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
- Блоее 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 шифрованным 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 Verizon Breach Repo

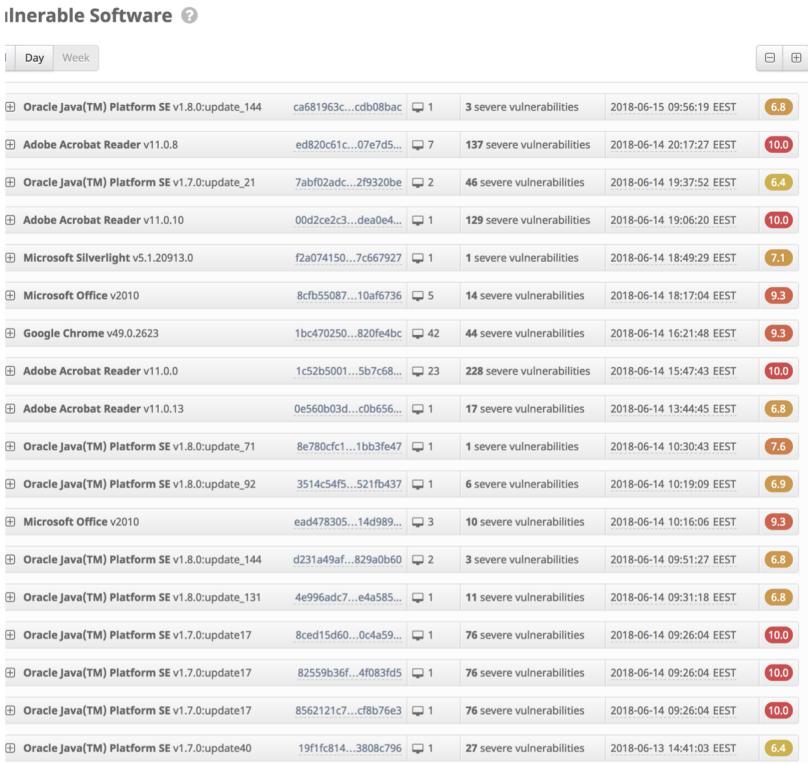
- “Все еще используются уязвимости”
- “Все патчи бесполе не патчим правильные вещи”

2017 Ci nual Cybersecurity Report

- “ ищут уязвимые браузеры и плагины. умышленники ищут возможности спользования непропатченного ПО”

Не позволяй угрозе попасть в сеть!

В реальной жизни

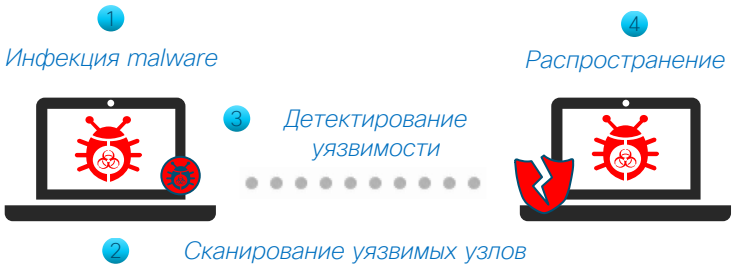


250 компьютеров, одна неделя…

Объяснение Threat Centric NAC

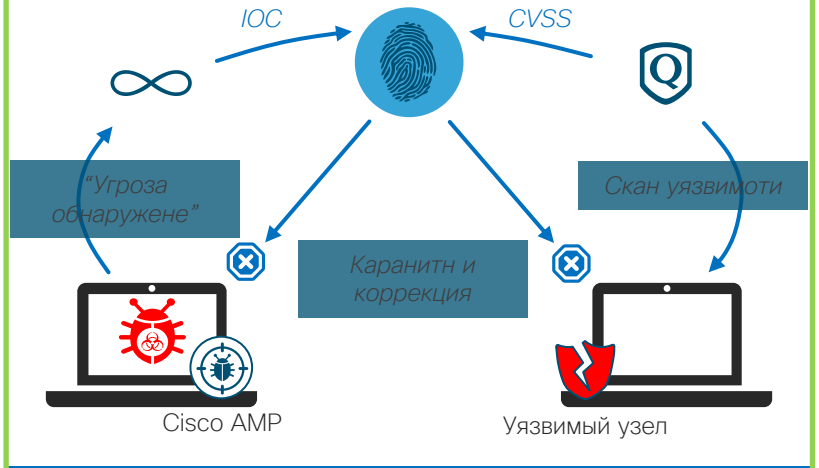
Уменьшить количество уязвимостей, сдержать угрозы

Проблема



Скомпрометированные узлы распространяют maware 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

Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC) | Advanced Malware Protection (AMP)

Threat Centric NAC

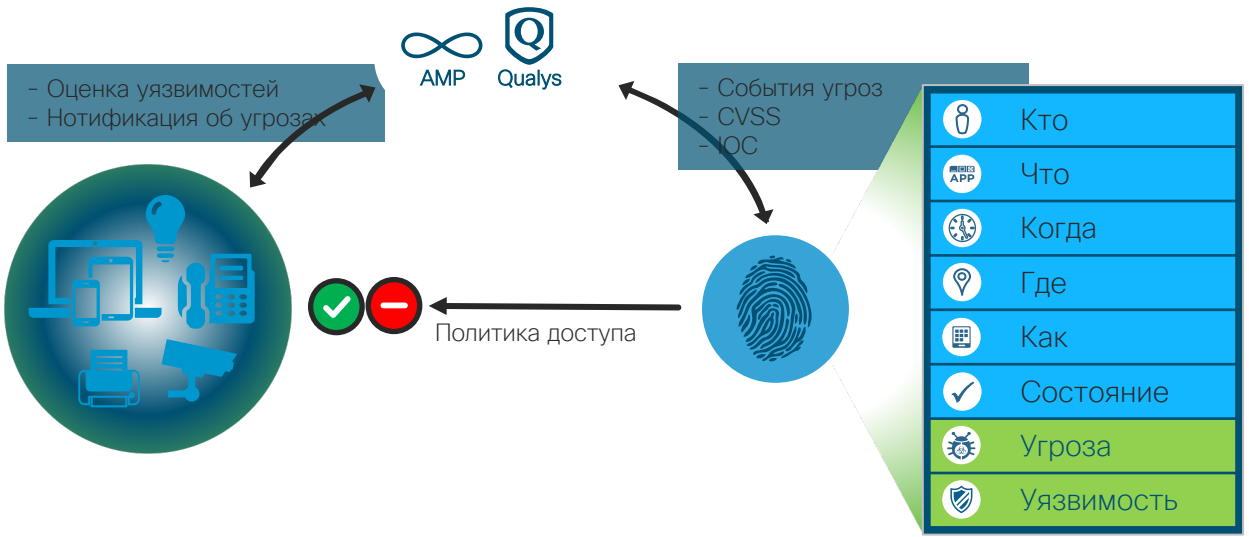
Cisco ISE защищает вашу сеть от брешей с помощью сегментации скомпрометированных и уязвимых узлов для исправления

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

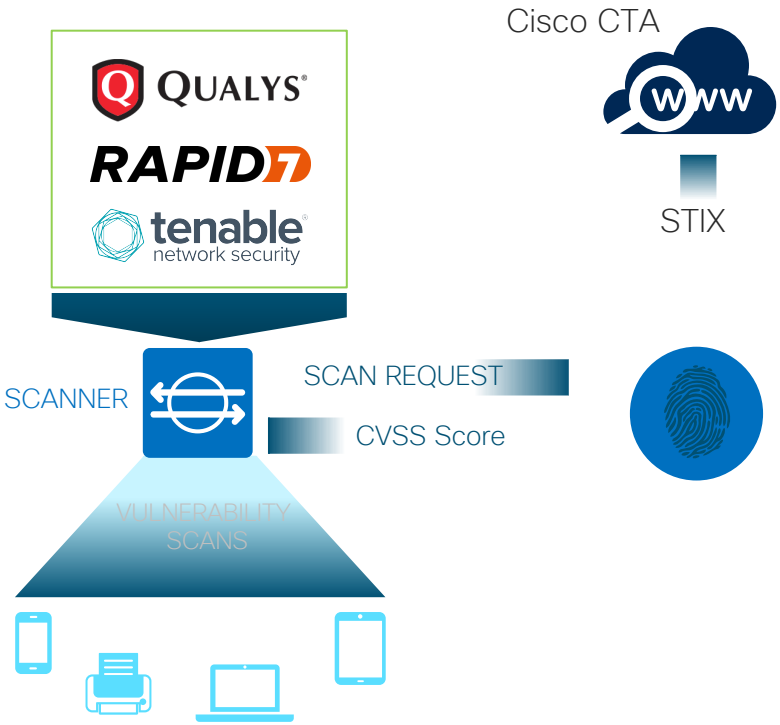


Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC)

Threat Centric NAC

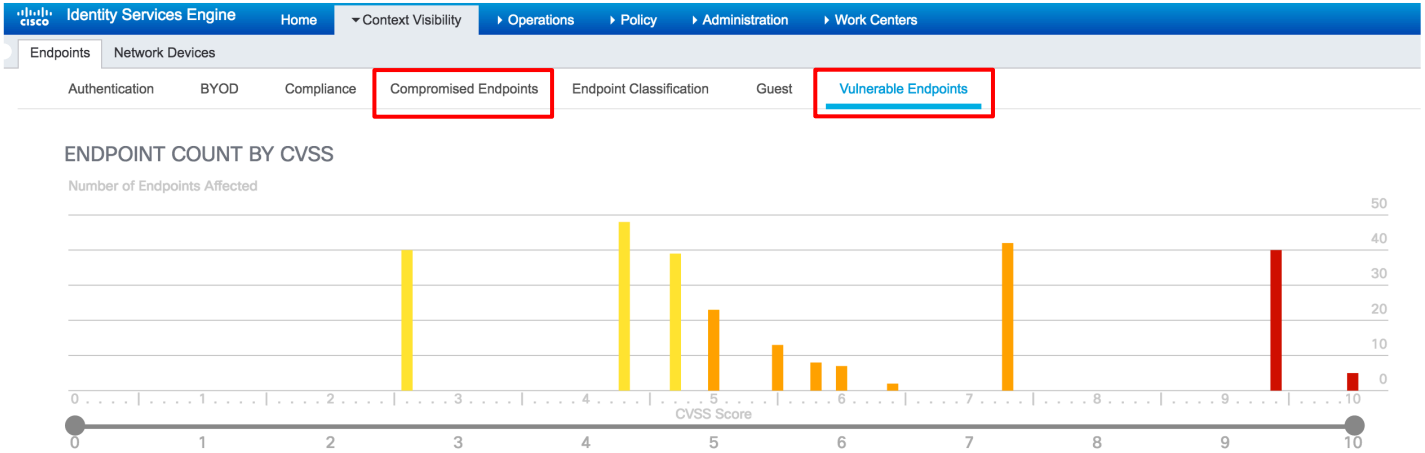
ISE 2.2

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



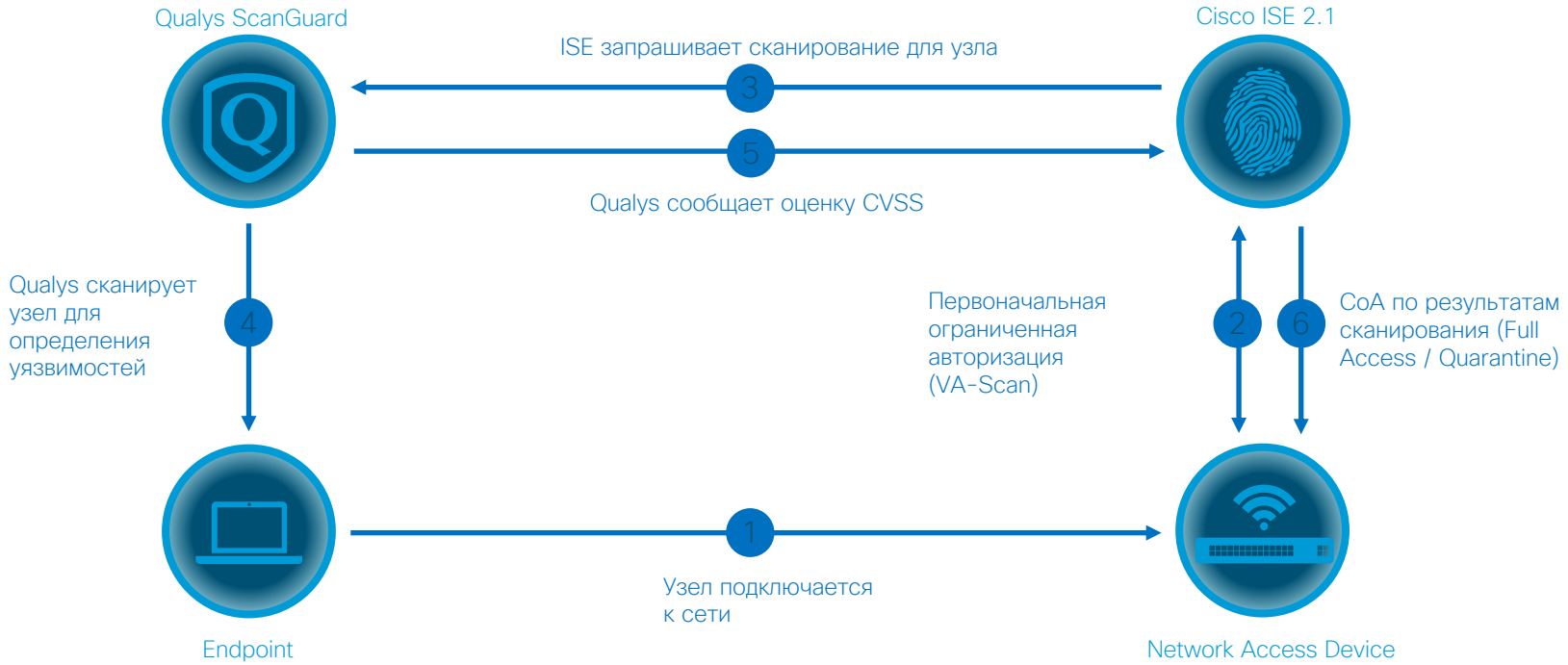
Атрибуты Threat Centric NAC появляются в Policy Administration Node.

Сервис TC-NAC работает на ‘Policy Services Node’.

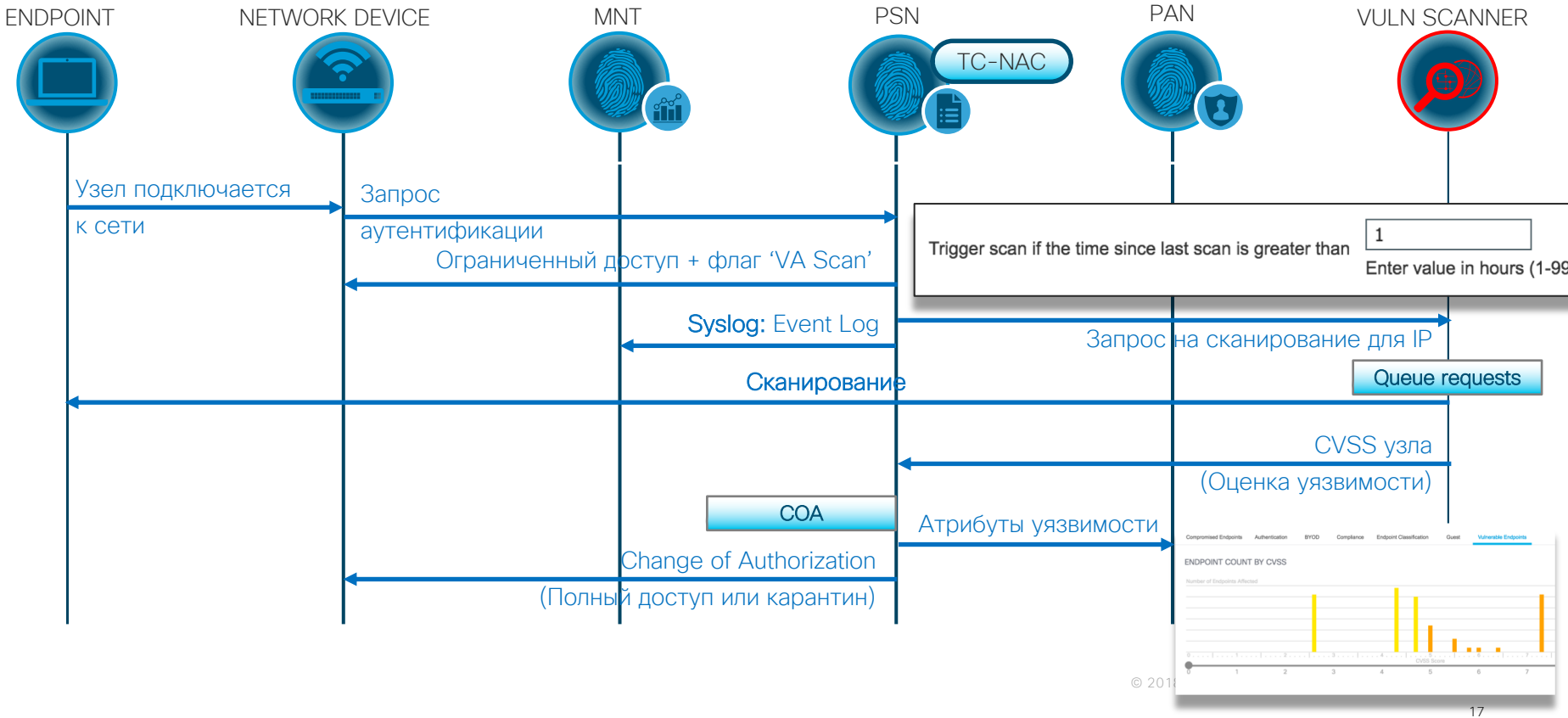
Требует ISE Apex лицензии

Контроль доступа, основанный на уязвимостях

Высокоуровневый процесс

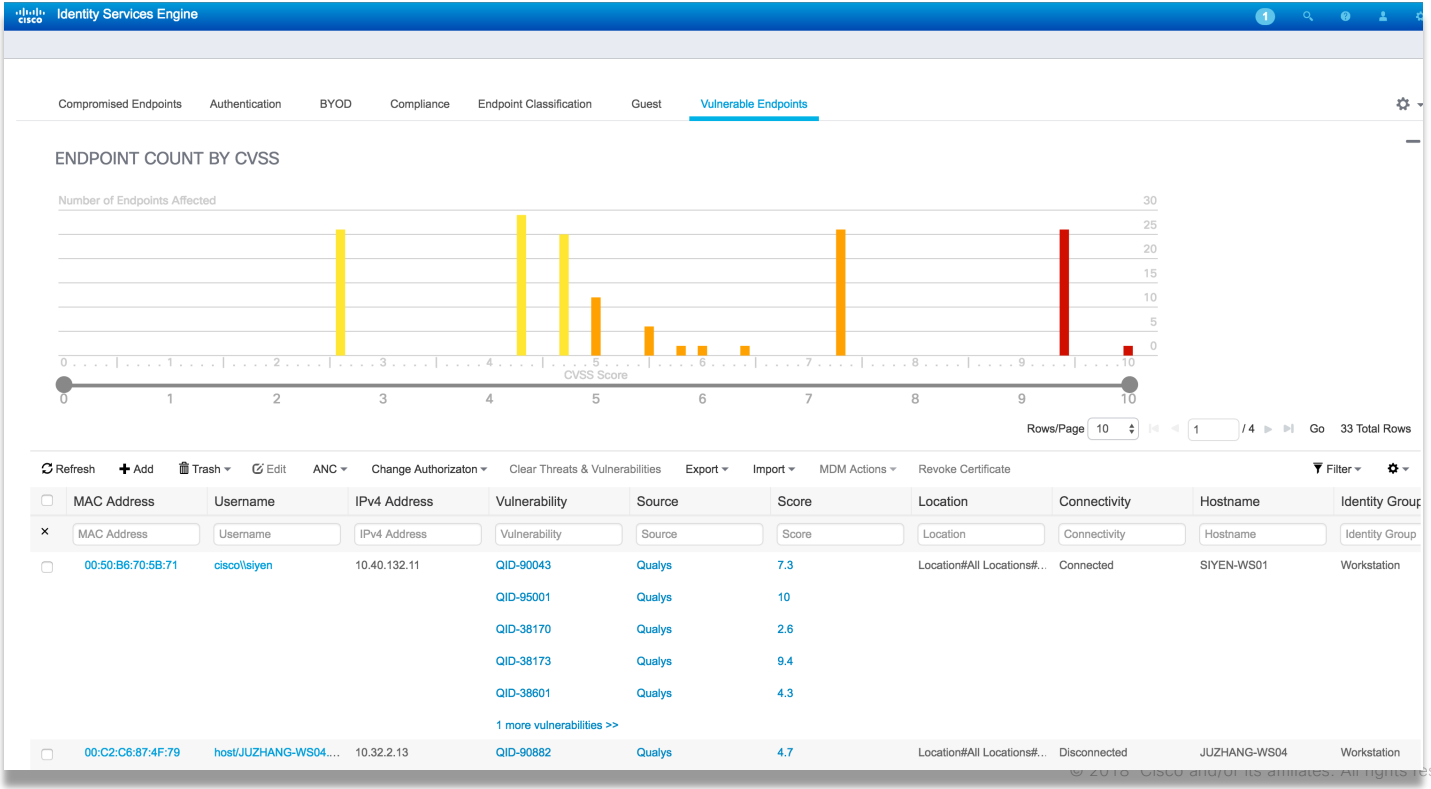


Контроль доступа с учетом уязвимостей



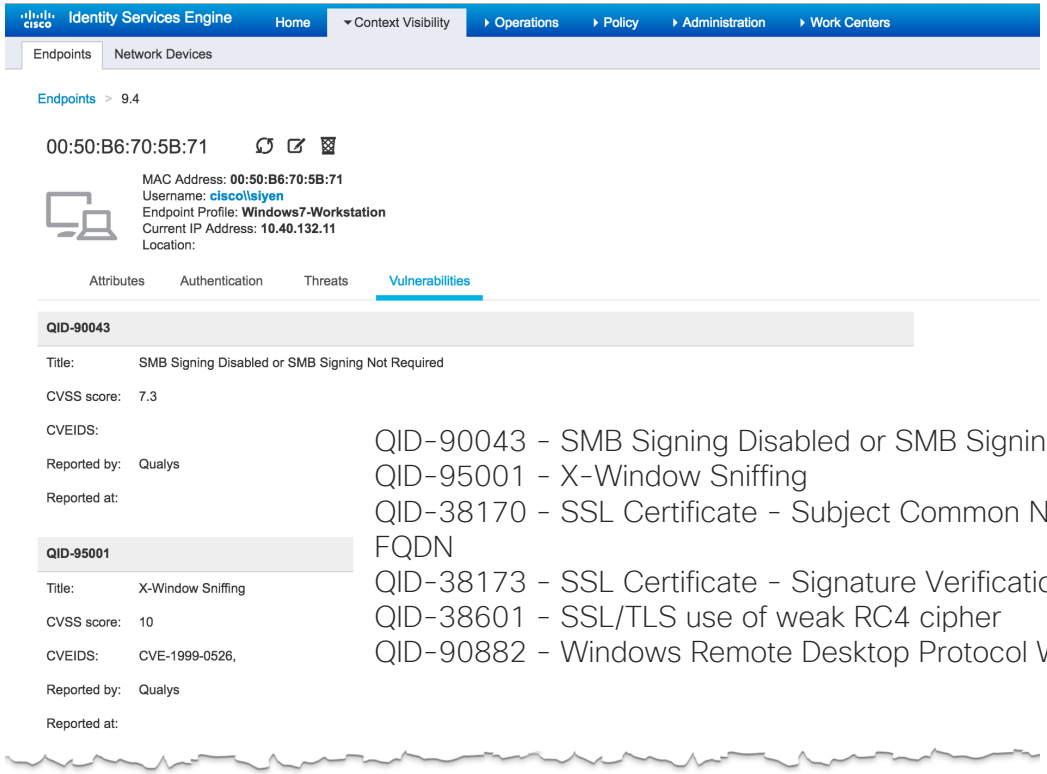
‘Уязвимые узлы’

Основано на Common Vulnerability Scoring System (CVSS)



‘Уязвимые узлы’

Основано на Common Vulnerability Scoring System (CVSS)

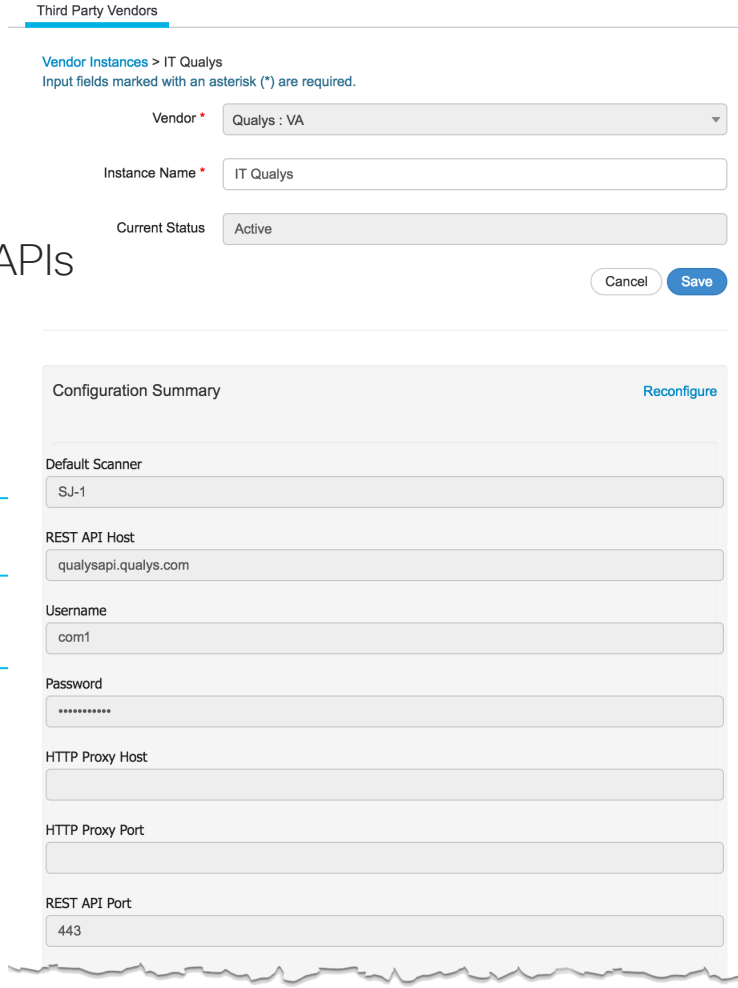


QID-90043 - SMB Signing Disabled or SMB Signing Not Required
QID-95001 - X-Window Sniffing
QID-38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN
QID-38173 - SSL Certificate - Signature Verification Failed Vulnerability
QID-38601 - SSL/TLS use of weak RC4 cipher
QID-90882 - Windows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

Настройка

Administration > Threat Centric NAC > Third Party Vendors

ISE «общается »с Qualys облаком через REST APIs



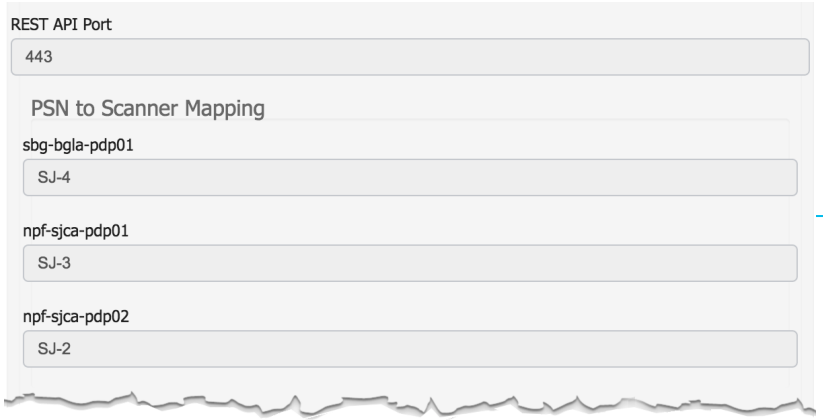
Сканер по умолчанию

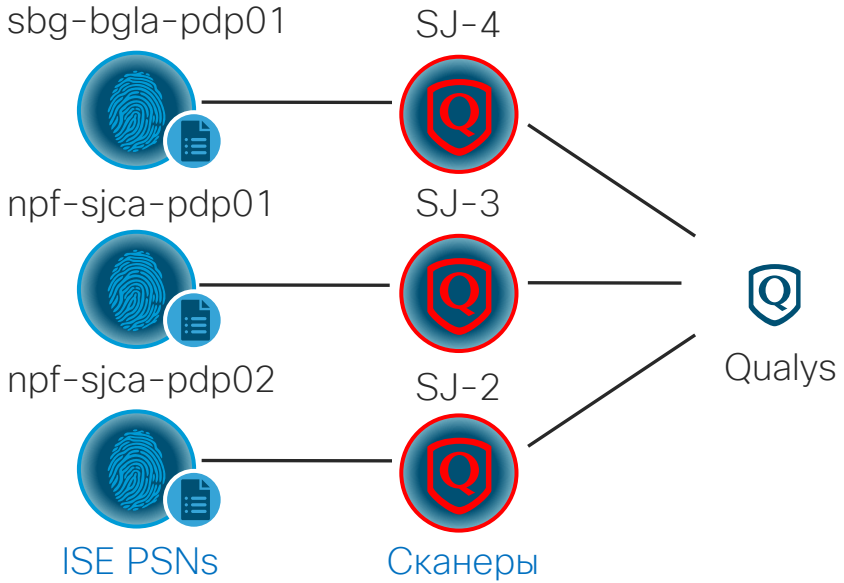
Qualys API адрес

Учетная запись

Привязка PSN к Scanner

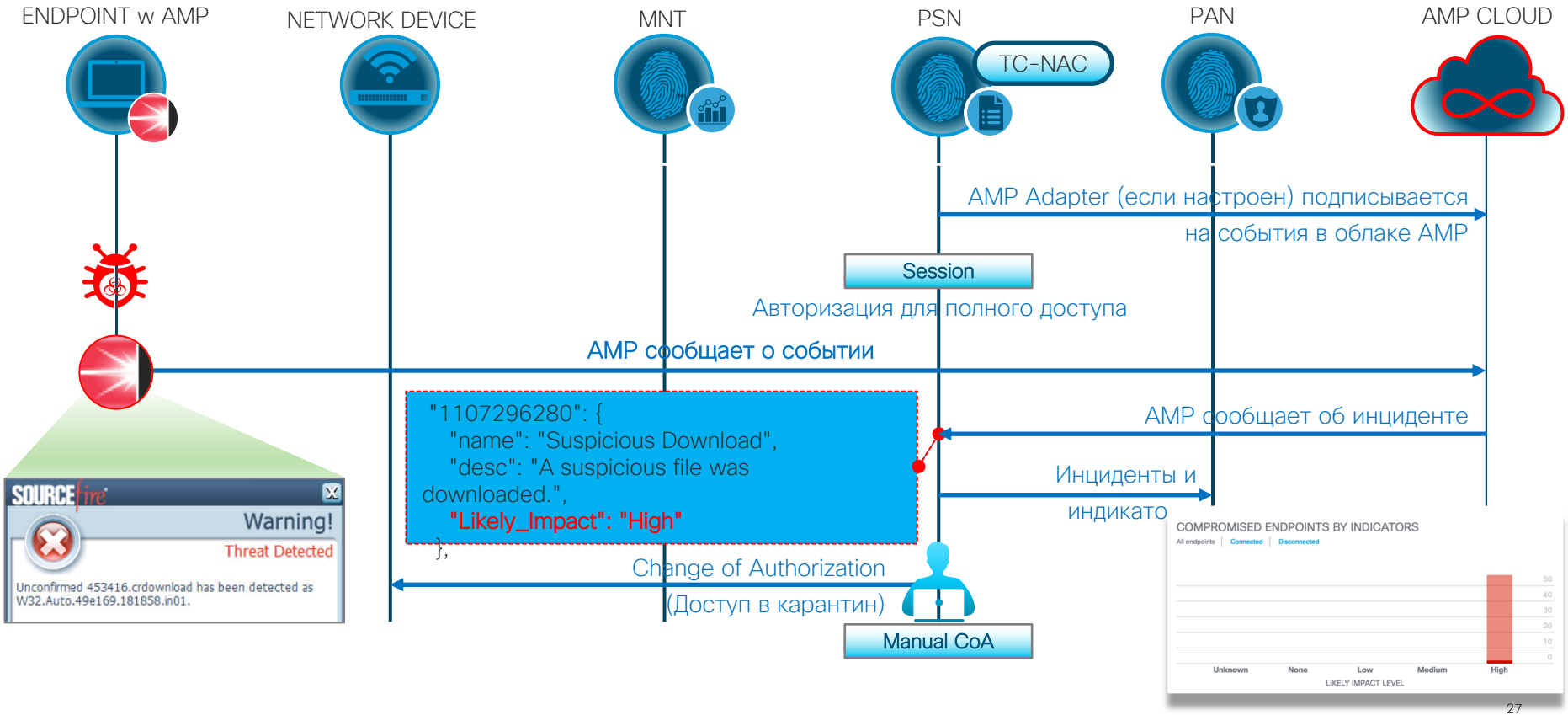
Administration > Threat Centric NAC > Third Party Vendors





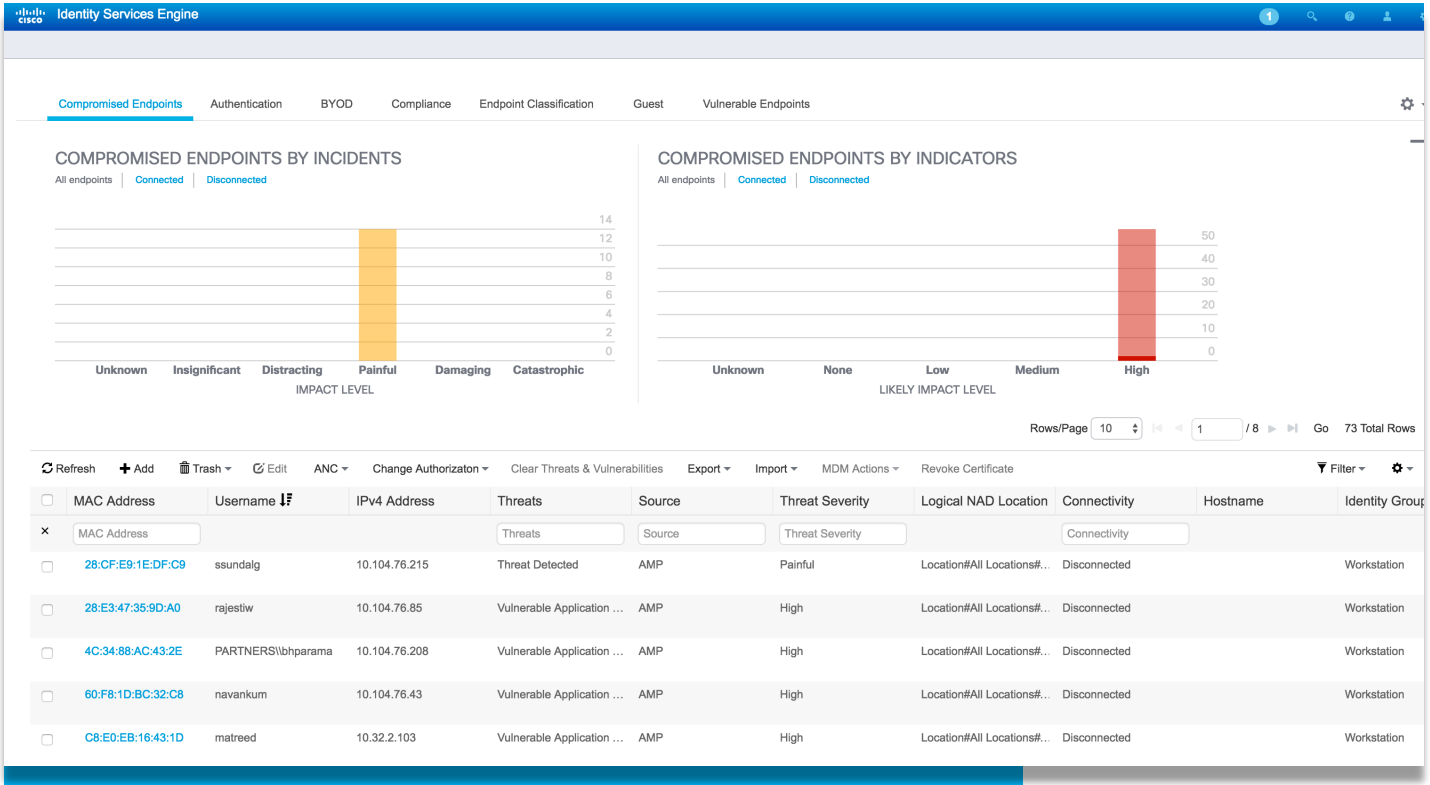
Виртуальные машины или устройства

Контроль доступа с учетом угроз



‘Скомпрометрированные узлы’

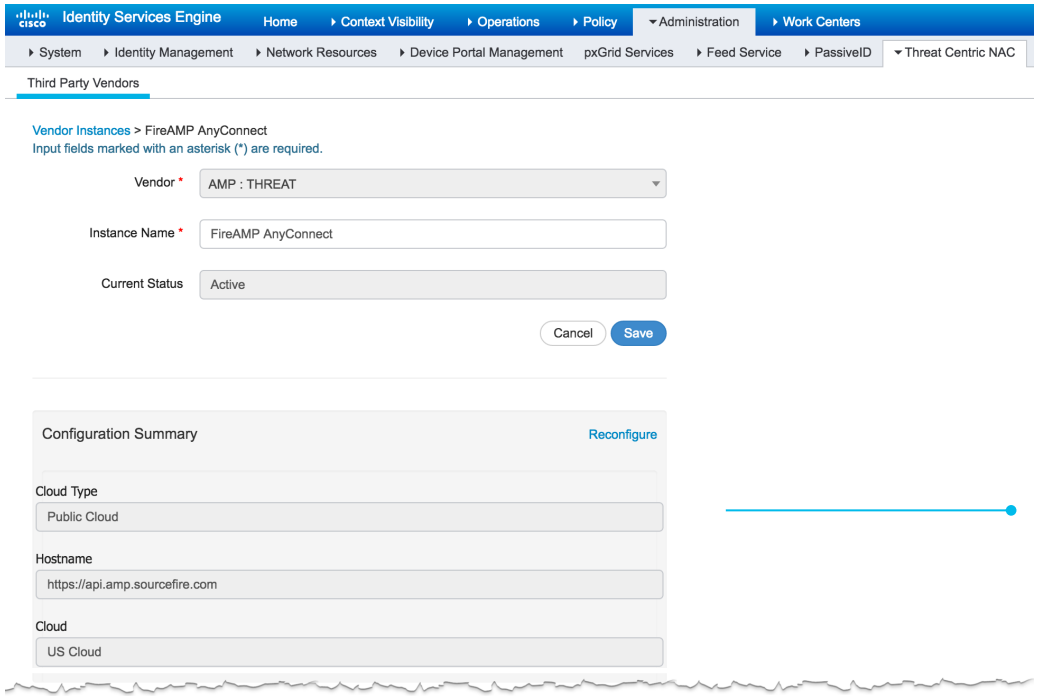
Основано на инцидентах и индикаторах



Формат Structured Threat Information Expression (STIX)

Настройка TC-NAC с AMP

Administration > Threat Centric NAC > Third Party Vendors

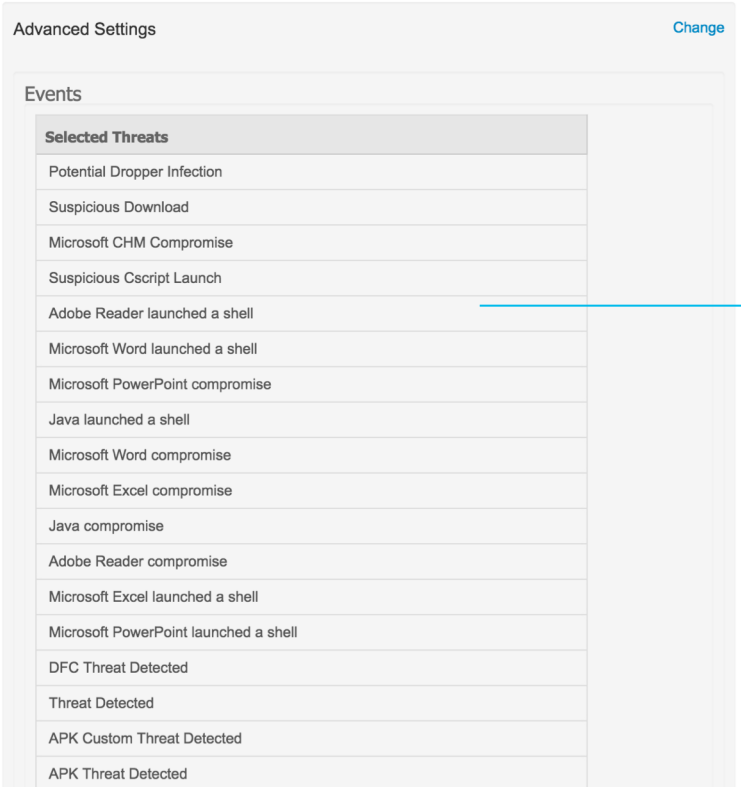


*Замечание: *AMP требует прямого доступа в Internet через SOCKS (port 1080) Стандартный прокси не заработает.*

Идентичная конфигурация для большинства конфигураций*

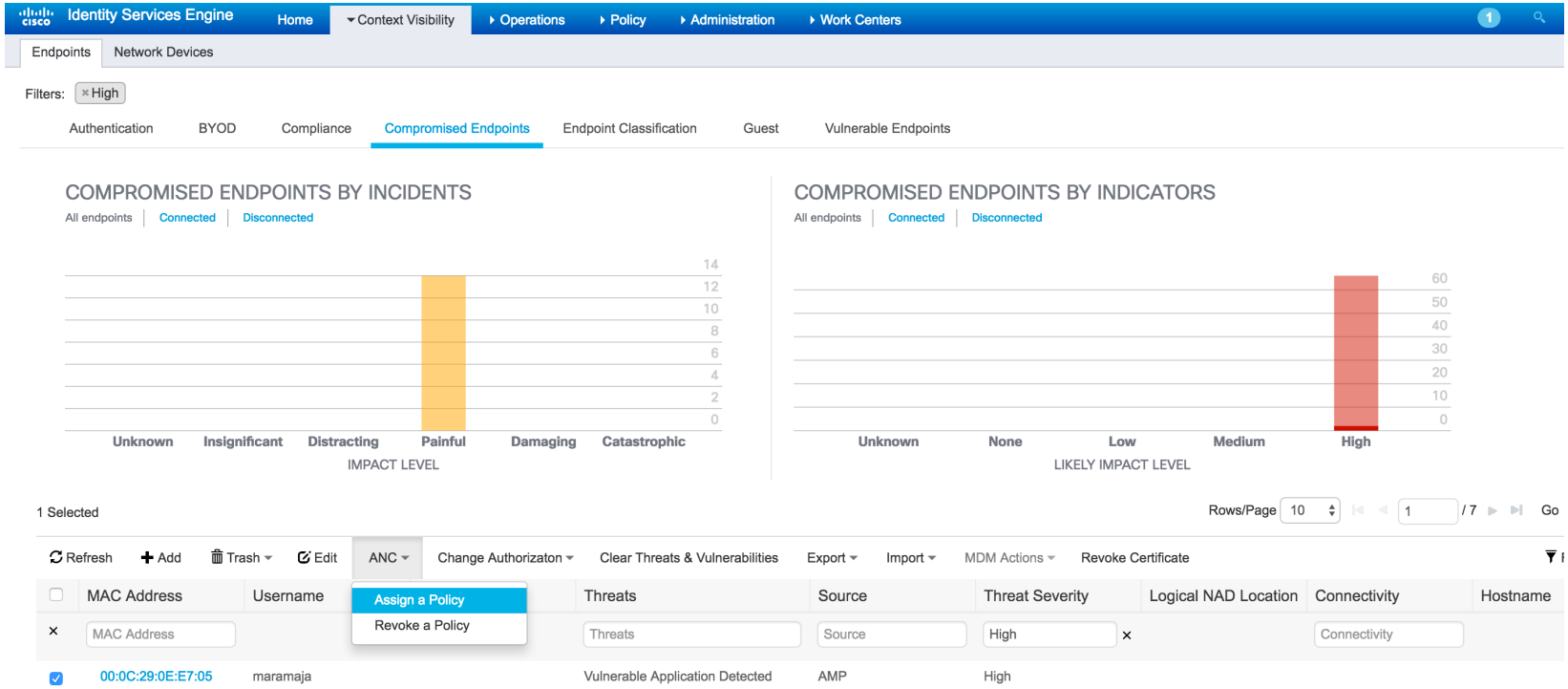
Настройка TC-NAC с AMP

Administration > Threat Centric NAC > Third Party Vendors

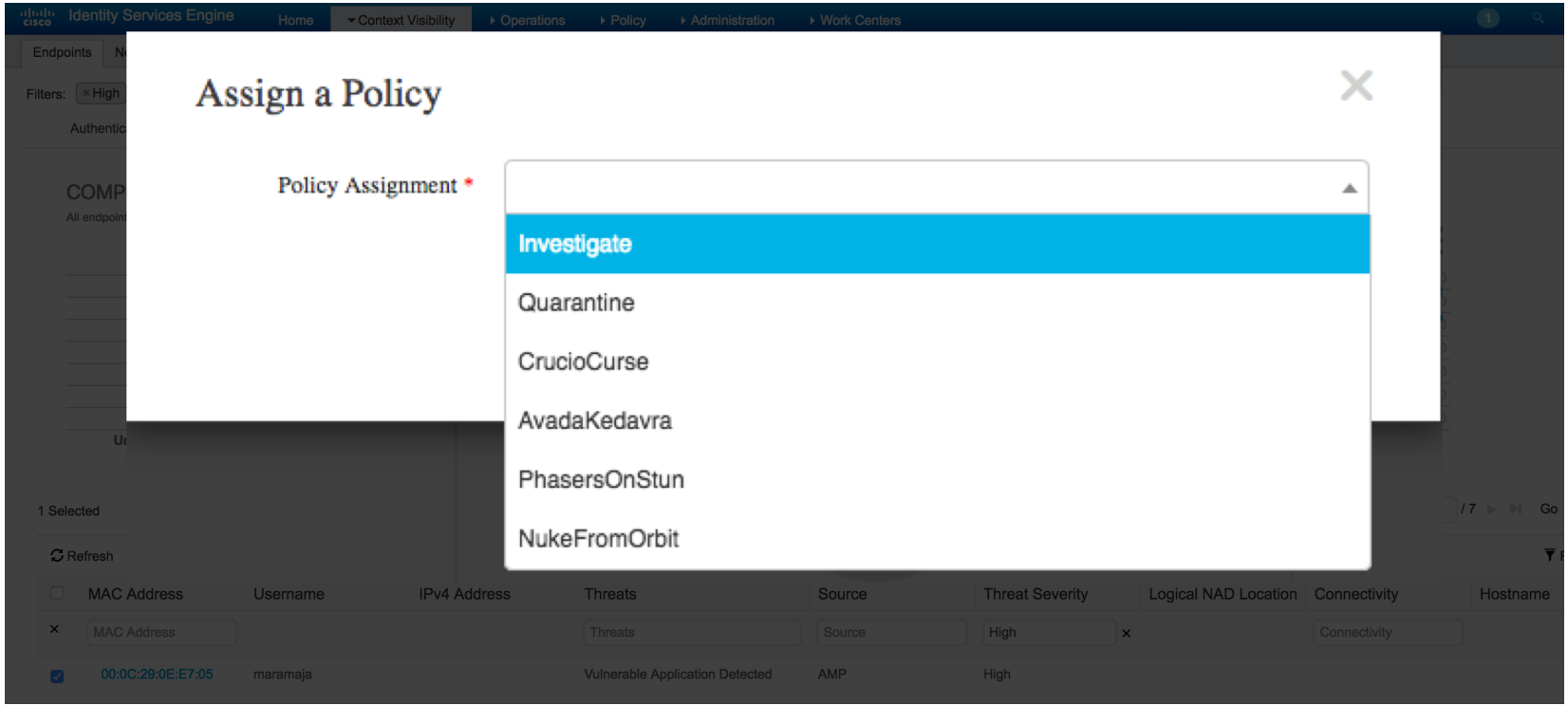


Можно отфильтровать.

Ручной карантин



Ручной карантин



Threat Centric NAC. Резюме

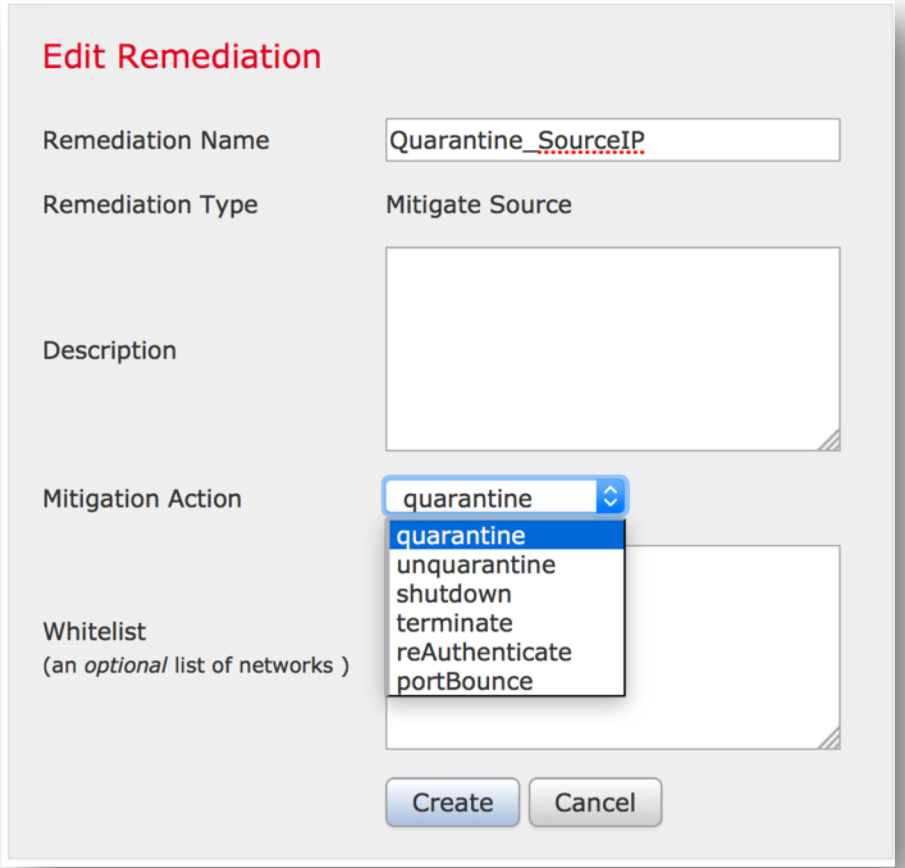
- Возможность **инициировать проверку уязвимостей**
- Инициация **принудительного сканирования** если это необходимо.
- Используйте эти результаты для генерации нормализованных результатов в формате Structured Threat Information Expression (STIX) format и оценки CVSS для оценки уязвимостей.
- ISE имеет 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

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



Интеграция AMP <-> ISE TC-NAC

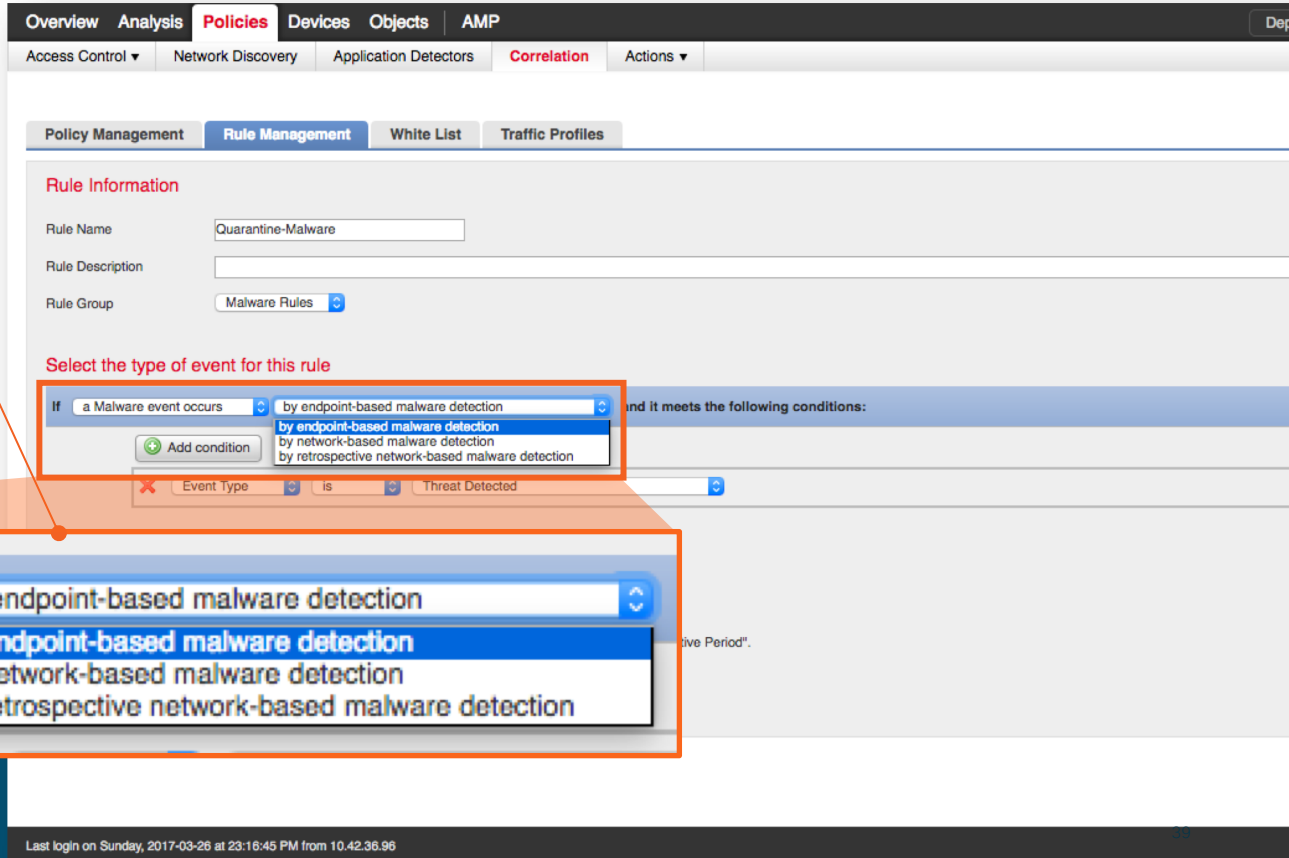
- Ограничена только ручным реагированием.
- Для автоматизации: Используйте Firepower Management Center*
  - Правило корреляции: Malware Event Occurred
  - Затем используйте ISE Remediation Module (Rapid Threat Containment)

*Совет дня

Правило корреляции FMC

События Malware

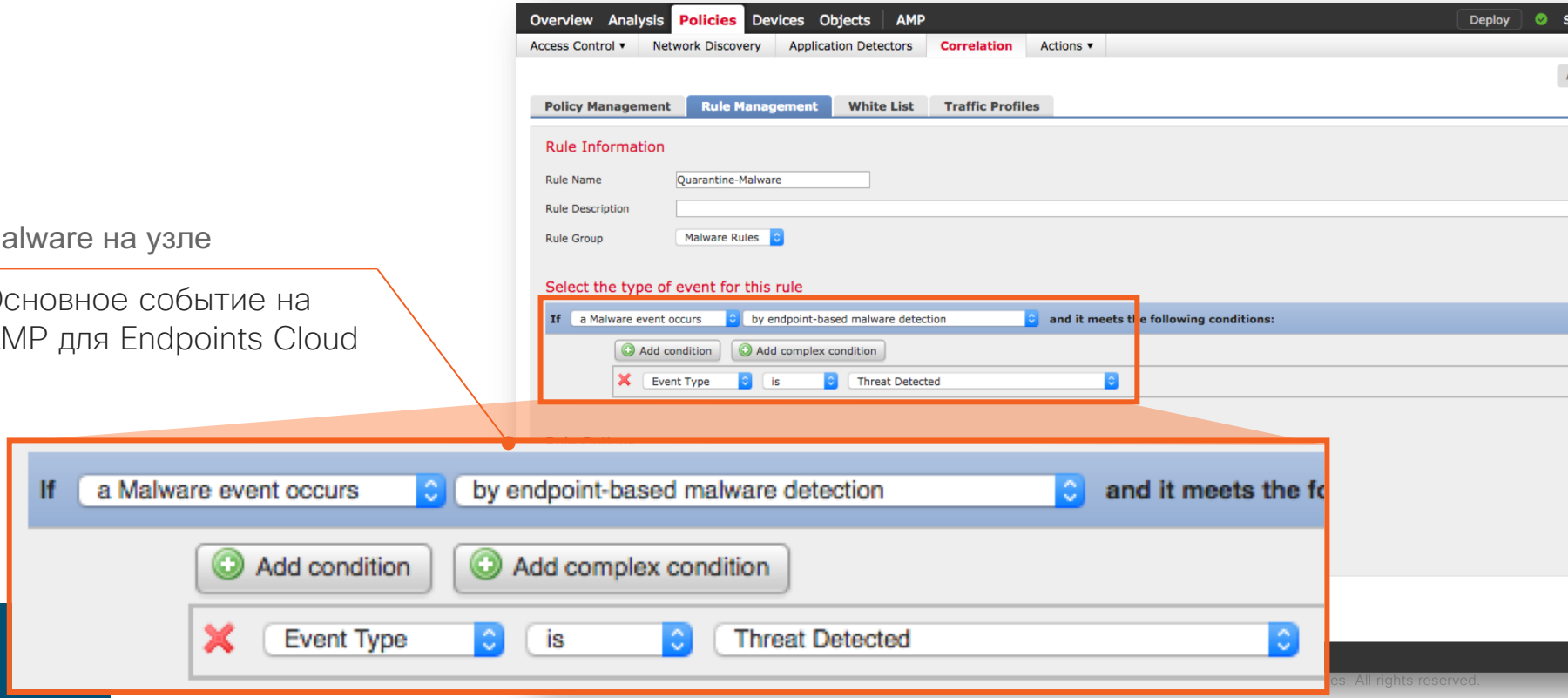
- Сеть
- Узел
- Ретроспектива



Правило корреляции FMC

Malware на узле

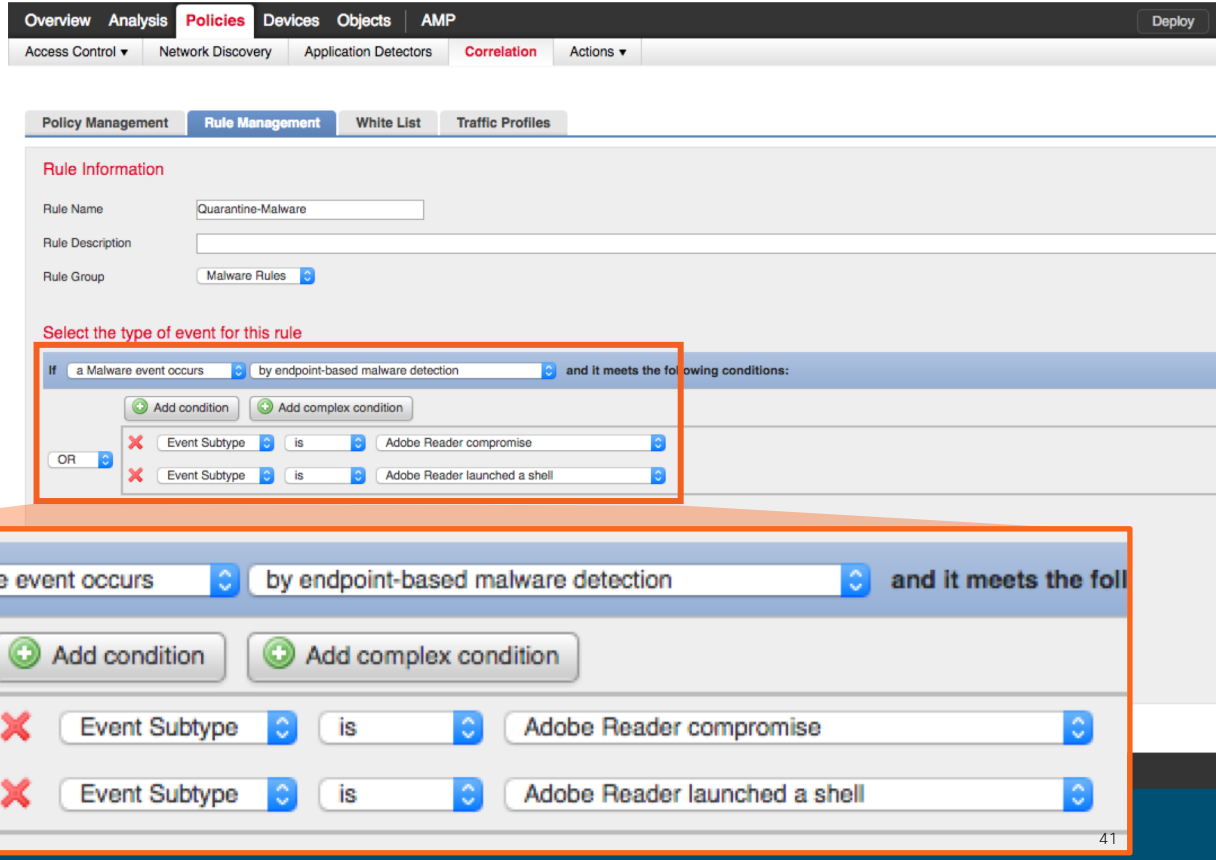
Основное событие на AMP для Endpoints Cloud



Правило корреляции FMC

Malware на узле

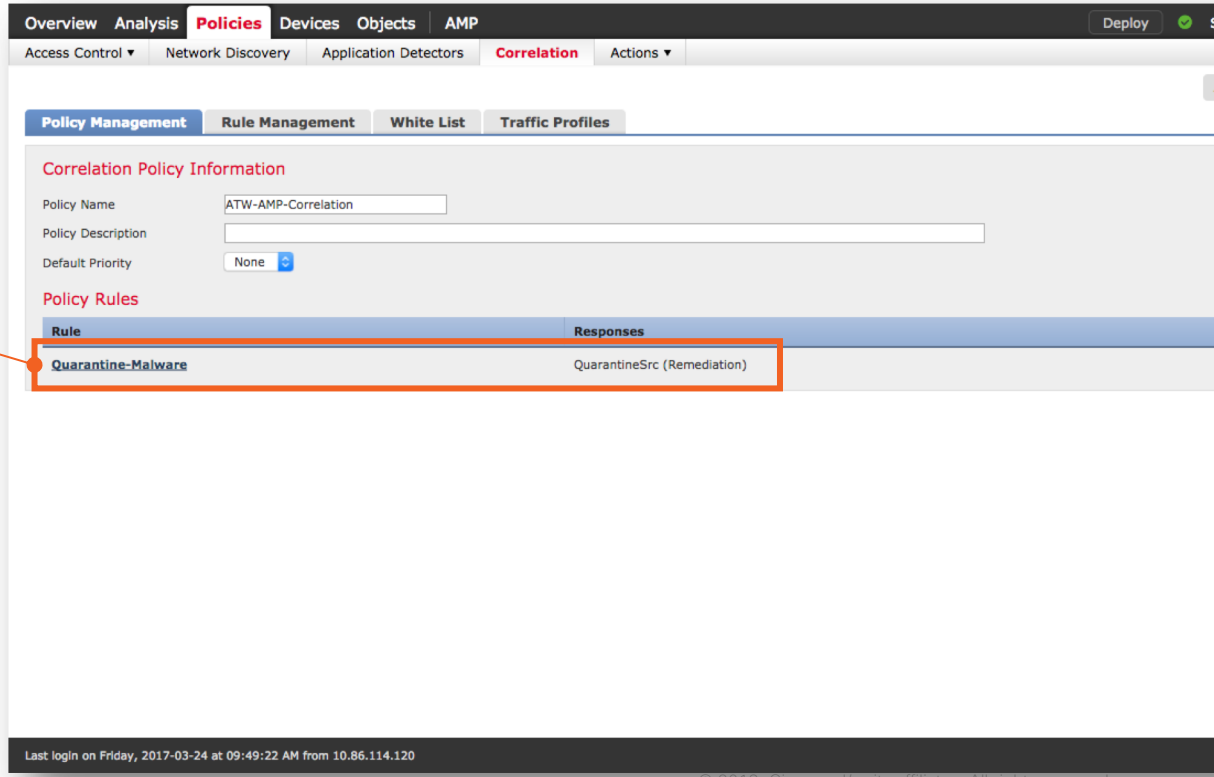
Определенные события
на AMP Endpoints Cloud



Коррекция

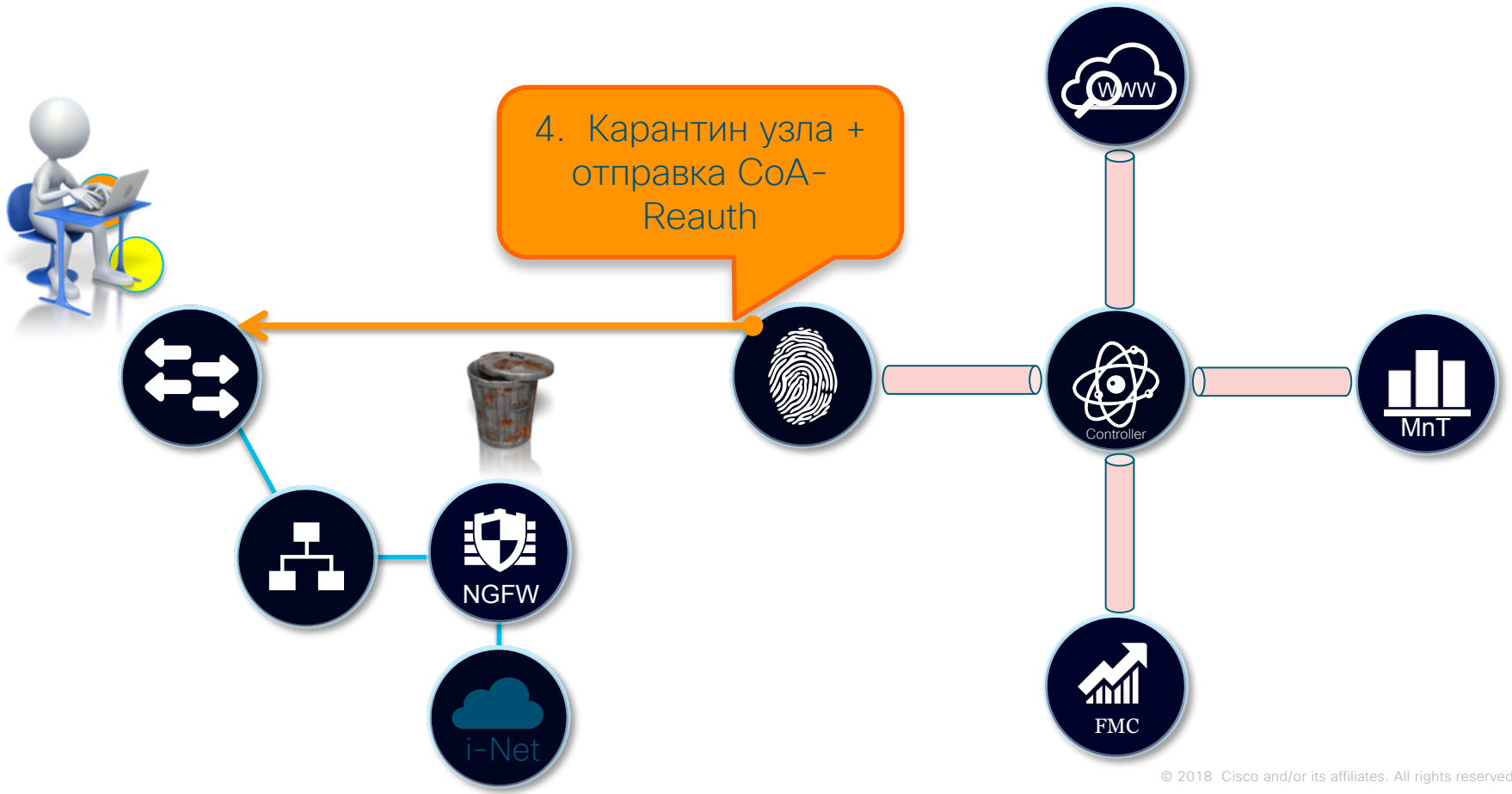
Карантин

Коррекция, которая запускает карантин EPS через pxGrid

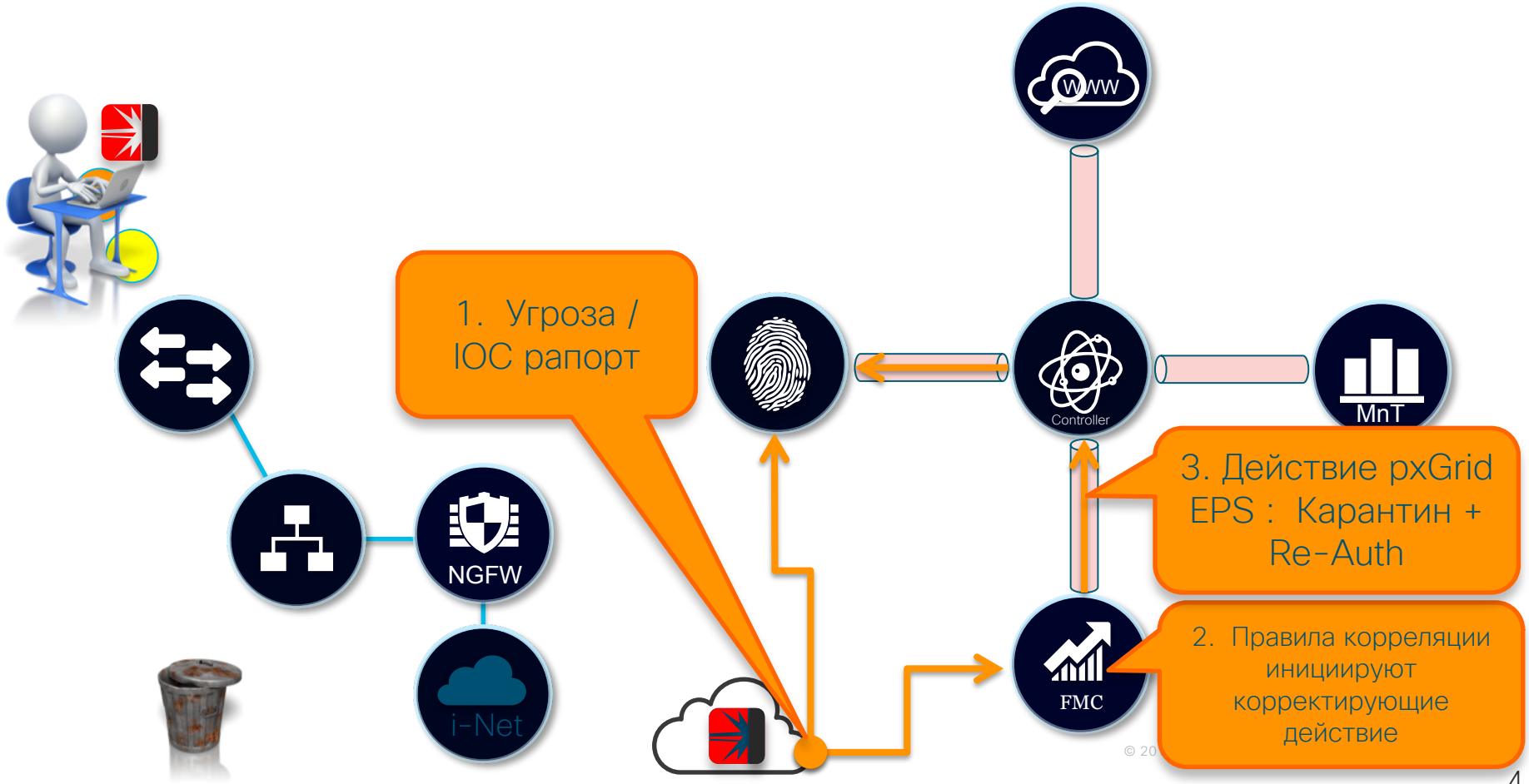


Rapid Threat Containment с Firepower Management Center и ISE

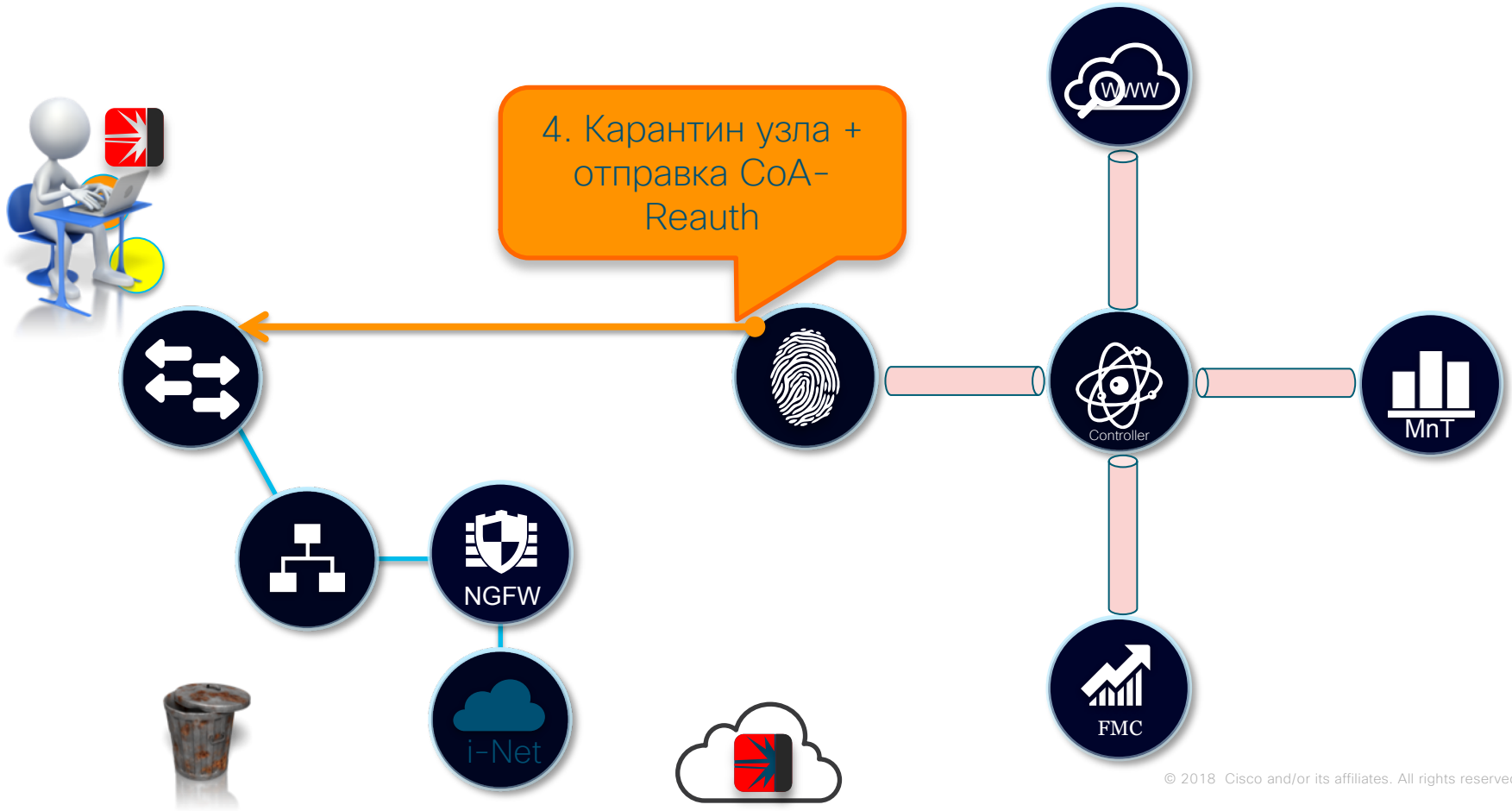
RCT с FMC и ISE



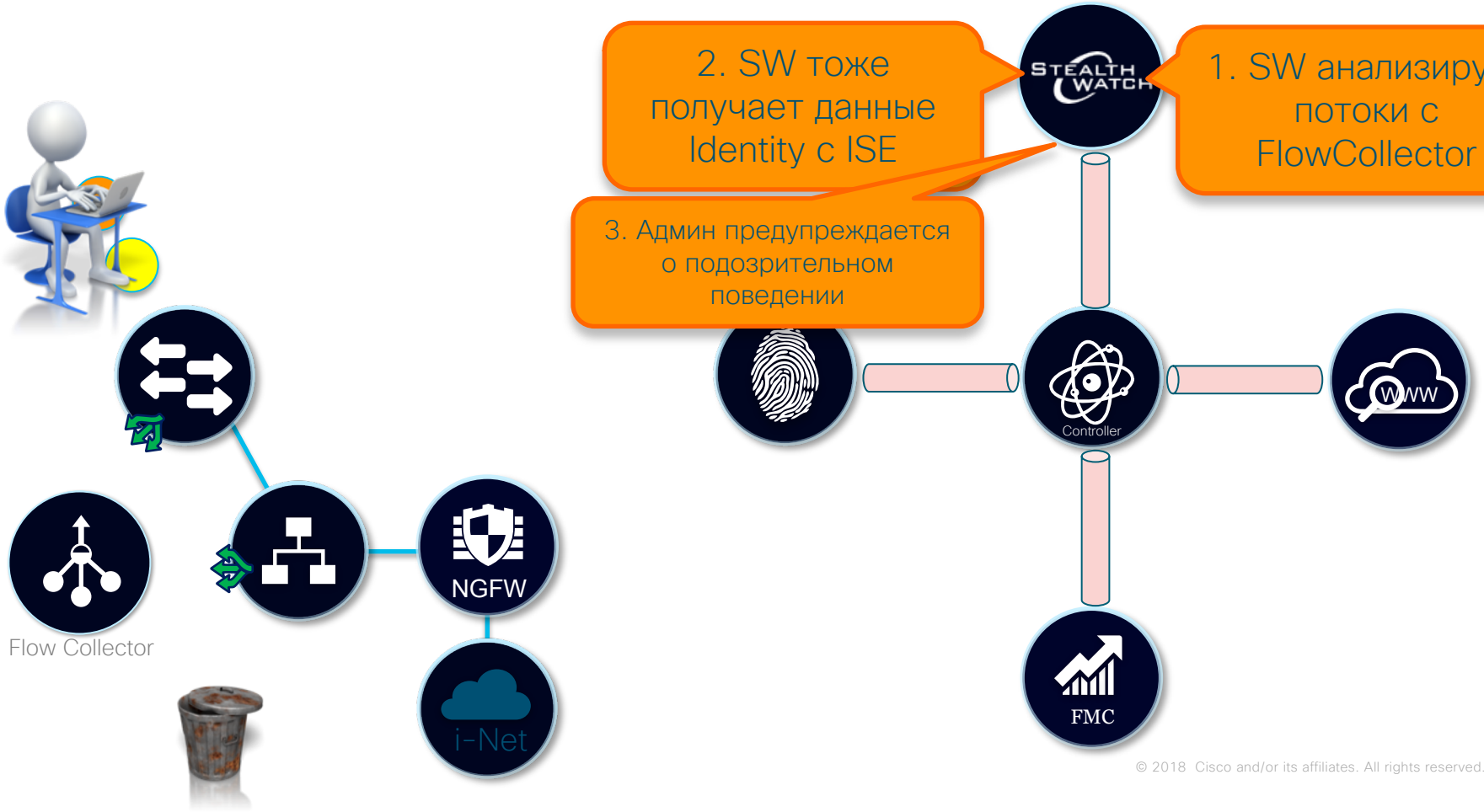
RTC с AMP, FMC и ISE



RTC с AMP, FMC и ISE



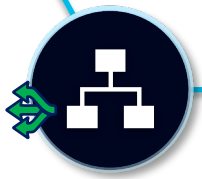
RTC с Stealthwatch и ISE



RTC с Stealthwatch и ISE

4. Админ инициирует карантин узла (EPS через pxGrid)

Flow Collector



5. Карантин узла + отправка CoA-Reauth

RTC с Stealthwatch и ISE

А если я хочу ANC без pxGrid?

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

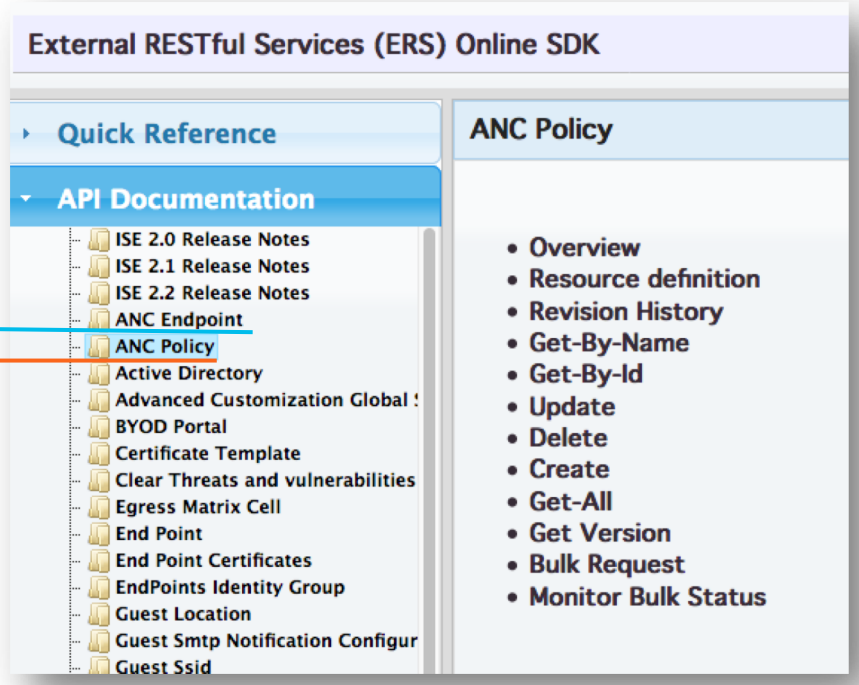
https://ISE:9060/ers/sdk

Step 1: ANC политика

Какие существуют политики

Step 2: ANC Endpoint

Назначение политики на узел



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

Operations > ANC

Policy List | Endpoint Assignment

List

Refresh | + Add | Trash | Edit

Policy Name
ANC-Quarantine
ANC-Investigate
ANC-Destroy
ANC-NukeFromOrbit

7.securitydemo.net:9060/ers/config/ancpolicy | Params | Send

Body | Pre-request Script | Tests

	application/vnd.com.cisco.ise.anc.ancpolicy.1.0+xml	Bulk Edit
Accept-Search-Result	application/vnd.com.cisco.ise.ers.searchresult.2.0+xml	
Authorization	Basic ZXJzYWRtaW46Q2lzY28xMjM=	
key	value	

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" xml
       .ers.ise.cisco.com">
3      <ns5: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
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="applica
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="appli
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="applicat
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>
```

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.w
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

Operations > ANC

Policy List | Endpoint Assignment

List

Refresh | + Add | Trash | Edit | EPS unquarantine

MAC Address	Policy Name	Policy Actions
00:50:56:B8:B1…	ANC-NukeFromOrbit	[PORT_BOUNCE]

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

Пример: Карантин узла

Условия

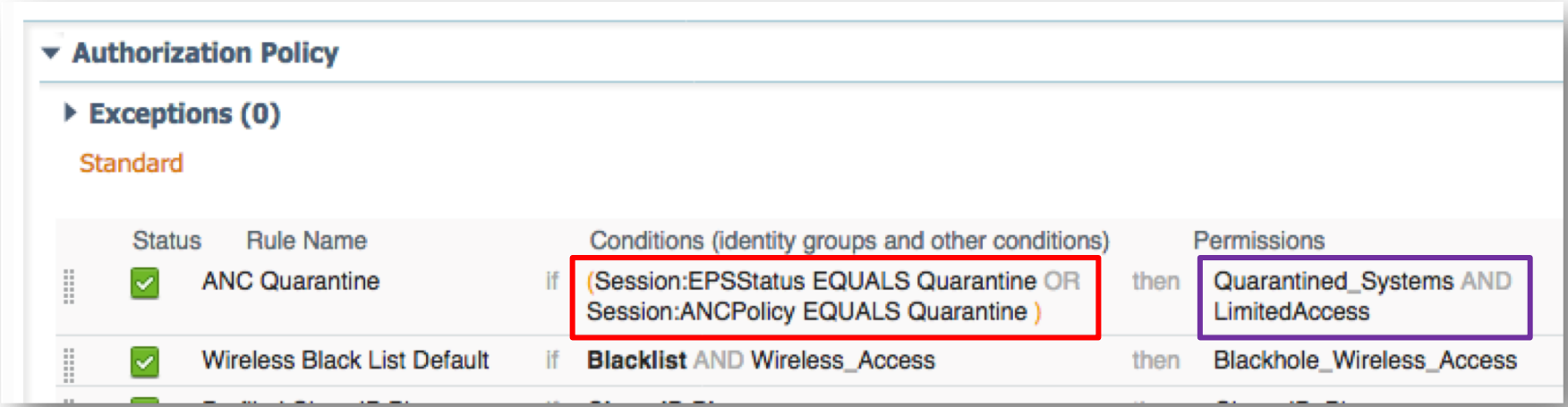
EPS в Quarantine

или

ANC в Quarantine

Результат

Ограниченный доступ + Тэг Quarantine



Пример: Запустить сканирование уязвимостей и расшифровку SSL

Условие

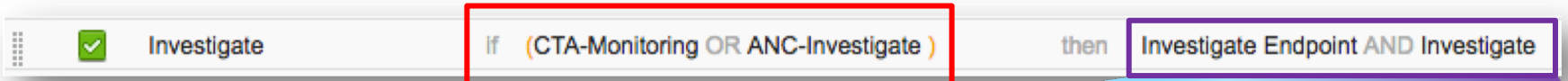
CTA Course of Action = Monitoring

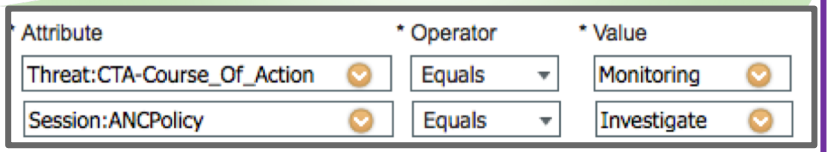
OR

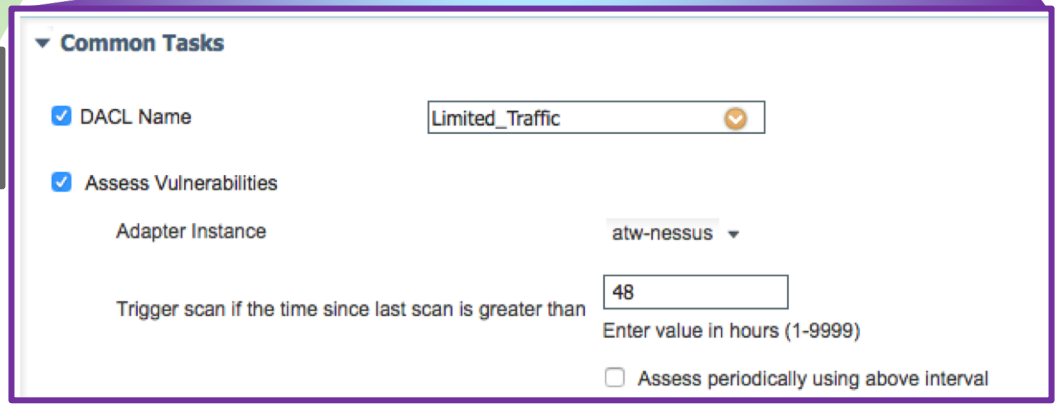
ANC = Investigate

Результат

Ограничение доступа + Скан уязв. + SGT Investigate







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 CTA “согласны”, затем выбросить из сети

FMC карантин = Скан уязвимостей и расшифровка SSL

Условие

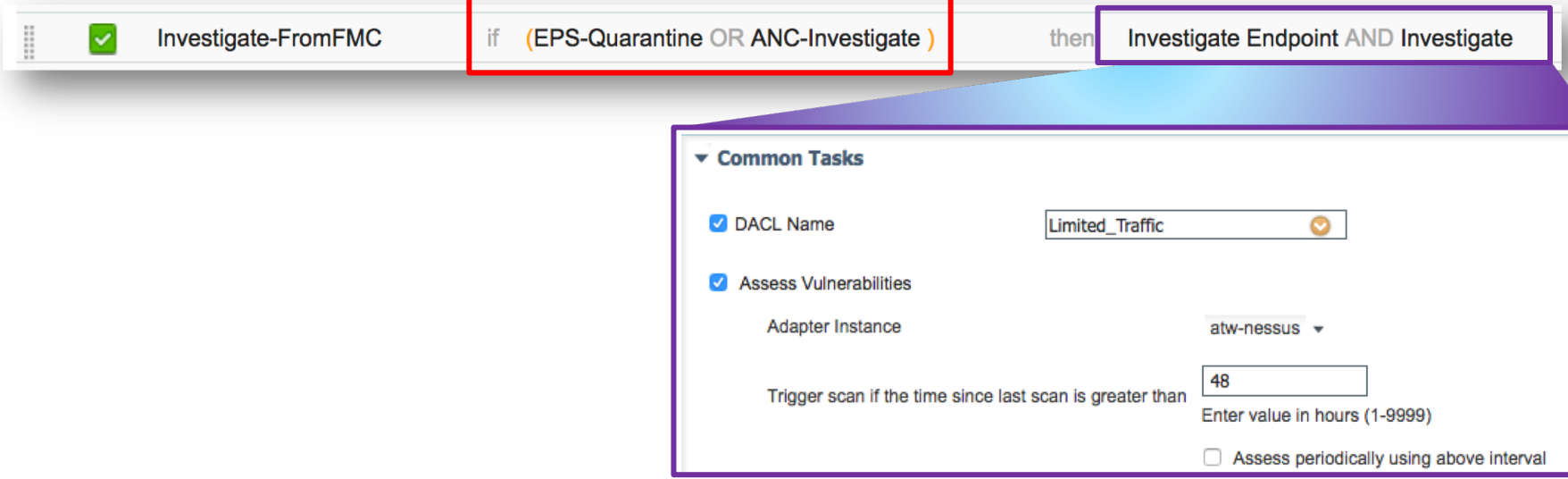
EPS = Quarantine

или

ANC = Investigate

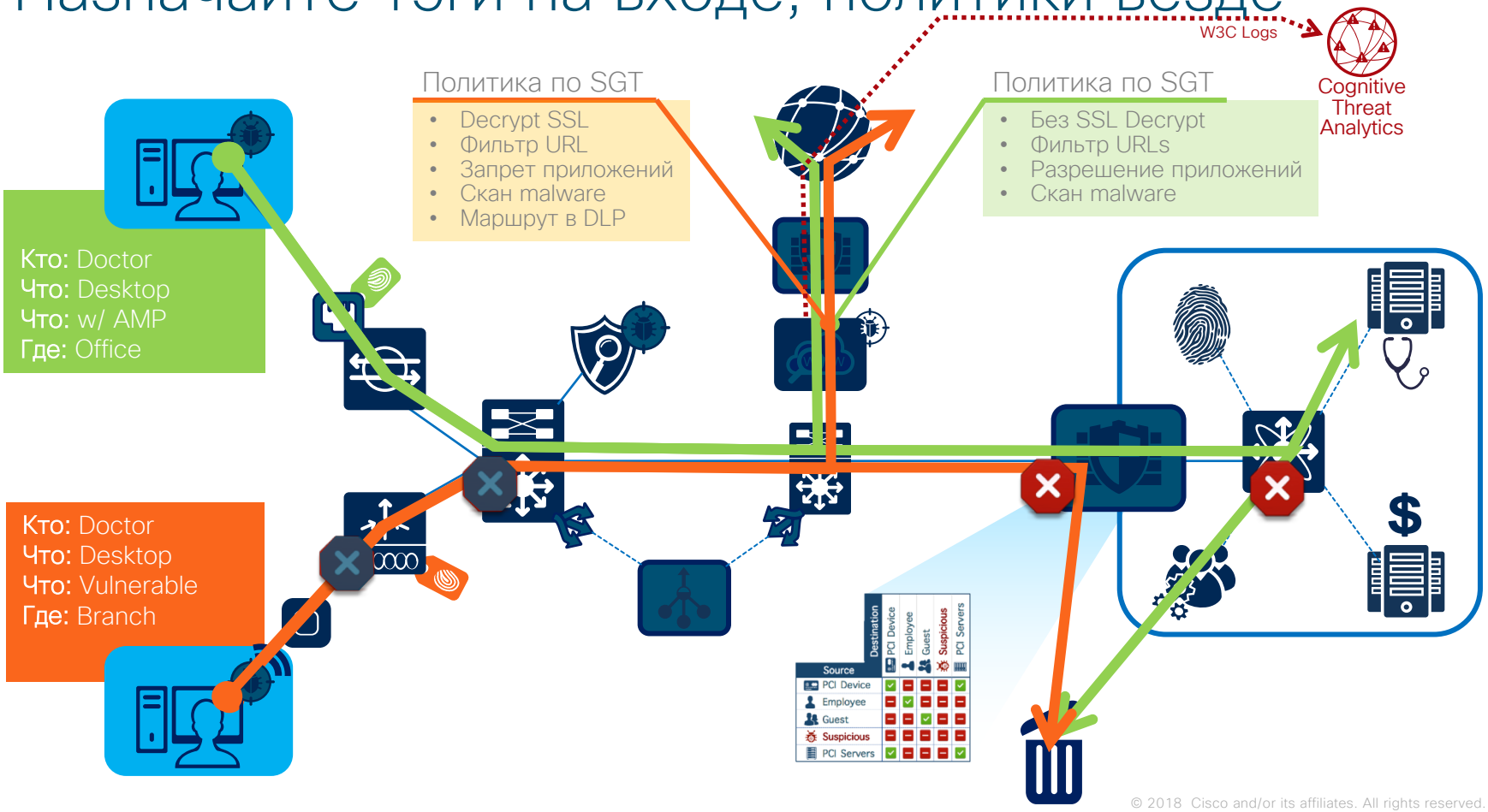
Результат

Огран. доступ + Скан уязв. + SGT Investigate



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

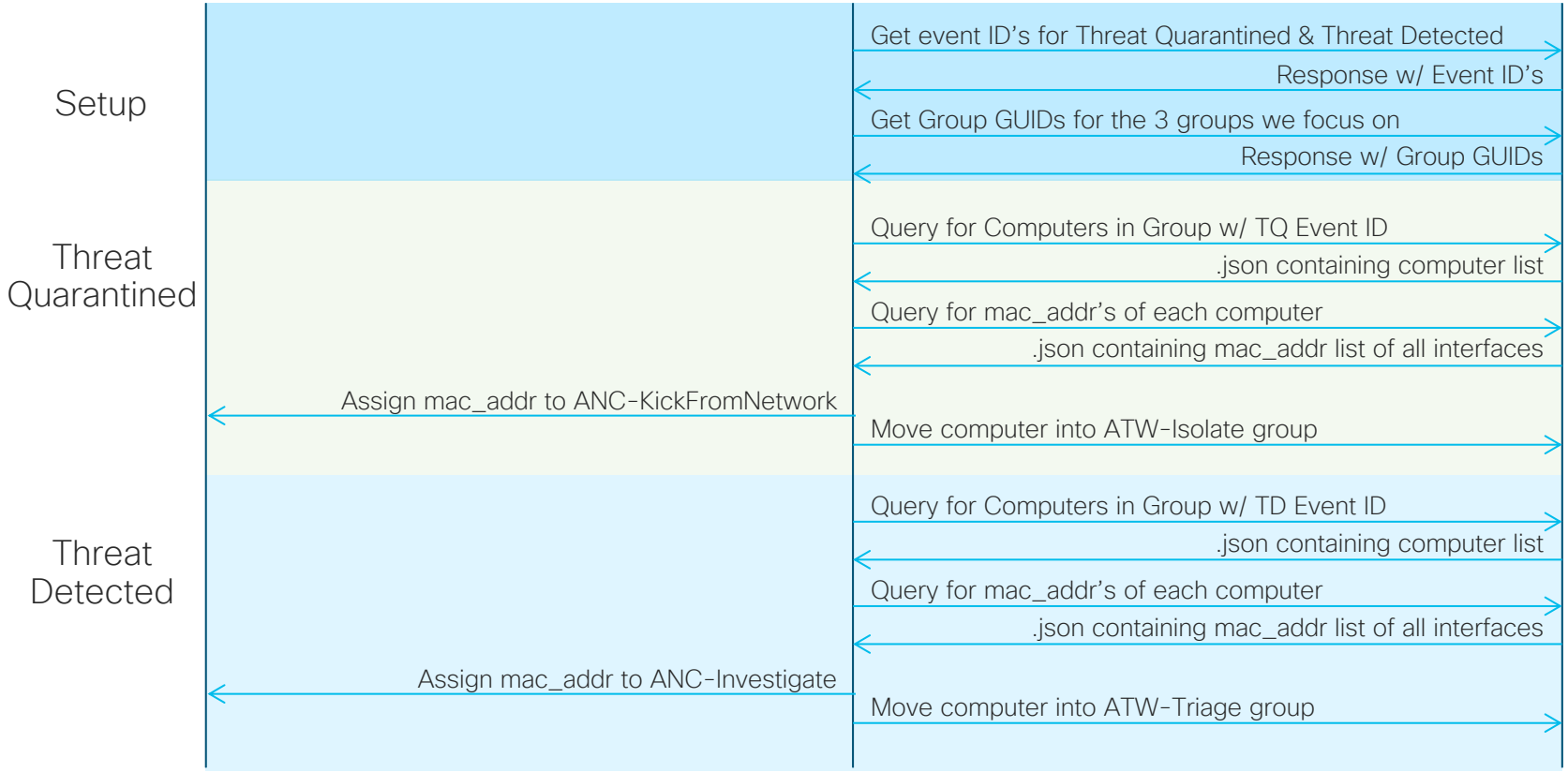
Скрипты Python RTC-AMP-ISE

- 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

ISE

Linux Server w/ Python

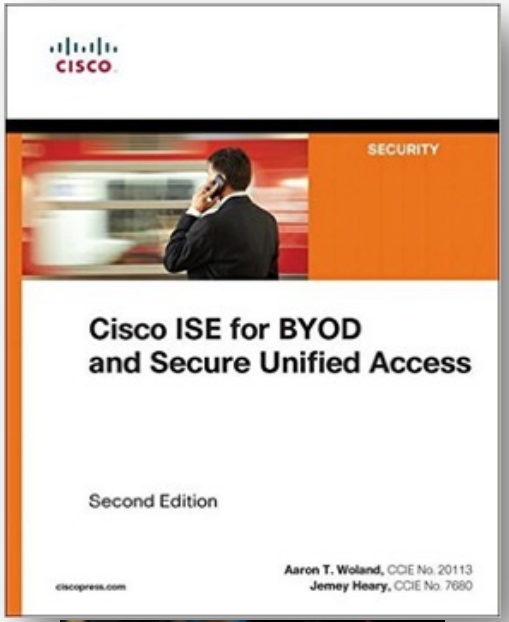
AMP



Заключение

Дополнительные ресурсы

- http://cs.co/ise-community
- Блог K. 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?


CISCO