



Интеграция безопасности, советы и рекомендации

Pavel Rodionov

Cybersecurity CSE, CCIE #11155, GREM

15 июня 2018

Программа

- Введение
- Термины и аббревиатуры
- TC-NAC
- Rapid Threat Containment
- Скрипты и автоматизация
- Заключение

Введение...



Pavel Rodionov

- Consulting Systems Engineer, Cisco Security
- Работаю в Cisco с февраля 2008
- Более 20+ лет опыта работы с сетями и IT безопасностью
- CCIE# 11155 (Routing and Switching)
- Отвечаю за Украину и СНГ

Термины и аббревиатуры

- **Карантин** – термин, который для каждого означает что-то свое
- **Endpoint Protection Services (EPS)** – Добавлен ISE 1.2. В версии 1.3 расширен с помощью pxGrid.
 - Может только поместить узел в карантин.
 - Используется с или без pxGrid
- **Adaptive Network Control (ANC)** – EPS переименован в ANC в 1.4. Новый функционал ANC добавлен в 2.0.
 - Создает классификацию ANC (также: name spaces) – и узлы могут быть привязаны к этой классификации.
 - Quarantine, Kick_off_Network, Investigate, Nuke_From_Orbit, etc.
 - Используется с или без pxGrid с v2.2+.
- **Rapid Threat Containment (RTC)** – “уровень решения” интеграции продуктов, которые используют ANC или EPS
- **Change of Authorization (CoA)** – Возможность динамически изменять уровень доступа, которое имеет узел в сети
- **Course of Action (CoA)** – Рекомендованное корректирующее действие для инфицированной системы.
- **TrustSec** – Простой тэг, который представляет полный контекст для узла/пользователя

Термины и аббревиатуры

- **Platform eXchange Grid (pxGrid)** – Шина связи (не API), созданная для быстрого обмена данными о безопасности, без необходимости использовать точечные API или привязки к приложениям.
 - Использует модель Publish/Subscribe (Pub/Sub) для обмена информацией.
 - Имеет механизмы Central, Proxy, и Broker.
- **Structured Threat Information Expression (STIX)** – Язык, который используется для обмена информацией Cyber Threat Intelligence (CTI), или: информация об угрозах.
 - Это формат, а не транспортный протокол. Он требует что-то вроде TAXII или pxGrid для того, чтобы передавать информацию между потребителями и источниками.
- **Trusted Automated eXchange of Intelligence Information (TAXII)** – Протокол, который используется для обмена CTI по зашифрованным каналам (HTTPS).
 - Создан специально для переноса STIX CTI.
 - Следует модели Publish / Subscribe (pub/sub), похожей на pxGrid – но только централизованной.
- **Common Vulnerability Scoring System (CVSS)** – Открытый стандарт для оценки серьезности компьютерных уязвимостей.

Threat Centric NAC (TC-NAC)

Векторы атак в новостях

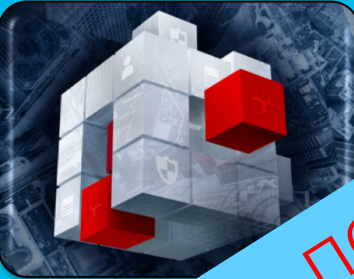
2016 Data Breach Investigations Report

verizon

89% of breaches had a financial or espionage motive.

2016 Verizon Breach Report

- “Все еще используются уязвимости”
- “Все патчи бесполезны, если не патчим правильные вещи”



2017 Cisco Annual Cybersecurity Report

- “Угроза исходят уязвимые браузеры и плагины.”
- “Угроза от злоумышленники ищут возможности использования непропатченного ПО”

Не позволяй угрозе попасть в сеть!

В реальной жизни

Inerable Software ?

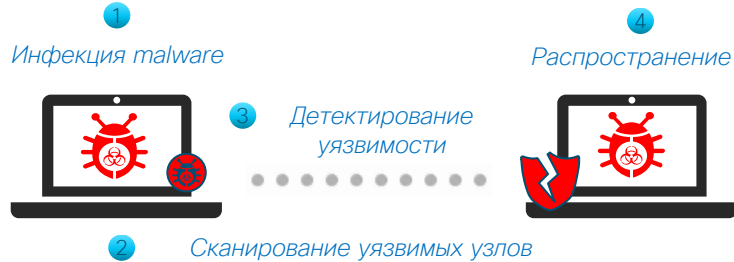
Day	Week					
+		Oracle Java(TM) Platform SE v1.8.0:update_144	ca681963c...cdb08bac	1	3 severe vulnerabilities	2018-06-15 09:56:19 EEST 6.8
+		Adobe Acrobat Reader v11.0.8	ed820c61c...07e7d5...	7	137 severe vulnerabilities	2018-06-14 20:17:27 EEST 10.0
+		Oracle Java(TM) Platform SE v1.7.0:update_21	7abf02adc...2f9320be	2	46 severe vulnerabilities	2018-06-14 19:37:52 EEST 6.4
+		Adobe Acrobat Reader v11.0.10	00d2ce2c3...dea0e4...	1	129 severe vulnerabilities	2018-06-14 19:06:20 EEST 10.0
+		Microsoft Silverlight v5.1.20913.0	f2a074150...7c667927	1	1 severe vulnerabilities	2018-06-14 18:49:29 EEST 7.1
+		Microsoft Office v2010	8cfb55087...10af6736	5	14 severe vulnerabilities	2018-06-14 18:17:04 EEST 9.3
+		Google Chrome v49.0.2623	1bc470250...820fe4bc	42	44 severe vulnerabilities	2018-06-14 16:21:48 EEST 9.3
+		Adobe Acrobat Reader v11.0.0	1c52b5001...5b7c68...	23	228 severe vulnerabilities	2018-06-14 15:47:43 EEST 10.0
+		Adobe Acrobat Reader v11.0.13	0e560b03d...c0b656...	1	17 severe vulnerabilities	2018-06-14 13:44:45 EEST 6.8
+		Oracle Java(TM) Platform SE v1.8.0:update_71	8e780cfc1...1bb3fe47	1	1 severe vulnerabilities	2018-06-14 10:30:43 EEST 7.6
+		Oracle Java(TM) Platform SE v1.8.0:update_92	3514c54f5...521fb437	1	6 severe vulnerabilities	2018-06-14 10:19:09 EEST 6.9
+		Microsoft Office v2010	ead478305...14d989...	3	10 severe vulnerabilities	2018-06-14 10:16:06 EEST 9.3
+		Oracle Java(TM) Platform SE v1.8.0:update_144	d231a49af...829a0b60	2	3 severe vulnerabilities	2018-06-14 09:51:27 EEST 6.8
+		Oracle Java(TM) Platform SE v1.8.0:update_131	4e996adc7...e4a585...	1	11 severe vulnerabilities	2018-06-14 09:31:18 EEST 6.8
+		Oracle Java(TM) Platform SE v1.7.0:update17	8ced15d60...0c4a59...	1	76 severe vulnerabilities	2018-06-14 09:26:04 EEST 10.0
+		Oracle Java(TM) Platform SE v1.7.0:update17	82559b36f...4f083fd5	1	76 severe vulnerabilities	2018-06-14 09:26:04 EEST 10.0
+		Oracle Java(TM) Platform SE v1.7.0:update17	8562121c7...cf8b76e3	1	76 severe vulnerabilities	2018-06-14 09:26:04 EEST 10.0
+		Oracle Java(TM) Platform SE v1.7.0:update40	19f1fc814...3808c796	1	27 severe vulnerabilities	2018-06-13 14:41:03 EEST 6.4

250 компьютеров, одна неделя...

Объяснение Threat Centric NAC

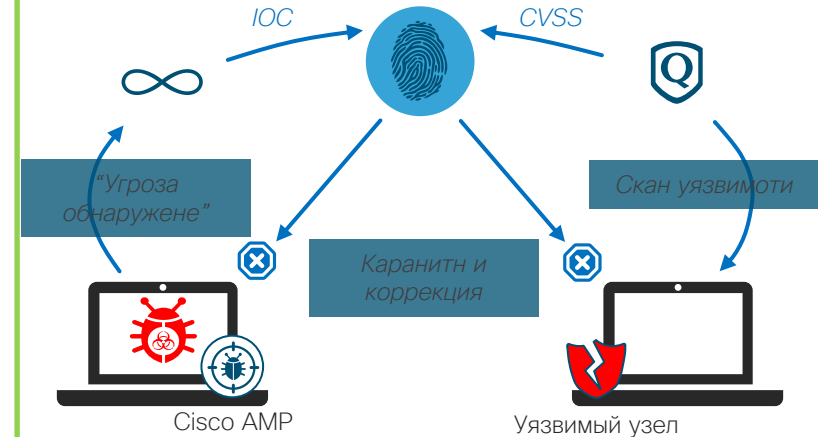
Уменьшить количество уязвимостей, сдержать угрозы

Проблема



Скомпрометированные узлы распространяют malware с помощью поиска известных уязвимостей в сети

Решение



Пометить скомпрометированные и уязвимые узлы и ограничить доступ в сегмент коррекции

Большинство AMP4E разворачиваются в режиме Audit

Threat Centric NAC

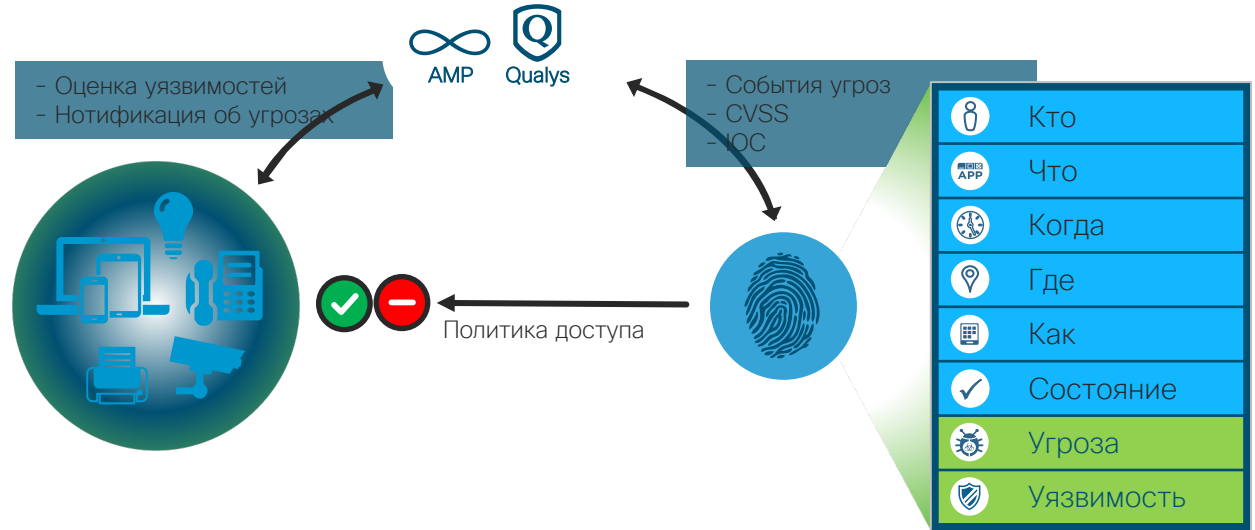
Cisco ISE защищает вашу сеть от брешей с помощью сегментации скомпрометированных и уязвимых узлов для исправления

Дополняет Posture
Данные об уязвимостях говорят об оценке состояния узла «извне»

Расширенное управление
поддерживается информацией об угрозах и данными оценки уязвимостей

Быстрое реагирование
с автоматизированной политикой, обновляемой в реальном времени на основании данных уязвимостей и метрики угроз.

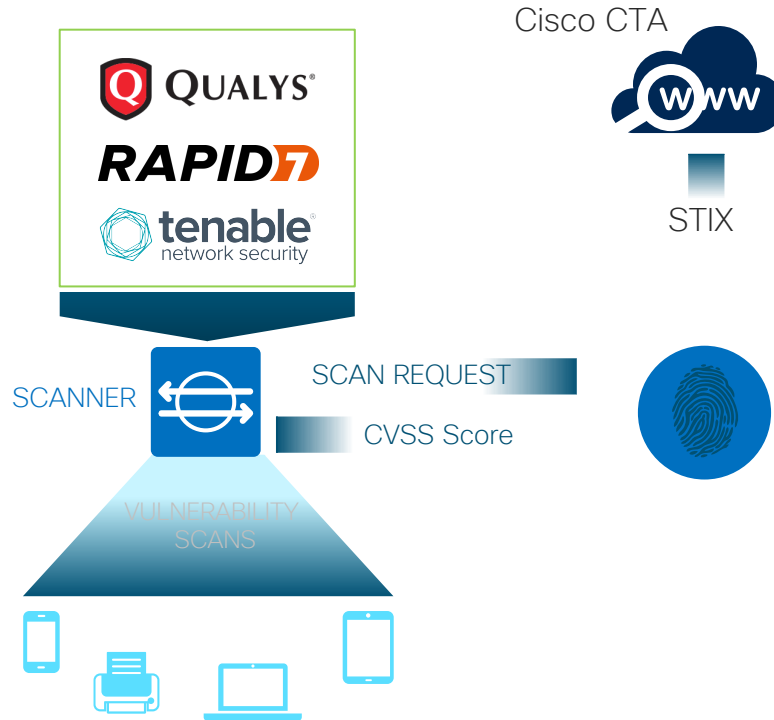
Создает политики авторизации ISE на основании информации об угрозах и уязвимостях



Threat Centric NAC

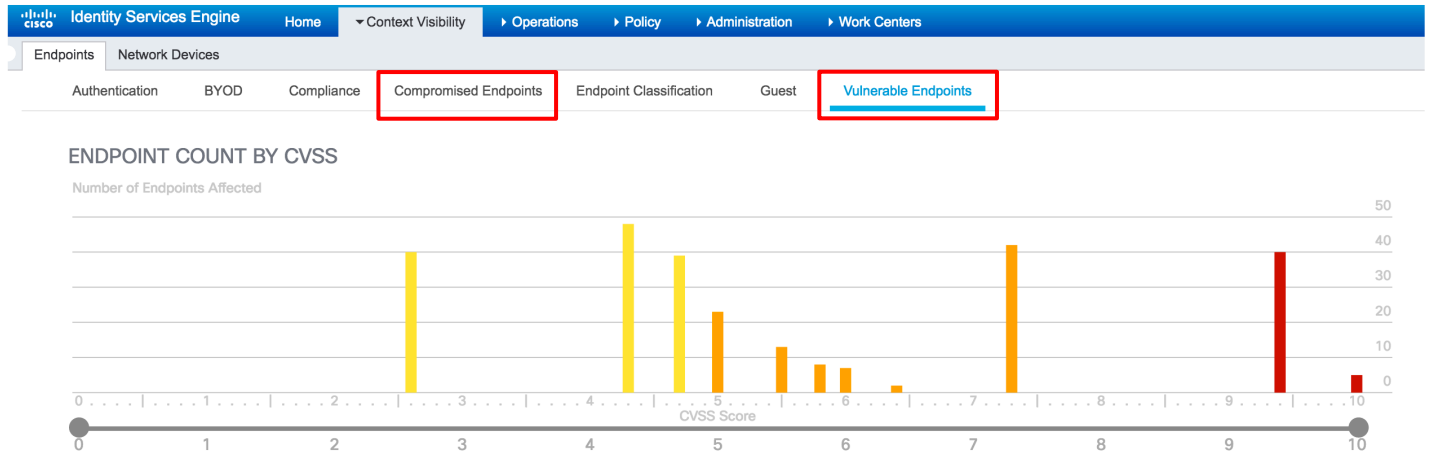
ISE 2.2

Выберите вендора оценки уязвимостей



- В ISE 2.2, TC-NAC поддерживает Tenable, Cisco Threat Analytics (CTA) и Rapid7.
- Стандартный “listener” поддерживается для угроз с использованием шаблонов STIX с автоматическим карантином для критически инфицированных узлов

TC-NAC сервис на ISE



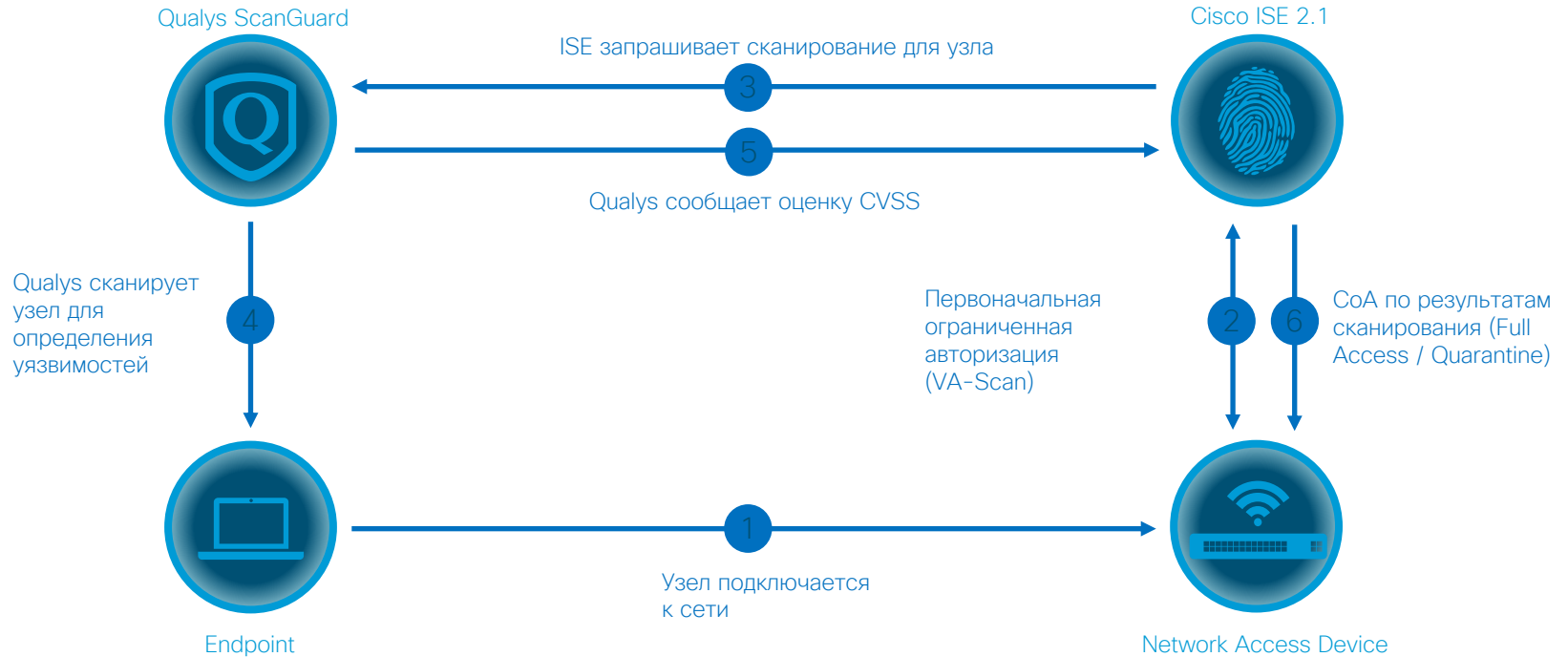
Атрибуты Threat Centric NAC появляются в Policy Administration Node.

Сервис TC-NAC работает на 'Policy Services Node'.

Требует ISE Арех лицензии

Контроль доступа, основанный на уязвимостях

Высокоуровневый процесс



Контроль доступа с учетом уязвимостей

ENDPOINT

NETWORK DEVICE

MNT

PSN

PAN

VULN SCANNER



Узел подключается к сети

Запрос аутентификации
Ограниченный доступ + флаг 'VA Scan'

Syslog: Event Log

Сканирование

CVSS узла
(Оценка уязвимости)

Атрибуты уязвимости

Change of Authorization
(Полный доступ или карантин)

Trigger scan if the time since last scan is greater than
Enter value in hours (1-99)

Запрос на сканирование для IP

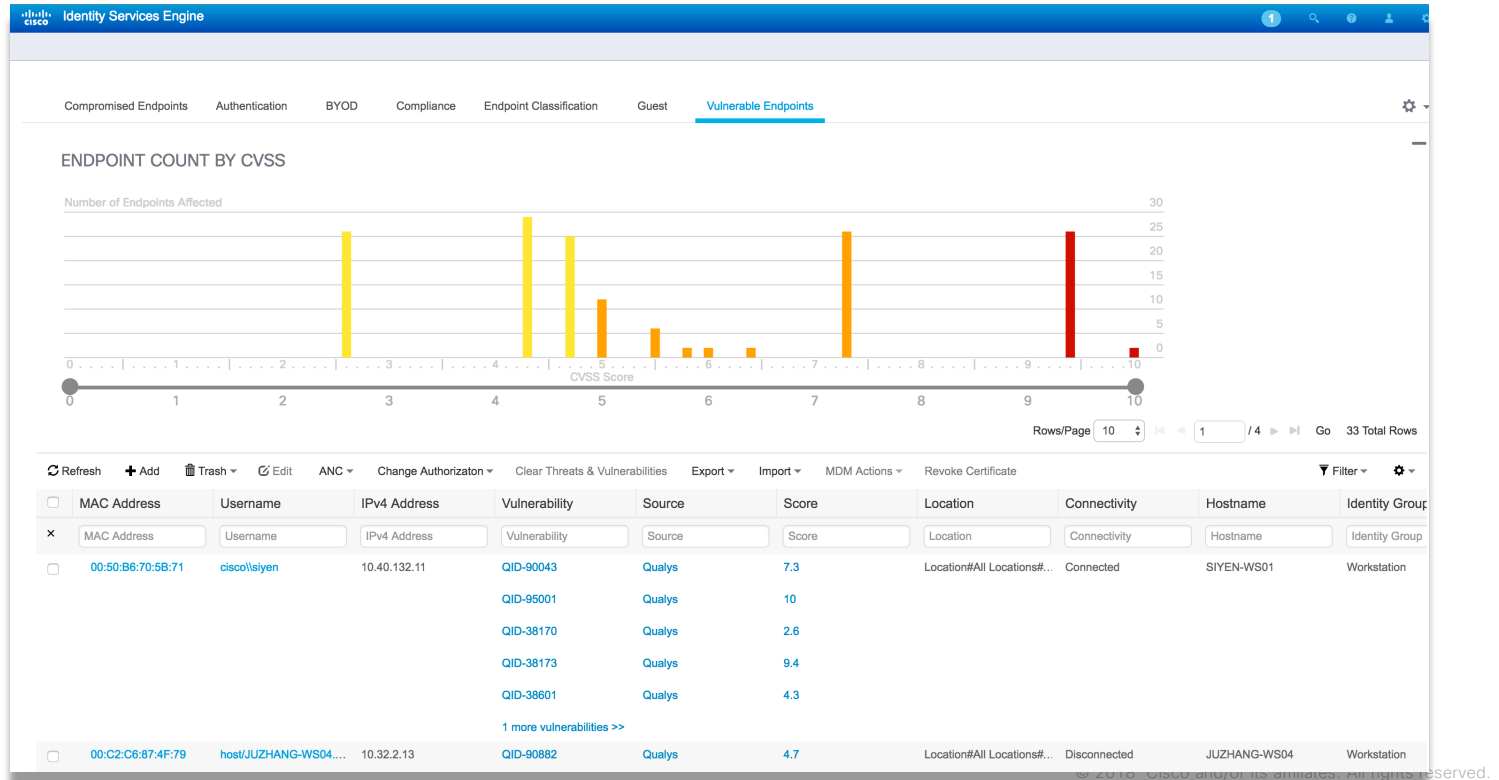
Queue requests

COA



‘Уязвимые узлы’

Основано на Common Vulnerability Scoring System (CVSS)



‘Уязвимые узлы’

Основано на Common Vulnerability Scoring System (CVSS)

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Cisco Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area shows 'Endpoints > 9.4' and a device with MAC address 00:50:B6:70:5B:71, Username: cisco\sllyen, Endpoint Profile: Windows7-Workstation, and Current IP Address: 10.40.132.11. The 'Vulnerabilities' tab is active, showing two entries:

Vulnerability ID	Title	CVSS score	Reported by	Reported at
QID-90043	SMB Signing Disabled or SMB Signing Not Required	7.3	Qualys	QID-90043 - SMB Signing Disabled or SMB Signing Not Required QID-95001 - X-Window Sniffing QID-38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN
QID-95001	X-Window Sniffing	10	Qualys	QID-38173 - SSL Certificate - Signature Verification Failed Vulnerability QID-38601 - SSL/TLS use of weak RC4 cipher QID-90882 - Windows Remote Desktop Protocol Weak Encryption Method Allowed

Настройка

Administration > Threat Centric NAC > Third Party Vendors

ISE «общается» с Qualys облаком через REST APIs

Сканер по умолчанию

Qualys API адрес

Учетная запись

Third Party Vendors

[Vendor Instances](#) > IT Qualys

Input fields marked with an asterisk (*) are required.

Vendor * Qualys : VA

Instance Name * IT Qualys

Current Status Active

Cancel

Save

Configuration Summary

[Reconfigure](#)

Default Scanner

SJ-1

REST API Host

qualysapi.qualys.com

Username

com1

Password

HTTP Proxy Host

HTTP Proxy Port

REST API Port

443

Привязка PSN к Scanner

Administration > Threat Centric NAC > Third Party Vendors

REST API Port

443

PSN to Scanner Mapping

sbg-bgla-pdp01

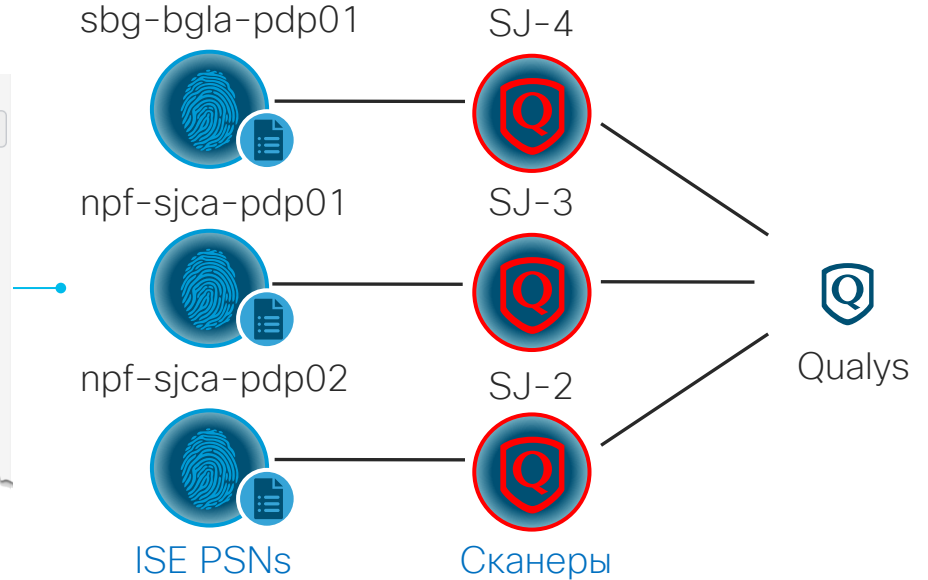
SJ-4

npf-sjca-pdp01

SJ-3

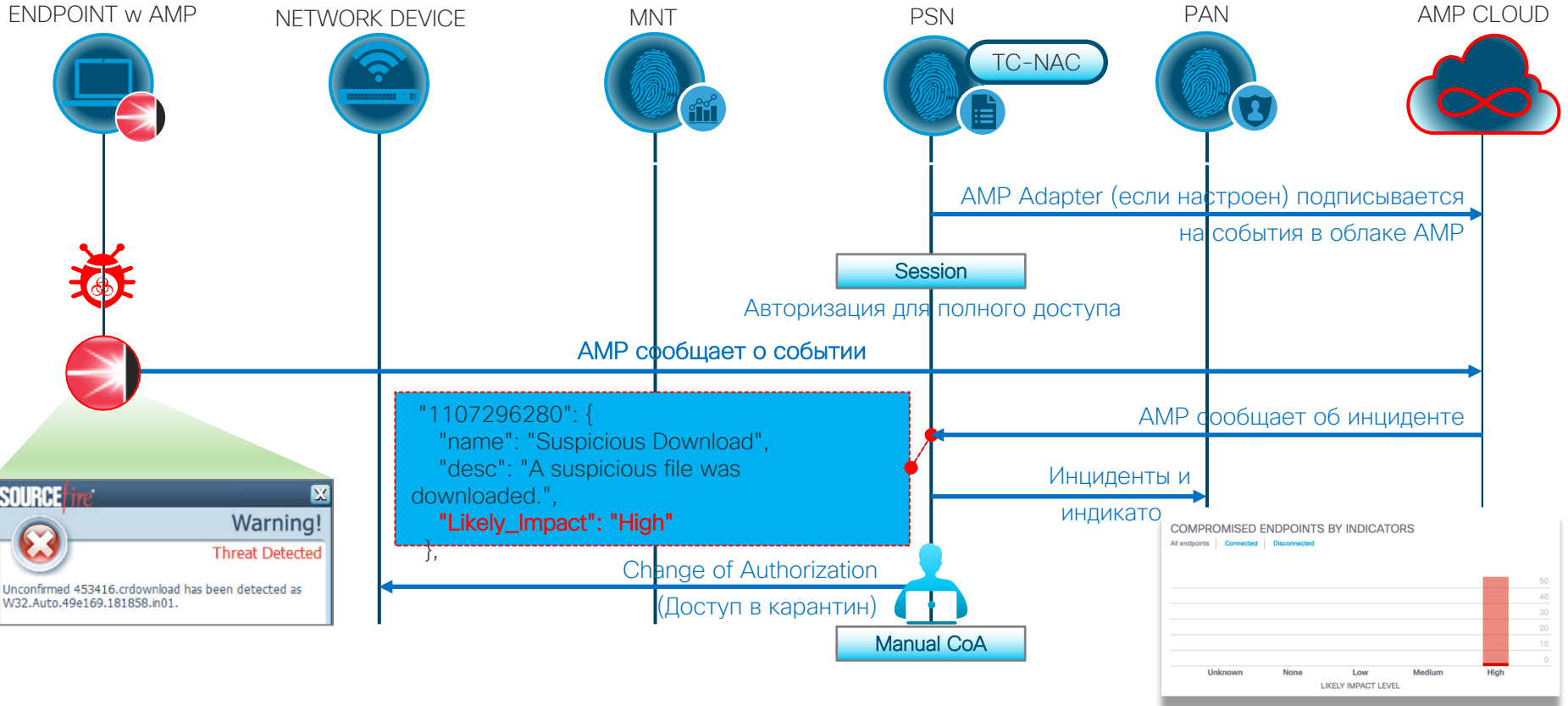
npf-sjca-pdp02

SJ-2



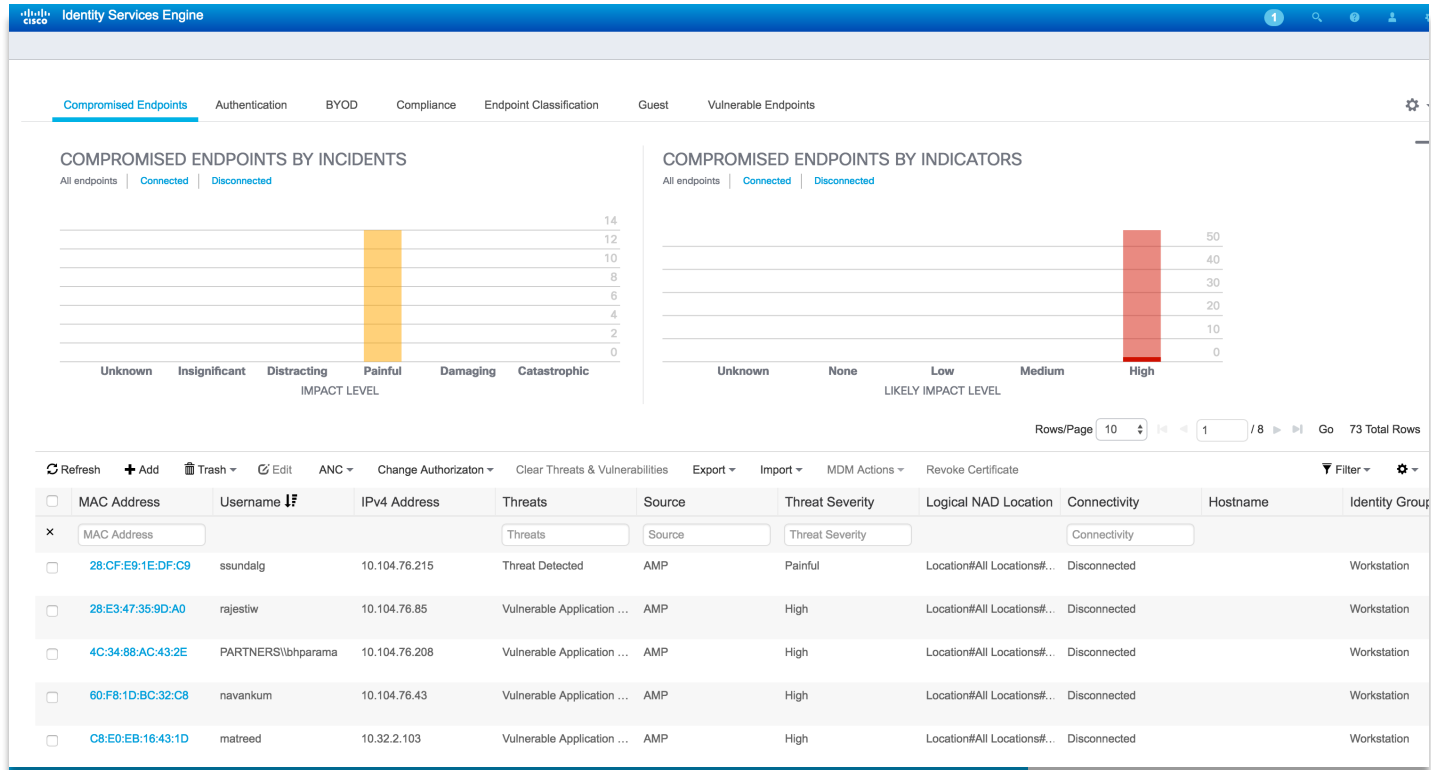
Виртуальные машины или устройства

Контроль доступа с учетом угроз



‘Скомпрометированные узлы’

Основано на инцидентах и индикаторах



Настройка TC-NAC с AMP

Administration > Threat Centric NAC > Third Party Vendors

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Third Party Vendors

Vendor Instances > FireAMP AnyConnect
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * FireAMP AnyConnect

Current Status Active

Cancel Save

Configuration Summary [Reconfigure](#)

Cloud Type
Public Cloud

Hostname
https://api.amp.sourcefire.com

Cloud
US Cloud

**Замечание: AMP требует прямого доступа в Internet через SOCKS (port 1080) Стандартный прокси не заработает.*

Идентичная конфигурация для большинства конфигураций*

Настройка TC-NAC с AMP

Administration > Threat Centric NAC > Third Party Vendors

Advanced Settings Change

Events

Selected Threats
Potential Dropper Infection
Suspicious Download
Microsoft CHM Compromise
Suspicious Cscript Launch
Adobe Reader launched a shell
Microsoft Word launched a shell
Microsoft PowerPoint compromise
Java launched a shell
Microsoft Word compromise
Microsoft Excel compromise
Java compromise
Adobe Reader compromise
Microsoft Excel launched a shell
Microsoft PowerPoint launched a shell
DFC Threat Detected
Threat Detected
APK Custom Threat Detected
APK Threat Detected

Можно отфильтровать.

Ручной карантин

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Filters: High

Authentication BYOD Compliance **Compromised Endpoints** Endpoint Classification Guest Vulnerable Endpoints

COMPROMISED ENDPOINTS BY INCIDENTS

All endpoints | Connected | Disconnected

Incident Level	Count
Unknown	0
Insignificant	0
Distracting	0
Painful	14
Damaging	0
Catastrophic	0

COMPROMISED ENDPOINTS BY INDICATORS

All endpoints | Connected | Disconnected

Likely Impact Level	Count
Unknown	0
None	0
Low	0
Medium	0
High	60

1 Selected Rows/Page 10 / 7 Go

Refresh Add Trash Edit ANC Change Authorization Clear Threats & Vulnerabilities Export Import MDM Actions Revoke Certificate

	MAC Address	Username	Threats	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname
<input checked="" type="checkbox"/>	00:0C:29:0E:E7:05	maramaja	Vulnerable Application Detected	AMP	High			

Ручной карантин

The screenshot displays the Cisco Identity Services Engine (ISE) interface. A modal dialog titled "Assign a Policy" is open, showing a list of policies for assignment. The "Investigate" policy is currently selected and highlighted in blue. Other visible policies include "Quarantine", "CrucioCurse", "AvadaKedavra", "PhasersOnStun", and "NukeFromOrbit".

The background interface shows a table of endpoint data with the following columns: MAC Address, Username, IPv4 Address, Threats, Source, Threat Severity, Logical NAD Location, Connectivity, and Hostname. The table contains one row of data:

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname
00:0C:29:0E:E7:05	maramaja		Vulnerable Application Detected	AMP	High			

Threat Centric NAC. Резюме

- Возможность **инициировать проверку уязвимостей**
- Инициация **принудительного сканирования** если это необходимо.
- Используйте эти результаты для генерации нормализованных результатов в формате Structured Threat Information Expression (**STIX format** и **оценки CVSS** для оценки уязвимостей.
- ISE имеет возможность оценивать и **изменять доступ к сети** с помощью политик авторизации.
- Для использования результатов оценки уязвимости в политиках доступа ISE использует подход **“Невиновен пока не доказано”** поскольку используются данные не реального времени.

Rapid Threat Containment (RTC)

Rapid Threat Containment с Firepower Management Center и ISE



Полная поддержка
на FMC 5.4 и ISE
1.3+

- Использует pxGrid + Endpoint Protection Services (EPS)
- Примечание: ANC это NG версия старого EPS
- Функции EPS поддерживаются для совместимости

Загружается как
Remediation
Module на FMC

- Remediation Module предпринимает действия через вызов EPS pxGrid

Опции коррекции

- **Quarantine** – отправляет узел в карантин на основании IP
- **portBounce** – временно отключает узел от порта
- **Terminate** – прекращает сессию пользователя
- **Shutdown** – инициирует выключение порта, это запускает на коммутаторе команду "shutdown"
- **reauthenticate** – реаутентифицирует пользователя
- **UnQuarantine** – выключает карантин

Edit Remediation

Remediation Name:

Remediation Type: Mitigate Source

Description:

Mitigation Action:

- quarantine
- unquarantine
- shutdown
- terminate
- reAuthenticate
- portBounce

Whitelist
(an optional list of networks)

Интеграция AMP <-> ISE TC-NAC

- Ограничена только ручным реагированием.
- Для автоматизации: Используйте Firepower Management Center*
 - Правило корреляции: Malware Event Occurred
 - Затем используйте ISE Remediation Module (Rapid Threat Containment)

*Совет дня

Правило корреляции FMC

События Malware

- Сеть
- Узел
- Ретроспектива

The screenshot shows the 'Policy Management' section of the Cisco FMC interface, specifically the 'Rule Management' tab. The rule being configured is named 'Quarantine-Malware' and belongs to the 'Malware Rules' group. The 'Event Type' is set to 'Threat Detected'. The 'If' condition is currently set to 'a Malware event occurs' and is being edited to specify the detection method. A dropdown menu is open, showing options: 'by endpoint-based malware detection', 'by network-based malware detection', and 'by retrospective network-based malware detection'. The 'Add condition' button is visible below the dropdown.

This close-up view shows the 'If' condition configuration. The dropdown menu is open, displaying the following options: 'by endpoint-based malware detection', 'by network-based malware detection', and 'by retrospective network-based malware detection'. The 'Add condition' button is located to the left of the dropdown.

Правило корреляции FMC

Malware на узле

Основное событие на AMP для Endpoints Cloud

The screenshot displays the Cisco FMC Policy Management interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Policies' section is active, with sub-tabs for 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. The 'Correlation' tab is selected, and the 'Rule Management' sub-tab is active. The 'Rule Information' section shows the rule name 'Quarantine-Malware', an empty description, and the rule group 'Malware Rules'. Below this, the event type is set to 'a Malware event occurs' and the detection method is 'by endpoint-based malware detection'. A condition is defined: 'Event Type is Threat Detected'. The interface includes buttons for 'Add condition' and 'Add complex condition'.

Policy Management Rule Management White List Traffic Profiles

Rule Information

Rule Name: Quarantine-Malware

Rule Description:

Rule Group: Malware Rules

Select the type of event for this rule

If a Malware event occurs by endpoint-based malware detection and it meets the following conditions:

+ Add condition + Add complex condition

✗ Event Type is Threat Detected

If a Malware event occurs by endpoint-based malware detection and it meets the following conditions:

+ Add condition + Add complex condition

✗ Event Type is Threat Detected

Правило корреляции FMC

Malware на узле

Определенные события на AMP Endpoints Cloud

The screenshot shows the 'Policies' section of the FMC interface. The 'Rule Management' tab is active, displaying the configuration for a rule named 'Quarantine-Malware'. The rule is associated with the 'Malware Rules' group. The event type is set to 'a Malware event occurs by endpoint-based malware detection'. Below this, there are two conditions listed under an 'OR' operator: 'Event Subtype is Adobe Reader compromise' and 'Event Subtype is Adobe Reader launched a shell'. The interface includes navigation tabs like 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP', and sub-tabs like 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. A 'Deploy' button is visible in the top right corner.

This is a zoomed-in view of the rule conditions section from the screenshot above. It shows the 'If' clause: 'a Malware event occurs by endpoint-based malware detection and it meets the following conditions:'. Below this, there are two buttons: 'Add condition' and 'Add complex condition'. The conditions are listed under an 'OR' operator. The first condition is 'Event Subtype is Adobe Reader compromise' and the second is 'Event Subtype is Adobe Reader launched a shell'. Each condition has a red 'X' icon to its left, indicating it is a required condition.

Коррекция

Карантин

Коррекция, которая запускает карантин EPS через rxFrid

The screenshot displays the Cisco AMP web interface for policy management. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. Below this, a secondary navigation bar shows 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. The main content area is titled 'Policy Management' and contains sub-tabs for 'Rule Management', 'White List', and 'Traffic Profiles'. Under 'Correlation Policy Information', the 'Policy Name' is 'ATW-AMP-Correlation', 'Policy Description' is empty, and 'Default Priority' is 'None'. The 'Policy Rules' section contains a table with one rule highlighted by a red box:

Rule	Responses
Quarantine-Malware	QuarantineSrc (Remediation)

At the bottom of the interface, a footer indicates the last login on Friday, 2017-03-24 at 09:49:22 AM from 10.86.114.120.

Rapid Threat Containment с Firepower Management Center и ISE



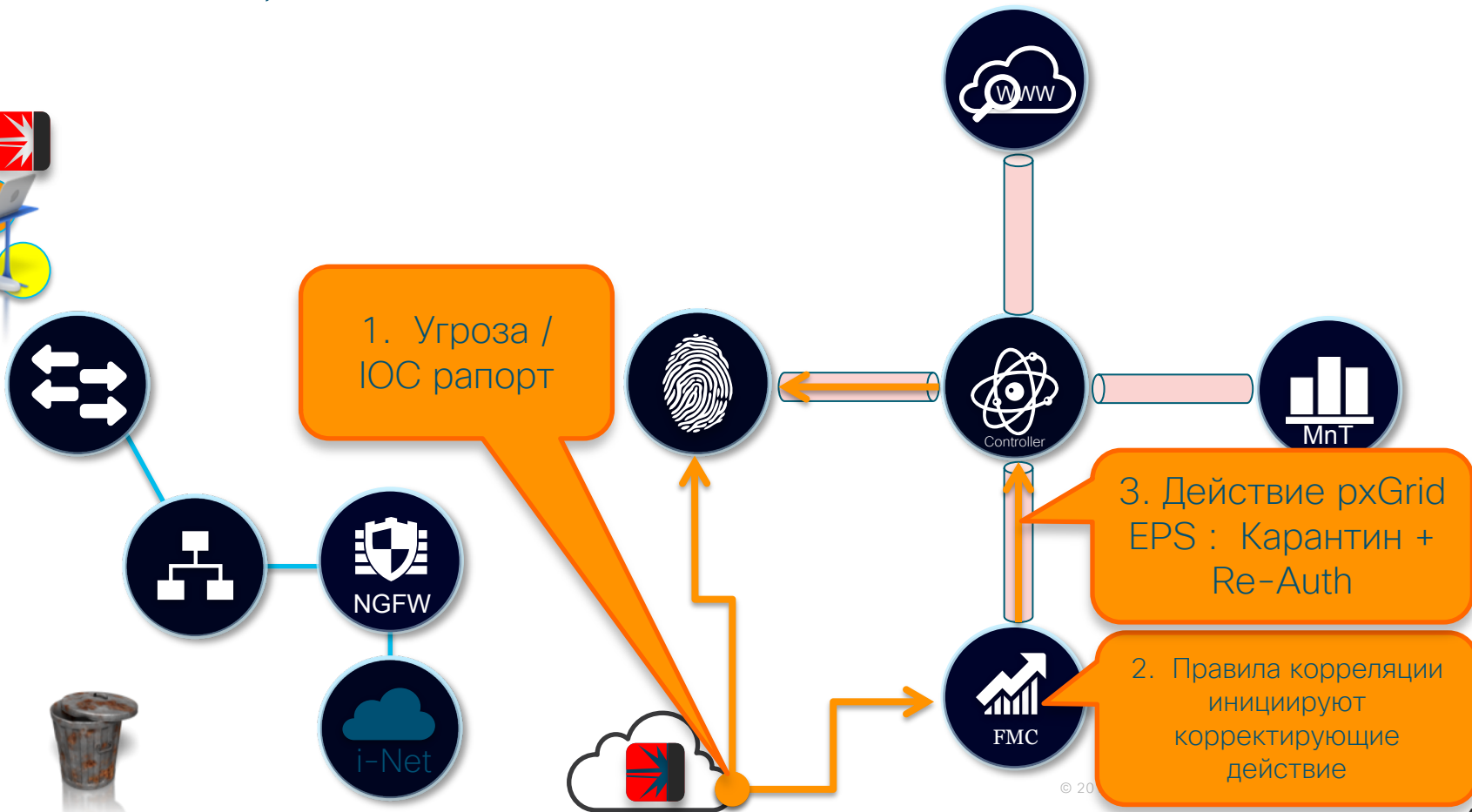
RCT с FMC и ISE



4. Карантин узла +
отправка CoA-
Reauth



RTC с AMP, FMC и ISE



© 20

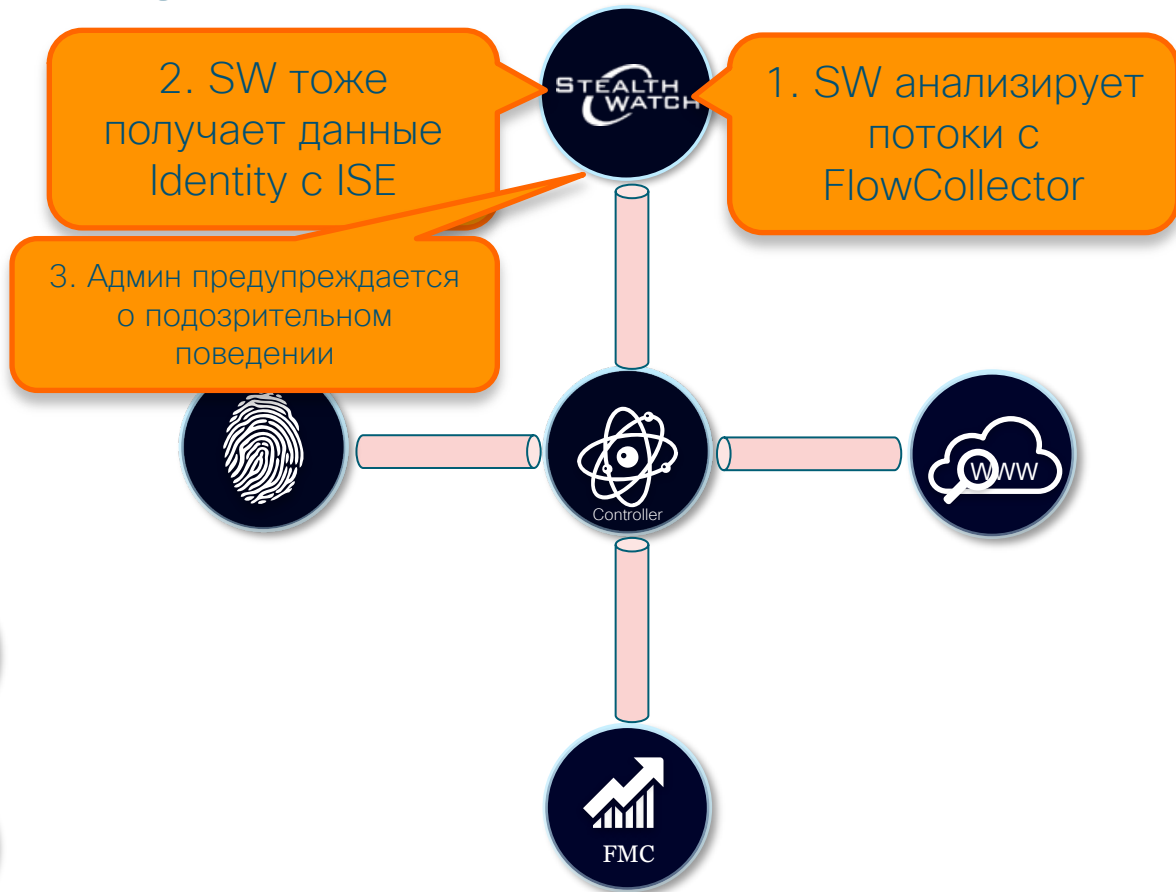
RTC с AMP, FMC и ISE



4. Карантин узла +
отправка CoA-
Reauth



RTC с Stealthwatch и ISE



RTC с Stealthwatch и ISE



4. Админ инициирует карантин узла (EPS через pxGrid)

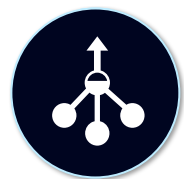


Host Summary

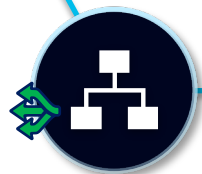
Host IP	10.1.41.105
Classify	History
Status:	Inactive
Hostname:	--
Host Groups:	Catch All
Location:	RFC 1918
Last Seen:	1/17/17 4:02 AM
Policies:	Inside
MAC Address:	--

Quarantine Unquarantine

5. Карантин узла + отправка CoA- Reauth



Flow Collector



RTC с Stealthwatch и ISE



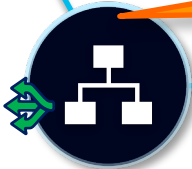
6. К новому состоянию сети применяются новые правила трафика

6а. Может запретить доступ (входящий)

6б. Может отфильтровать в сети (исходящий)



Flow Collector



А если я хочу ANC без pxGrid?

Я рад, что вы спросили...
Начиная с ISE 2.1, ANC
доступен через REST API.

<https://ISE:9060/ers/sdk>

Step 1: ANC политика

Какие существуют политики

Step 2: ANC Endpoint

Назначение политики на
узел

External RESTful Services (ERS) Online SDK

Quick Reference

API Documentation

- ISE 2.0 Release Notes
- ISE 2.1 Release Notes
- ISE 2.2 Release Notes
- ANC Policy
- Active Directory
- Advanced Customization Global !
- BYOD Portal
- Certificate Template
- Clear Threats and vulnerabilities
- Egress Matrix Cell
- End Point
- End Point Certificates
- EndPoints Identity Group
- Guest Location
- Guest Sntp Notification Configur
- Guest Ssid

ANC Policy

- Overview
- Resource definition
- Revision History
- Get-By-Name
- Get-By-Id
- Update
- Delete
- Create
- Get-All
- Get Version
- Bulk Request
- Monitor Bulk Status

А если я хочу ANC без pxGrid?

Get-All

Request:

Method:	GET
URI:	https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy
HTTP 'Accept' header:	application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml
HTTP 'Accept-Search-Result' Header:	application/vnd.com.cisco.ise.ers.searchresult.2.0+xml

Request Content:
N/A

https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy

Params Send

application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml	≡ ×	Bulk Edit
application/vnd.com.cisco.ise.ers.searchresult.2.0+xml	≡ ×	
Basic ZXjzYWRtaW46Q2l2Y28xMjM=	≡ ×	
key	value	

Operations > ANC

Policy List Endpoint Assignment

List

Refresh Add Trash Edit

<input type="checkbox"/>	Policy Name
<input type="checkbox"/>	ANC-Quarantine
<input type="checkbox"/>	ANC-Investigate
<input type="checkbox"/>	ANC-Destroy
<input type="checkbox"/>	ANC-NukeFromOrbit

Body Cookies Headers (7) Tests Status: 200 OK

Pretty Raw Preview XML

```
1 <?xml version="1.0" encoding="utf-8" standalone="yes"?>
2 <ns3:searchResult total="4" xmlns:ns5="ers.ise.cisco.com" xmlns:ers-v2="ers-v2" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ers.ise.cisco.com">
3 <rs:resources>
4 <ns5:resource id="ANC-Destroy" name="ANC-Destroy">
5 <link rel="self" href="https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy/ANC-Destroy" type="application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml" />
6 </ns5:resource>
7 <ns5:resource id="ANC-Investigate" name="ANC-Investigate">
8 <link rel="self" href="https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy/ANC-Investigate" type="application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml" />
9 </ns5:resource>
10 <ns5:resource id="ANC-NukeFromOrbit" name="ANC-NukeFromOrbit">
11 <link rel="self" href="https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy/ANC-NukeFromOrbit" type="application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml" />
12 </ns5:resource>
13 <ns5:resource id="ANC-Quarantine" name="ANC-Quarantine">
14 <link rel="self" href="https://atw-ise237.securitydemo.net:9060/ers/config/ancpolicy/ANC-Quarantine" type="application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml" />
15 </ns5:resource>
```

А если я хочу ANC без pxGrid?

apply

Request:

Method:	PUT
URI:	https://atw-ise237.securitydemo.net:9060/ers/config/ancendpoint/apply
HTTP 'Content-Type' header:	application/vnd.com.cisco.ise.anc.ancendpoint.1.0+xml; charset=utf-8
HTTP 'Accept' header:	application/vnd.com.cisco.ise.anc.ancendpoint.1.0+xml
Additional Attributes:	macAddress,ipAddress,policyName

Request Content:

```
XML
<?xml version="1.0" encoding="UTF-8"?>
<ns0:operationAdditionalData xmlns:ns0="ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <requestAdditionalAttributes>
    <additionalAttribute name="macAddress" value="value_0"/>
    <additionalAttribute name="ipAddress" value="value_1"/>
    <additionalAttribute name="policyName" value="value_2"/>
  </requestAdditionalAttributes>
</ns0:operationAdditionalData>
```

Operations > ANC

Policy List Endpoint Assignment

List

Refresh + Add Trash Edit EPS unquarantine

<input type="checkbox"/>	MAC Address	Policy Name	Policy Actions
<input type="checkbox"/>	00:50:56:B8:B1...	ANC-NukeFromOrbit	[PORT_BOUNCE]

PUT https://atw-ise237.securitydemo.net:9060/ers/config/ancendpoint/apply

Authorization Headers (3) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary Text

```
1 <ns0:operationAdditionalData xmlns:ns0="ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema">
2   <requestAdditionalAttributes>
3     <additionalAttribute name="macAddress" value="00:50:56:B8:B1:C7"/>
4     <additionalAttribute name="policyName" value="ANC-NukeFromOrbit"/>
5   </requestAdditionalAttributes>
6 </ns0:operationAdditionalData>
```

Body Cookies Headers (6) Tests

Важно: Действия RTC не обязательно должны быть только “Выбросить из сети”
- Можно разрешить ограниченный доступ и дополнительную инспекцию.

Пример: Карантин узла

УСЛОВИЯ

EPS
в
Quarantine

или

ANC
в
Quarantine

Результат

Ограниченный доступ
+
Тэг Quarantine

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	ANC Quarantine	if (Session:EPSStatus EQUALS Quarantine OR Session:ANCPolicy EQUALS Quarantine)	then Quarantined_Systems AND LimitedAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access

Пример: Запустить сканирование уязвимостей и расшифровку SSL

Условие

CTA Course of Action
=
Monitoring

OR

ANC
=
Investigate

=

Результат

Ограничение доступа
+
Скан уязв.
+
SGT Investigate

Investigate
 if (CTA-Monitoring OR ANC-Investigate)
 then Investigate Endpoint AND Investigate

Attribute	Operator	Value
Threat:CTA-Course_Of_Action	Equals	Monitoring
Session:ANCPolicy	Equals	Investigate

Common Tasks

DACL Name Limited_Traffic

Assess Vulnerabilities

Adapter Instance atw-nessus

Trigger scan if the time since last scan is greater than 48

Enter value in hours (1-9999)

Assess periodically using above interval

Автоматизация AMP коррекции в ISE через FMC

- FMC может назначить узел в “Quarantine”
 - Вместо выбрасывания из сети:
 - Инициировать скан уязвимостей
- После того, как FMC карантин и скан уязвимостей «согласны», выбросить узел из сети
- -Или- После того, как FMC карантин и СТА “согласны”, затем выбросить из сети

FMC карантин = Скан уязвимостей и расшифровка SSL

Условие

EPS
=
Quarantine

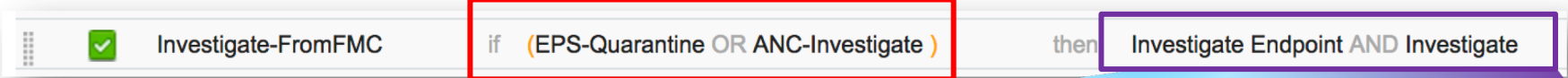
или

ANC
=
Investigate

=

Результат

Огран. доступ
+
Скан уязв.
+
SGT Investigate

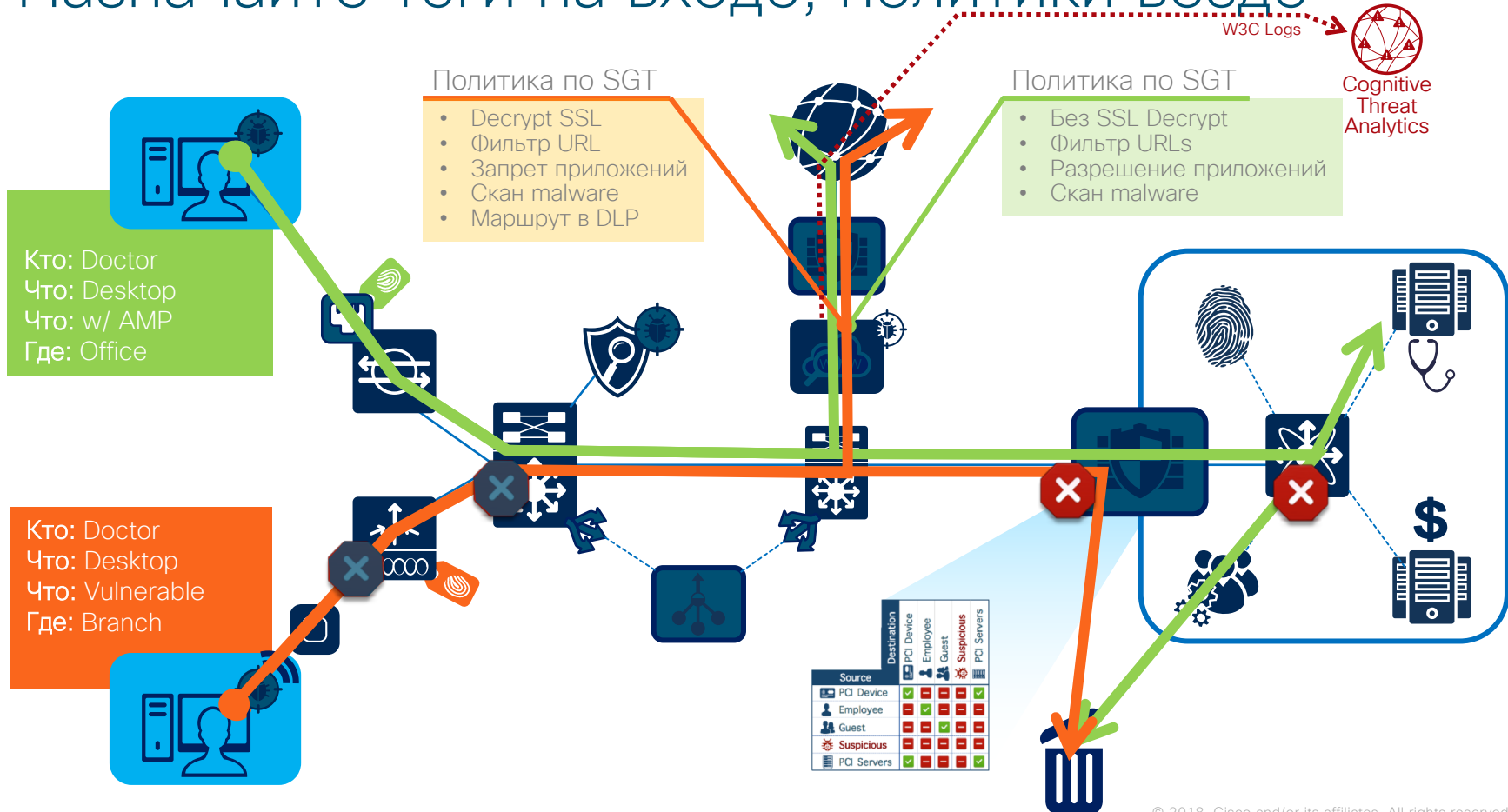


Common Tasks

- DACL Name**
- Assess Vulnerabilities**
 - Adapter Instance: atw-nessus
 - Trigger scan if the time since last scan is greater than:
Enter value in hours (1-9999)
 - Assess periodically using above interval

Рекомендации
профессионала:
Используйте для этого
тэги TrustSec

Назначайте тэги на входе, политики везде



Один маленький тэг и так много пользы

- Влияние на путь по сети (PBR)
- Настройка QoS
- SGT может инициировать определенную настройку порта на коммутаторе.
- Определение дальнейшей инспекции трафика
 - Т.е. отправка через Firepower IPS
- Определить политику на Web шлюзе
- Определить (упрощенно) политику Firewall
- Контроль трафика «восток-запад» (последовательное продвижение)

Автоматизация и скрипты

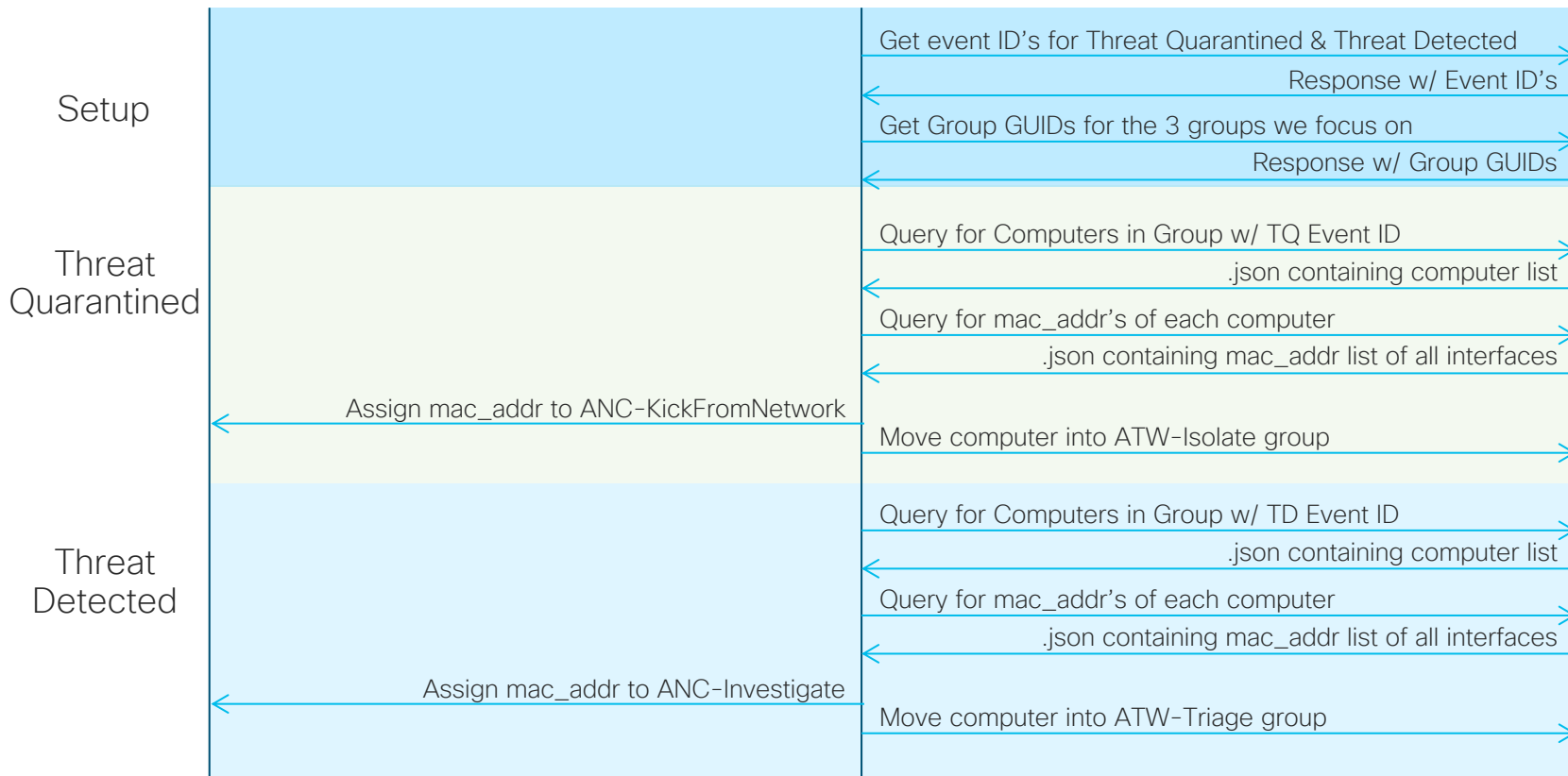
Скрипты Python RTC-AMP-ISE



- Скрипт для идентификации компьютеров в AMP с определенными событиями:
 - Threat Quarantined
 - Threat Detected
- Переместить компьютеры с этими событиями в новые AMP группы
 - ATW-Isolated – компьютеры с событиями Threat Quarantined
 - ATW-Triage – компьютеры с событиями Threat Detected
- Назначить метки ANC на узлы Rapid Threat Containment
 - ANC-KickFromNetwork – компьютеры с событиями Threat Quarantined
 - ANC-Investigate – компьютеры не из первой группы с событиями Threat Detected



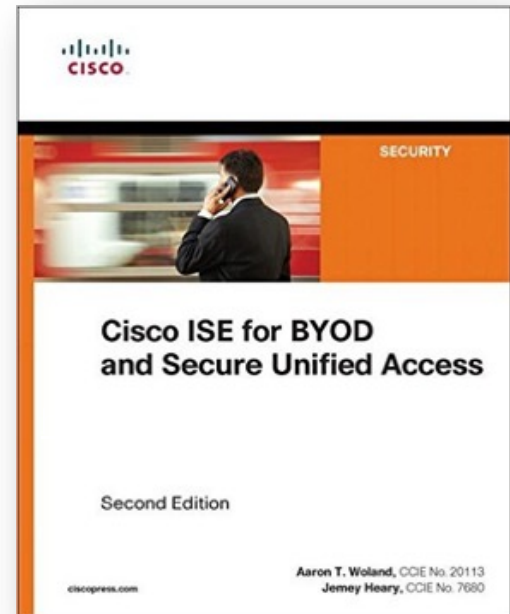
Linux Server w/ Python



Заключение

Дополнительные ресурсы

- <http://cs.co/ise-community>
- Блог К. McNamara: <http://www.network-node.com/blog/>
- Блог Aaron T. Woland :
<http://www.networkworld.com/blog/secure-network-access/>
- GitHub: <http://cs.co/ats-apis>



Вопросы?



