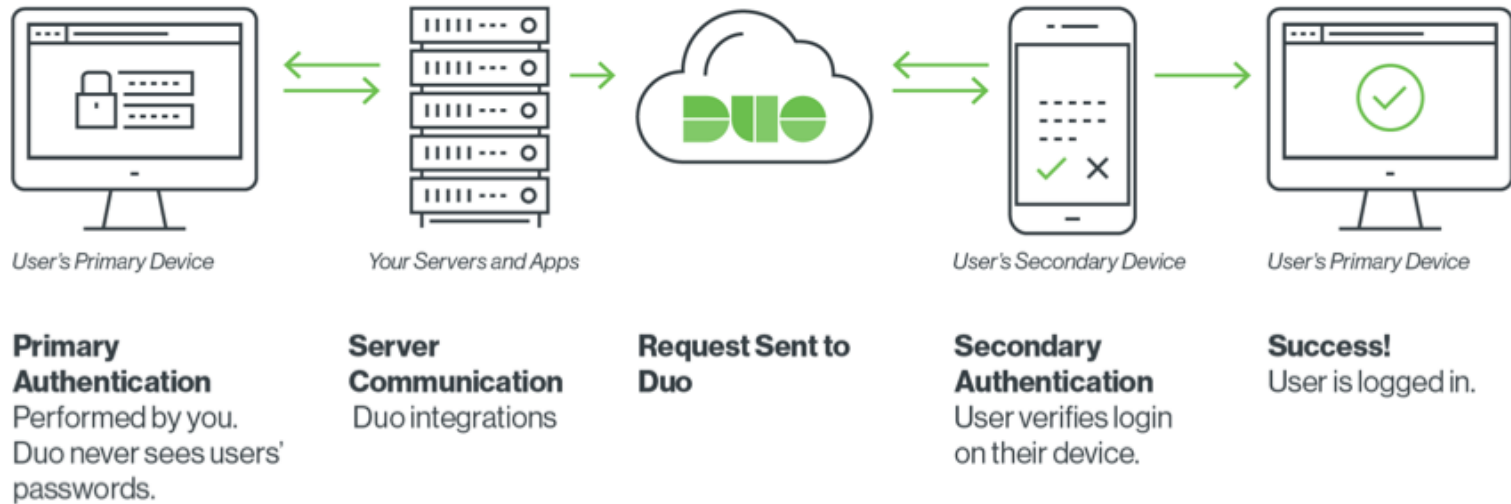


Duo Security is
now part of Cisco.



isco and/or its affiliates. All rights reserved.

Duo – обзор



Мультифакторная аутентификация (MFA)

Самый широкий спектр вариантов



Push



Soft Token



SMS



Звонок



U2F



И это!!!

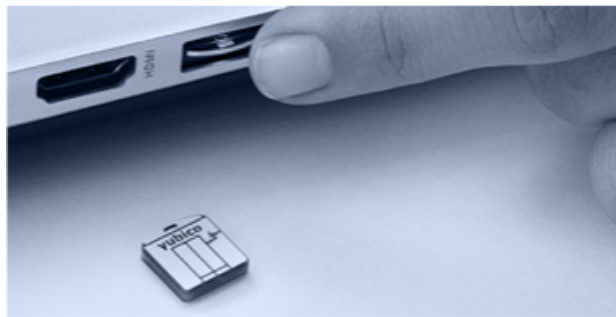
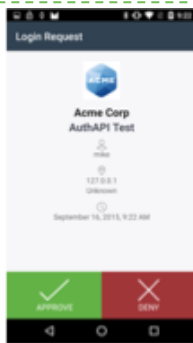


Biometrics



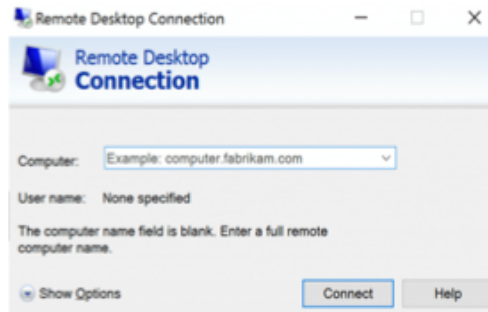
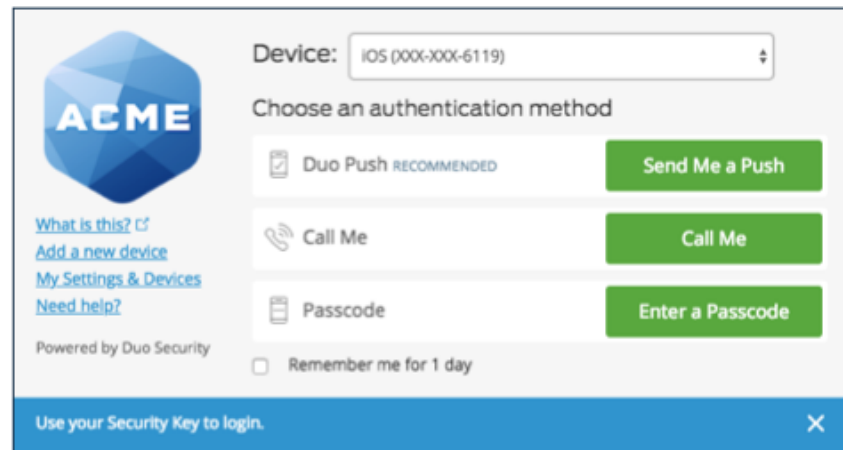
HW Tokens

Одна «галочка»



Что мы предлагаем

- Простое повышение уровня защищенности
- Защита доступа к конкретным системам
- Защита доступа, если вы используете RADIUS/LDAP
- Защита доступа к облачным приложениям
- Защита доступа к внутренним приложениям
- И даже немного posturing-a

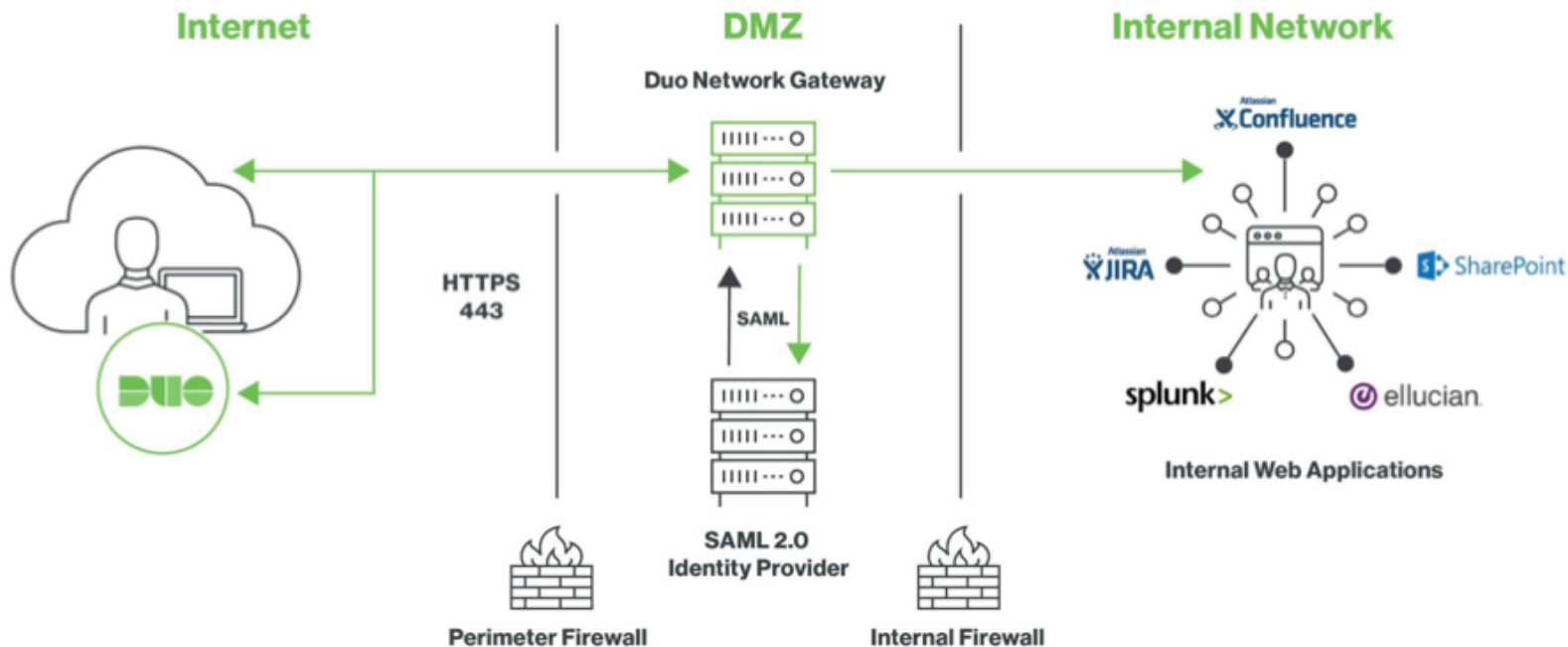


Более 60 SAML-приложений "из коробки"!

- [Adobe Document Cloud](#)
- [Amazon Web Services](#)
- [Asana](#)
- [BambooHR](#)
- [BlueJeans](#)
- [Bomgar](#)
- [Bonusly](#)
- [Box](#)
- [Canvas](#)
- [Cisco WebEx](#)
- [Clarizen](#)
- [CloudLock](#)
- [Confluence](#)
- [CrashPlan](#)
- [Datadog Desk](#)
- [DocuSign](#)
- [Dropbox](#)
- [Egnyte](#)
- [Evernote](#)
- [Expensify](#)
- [Freshdesk](#)
- [G Suite](#)
- [GitHub Enterprise](#)
- [GoToMeeting](#)
- [Greenhouse](#)
- [HackerOne](#)
- [Heroku](#)
- [Intacct](#)
- [JIRA](#)
- [Jamf Pro](#)
- [Jitbit](#)
- [Looker](#)
- [Marketo](#)
- [Meraki](#)
- [Namely](#)
- [New Relic](#)
- [Office 365](#)
- [OpenDNS](#)
- [PagerDuty](#)
- [Remedyforce](#)
- [RingCentral](#)
- [Robin](#)
- [Salesforce](#)
- [Samanage](#)
- [Sauce Labs](#)
- [ShareFile](#)
- [Signal Sciences](#)
- [Slack](#)
- [Smartsheet](#)
- [Splunk](#)
- [StatusPage.io](#)
- [SugarCRM](#)
- [Sumo Logic](#)
- [Syncplicity](#)
- [Tableau](#)
- [Tableau Online](#)
- [Udemy](#)
- [UserVoice](#)
- [Workplace by Facebook](#)
- [Zendesk](#)
- [Zoom](#)

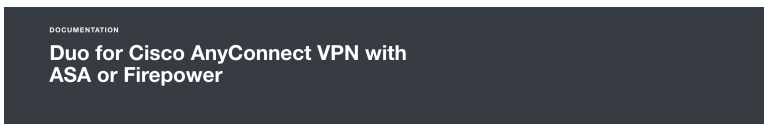
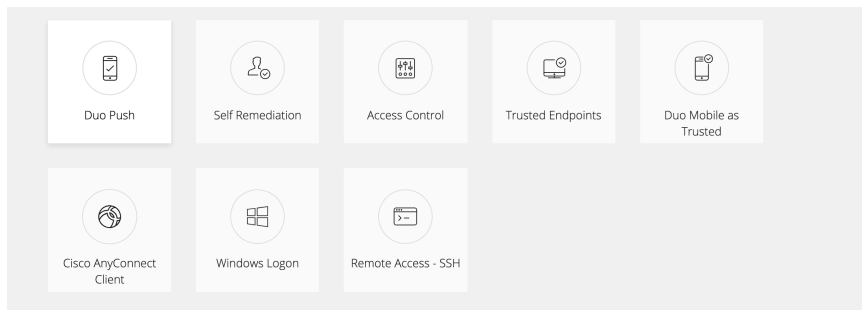
И другие

Всё ещё строите VPN для доступа к web-приложениям? Мы можем помочь и с VPN, но:



«Потрогать» бы?

- <https://demo.duo.com/>
- Телефон Ваш, а стенды наши – реалистичные сценарии



Contents

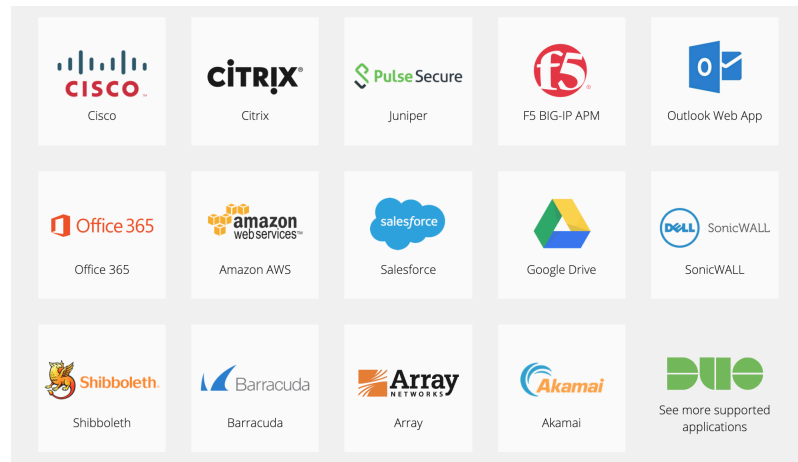
Cisco ASA with AnyConnect

ASA SSL VPN using SAML
ASA SSL VPN using RADIUS
ASA SSL VPN using LDAPs
Cisco Firepower with AnyConnect

Duo integrates with your Cisco ASA or Firepower VPN to add tokenless two-factor authentication to AnyConnect logins.

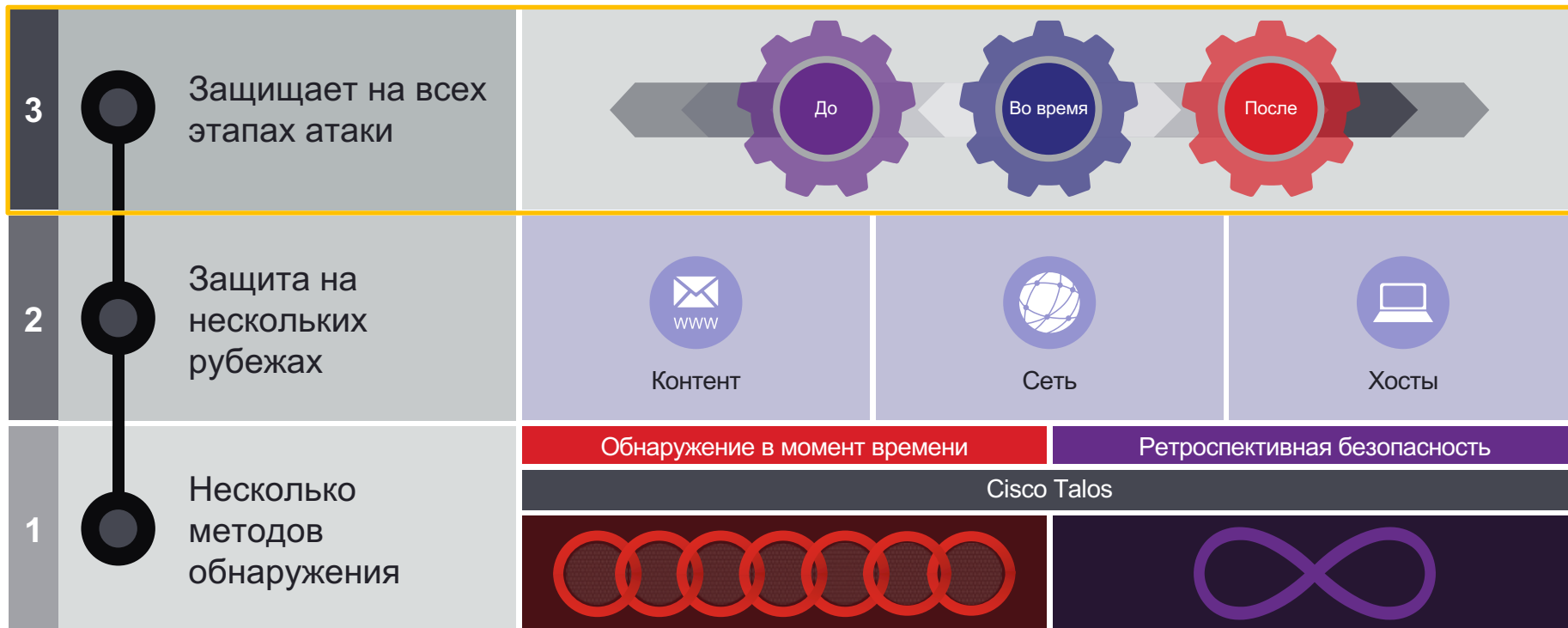
Duo can add two-factor authentication to ASA and Firepower VPN connections in a variety of ways. Learn more about these configurations and choose the best option for your organization.

Cisco ASA with AnyConnect



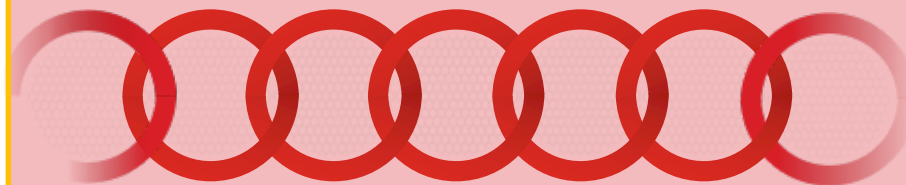
Cisco AMP (4E и не только)

3 преимущества Cisco AMP



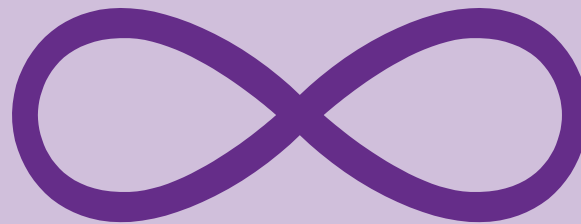
В Cisco AMP учтен как план А, так и план Б

Обнаружение в момент времени



Репутация и поведенческий анализ

Ретроспективная безопасность



Непрерывная защита

Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

Фильтрация по репутации

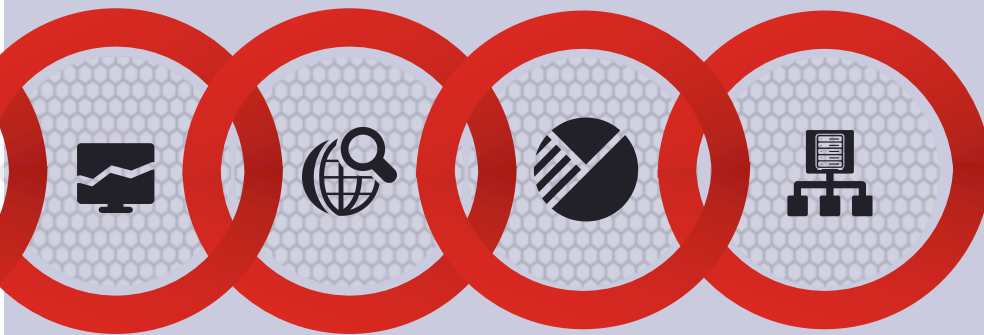


Идентичная
сигнатура

Нечеткие
идентифицирующие
метки

Машинное
обучение

Поведенческое обнаружение



Признаки
компрометации

Динамический
анализ

Расширенная
аналитика

Сопоставление
потоков устройств

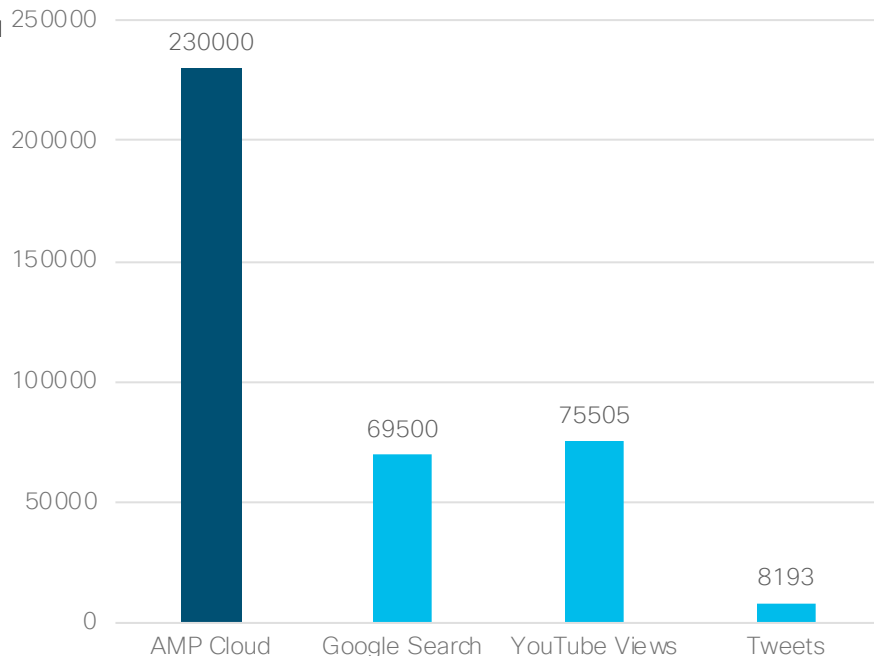


AMP for Endpoints

Более 34% файлов, признанных вредоносными **Talos**, не считались таковыми в Virus Total на момент анализа



Обращения к облаку: пик 230K QPS в 2018



Источник: AMP Cloud and <http://www.internetlivestats.com>

А также...

ПРЕДОТВРАЩЕНИЕ

Время обнаружения
(TTD)

В памяти

Защита системы

Предотвращение
эксплоитов

На диске

AMP Cloud

MAP

Tetra

Пользовательские
индикаторы

Пост-инфекция

DFC

CTA

Cloud IOC

Client Side IOC

И ещё одна платформа

Cisco AMP Visibility

=

Cisco Visibility

=

Cisco Threat Response*



How to Enable Cisco Threat Response

<https://visibility.amp.cisco.com/>
<https://visibility.eu.amp.cisco.com/>

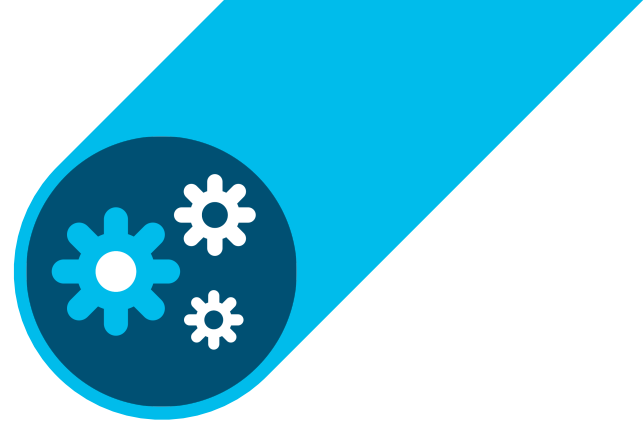
Cisco Threat Response



- Ключевой элемент интегрированной архитектуры Cisco
- Обеспечивает локализацию глобальных данных threat intelligence в контекст безопасности инфраструктуры организации
- Снижает сложность за счет
 - обогащения сведений о *наблюдаемых объектах* автоматически из нескольких источников (ускорение понимания)
 - представления результатов в интуитивно понятной форме в рамках одной системы (ускорение осознания)
- Помогает выделить вредоносные *наблюдаемые объекты* и ускорить реагирование на инциденты
- Помогает специалистам по расследованию инцидентов лучше понимать ситуацию в их инфраструктуре, собирая и комбинируя threat intelligence, доступную от Cisco и сторонних организаций

Основные термины и идеи Threat Response

- Modules (Модули)
- Observables (Наблюдаемые объекты)
- Investigate UI (Графический интерфейс специалиста по расследованию)
- Judgements (Суждения)
- Verdicts (Вердикты)
- Sightings (Обнаружение)
- Indicators (Индикаторы)
- Targets (Цели)
- Snapshots (Моментальный снимок)
- Casebooks (Справочники)



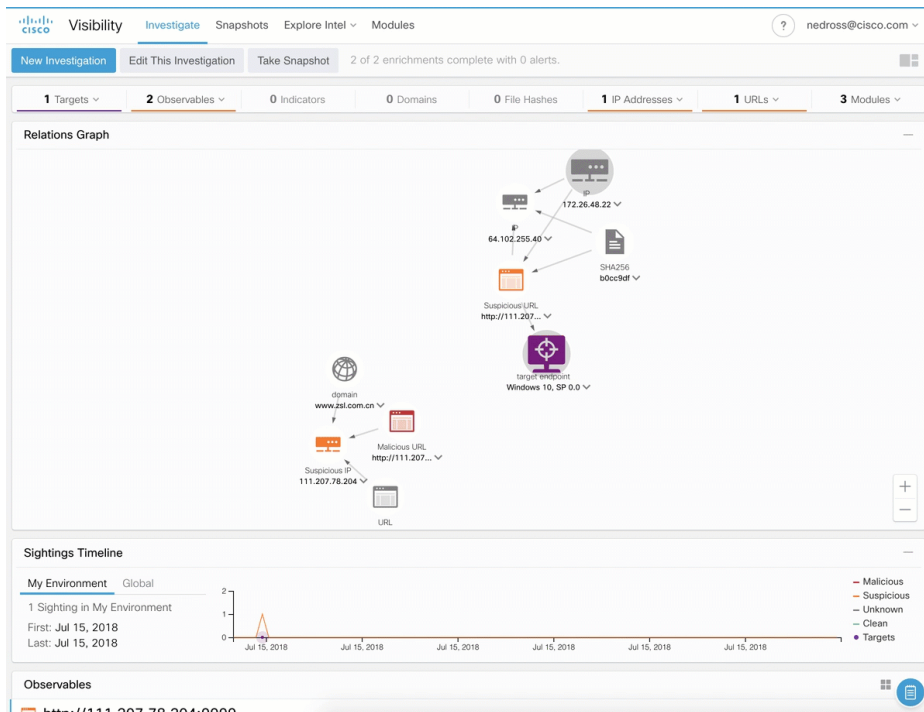
Использование Cisco Threat Response

Я – заказчик Cisco, использующий Cisco Threat Response

Моя команда может

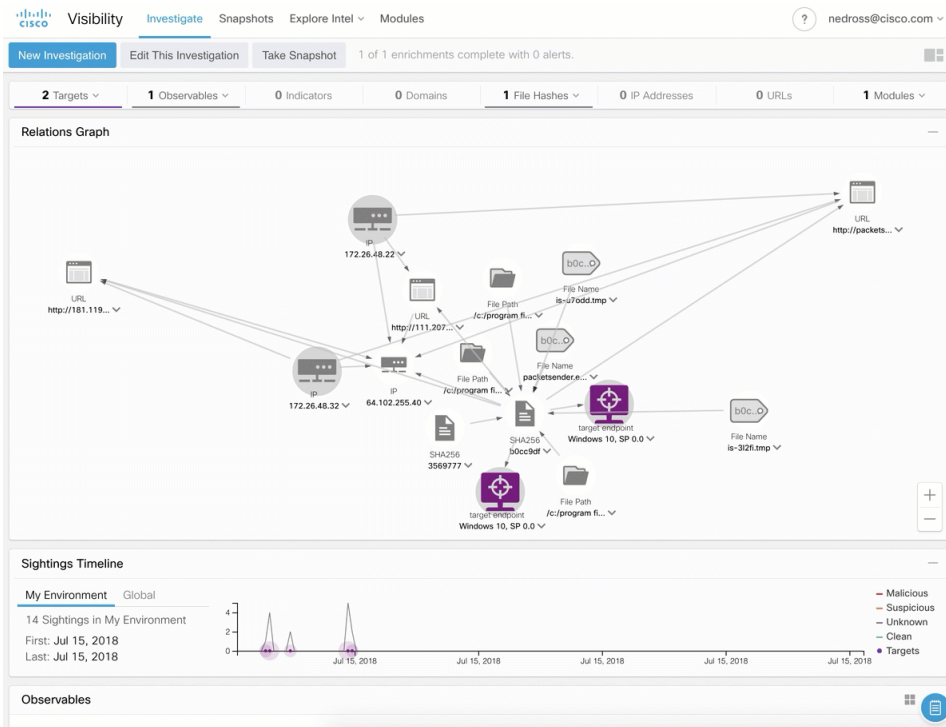
- оперативно оценивать наблюдаемые объекты
- блокировать и разблокировать домены из Cisco Threat Response
- блокировать и разблокировать исполнение файлов из Cisco Threat Response
- анализировать следы, ассоциированные с известными кампаниями, и немедленно оценивать воздействие кампании на организацию
- сохранить моментальные снимки расследований для дальнейшего анализа
- документировать результаты работы над инцидентом с помощью журналов
- легко интегрировать Cisco Threat Response в существующие процессы и собственные инструменты

Оперативная оценка наблюдаемых объектов



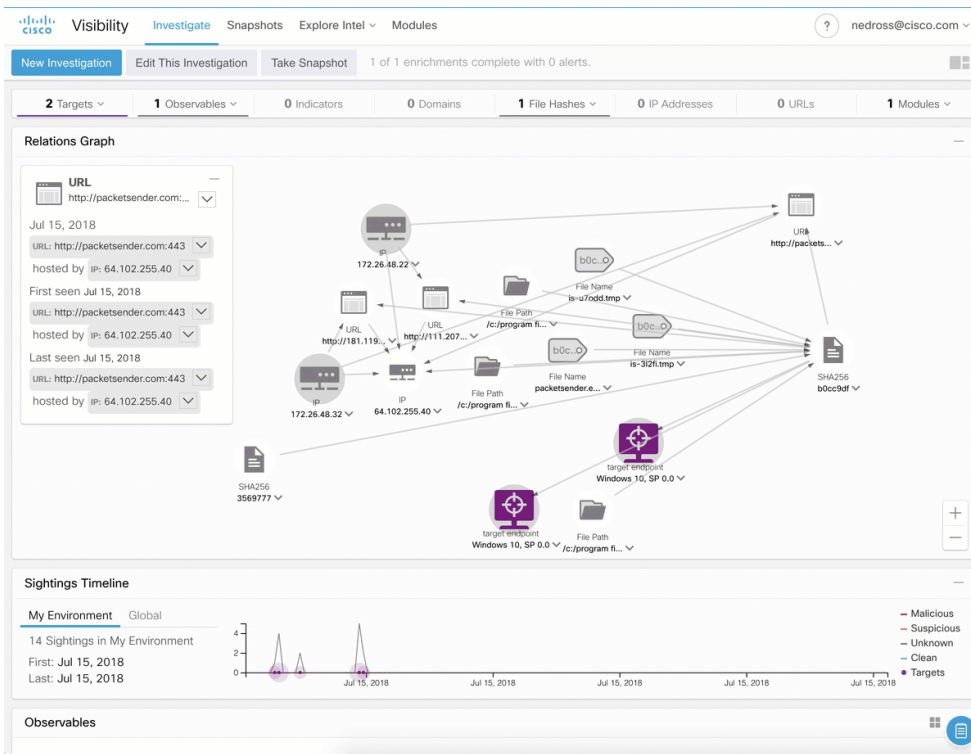
- Неизвестная диспозиция
- (почти) Моментальное представление воздействия на организацию
- Сведения о запуске кода и взаимодействиях

Моя команда может блокировать и разблокировать домены



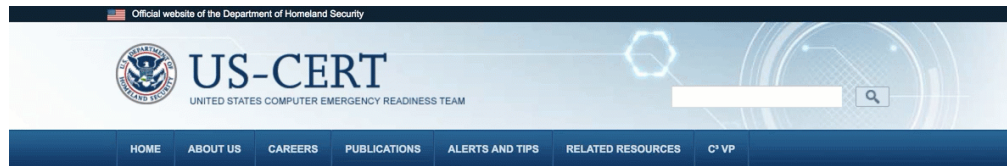
- Реализовать блокирование из Cisco Threat Response
- Блокировать через Cisco Umbrella
- Интеграционный API для блокирования и разблокирования

Моя команда может блокировать и разблокировать исполнение файлов



- Блокирование реализуется через Cisco Threat Response.
- Блокирование обеспечивается Cisco AMP for Endpoints.
 - и через AMP Unity в NGFW, WSA, ESA и т.д.
- Интеграционный API для блокирования и разблокирования

Анализ следов, ассоциированных с известными кампаниями, и оценка воздействия



Information For

Control System Users

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats.

HIDDEN COBRA - North Korean Malicious Cyber Activity

The information contained on this page is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) to provide technical details on the tools and infrastructure used by cyber actors of the North Korean government. The intent of sharing this information is to enable network defenders to identify and reduce exposure to North Korean government cyber activity. The U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA.

For more information, see:

- June 14, 2018: Malware Analysis Report (10135536-12) – North Korean Trojan: TYPEFRAME
- May 29, 2018: Alert (TA18-149A) HIDDEN COBRA – Joannap Backdoor Trojan and Brambul Server Message Block Worm
- May 29, 2018: Malware Analysis Report (MAR-10135536-3) – HIDDEN COBRA RAT/Worm
- March 28, 2018: Malware Analysis Report (MAR-10135536.11) – North Korean Trojan: SHARPKNOT
 - STIX file for MAR-10135536.11
- February 13, 2018: Malware Analysis Report (MAR-10135536-F) – North Korean Trojan: HARDRAIN
 - STIX file for MAR-10135536-F
- February 13, 2018: Malware Analysis Report (MAR-10135536-G) – North Korean Trojan: BADCALL
 - STIX file for MAR-10135536-G
- December 21, 2017: Malware Analysis Report (MAR-10135536) – North Korean Trojan: BANKSHOT
 - STIX file for MAR-10135536
- November 14, 2017: Alert (TA17-318A) HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL
- November 14, 2017: Alert (TA17-318B) HIDDEN COBRA – North Korean Trojan: Volgmer
- August 23, 2017: Malware Analysis Report (MAR-10132963) – Analysis of Delta Charlie Attack Malware
 - STIX file for MAR-10132963
- June 13, 2017: Alert (TA17-164A) HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure
- May 12, 2017: Alert (TA17-132A) Indicators Associated With WannaCry Ransomware

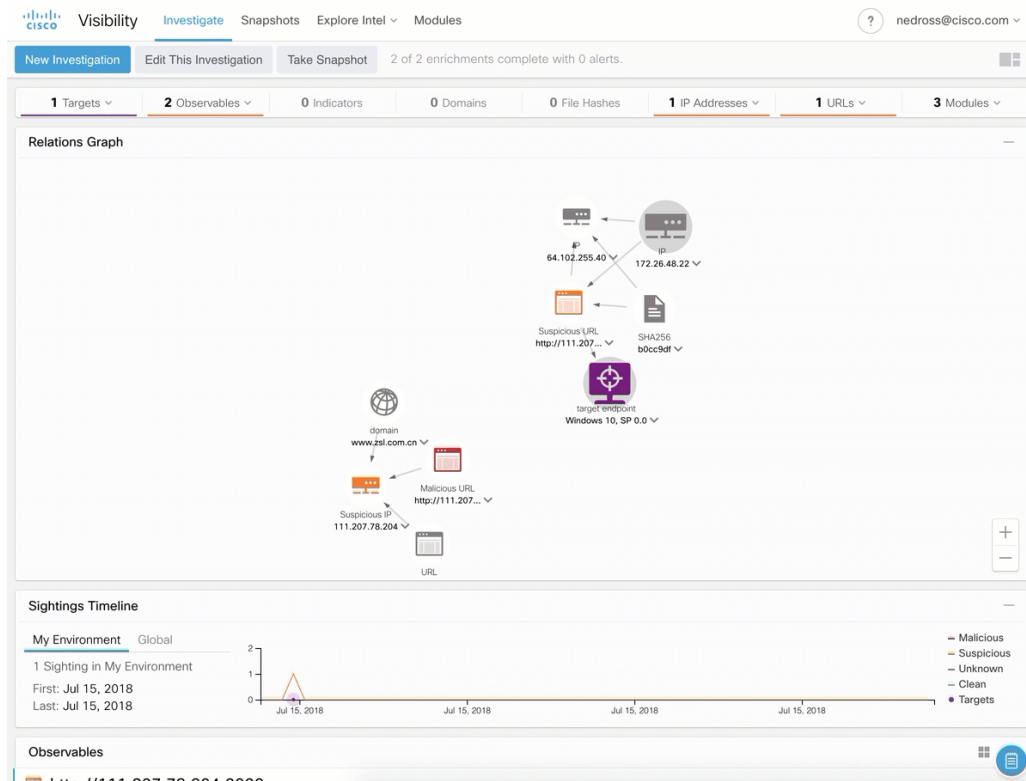
- Пострадавшие (цели)
- Дополнительные IP-адреса
- Ассоциированные программы

I Want To

Subscribe to Alerts

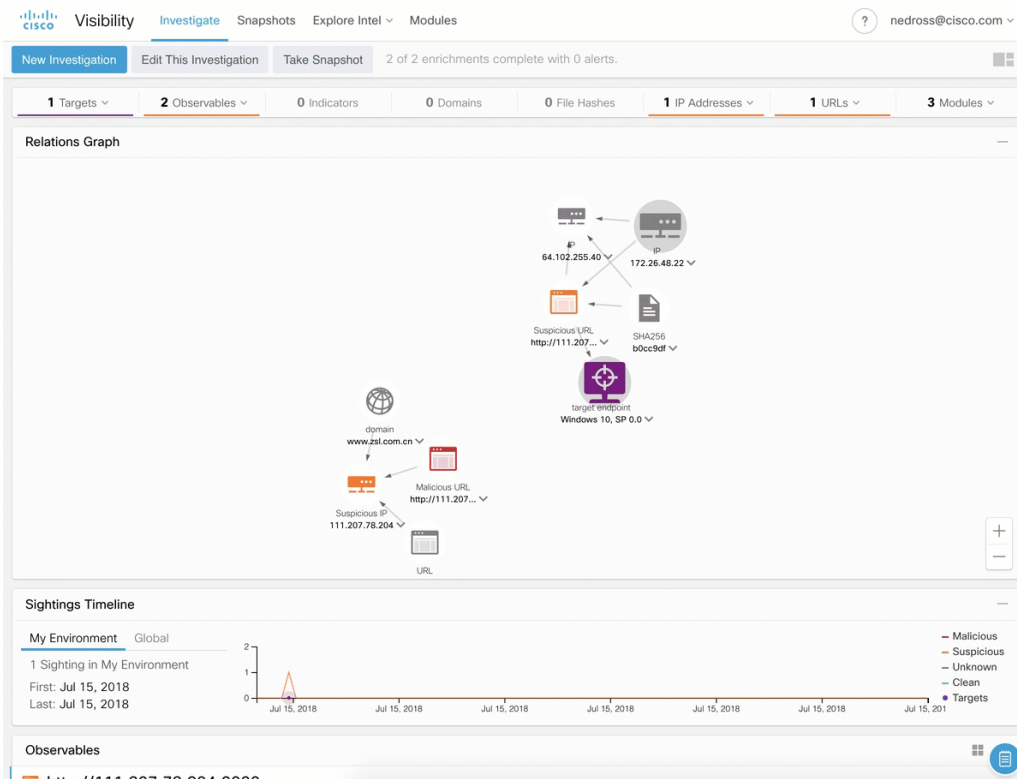
Contact Us

Моя команда может сохранять моментальные снимки расследований



- В определенное время
- Ссылка
- Возможность дальнейших расследований

Моя команда может документировать результаты анализа



Журналы работы над кейсами

- Доступны из множества продуктов
 - Официально интегрированные продукты
 - Неинтегрированные, но доступные через web продукты
- Записи и наблюдения для непрерывности процесса
- Немедленный доступ к
 - Вердиктам
 - Операциям реагирования

Моя команда может интегрировать Cisco Threat Response в существующие процессы

Cisco Threat Response разработан для интеграции с другими продуктами по ИБ через URL, который позволяет вам выстраивать эффективные процессы.

Примеры ниже исходят из того, что Cisco Threat Response располагается по адресу:
<https://visibility.amp.cisco.com>

Вы можете выполнить расследование, передавая поисковую строку через параметр q, который идет после фрагмента #/investigate в URL.

Разрешено использовать несколько поисковых элементов, просто разделяя их пробелом.

Убедитесь, что URL правильно использует все параметры.

<https://visibility.amp.cisco.com/#/investigate?q=domain.com>

<https://visibility.amp.cisco.com/#/investigate?q=google.com%0A8.8.8.8%0A6732417baa49b873d72747c0ef46f8d1>

Вы можете искать индикаторы, суждения (Judgements) и факты обнаружения (Sightings) на странице Explore. Аналогично странице Investigate, передайте поисковый запрос после параметра q для поиска интересующих угроз:

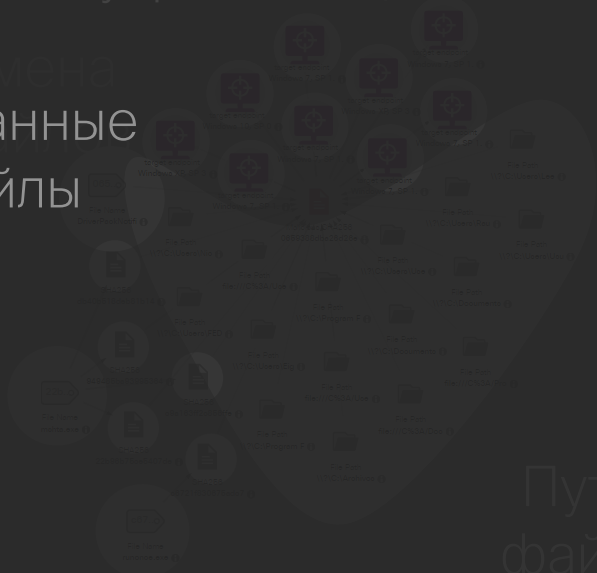
<https://visibility.amp.cisco.com/#/explore/indicators?q=rat>

<https://visibility.amp.cisco.com/#/explore/judgements?q=rat%20ip>

<https://visibility.amp.cisco.com/#/explore/sightings?q=662472b8378274eda5cc848536cba2db1d27f8ad>

Внутренние цели

Имена
Связанные
файлы



Пути
файла

0659386d1ba26a26e7d4a6a82e4331216210a2164d1664

My Environment

4 earnings in My Environment

Start: Mar 31, 2010

End: Apr 1, 2010

Investments (1)

Метка	Описание	Видео	Ссылка	Тег	Ссылка
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				
1000000	Метрика				

Локальное
обнаружение

Глобальные данные

Резюме

Cisco Threat Response снижает сложность растущего числа инструментов для расследования

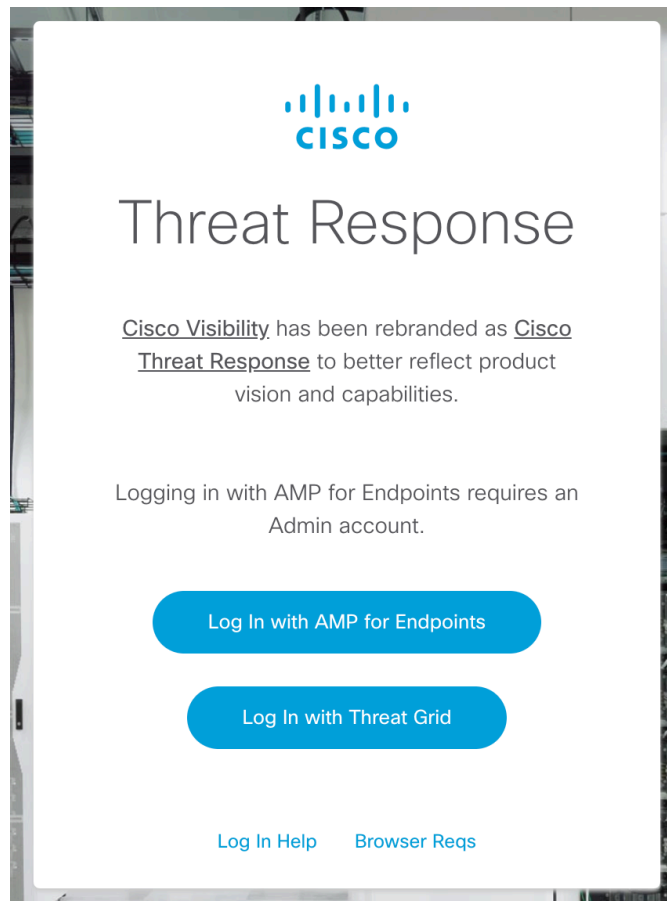
- Соединяет внешние данные threat intelligence с внутренними данными логов
- Комбинирует данные из множества источников – Cisco и сторонних организаций
- Единое окно для многих задач по реагированию на инциденты
- До, во время и после атаки
- Снижает время расследования, приоритезации и реагирования


СКОЛЬКО ЭТО СТОИТ?

- Вы приобретаете AMP for Endpoints? Бесплатно!
- Вы приобретаете Cisco Threat Grid? Бесплатно!
- В ближайшем будущем WSA, ESA, Firepower...

Вы уже пользуетесь одним из этих решений?

У вас уже есть доступ!





Threat Response

Cisco Visibility has been rebranded as Cisco Threat Response to better reflect product vision and capabilities.

Logging in with AMP for Endpoints requires an Admin account.

[Log In with AMP for Endpoints](#)

[Log In with Threat Grid](#)

[Log In Help](#) [Browser Reqs](#)

Слайды и пара сценариев... но речь же про IR

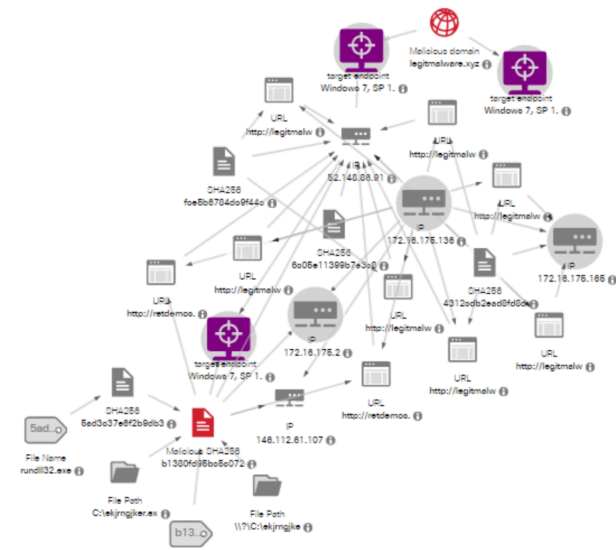
Российская команда Cisco Security регулярно проводит бесплатные Threat Hunting Workshop-ы, помогая партнёрам и заказчикам получить опыт работы с Cisco Threat Response (и другими продуктами Cisco).

Следите за новостями, регистрируйтесь и участвуйте.

Если у вас есть группа специалистов, которым целесообразно посетить такой семинар, напишите нам на security-request@cisco.com!

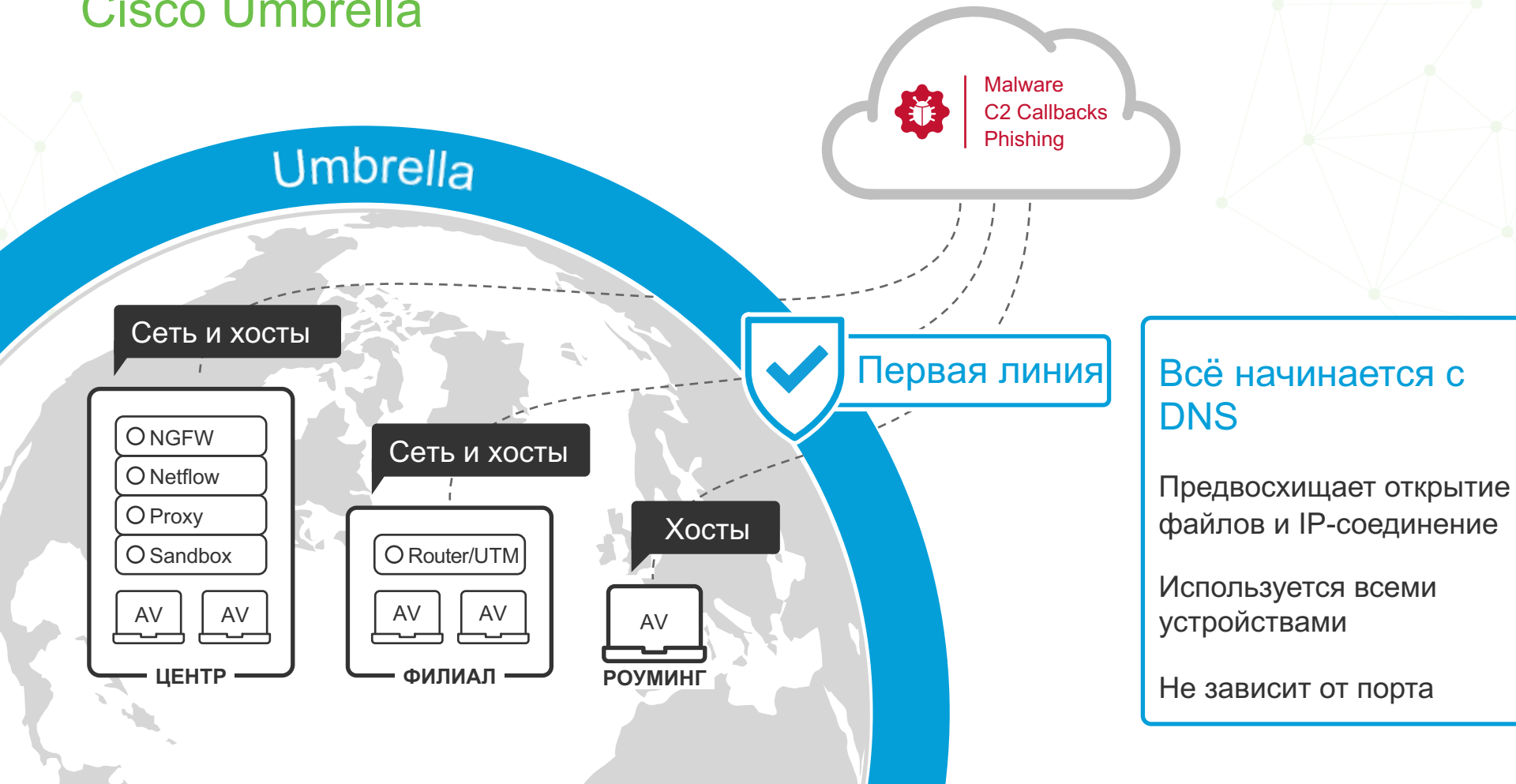
Threat Hunting Workshop

Hands On with Cisco Security Products



Umbrella

Cisco Umbrella



Сеть и хосты

○ NGFW

○ Netflow

○ Proxy

○ Sandbox

AV

AV

ЦЕНТР

Сеть и хосты

○ Router/UTM

AV

AV

ФИЛИАЛ

Хосты

AV

РОУМИНГ

Первая линия

Malware
C2 Callbacks
Phishing

Всё начинается с
DNS

Предвосхищает открытие
файлов и IP-соединение

Используется всеми
устройствами

Не зависит от порта

Архитектура Cisco Umbrella

КАТЕГОРИЯ	IDENTITY
MALWARE	INTERNAL IP
C2 CALLBACK	HOSTNAME
PHISHING	AD USER
CUSTOM (API)	HOSTNAME

Umbrella
(Блокирование)



Cloud Security

Investigate
(Аналитика)



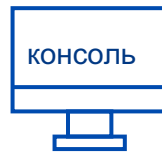
СТАТУС И УРОВЕНЬ
СВЯЗИ
ВЗАИМОДЕЙСТВИЯ
АТРИБУЦИЯ
ШАБЛОНЫ И ГЕО-
данные



208.67.222.222



ДОМЕН, IP, ASN, EMAIL, ХЭШ



КОНСОЛЬ

API



SIEM
и т.п.

Umbrella Resolver: обработка запросов

Результат

Изначально запрошенный ресурс или страница блокировки

Контроль безопасности

- DNS- и IP-фильтрация
- Инспекция подозрительных доменов через прокси
- SSL-decryption доступен

Интернет-трафик

Внутри сети и за её пределами



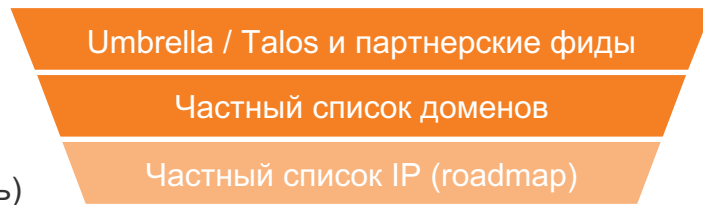
Блокировка на лету - аналитика офлайн

- Широта покрытия всех портов и глубина инспекции рискованных доменов

DNS- и IP-уровень

- Запрос Домена
- IP ответ (DNS-уровень)
или соединение (IP-уровень)

Блокировка на лету



РАЗРЕШИТЬ, БЛОКИРОВАТЬ ИЛИ PROXY

Оффлайн-аналитика

ПРЕДИКТИВНЫЕ ОБНОВЛЕНИЯ

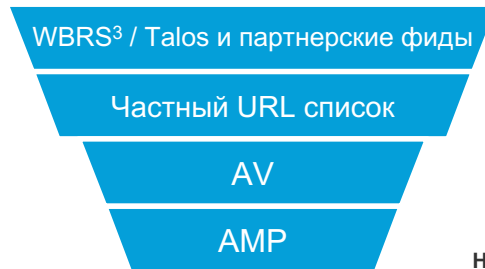


UMBRELLA
STATISTICAL
MODELS

ТЕЛЕМЕТРИЯ ВСЕГО ИНТЕРНЕТ

HTTP/S уровень

- URL запрос
- Хэш файла



РАЗРЕШИТЬ, БЛОКИРОВАТЬ ИЛИ АНАЛИЗИРОВАТЬ

НЕИЗВЕСТНЫЕ ФАЙЛЫ



AMP
THREAT
GRID

Зачем заказчику проводить пилоты Umbrella?

- ✓ Легкий способ попробовать Umbrella
- ✓ Не требует поставки оборудования или поддержки софта
- ✓ Внедрение менее чем за 30 минут, немедленные результаты
- ✓ Демонстрация пользы: немедленное блокирование ВПО
- ✓ Реальные результаты, которые легко проверить – и хотя бы наведение порядка за счет пилота!

Безопасность доступа к
облачным ресурсам и
сервисам (CAS)

- Cisco Threat Intelligence
- Cisco Threat Response
- Cisco Platform Exchange

Безопасность
электронной
почты

EMM-решения

Безопасный
доступ в
интернет (SIG)

Защищенные сети
SD-WAN /
маршрутизаторы

Борьба со
сложными
угрозами

Контроль доступа
к сети/идентификация и
аутентификация

Системы
обеспечения
безопасности
web-трафика

Коммутаторы
и точки
доступа

- Threat Intel/активная защита
- Полный объективный контроль
- Автоматизация управления политиками
- Осведомленность о контексте

Современные
МСЭ/СПВ

Защита
облачных
нагрузок

Системы
анализа трафика

Мы продолжаем развитие!



