The bridge to possible

Демистификация XDR и SecureX

Pavel Rodionov
Technical Solutions Architect. CCIE 11155, CISSP, GREM
prodiono@cisco.com

Agenda

- XDR в понимании аналитиков
- Обзор XDR и SecureX
- Как подключиться к решениям Cisco
- SecureX оркестрация
- Примеры оркестрации
- Заключение

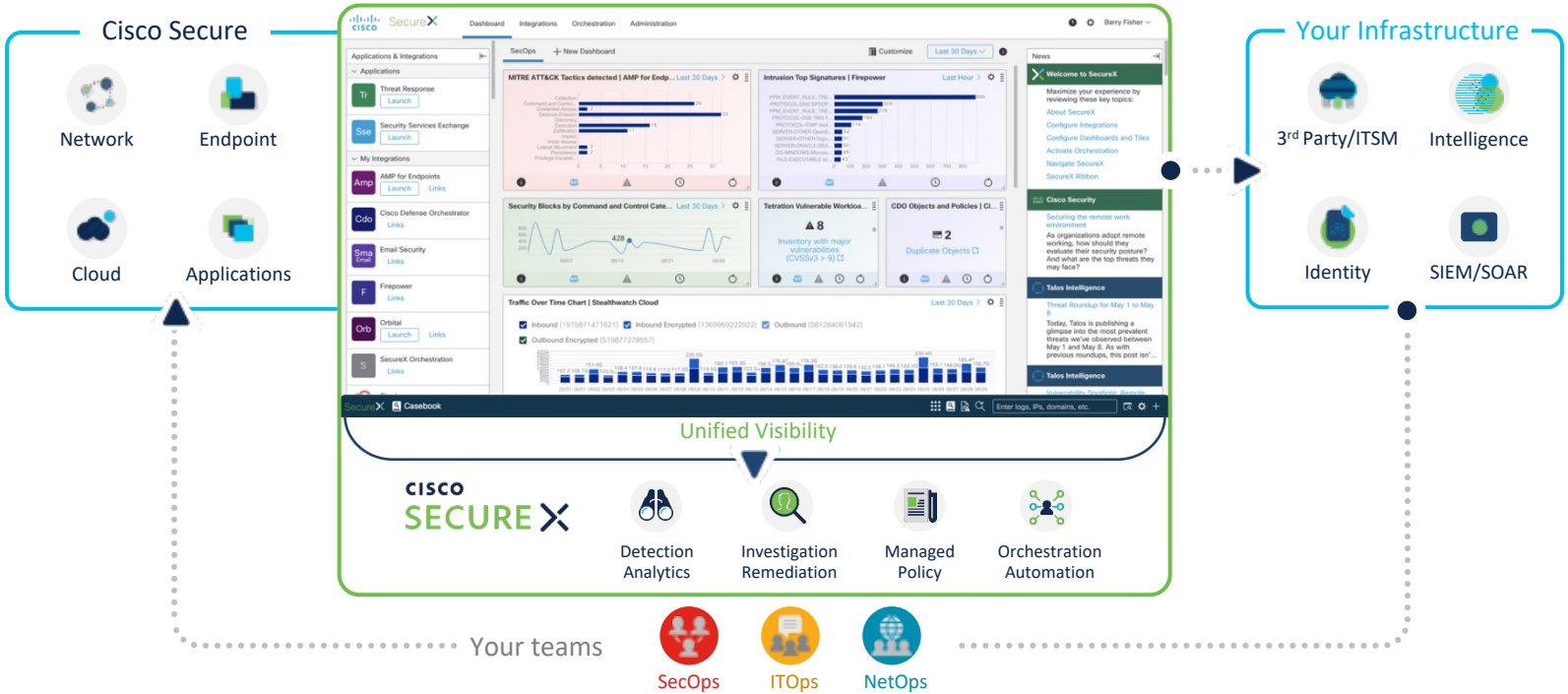
Будет демо!

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Обзор XDR и SecureX

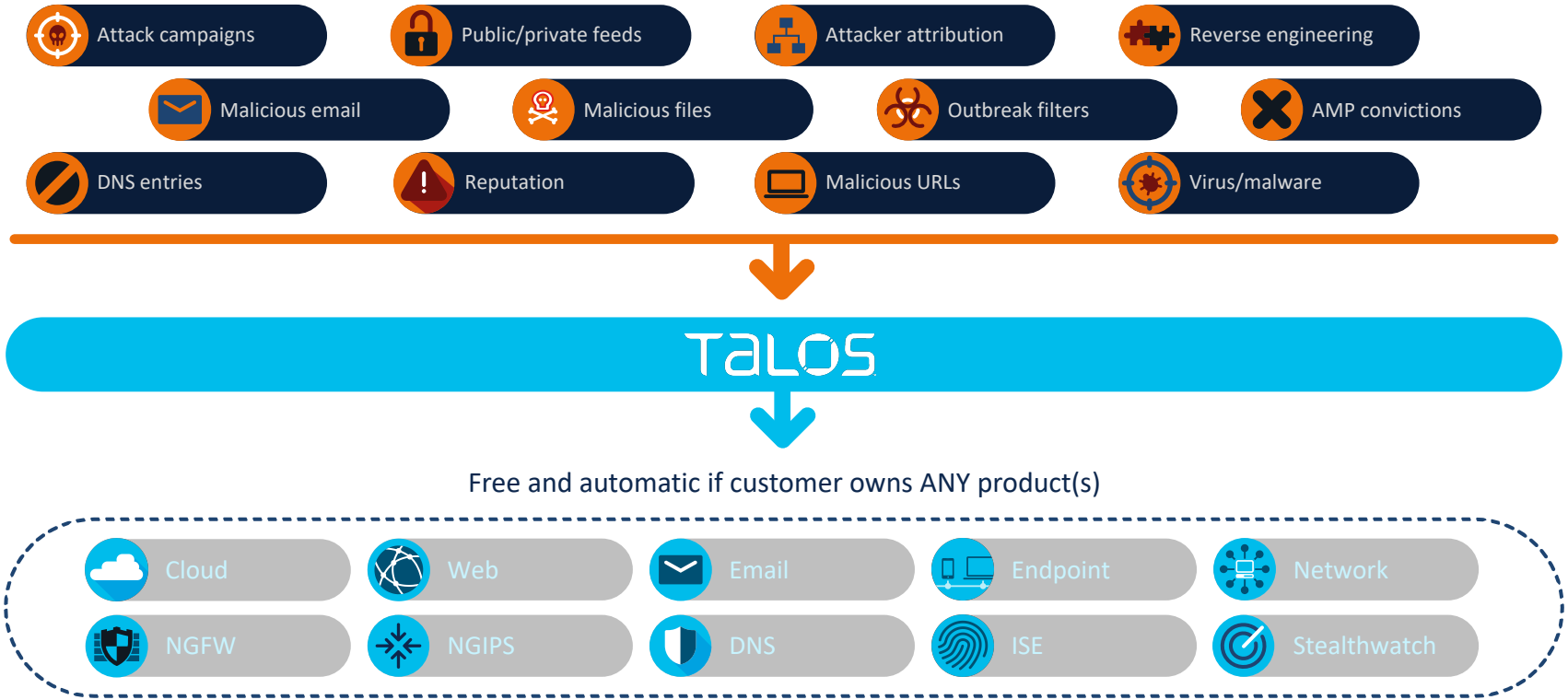
Введение в SecureX

- Облачная, встроенная в наше портфолио платформа безопасности



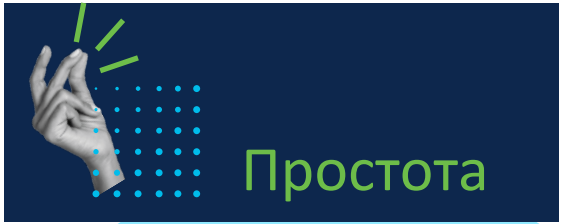
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

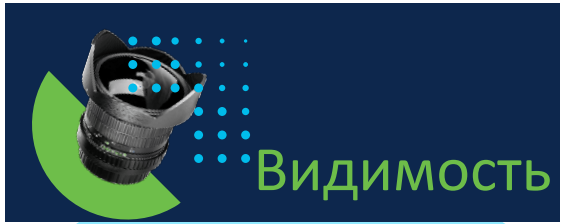
Поддерживается лучшей командой безопасности в индустрии



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX это облачная платформа безопасности





SECURE X

Интеграции
встроенные, настроенные или пользовательские

ribbon и sign-on
никогда не оставляет вас без контекстка

dashboard
Настраивает с тем, что для вас важно

threat response
Ядро платформы

Оркестрация
drag-drop GUI for no/low code

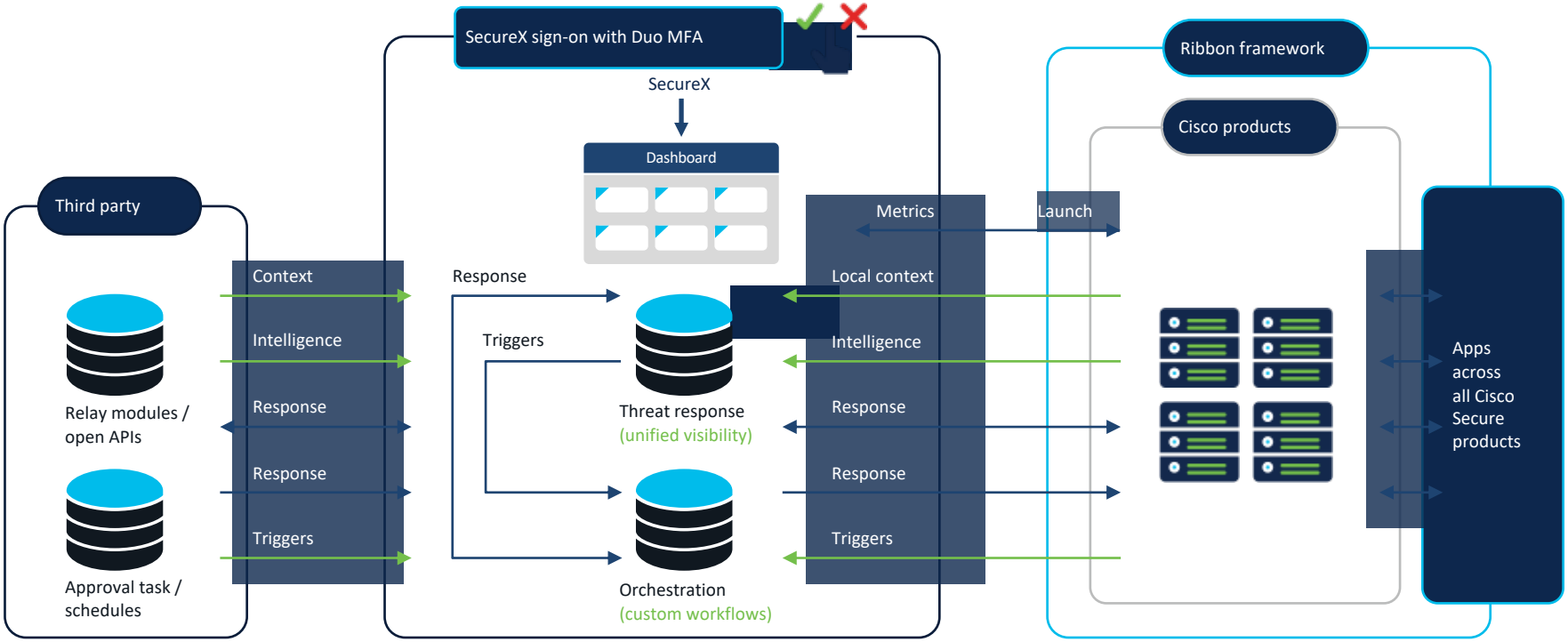
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Возможность увидеть и установить атаку за минуты

Ваш SecOps с SecureX threat response

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX архитектура



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Как выглядит унифицированная видимость

Перед: “Я кручусь на кресле чтобы увидеть то, что важно”

После: “Я моментально вижу то, что имеет значение для меня”

Go To:
SecureX dashboard and ribbon deep dive

“We can view ROI metrics and operational measures across many products in one or more customizable dashboards”

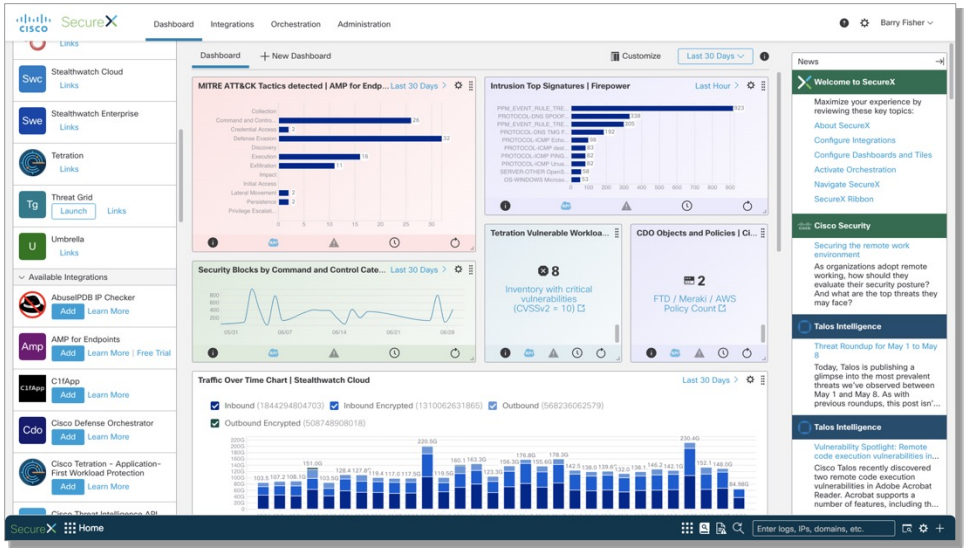
“We never lose context as the ribbon follows us everywhere when we use the Cisco Secure portfolio”

“We can try other platform integrations with a click before we buy”

“Our SOC knows latest intel from the largest threat research team on the planet”

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Новый уровень видимости с SecureX dashboard

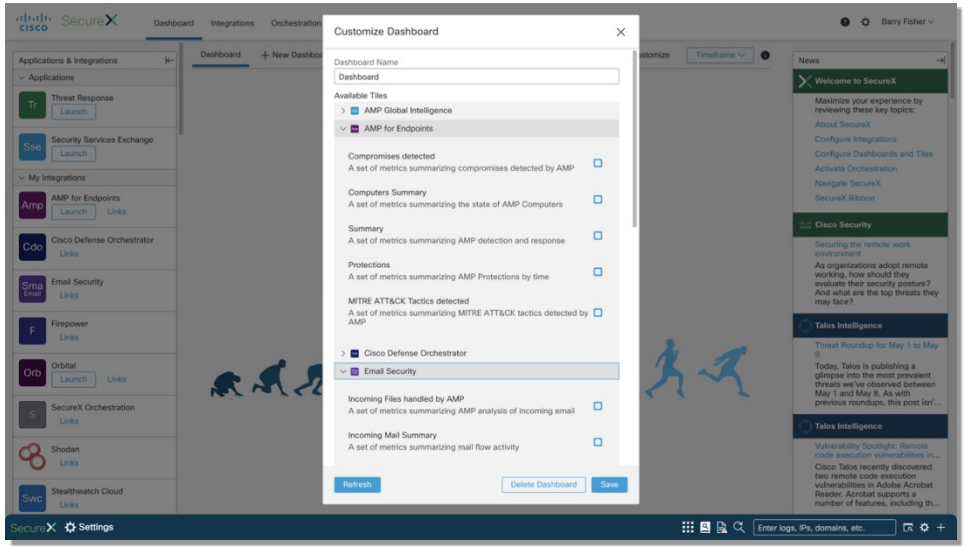


- Приложения (слева)
  Просмотр, запуск или тестирование интегрированных продуктов
- Плитки (центр)
  Представляет метрики и операционные результаты работы интегрированных продуктов
- Новости (справа)
  Обновления продуктов, новости безопасности и блог-посты

Понять, что имеет значение с первого взгляда

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Делайте то, что хотите с настраиваемыми дашбордами



- До 20 дашбордов на пользователя
- 60+ плиток доступно для 12+ различных продуктов Cisco
- Настройка плиток по расположению, размеру, времени, масштабу, и т.д.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

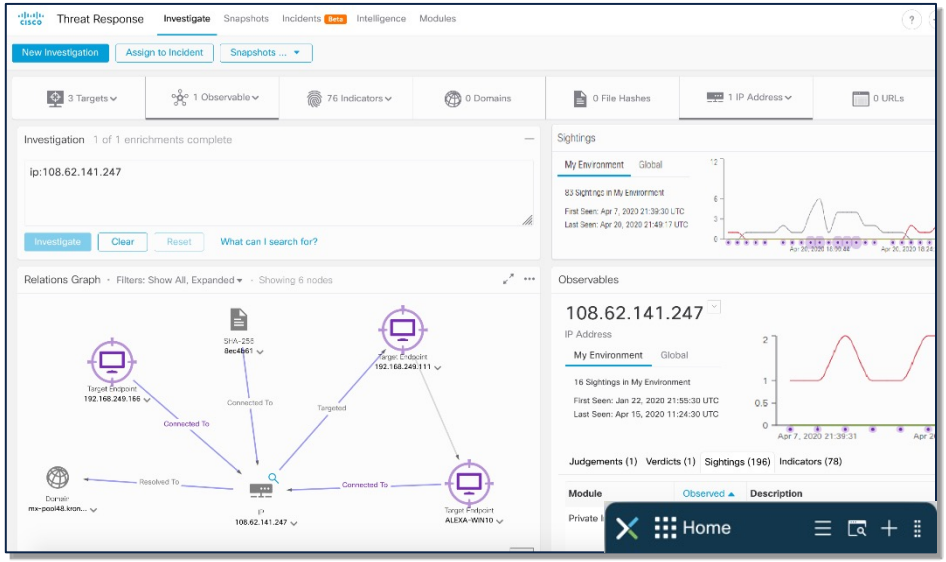
Ускорить проведение расследований в SecureX

SecureX threat response

Агрегирование и запрос глобальной информации и локального контекста из одного окна

Визуализация влияния угроз в вашей среде

Предпринимайте немедленные действия для изоляции угроз и блокирования выполнения файлов
Автоматизация процессов с действиями разрешения для улучшения взаимодействия



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

C Cisco SecureX Threat Response

Моя команда может:

Быстрее отвечать на вопросы о наблюдаемых индикаторах.

Блокировать и разблокировать домые.

Блокировать и разблокировать выполнение файлов

Изолировать узлы

Охотиться на наблюдаемые индикаторы, которые ассоциированы с известной атакой и немедленно видеть влияние

Сохранять снимки процесса расследования для последующего анализа.

Документировать анализ в casebook из всех интегрированных web инструментах, включая API

Просто интегрировать CTR в существующие инструменты

Сохранять свою собственную threat intel и использовать ее в расследованиях

Единая точка для расследования угроз

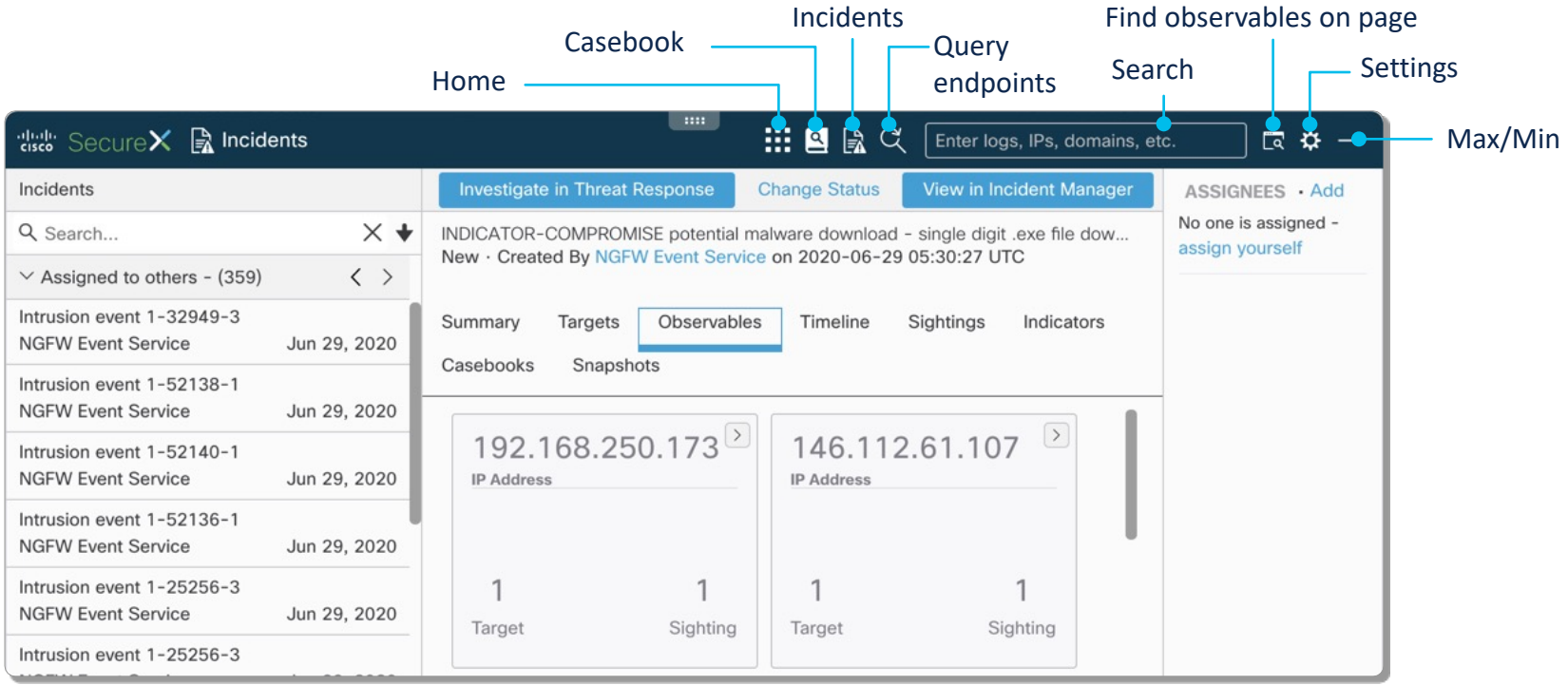
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX ribbon

- SecureX ribbon позволяет вам переносить наболее релевантных контекст безопасности и threat intelligence по всем вашим продуктам
- Транспортная структура для функциональности: возьмите с собой возможности SecureX и интегрированных продуктов, когда вы переходите на консоль любого другого продукта
- Связывает продукты вместе и обеспечивает унифицированный опыт и широкие возможности реагирования для всех продуктов.
- Возможность перекрестного запуска: переход к любым другим продуктам с ленты
- Ленточные приложения: при посредничестве SecureX, предоставляются SecureX и другими продуктами.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Никогда не теряйте контекст с SecureX ribbon

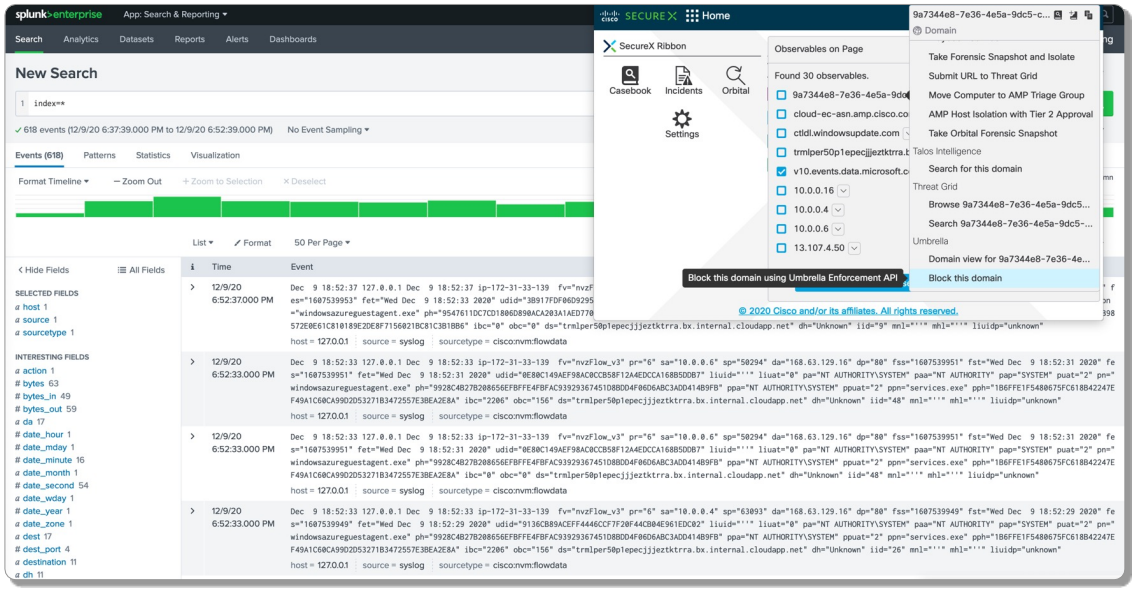


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Берите SecureX вместе с собой

The SecureX ribbon extension

- **Простое подключение к сторонни инструментам.** Извлекайте наблюдаемые индикаторы в ленту из сторонних инструментов и переходите к расследованию.
- **Начните расследование из браузера за минуты.** Это реальное время для начала использования. Быстро запрашивайте узлы и выполняйте ответные действия, не выходя из браузера.
- **Лучше взаимодействуйте с командой безопасности.** Создавайте или добавляйте обращения прямо из браузера и делитесь ими с командой.



Cisco SecureX

Начало работы

Идентификация и тенанты (SSO)

Подключение, Ribbon и запуск консоли

Security Services Exchange

NGFW Integration

Программа

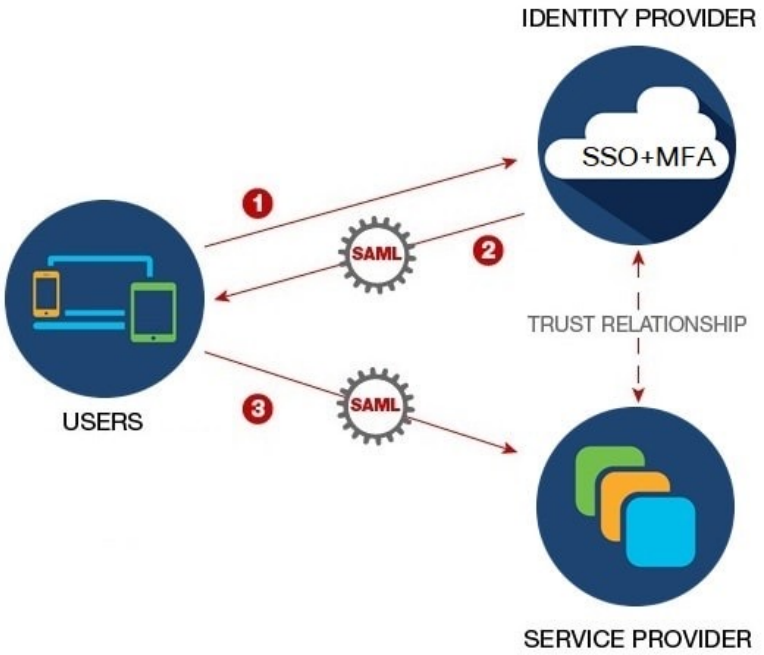
- Регистрация
- Идентификация и тенанты
- Подключение, Ribbon и запуск консоли
- Security Services Exchange
- Интеграция NGFW

cisco Secure

© 2020 Cisco and/or its affiliates. All rights reserved.

Опции аутентификации SecureX

- SecureX Sign-On:
  - С помощью SecureX Sign-On вы легко получаете доступ ко всем вашим продуктам безопасности, которые отображаться в дашборде.
  - Интеграция с с Duo MFA защищает и упрощает аутентификацию. Одно уведомление, одно нажатие, один доступ

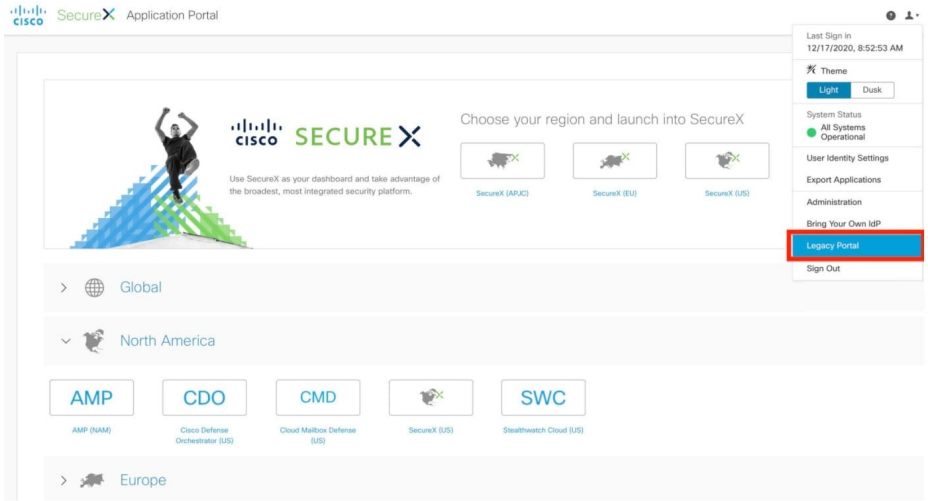


© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

Опции аутентификации SecureX (продолжение)

- SecureX Sign-On:
  - Вы можете создать новую учетную запись и подписаться на SecureX
  - Или
    - Вы можете использовать учетные записи Cisco или MS Azure для регистрации на SecureX портале



© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

Регистрация на SecureX портале

1. https://sign-on.security.cisco.com
2. Если у вас есть учетная запись:
   - Вводите username (email)
   - Нажимаете next и вводите пароль
   - Нажимаете Sign In
   - Или выбираете альтернативный метод входа
     - Через cisco.com
     - Через Microsoft

© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

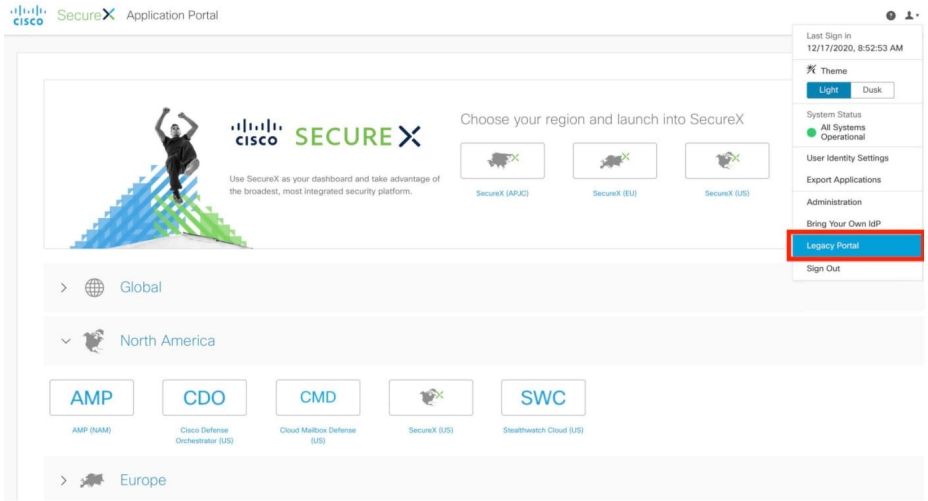
Регистрация на SecureX портале

1. https://sign-on.security.cisco.com
2. Если у вас нет учетной записи:
   - Нажимаете Create a SecureX Sign-On
   - Заполняете форму и нажимаете на Register
   - Находите письмо от Cisco Activate Account и нажимаете на Activate Account
   - Настраиваете MFA с помощью настройки Duo Security. Если вы уже используете Duo, тогда вы получите активационный код, если нет – регистрируете устройство
   - Выбираете security Image
   - Нажимаете Create My Account

© 2020 Cisco and/or its affiliates. All rights reserved.

Регистрация на SecureX портале

- Какие действия дальше
  - Выберите ваш регион и запустите SecureX
  - Запускайте любое приложение путем клика на него, пароль не требуется
    - Если у вас уже есть доступ к приложению, оно запуститься
    - Если нет, вы можете инициировать тестирование
  - Вы можете создать свой собственный портал в Duo или Azure, для этого кликните на настройки пользователя и выберите Export Applications



© 2020 Cisco and/or its affiliates. All rights reserved.

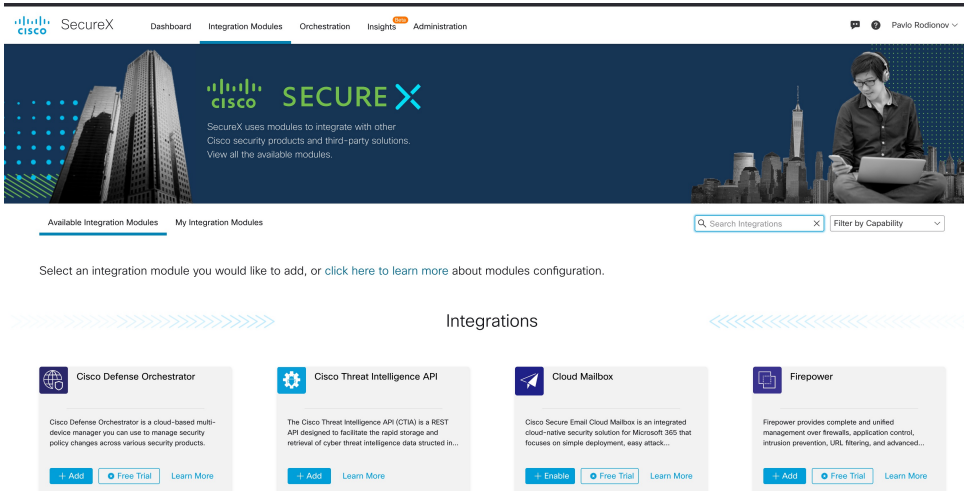
cisco Secure

Процесс регистрации на портале SecureX

- Демо регистрации портала
  - https://youtu.be/E_Sq4VdFKcg?t=2971

Добавляем источники данных в SecureX

- Добавление из меню Integrations
- Присутствуют наборы стандартных модулей интеграции
- Интеграция со всеми облачными приложениями через API
- Интеграция с локальными решениями (ESA, WSA, SMA, Firepower etc.) через Security Services Exchange (SSE)

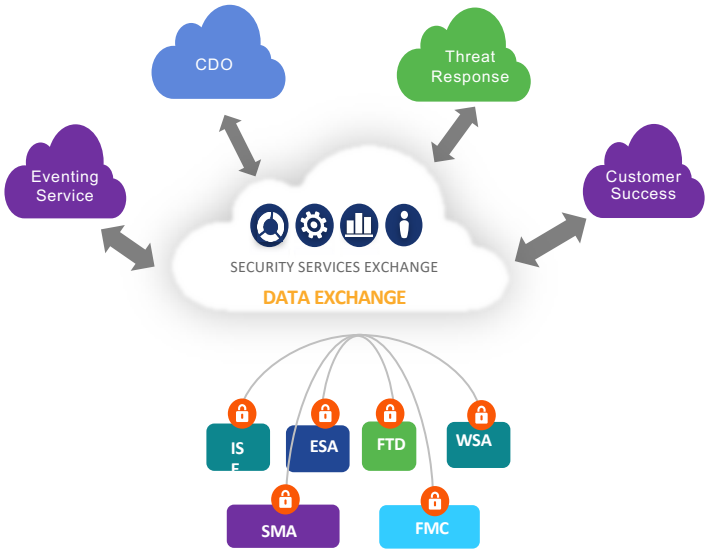


© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

А зачем нужен SSE?

- Security Services Exchange (SSE) требуется, чтобы получать/обрабатывать события их локальной инфраструктуры
- Эти события затем обрабатываются SecureX, Threat Response, Security Analytics and Logging и т.д.
- Вам не нужен SSE, если вы интегрируетесь только с облачными решениями Cisco (AMP, SWC, Umbrella etc



© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

Регистрация источников SecureX

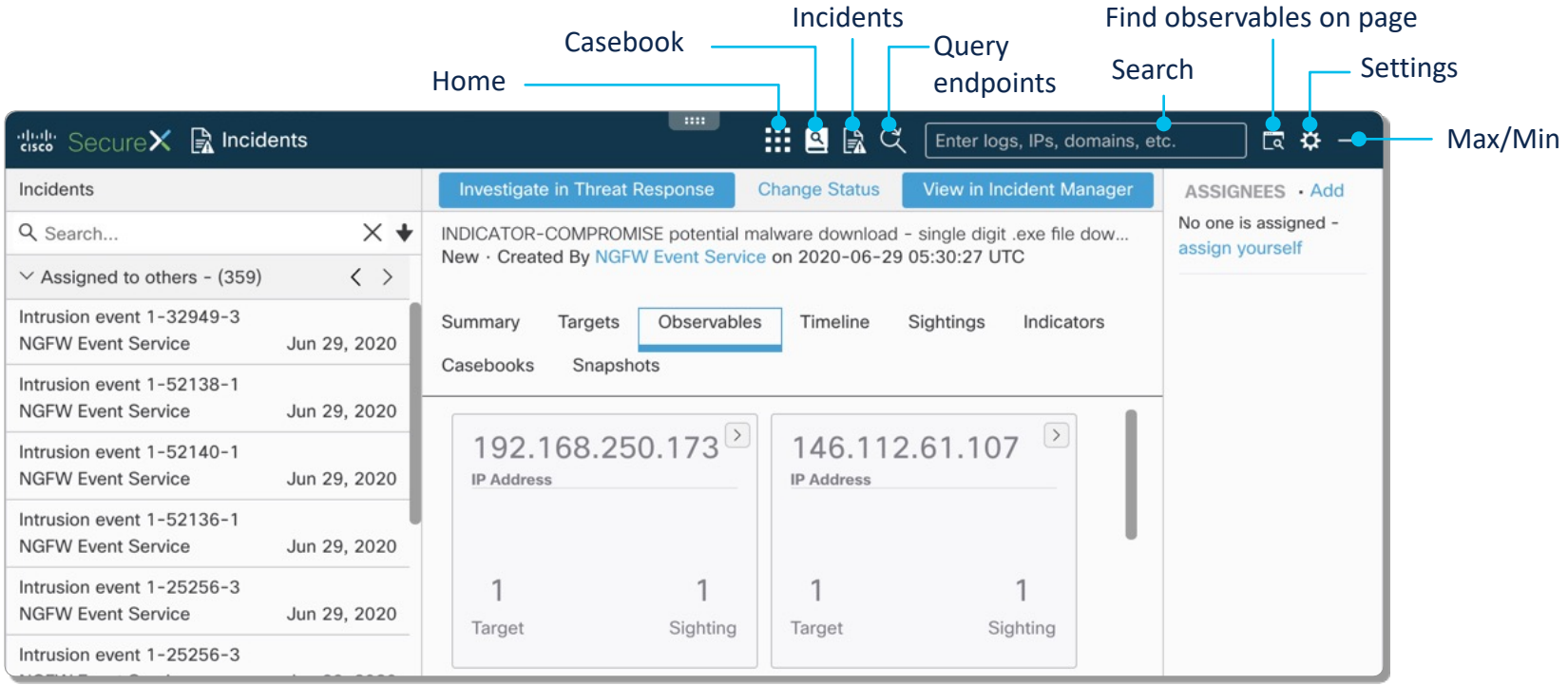
- Регистрация Cisco Secure Endpoint (AMP), Umbrella и NGFW
  - https://youtu.be/E_Sq4VdFKcg?t=3360

SecureX ribbon

- SecureX ribbon позволяет вам переносить наболее релевантных контекст безопасности и threat intelligence по всем вашим продуктам
- Транспортная структура для функциональности: возьмите с собой возможности SecureX и интегрированных продуктов, когда вы переходите на консоль любого другого продукта
- Связывает продукты вместе и обеспечивает унифицированный опыт и широкие возможности реагирования для всех продуктов.
- Возможность перекрестного запуска: переход к любым другим продуктам с ленты
- Ленточные приложения: при посредничестве SecureX, предоставляются SecureX и другими продуктами.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Никогда не теряйте контекст с SecureX ribbon

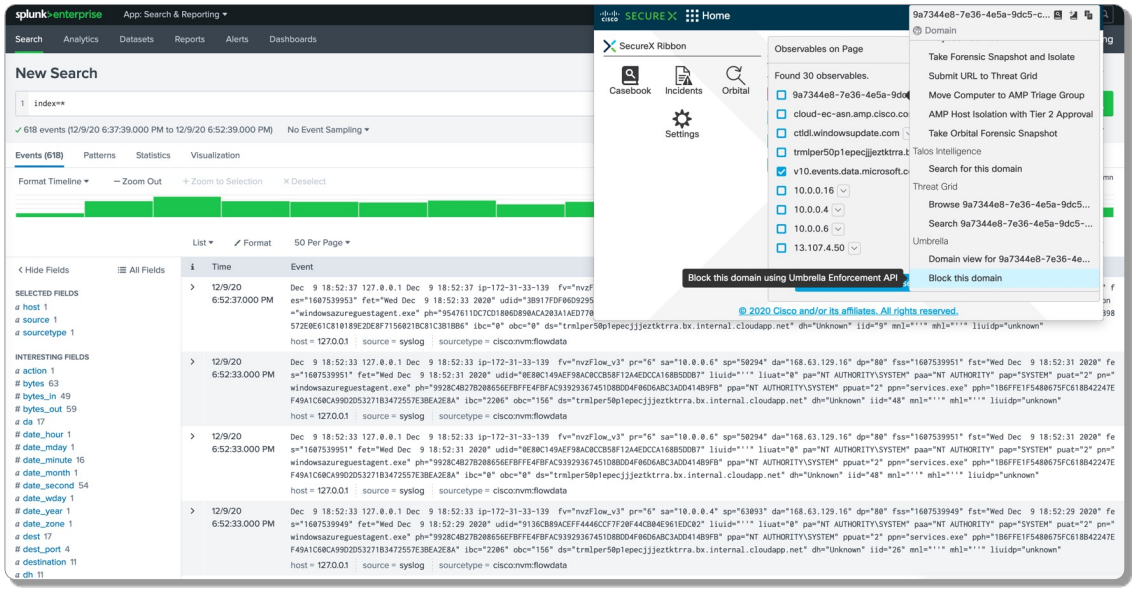


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Берите SecureX вместе с собой

The SecureX ribbon extension

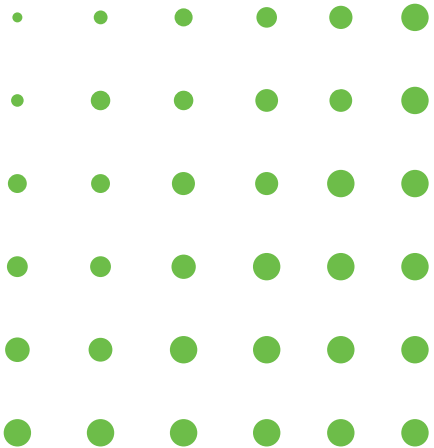
- **Простое подключение к сторонни инструментам.** Извлекайте наблюдаемые индикаторы в ленту из сторонних инструментов и переходите к расследованию.
- **Начните расследование из браузера за минуты.** Это реальное время для начала использования. Быстро запрашивайте узлы и выполняйте ответные действия, не выходя из браузера.
- **Лучше взаимодействуйте с командой безопасности.** Создавайте или добавляйте обращения прямо из браузера и делитесь ими с командой.



Начало работы с SecureX Ribbon

- Активация SecureX Ribbon Add-on
  - https://youtu.be/E_Sq4VdFKcg?t=3896

SecureX
Device Insights

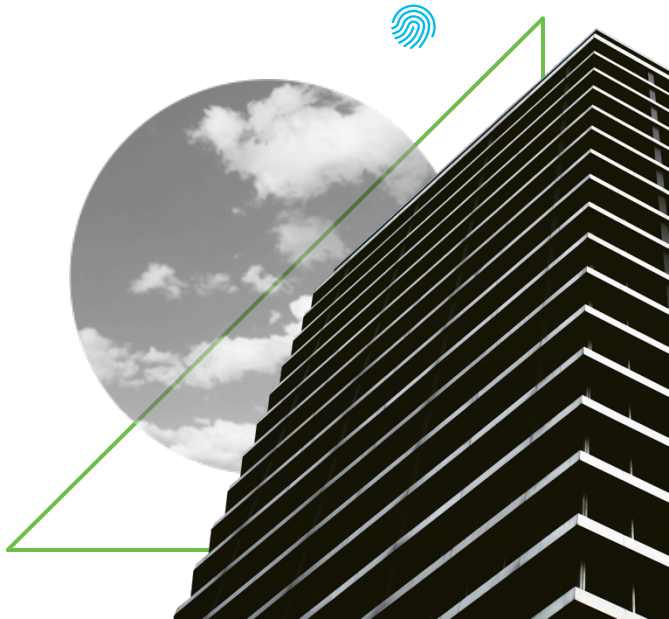


SecureX device insights предлагает бесшовный, безагентсвкий унифицированный вид всех устройств в вашей организации для того, чтобы снизить поверхность атаки

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

С Device Insights вы сможете ответить на эти важнейшие вопросы.

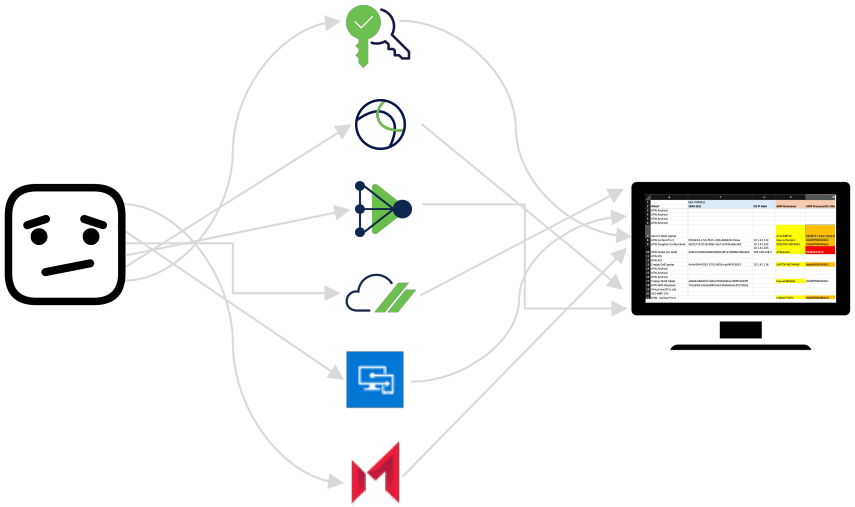
- Какие **типы устройств** подключены к вашей среде?
- Какие **пользователи** получают доступ к этим устройствам?
- Где они **находятся?**
- Какие **уязвимости** ассоциированы с этими устройствами?
- Какие **агенты безопасности** установлены?
- **У вас последнее ПО безопасности**?



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Customers are doing this themselves

- Создаются собственные инструменты, чтобы это сделать:
  - Используются скрипты
  - Пишутся внутренние приложения
  - Excel таблицы
- Подтягиваются детали о всех узлах из всех источников
- Множество источников, множество подключений, весьма запутанно.



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

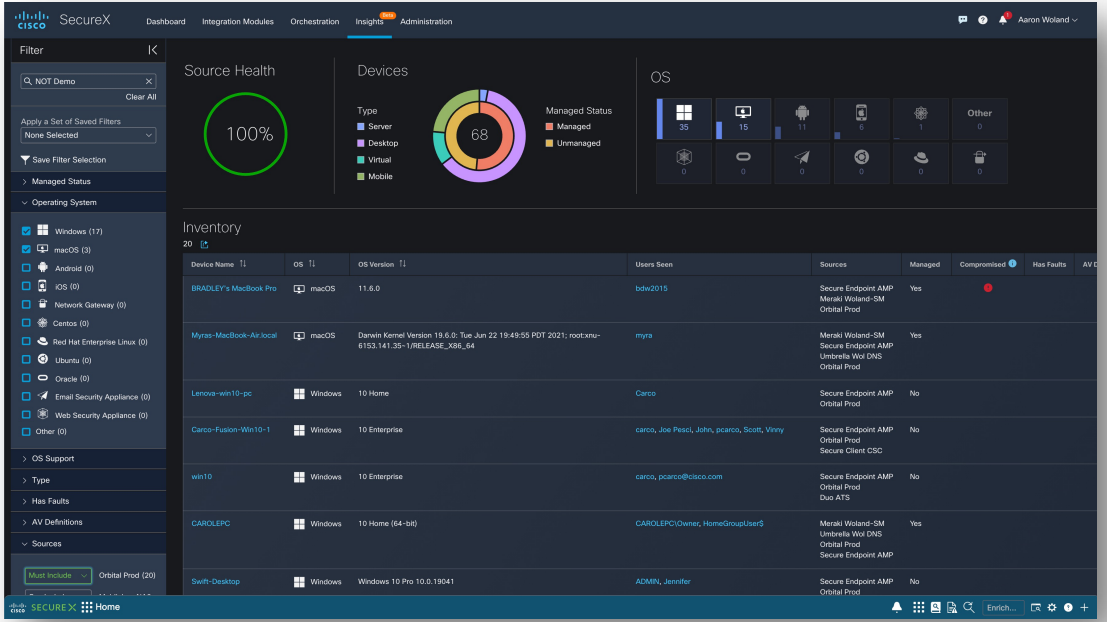
- Источники
  - *DM’s, EDRs, Duo, Orbital, и т.д…*
- Учетная таблица
  - *Фильтруемая, сортируемая, настраиваемая и экспортируемая*
- *Детали устройства*
  - *Консолидированные детали от всех источников*
  - *Возможность переключения в консоль*

SecureX Device Insights

Device Insights создан для консолидации, обнаружения, нормализации и работы с вашим реестром устройств

Device Insights унифицирует несколько Device Managers, EDR, AV и другие продукты безопасности узлов

SxDI затем отображает детали, которые предоставляют эти решения в одном унифицированном виде в рамках SecureX.

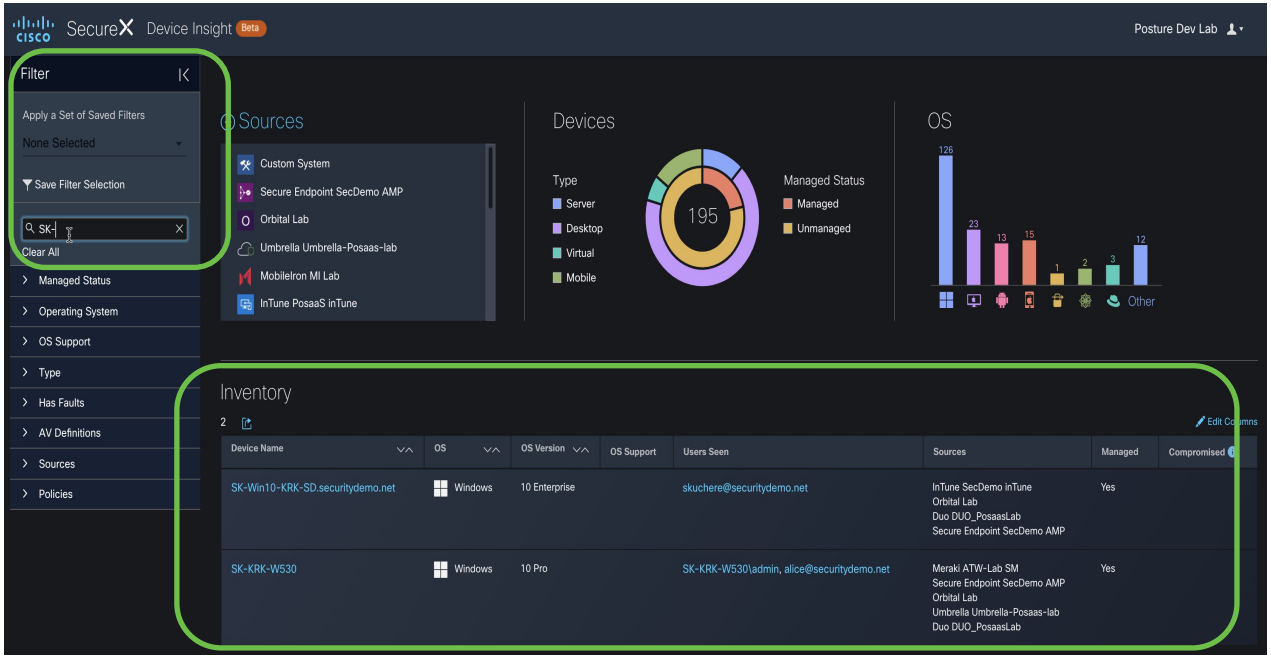


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Device Insights: Расследование/сбор данных

Гибкий поиск

- Возможность сохранения параметров поиска
- Поиск среди:
  - Версия ОС
  - IP адрес
  - Имя пользователя
  - Имя хоста



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Обогащенный консолидированный вид узлов

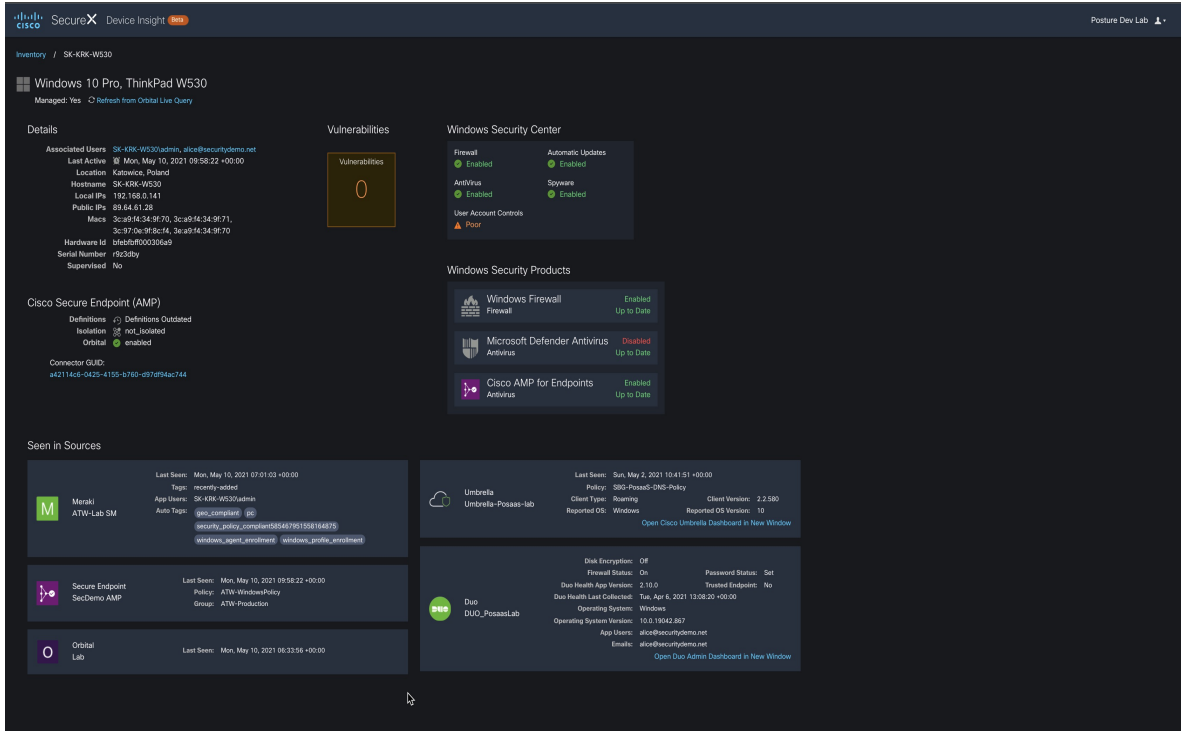
Данные собираются из множества источников

MDM's

- Meraki и сторонние

Продукты безопасности

- Cisco Secure Endpoint (AMP)
- Orbital
- Umbrella
- DUO



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ценная информация об узле

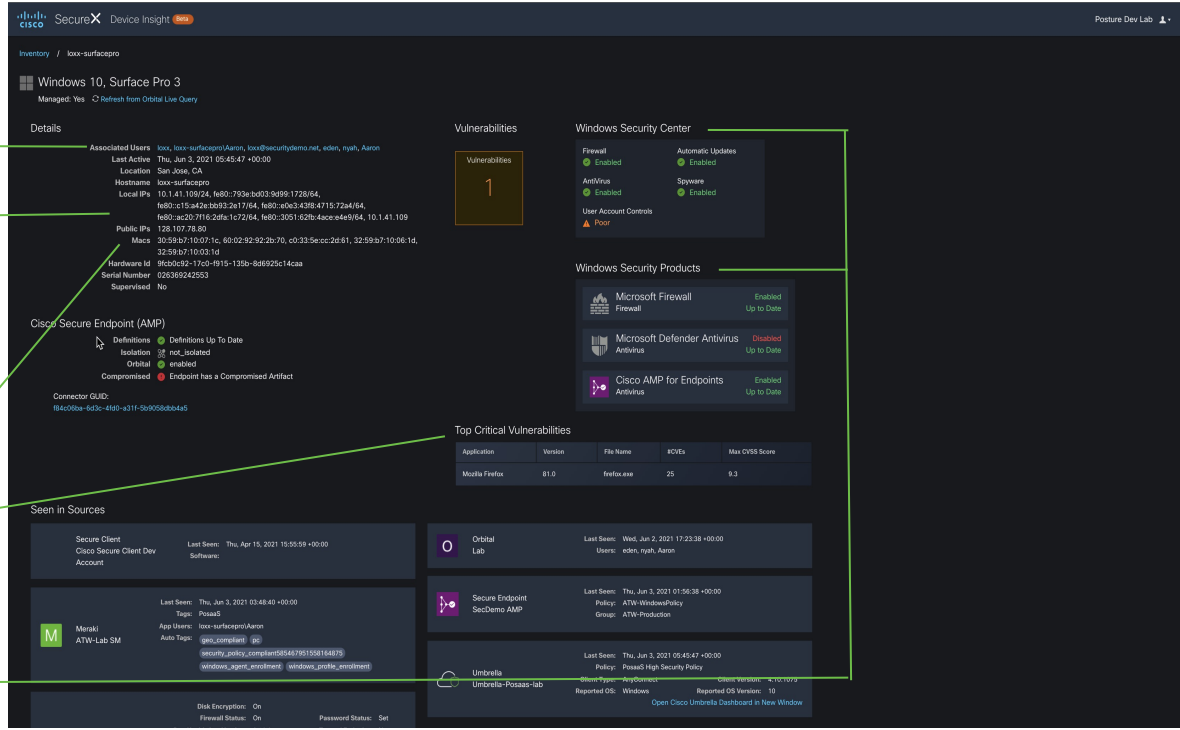
Пользователи на узле

- Где мы видели этот узел
  - IP адреса
    - локальные и глобальные

Mac адреса

Уязвимости

Windows Security Center Status из Orbital



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Погружение в Windows Security Center

- Firewall включен.
- Автообновления включены
- Антивирус включен
- AntiSpyWare включено
- UAC выключено

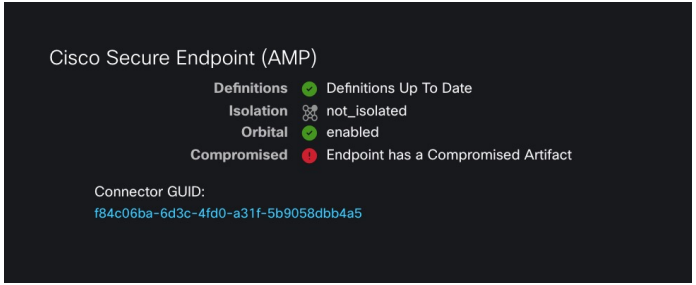
Зарегистрированные продукты безопасности Windows

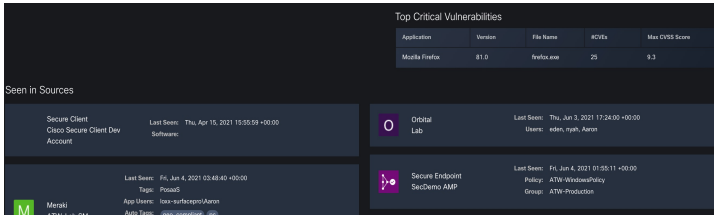
- Используется MS Firewall и обновлен
- Microsoft Defender AV выключен но обновлен
- Cisco Secure Endpoints (AMP) включен и обновлен
- Cisco Secure Endpoint (AMP) сообщает про критическую уязвимость в Firefox

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Endpoint (AMP)

- Статус
  - Cisco Secure Endpoint установлен
  - Endpoint не изолирован
  - Orbital включен
  - Endpoint скомпрометированан
- Переключайтесь с консоль AMP путем клика на Connector GUID.
- Детали компрометации
- Секции источников:
  - Cisco Secure Endpoint (AMP)
    - Политика, группа и последняя дата обнаружения





© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Поддерживаемые на момент запуска источники

- Поддержка источников от Cisco и сторонних
  - Больше будет после официального релиза
  - Типы источников:
    - Device Managers
    - EDR
    - Zero Trust Access Control

Duo Access
Duo Beyond

Secure Endpoint

Umbrella (DNS)
Win / macOS only

Meraki SM

Secure Client

Orbital

3rd Party MDMs

Microsoft InTune

Mobile Iron

Airwatch

Custom CSVs

Jamf Pro

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX Device Insights

- SecureX Device Insights демо
  - https://youtu.be/E_Sq4VdFKcg?t=4280

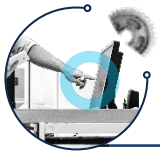
Демистификация SecureX: Оркестратор

Agenda

- Почему оркестрация?
- Построение процессов
  - SXO основы
  - Адаптеры
  - REST APIs
  - Условия и логика циклов
  - Переиспользование Workflows и Atomics
- Заключение

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Автоматизация и оркестрация



Автоматизация

Возможность выполнения индивидуальных повторяющихся задач.

Зачем нужна автоматизация?

“Мне нужно быстрее развертывать новые сервисы; Клиент меня торопит.”

“У меня есть повторяющиеся задачи, которые мы выполняем вручную - мне нужно высвободить людей для выполнения другой работы с более высоким приоритетом.”

“Мне нужно сделать более с меньшими затратами” (уменьшение бюджета)

Оркестрация

Упорядочивание и координация автоматизированных и неавтоматизированных задач, в конце концов создающее консолидированный процесс или workflow.

Зачем нужна оркестрация?

“Я хочу объединить свои системы, чтобы достичь непрерывного рабочего процесса, отражающего жизненный цикл нашего сервиса - запрос, реализация, поддержка, модификация, вывод из эксплуатации..”

Поставщики предлагают множество инструментов управления - одни предоставляют услуги, другие - мониторинг - почему их нельзя объединить в одно решение?

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Представляем оркестрацию SecureX

Простая автоматизация процессов с интерфейсом drag-drop no/low-code

Расследование

Сократите время исследования и отклика с помощью автоматизации рабочих процессов и сценариев

Автоматизация

Устранение повторяющихся задач и сокращение среднего времени восстановления, чтобы повысить производительность и сосредоточиться на критически важных проектах.

Интеграция

Уникальный подход для быстрой интеграции с другими системами и решениями для расширения вашего набора инструментов

Масштабирование

Автоматизация, которая бесконечно масштабируется и никогда не берет выходной

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Оркестрация SecureX

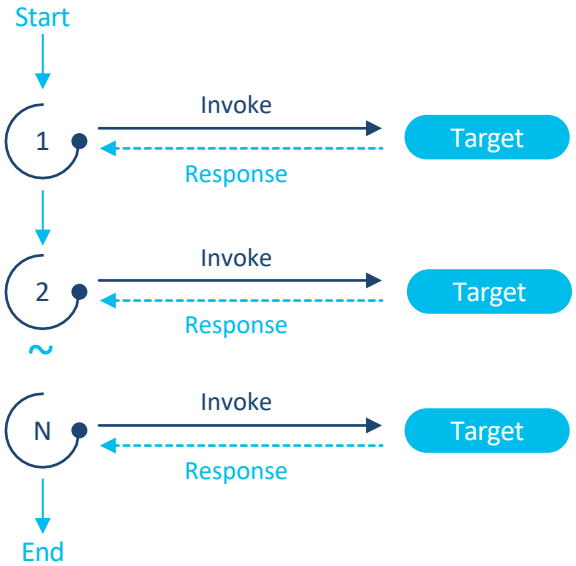
Облачная , микросервисная архитектура с дизайном “API-first”

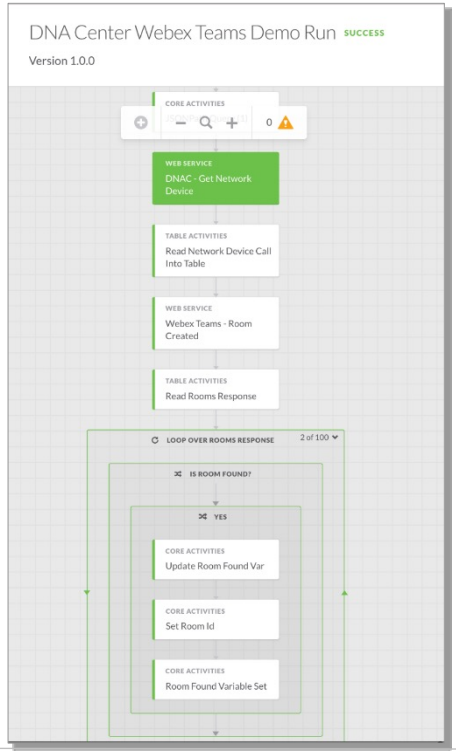
- Высокопроизводительная, масштабируемая и безопасная
- Переиспользуемая и встраиваемая

Интуитивный drag-drop UI с визуальными процессами

Объединяет гибкие адаптеры для создания новых интеграций

- Автоматизация заданий в соответствии с расписанием или внешними событиями





© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

”Каждая битва выигрывается

ПЕРЕД ТЕМ

как происходит”

Sun Tzu

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX оркестрация: что мы будем делать если...?

Взломан лаптоп директора!

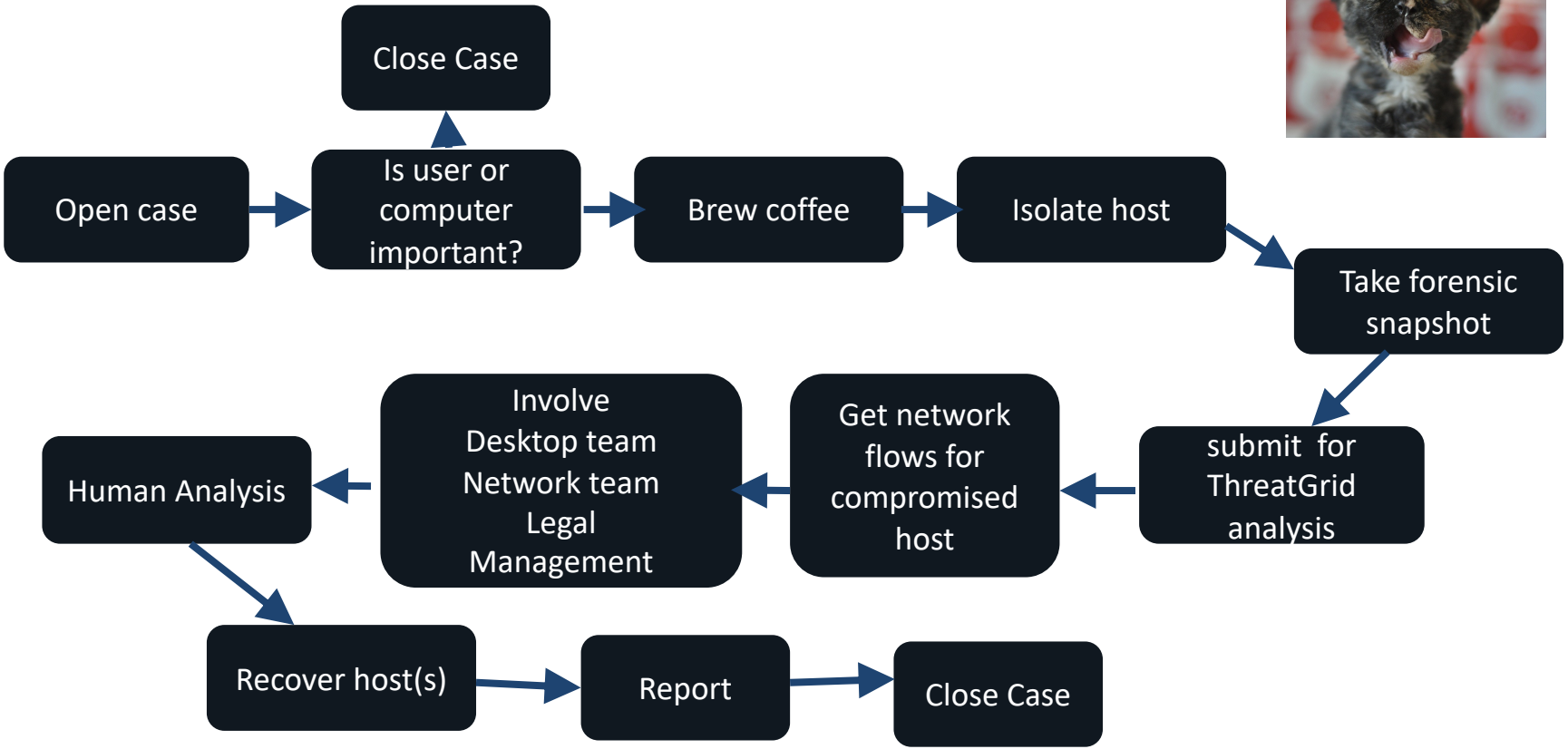
Превышена пропускная способность VPN

Вирус в нашей производственной цепочке!

Скомпрометированы Web сервера

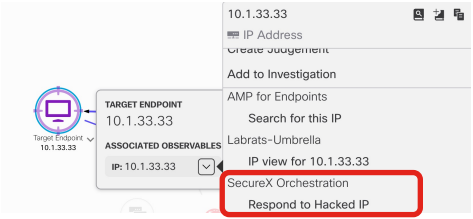
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Зачем нам нужны процессы



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Процесс: ”Реагирование на взломанный IP”



Webex Teams

servicenow

Involve Team!

Get user info from IP

AD

ISE

Isolate host

AMP

Forensic snapshot

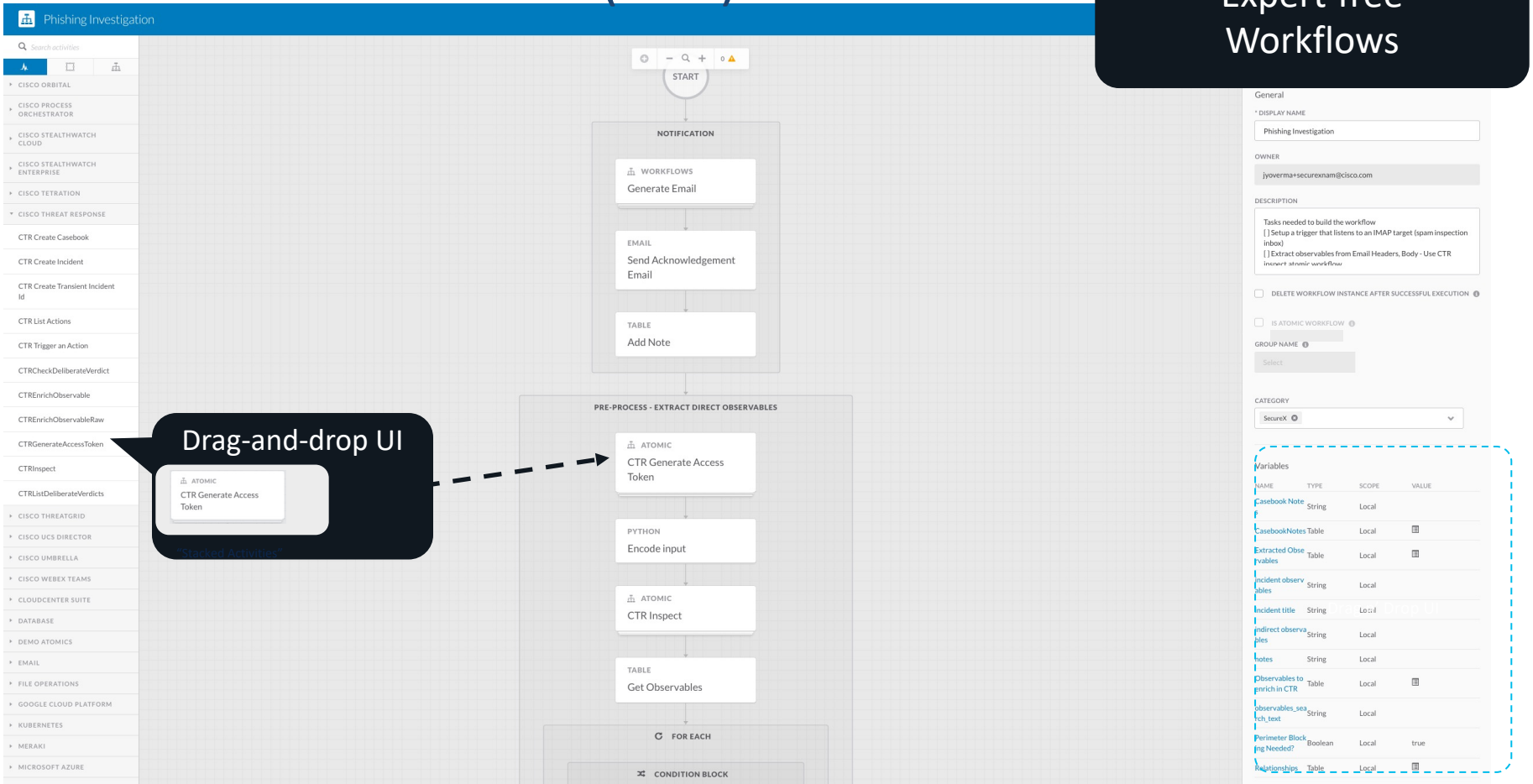
cisco SECURE X Casebook

Create Report/Casebook

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

SecureX Orchestrator (SXO)

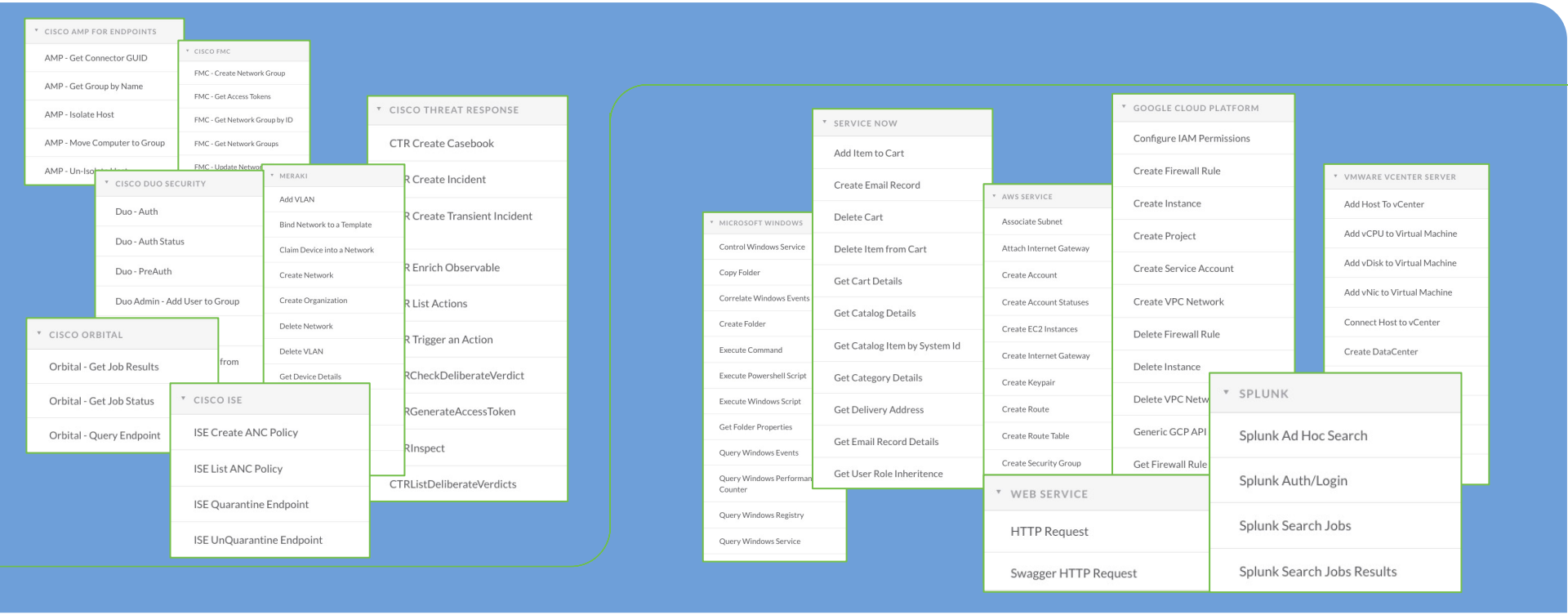
"Expert-free" Workflows



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Интеграция с Cisco и сторонними инструментами

"Expert-free" interoperability



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Предварительные условия

Он бессерверный!

- Не обязательно знать:
  - OS экспертиза: Linux/Windows
  - Массу библиотек
  - языки программирования: C, Java, C#, ...
- Очень полезно знать:
  - Логика : ”if-then”, ”while true”
  - Базовые понятия REST APIs и JSON

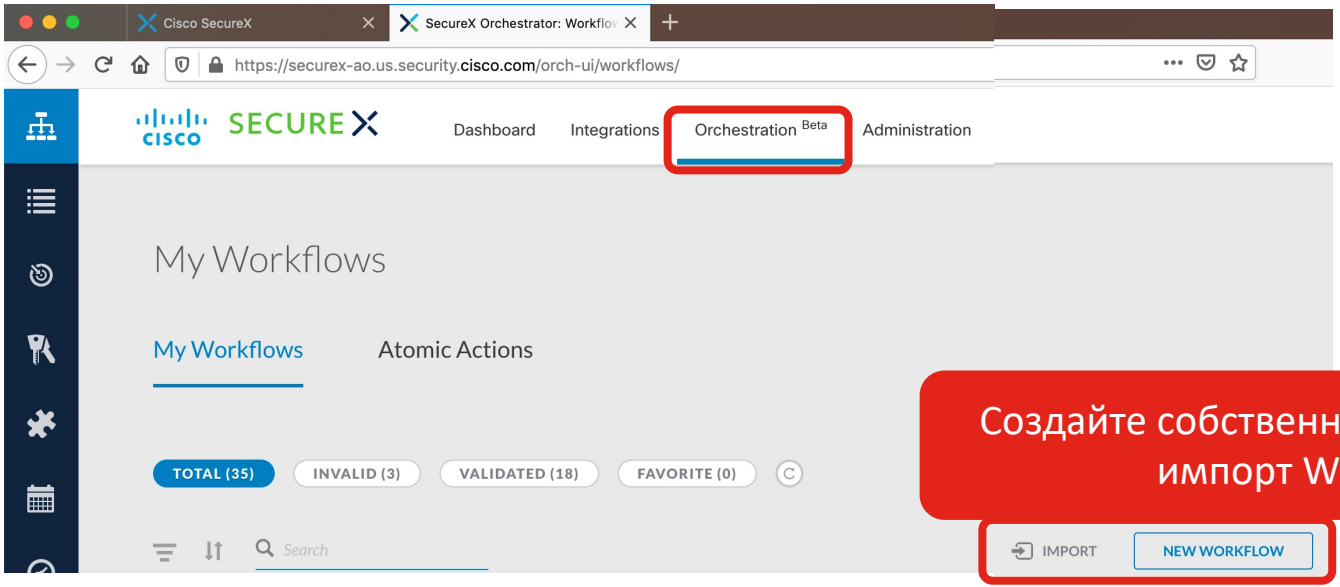
“Expert-free” Workflows

Cross Department

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Доступ к SXO

- Прямой доступ из меню
- Создание или импорт Workflow...

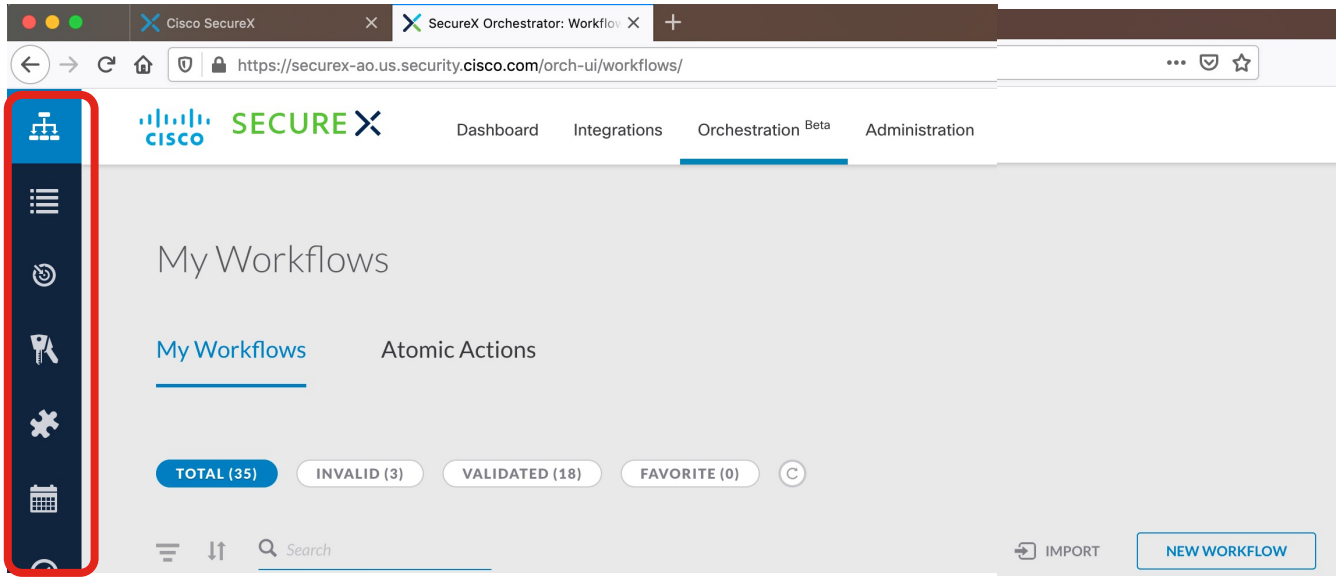


Создайте собственный Workflow или импорт Workflow

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Окрестрация SXO

- Слева: Компоненты, которые используются всеми workflows

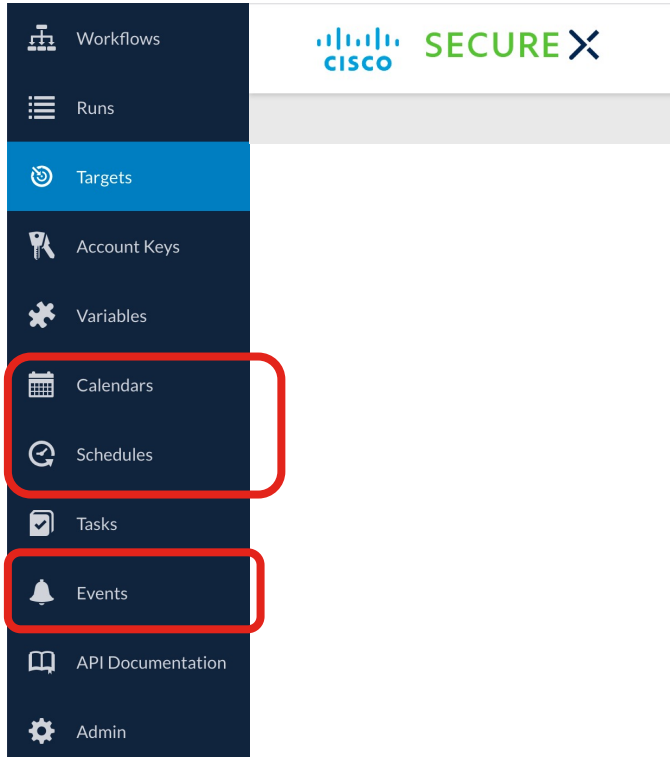


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Компоненты, релевантные для Workflows (1)

Когда запускать?

- Календарь
- Расписания
- События



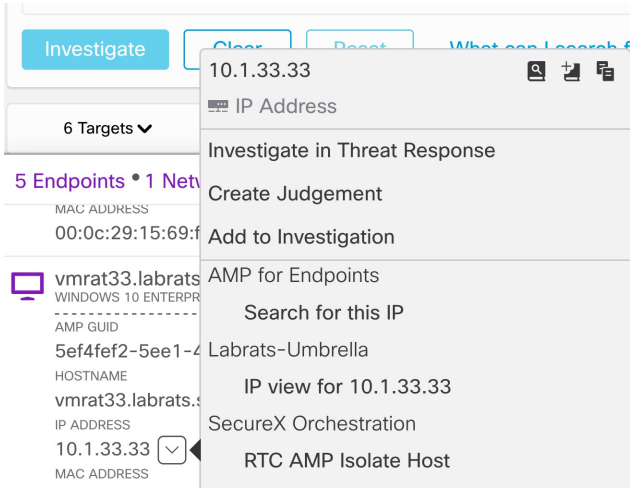
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Когда выполнять Workflow?

Вручную

- Из консоли SXO

- Из Threat Response

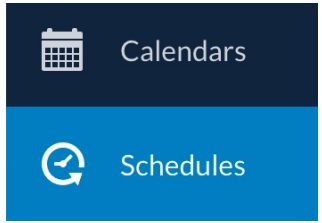


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Когда выполнять Workflow?

Автоматически

- По расписанию
  - Каждый день в 09.00



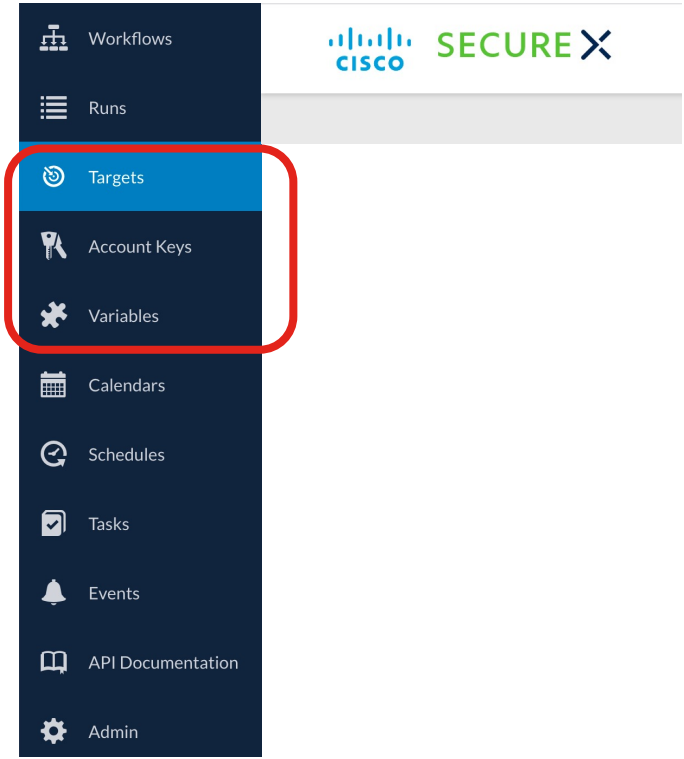
- По событию
  - API вызов

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Компоненты, релевантные для (2)

- Targets
- Account Keys
- Variables

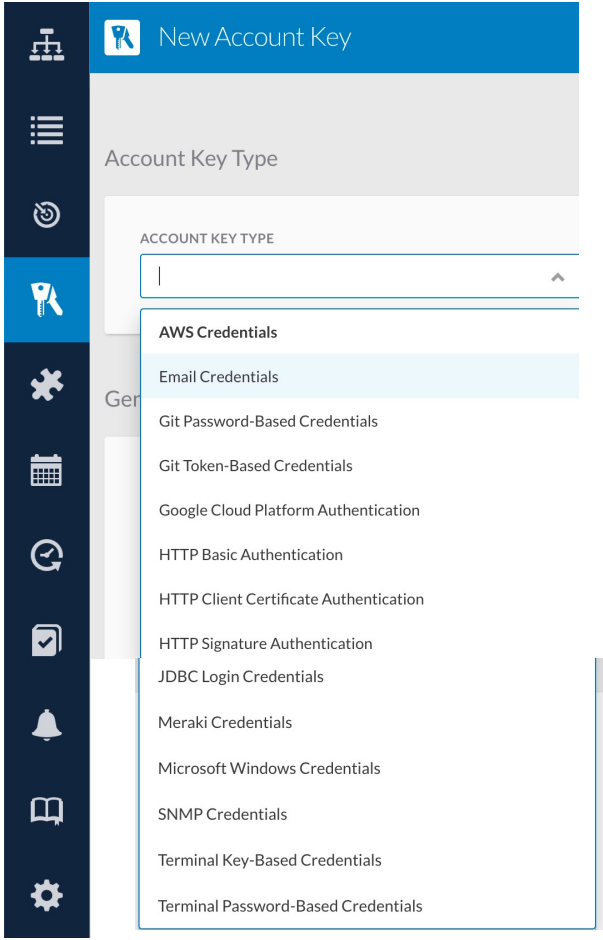
Components used inside your workflow



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Account Keys

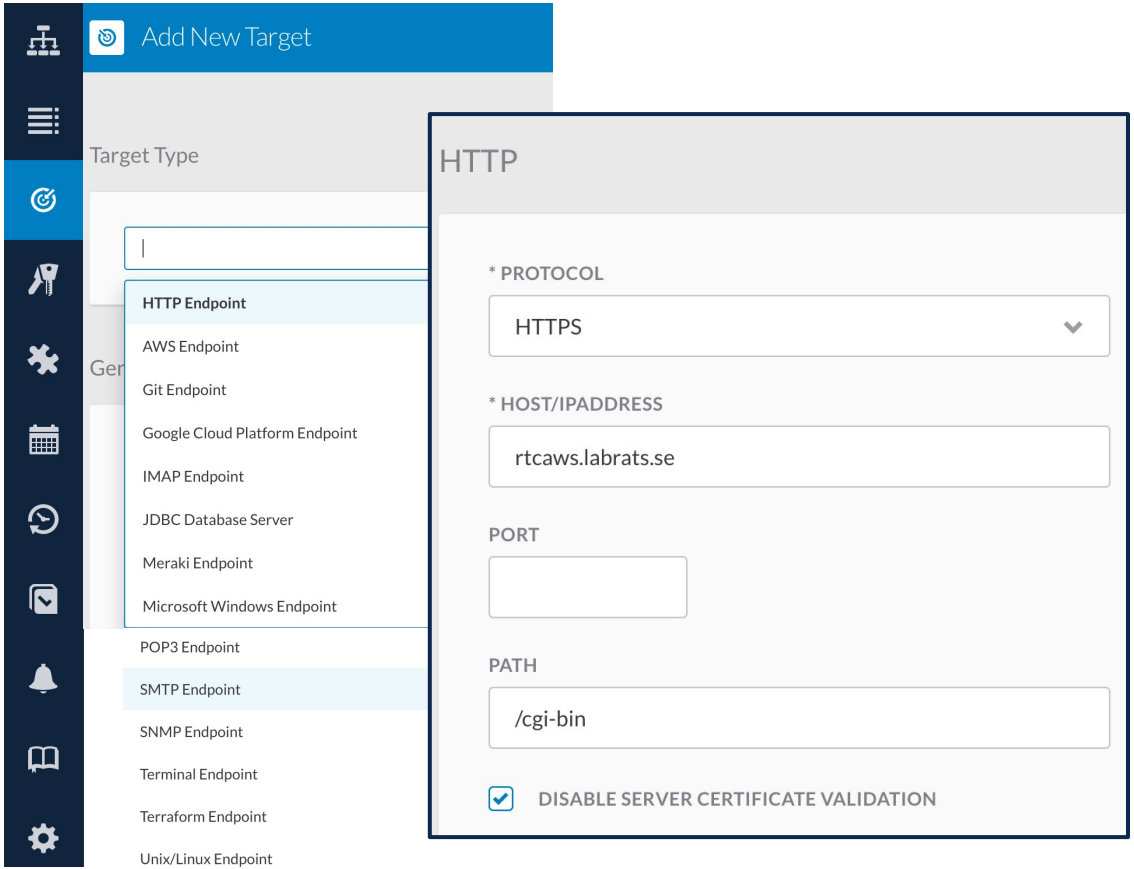
- Сохраняет учетные записи для
  - AWS
  - Email
  - Git
  - Google Cloud
  - HTTP
  - Meraki
  - Microsoft Windows
  - SNMP
  - Terminal
  - .....



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Targets

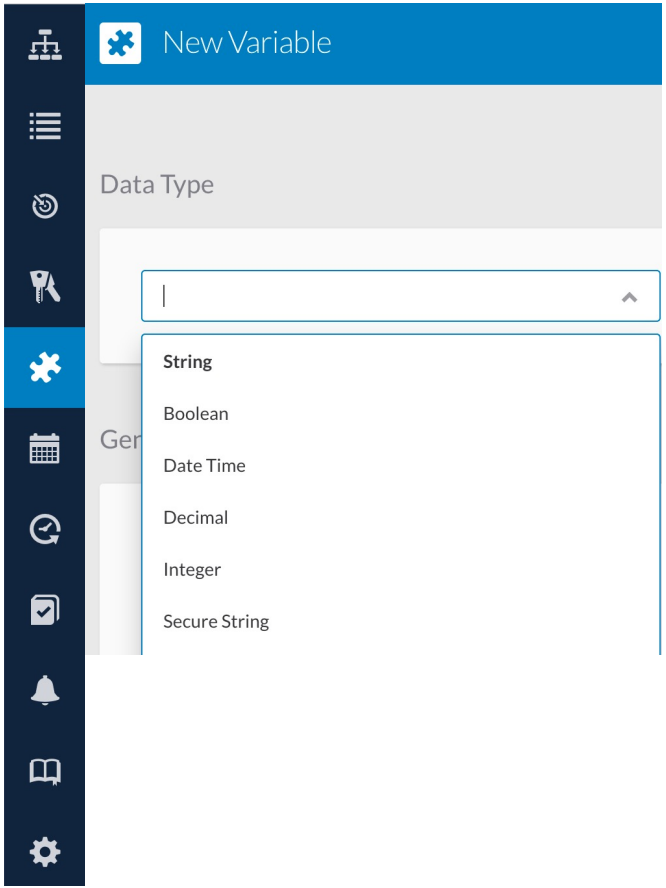
- Цели активности
  - HTTP
  - AWS
  - Google
  - Git
  - Meraki
  - Microsoft
  - POP3/SMTP
  - SNMP
  - Unix
  - ....



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

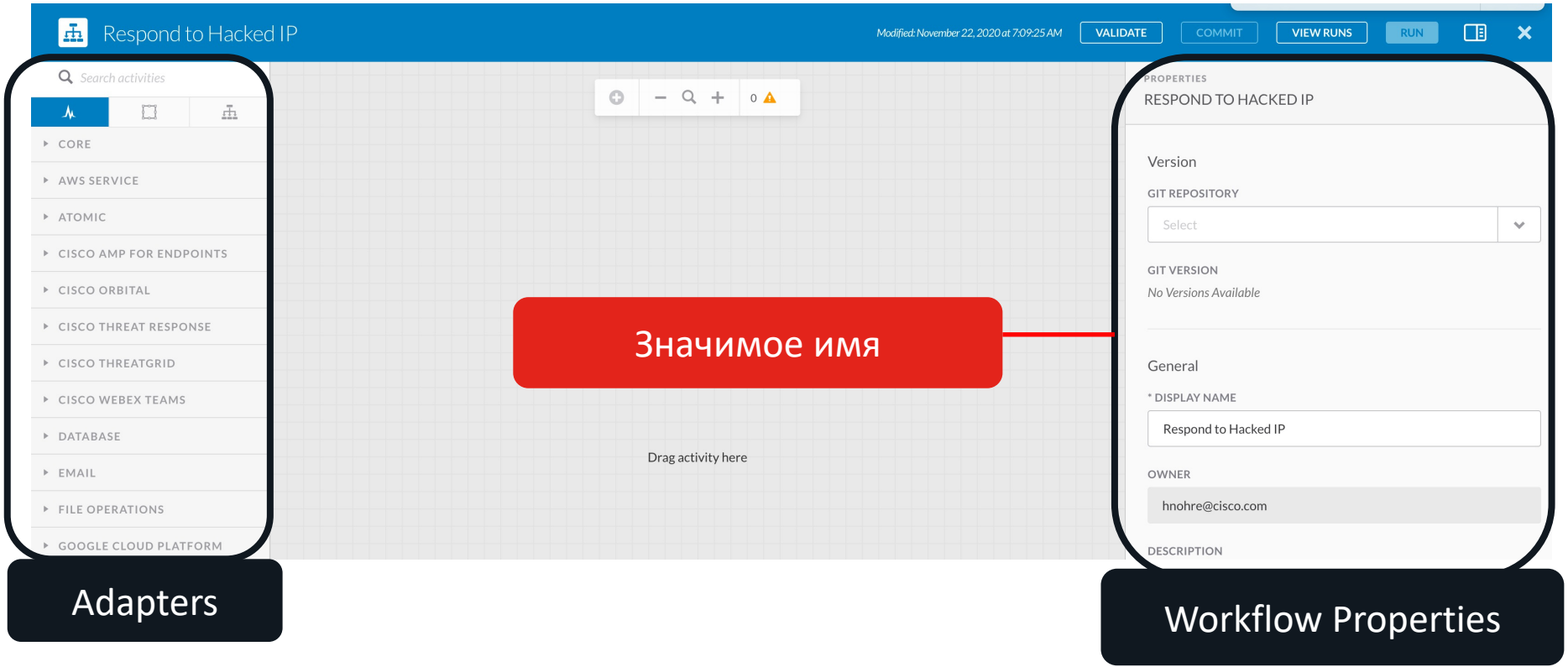
Переменные

- Сохраняет данные определнного типа
  - String: ”10.1.33.33” , ”hacke”
  - SecureString: ”**********”
  - Boolean: true or false
  - Integer: 1, 2, 3 .....
  - Date Time
- Может быть глобальные
  - Читаются или модифицируются любым workflow
- ...или локальные для Workflow
  - только работают с workflow



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Создание Worfklow: Adapters и Properties

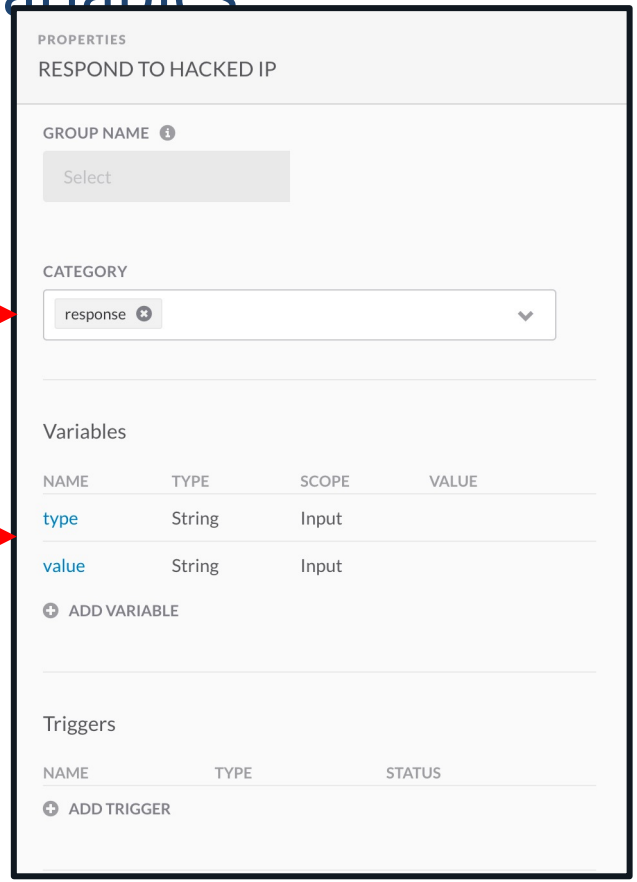


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workflow Properties: Category и Variables

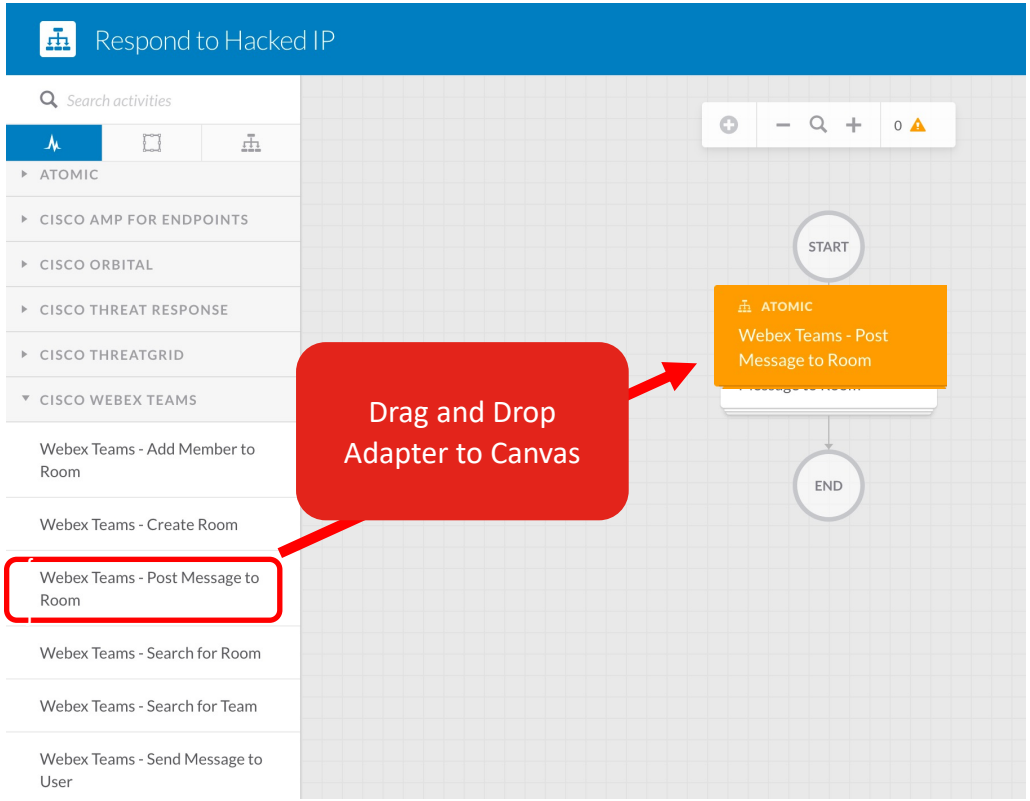
- Category: Добавить ”response” для того, чтобы использовать действие в CTR
- Переменные:
  - Помните как CTIM представляет значение ip

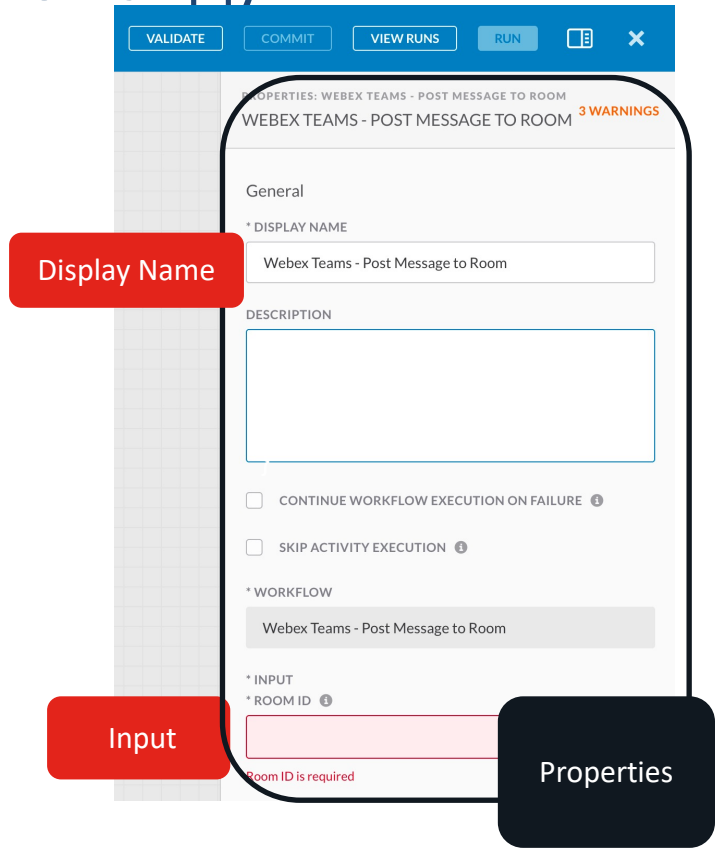
```
{
”type”: “ip”,
“value”:”10.1.33.33”
}
```



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Первая активность: подключите команду!



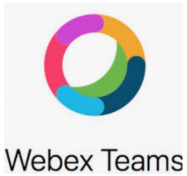


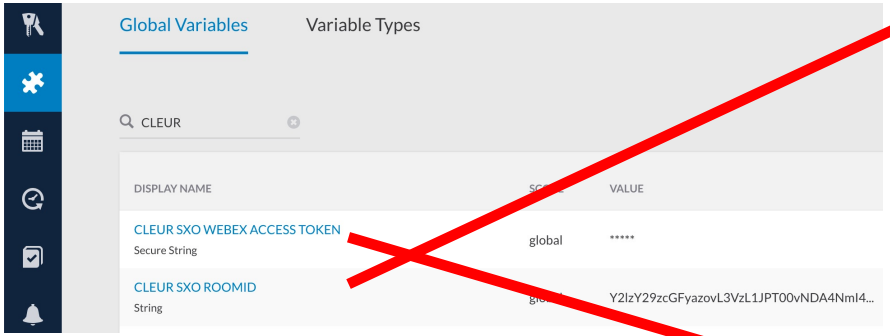
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

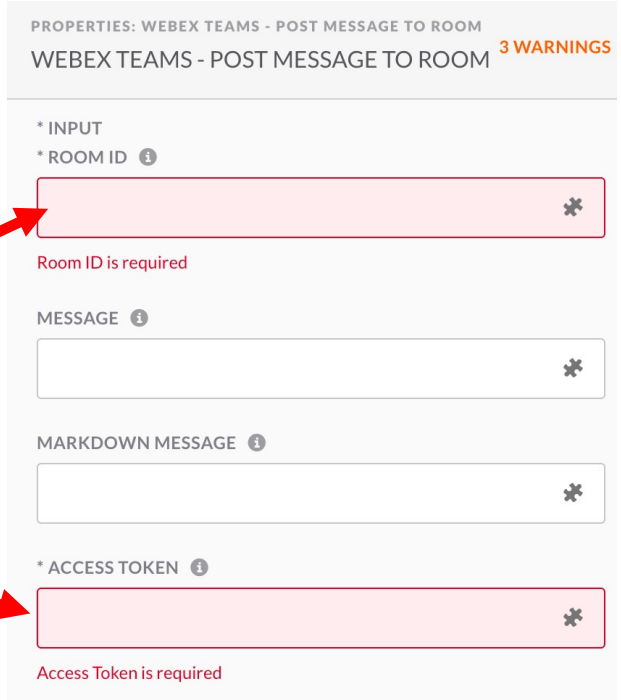
Определите ввод для ”Post Message to Room”

Adapter Type

Store Necessary Adapter Information in SXO Global Variables



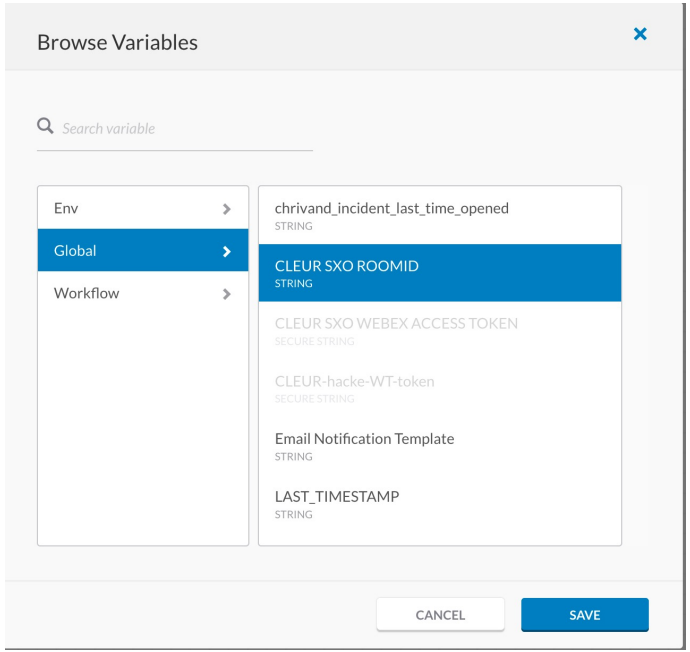


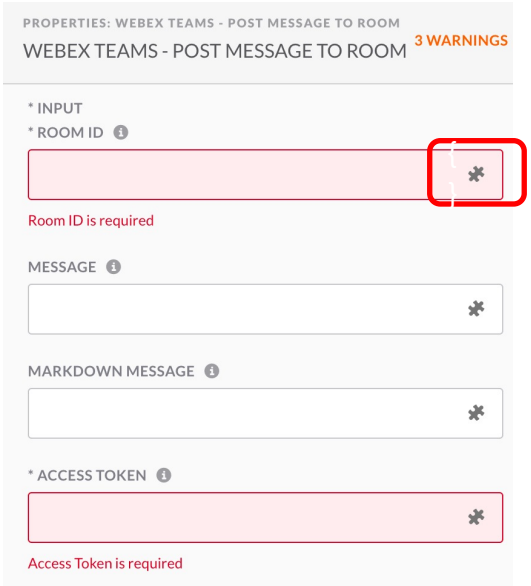


*how to get Room ID and Access token, see https://github.com/.....

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

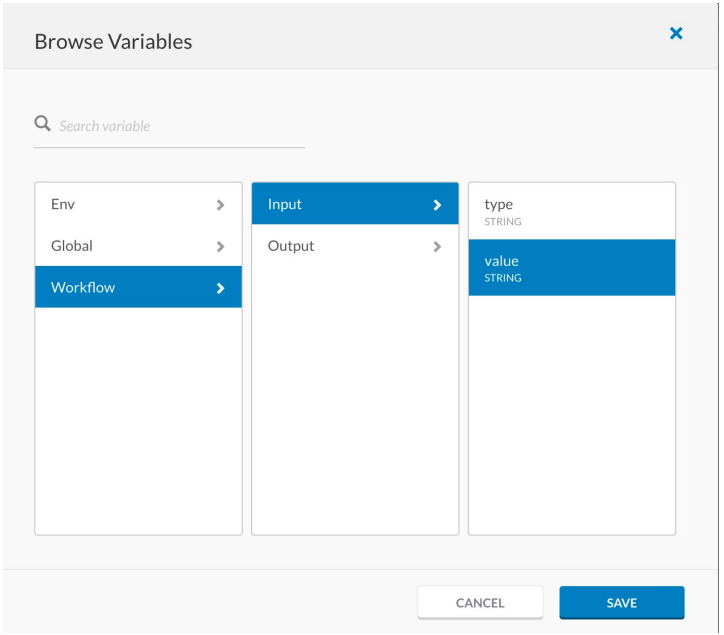
Выбор Variables из Global Variables

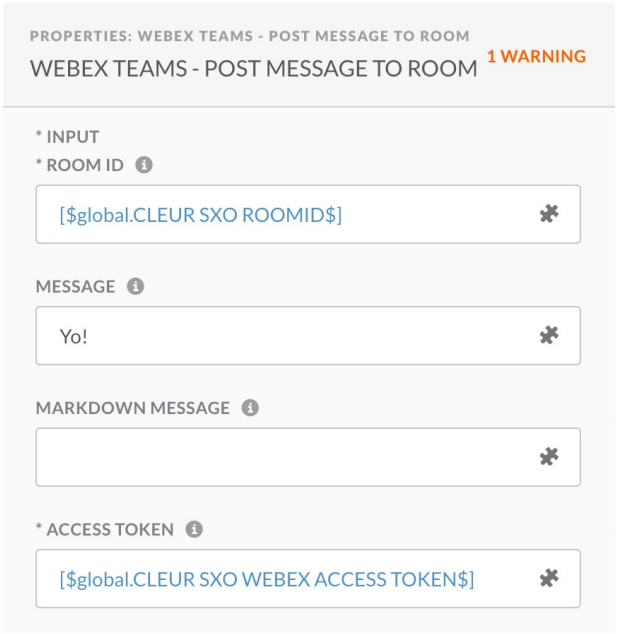




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Выбор Input Variables из Workflow

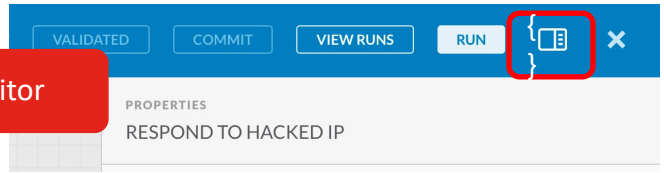




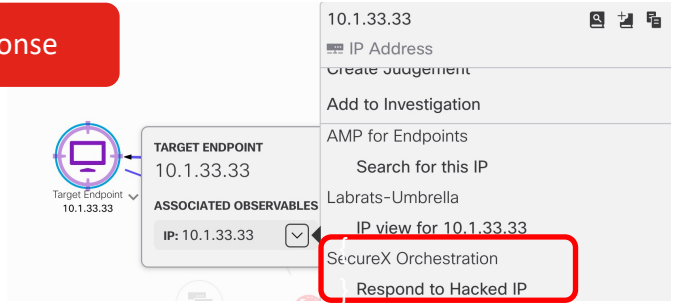
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

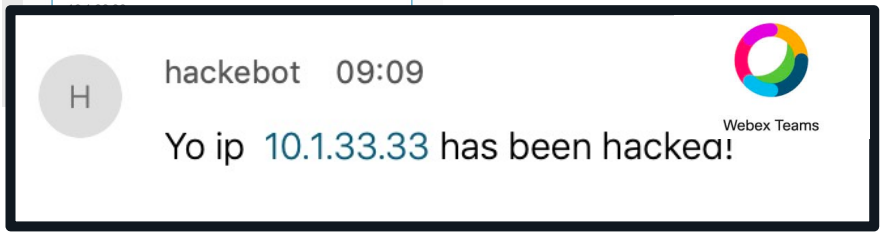
Запуск Workflow

Workflow Editor



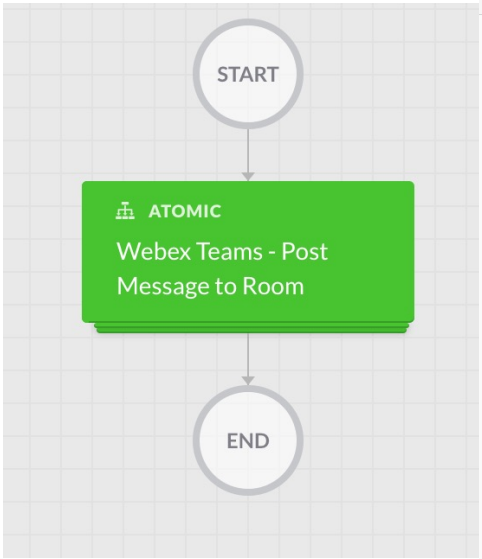
Threat Response

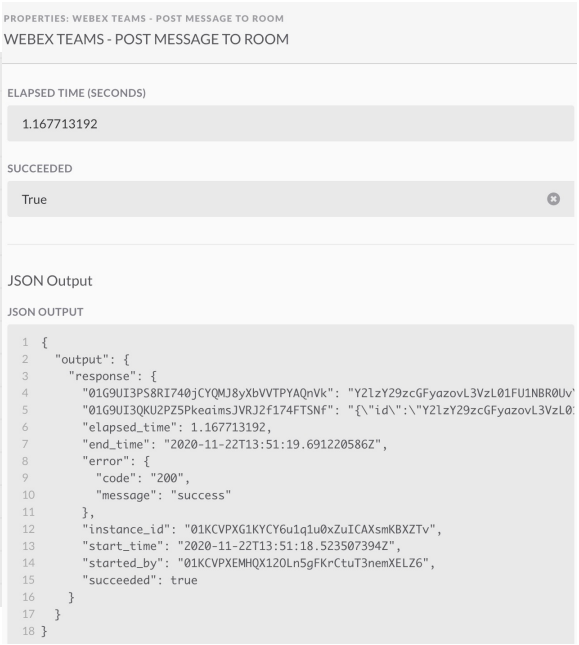




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Просмотр запусков Workflow и Activities

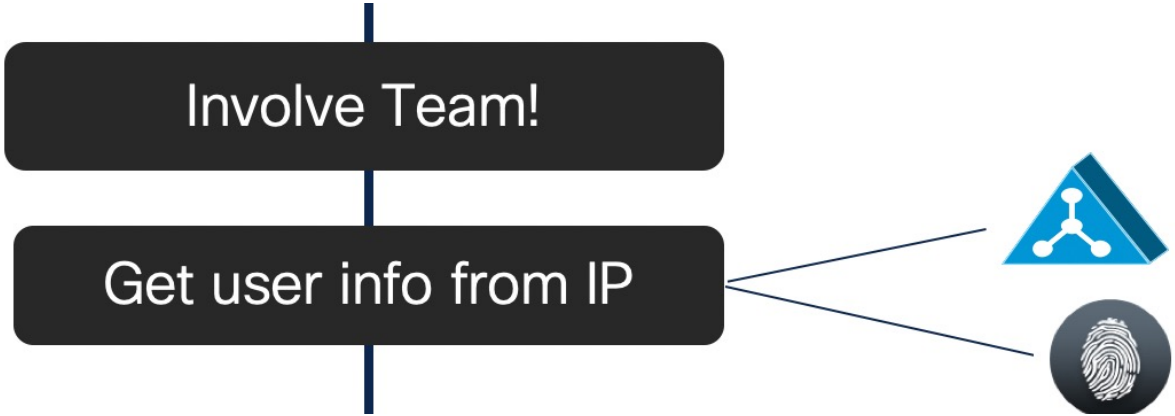




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Взаимодействие с произвольным REST APIs

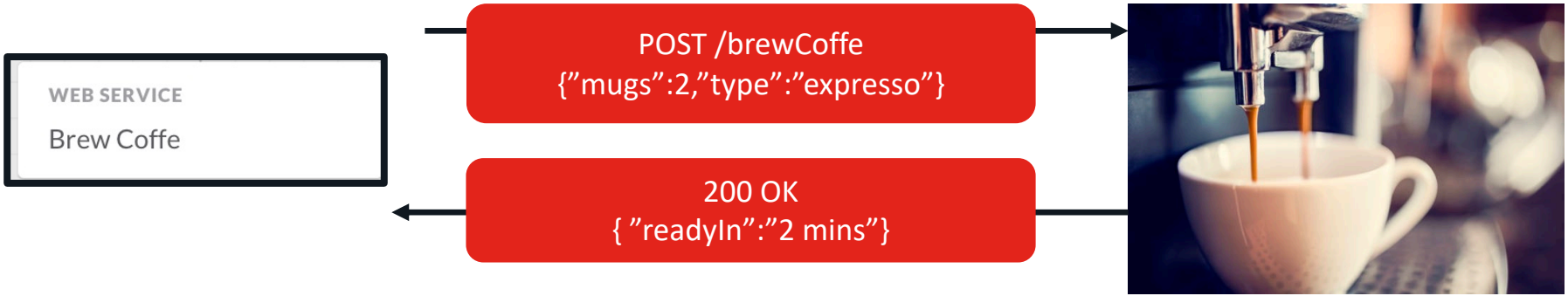
- Возможность взаимодействовать с любым REST APIs
- … например – получить информацию из ISE и/или Active Directory?



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

JSON

- JSON передает произвольную информацию между системами
- Works with any environment and programming language
- Easy to read (and get the hang of)



https://www.w3schools.com/js/js_json_intro.asp

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

JSON

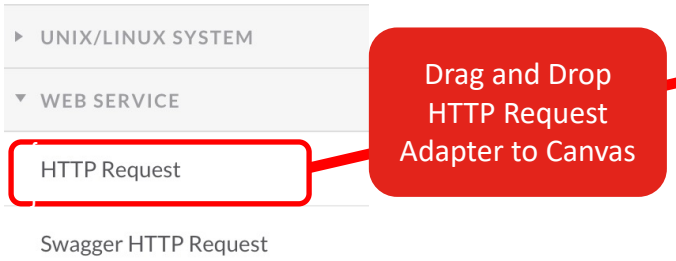
- JSON передает произвольную информацию между различными системами
- Работает в любой среде и с любой системой
- Легко читать...

https://www.w3schools.com/js/js_json_intro.asp

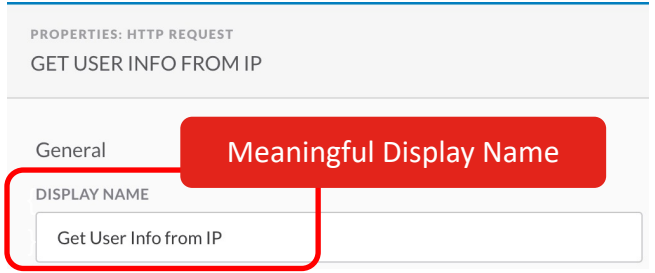

```
{
"rtcResult": "OK",
"ad_info": {
"memberOf": [
"CN=Cats,CN=Users,DC=labrats,DC=se",
"CN=PostureCheck,OU=Lab,DC=labrats,DC=se",
"CN=CiscoSEs,OU=Users,OU=Cisco,DC=labrats,DC=se",
"CN=Network Configuration
Operators,CN=Builtin,DC=labrats,DC=se"
],
"mail": "garfield@labrats.se",
"badPasswordTime": "2020-09-17 07:50:58.268549+00:00",
"lastLogon": "2020-11-24 08:53:32.617270+00:00",
"badPwdCount": "0",
"userPrincipalName": "garfield@labrats.se",
"distinguishedName": "CN=garfield,DC=labrats,DC=se",
"sAMAccountName": "garfield"
},
"ise_info": {
"macAddress": "00:50:56:8B:95:4A",
"endpointOperatingSystem": "Windows 10 Enterprise",
"ctsSecurityGroup": "SGcats",
}
}
```

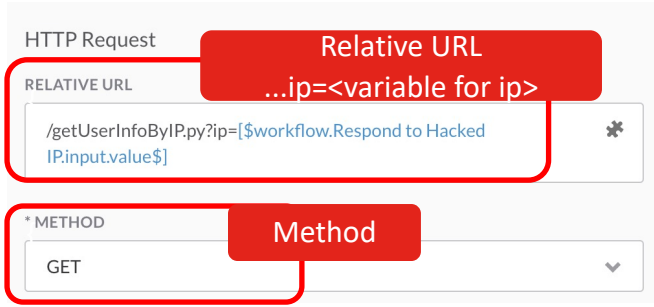

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

REST API: Получить User info из IP



Drag and Drop HTTP Request Adapter to Canvas

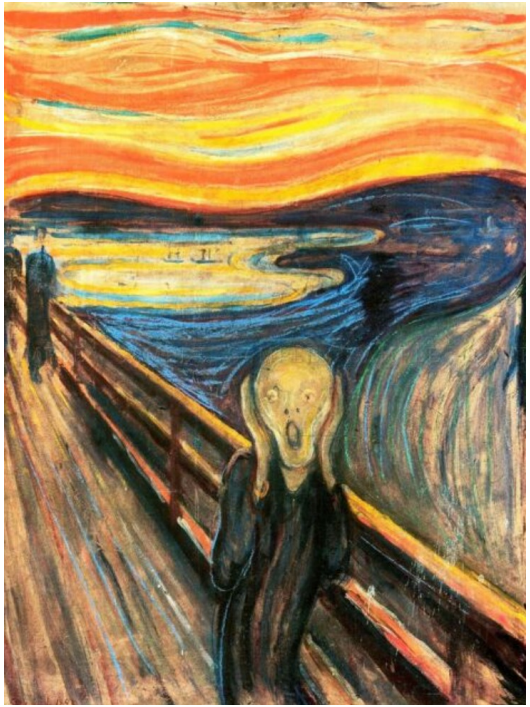




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

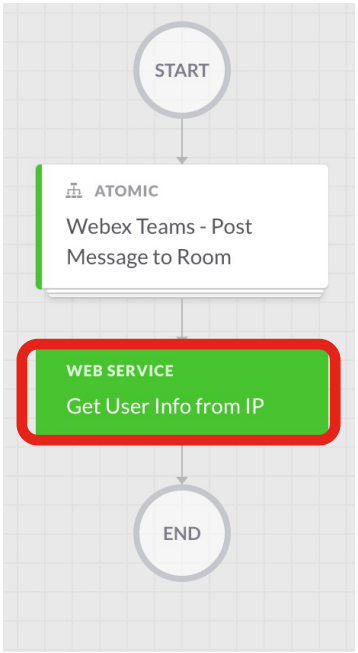
REST API аутентификация

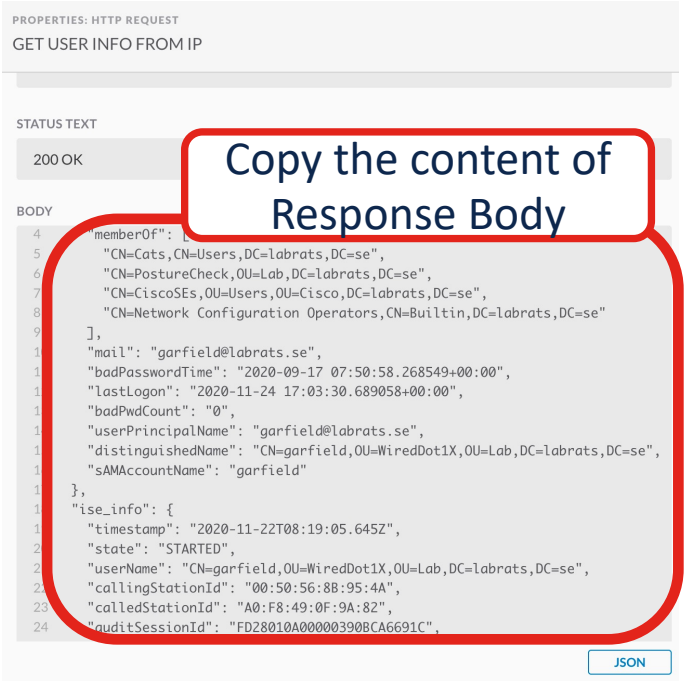
- Разные APIs используют разные методы аутентификации
  - Basic Authentication
  - Cookies
  - Bearer Tokens
  - JWT
  - Client certificates
  - Proprietary...



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Запуск Workflow и получение реакции

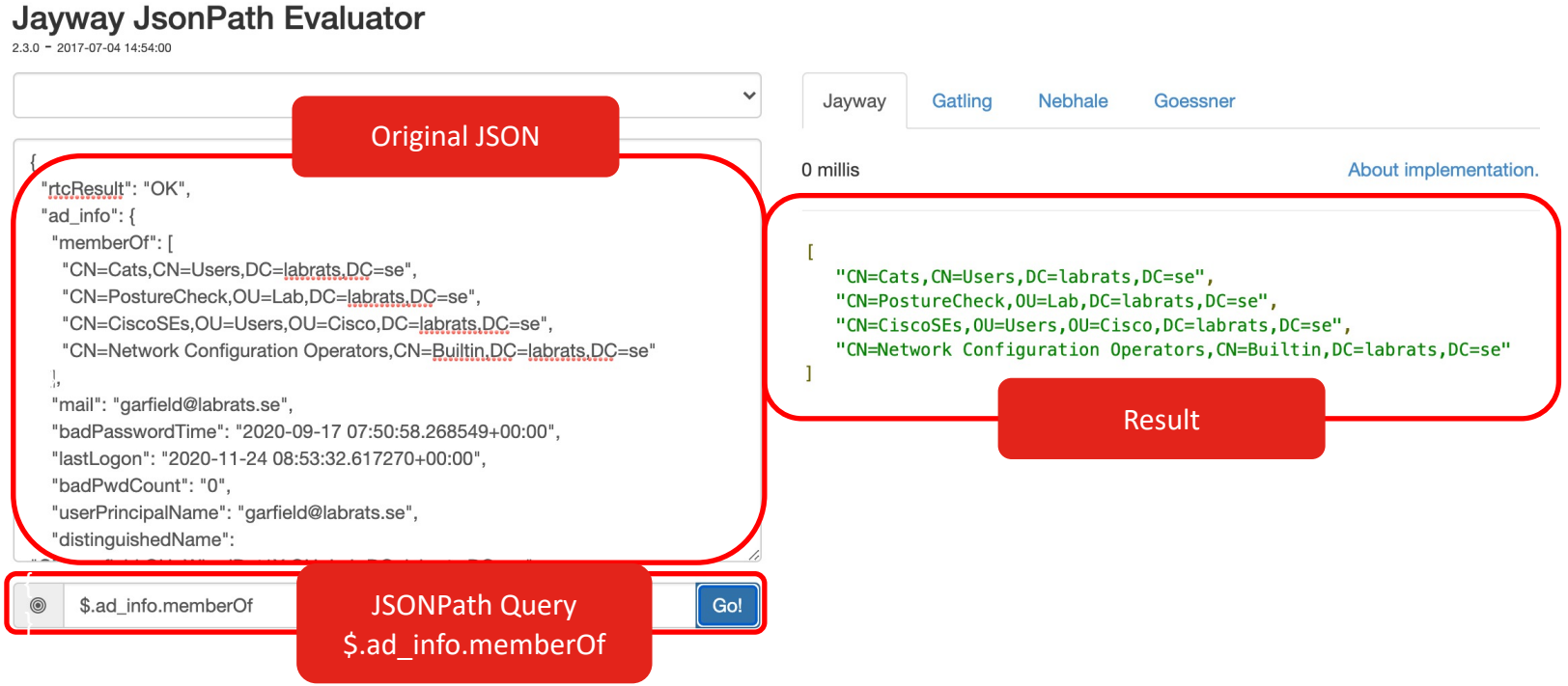




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

JSONPath запросы

- Язык для получения релевантной информации из JSON
- Tip: используйте инструмент, https://jsonpath.herokuapp.com/



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Запуск Workflow для получения результатов

PROPERTIES: JSONPATH QUERY

EXTRACT USER INFO FROM RESPONSE

SUCCEEDED

True

JSONPATH QUERIES

AD GROUPS

["CN=Cats,CN=Users,DC=labrats,DC=se","CN=PostureCheck,OU=Lab,DC=labrats,DC=se","CN=CiscoSEs,OU=Users,OU=Cisco,DC=labrats,DC=se","CN=Network Configuration Operators,CN=Builtin,DC=labrats,DC=se"]

USER PRINCIPAL NAME

garfield@labrats.se

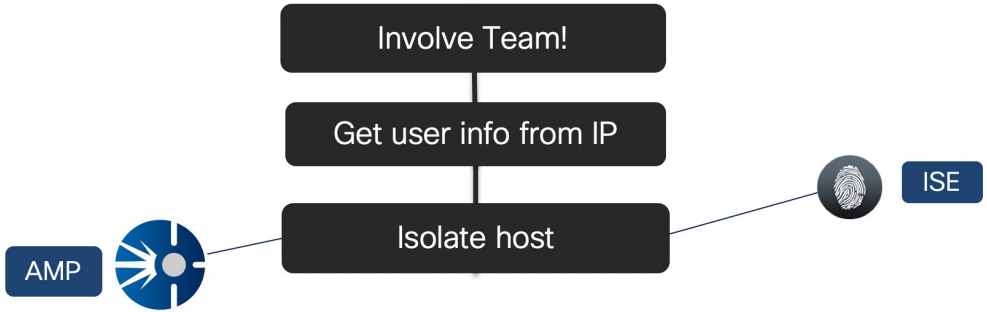
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Изоляция хоста

- Простая изоляция с AMP (если AMP установлен) или ISE (через middleware)

CISCO AMP FOR ENDPOINTS

- AMP - Get Connector GUID
- AMP - Isolate Host
- AMP - Move Computer to Group
- AMP - Un-Isolate Host

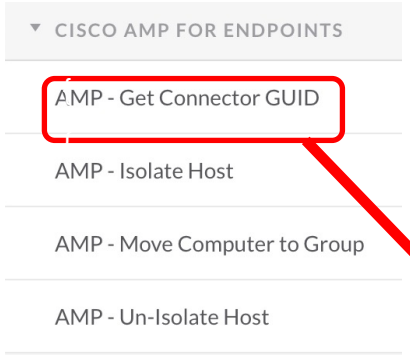


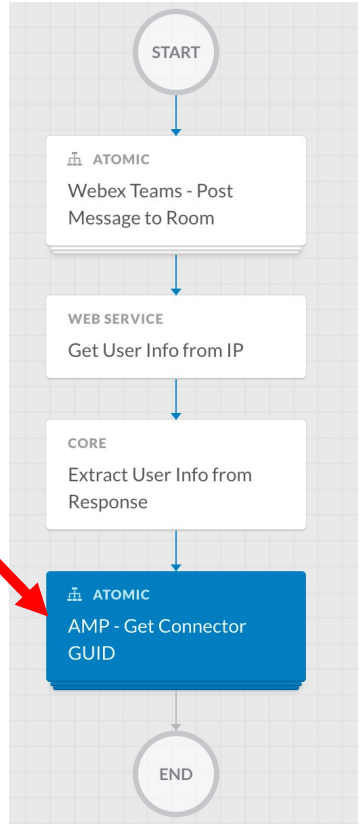
ATOMIC

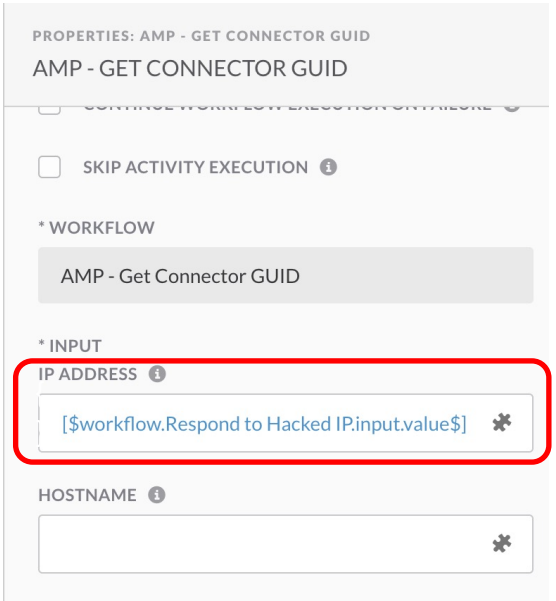
- GetUserId
- RTC Apply ANC
- RTC CTR Create Casebook
- RTC Clear ANC

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Узнать AMP GUID из IP адреса

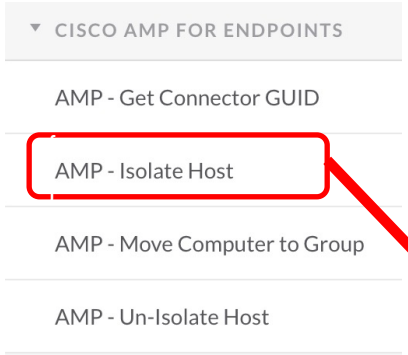


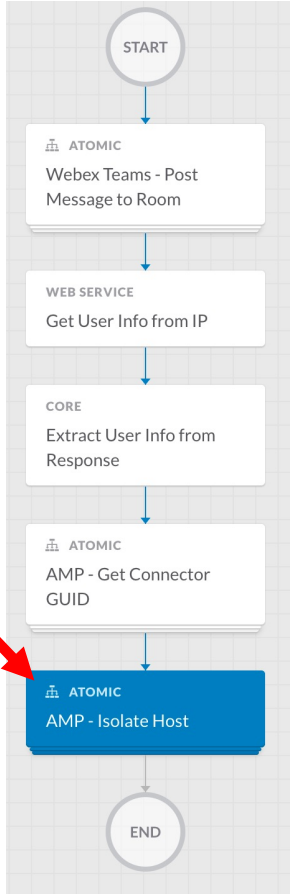


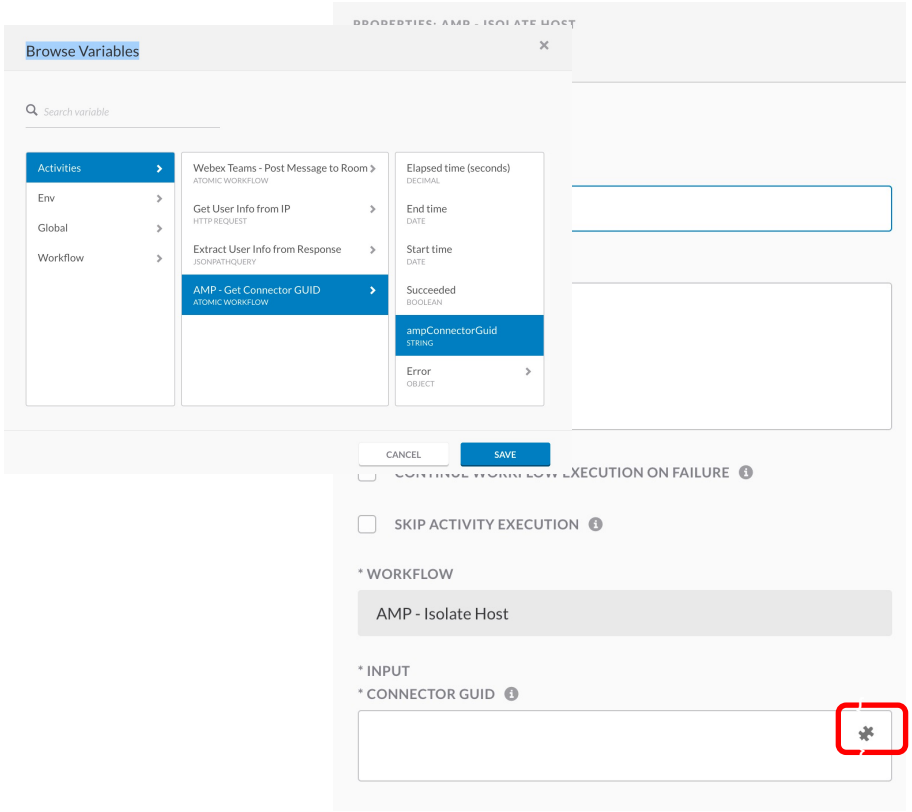


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

AMP Host Isolation



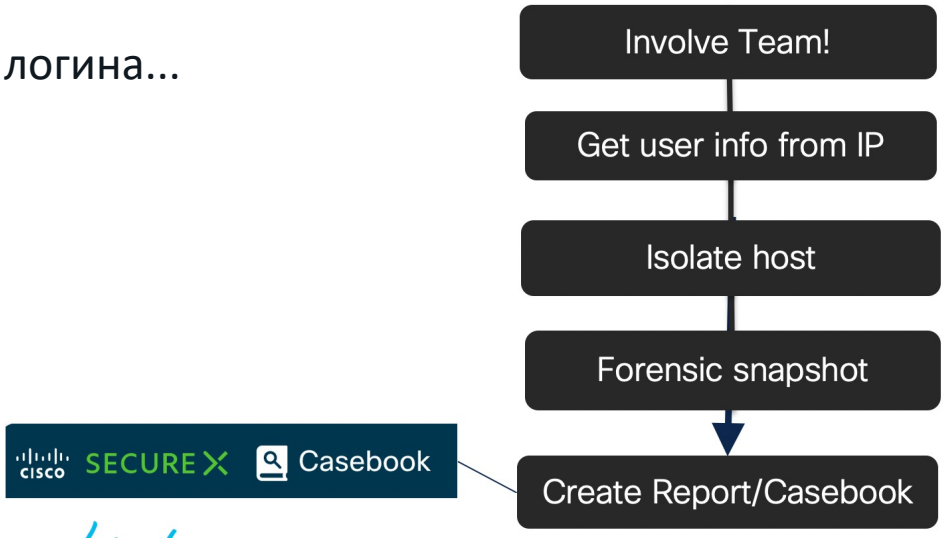




© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Создать отчет (Casebook)

- Отчет об инцидентах может быть обязателен (GDPR и т.д.)
- Что мы включаем в отчет
  - Пользовотеля, AD groups, время логина...
  - Device type, OS, location, SGT...
  - Статус изоляции
  - Линк на forensic snapshot
  - ...



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ключ к успеху – это подготовка

- Определение процессов для сценариев ”what-if” критично
- Оркестрация SecureX позволяет автоматизировать процессы
- ...и это проще, чем вы думаете!
- Он бессерверный! не зависит от среды, языков программирования, железа...
- Уже есть много интеграций!
- ...и вы можете создать свои!

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Как быстро получить результат

Agenda

GitHub репозиторий

- Доступный контент
- Документация

Встроенные Workflows

- Варианты и примеры
- Phishing Investigation
- Response Workflows

Создание своих

- Workflows
- Atomic Actions

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

1

GitHub репозиторий

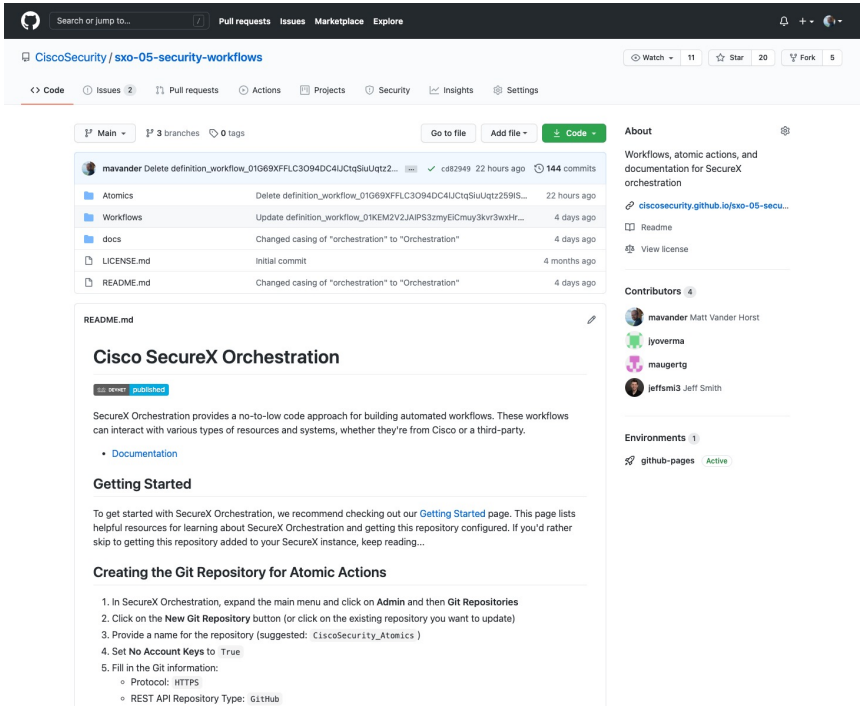
Важное замечение

Весь контент в SecureX Orchestration GitHub предлагается “as-is” под лицензией Cisco Sample Code.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

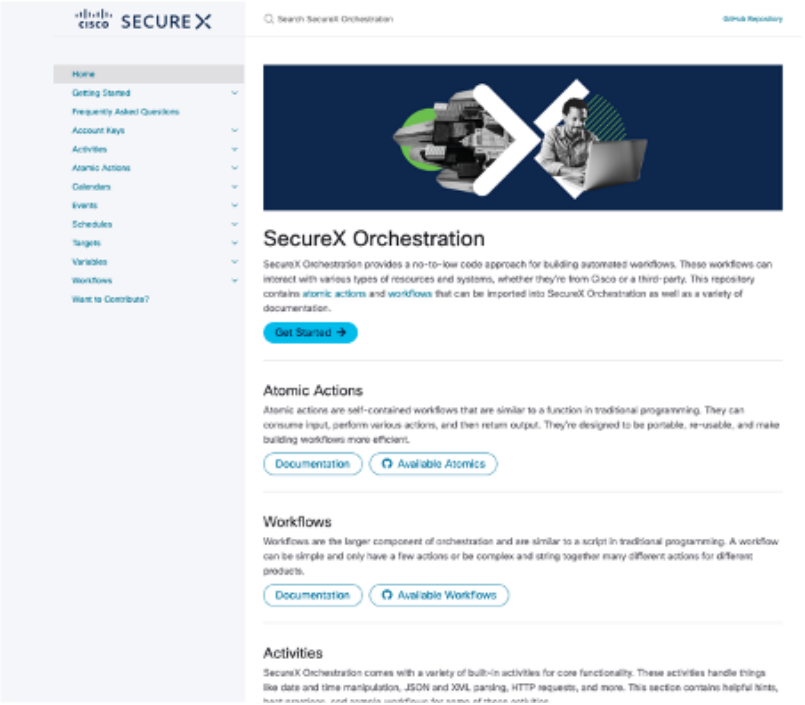
Orchestration Content

https://cs.co/SXO_repo



Documentation

https://cs.co/SXO_docs

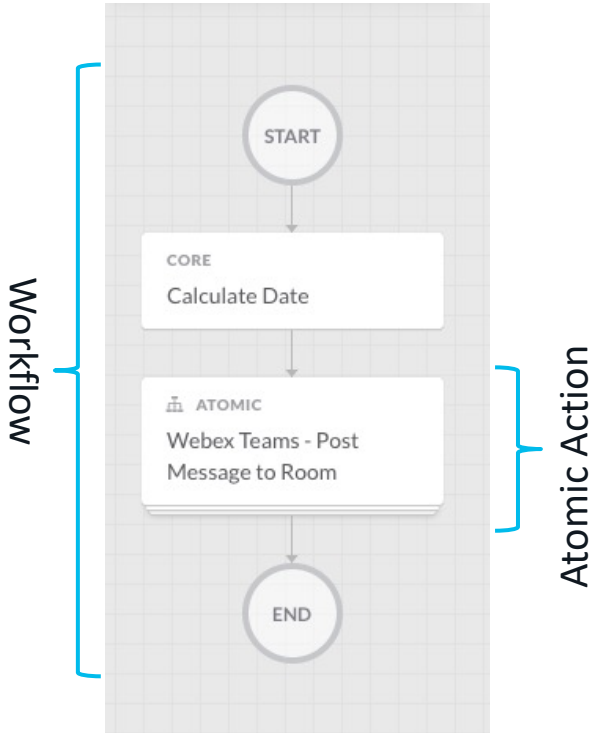


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Контент

https://cs.co/SXO_repo

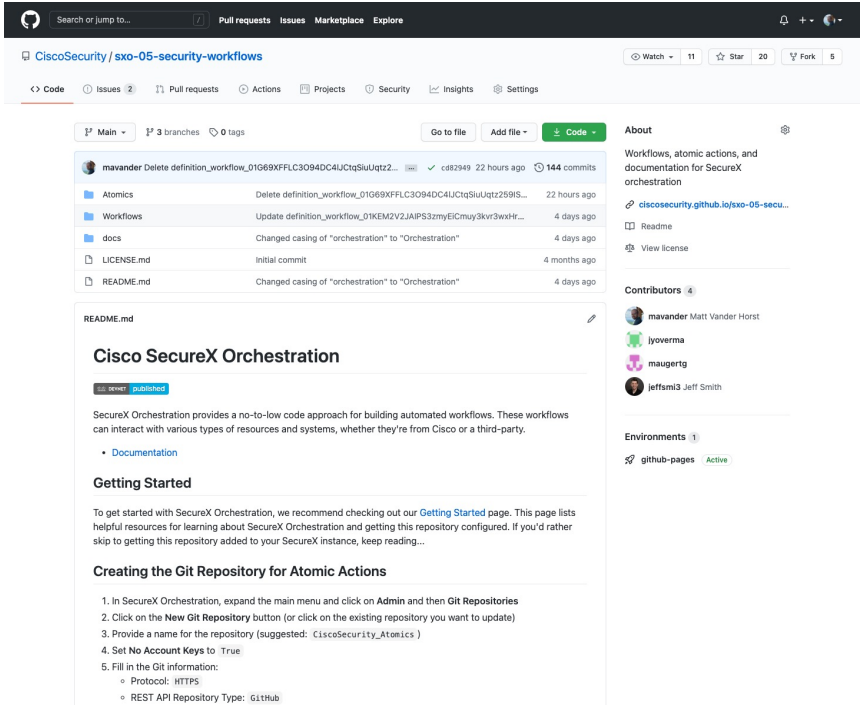
- Atomic Actions
  - Библиотека действий для разных продуктов
  - Включает как Cisco так и сторонние продукты
- Workflows
  - Различные варианты использование Proof of Concept
  - Примеры для определенных концепций



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

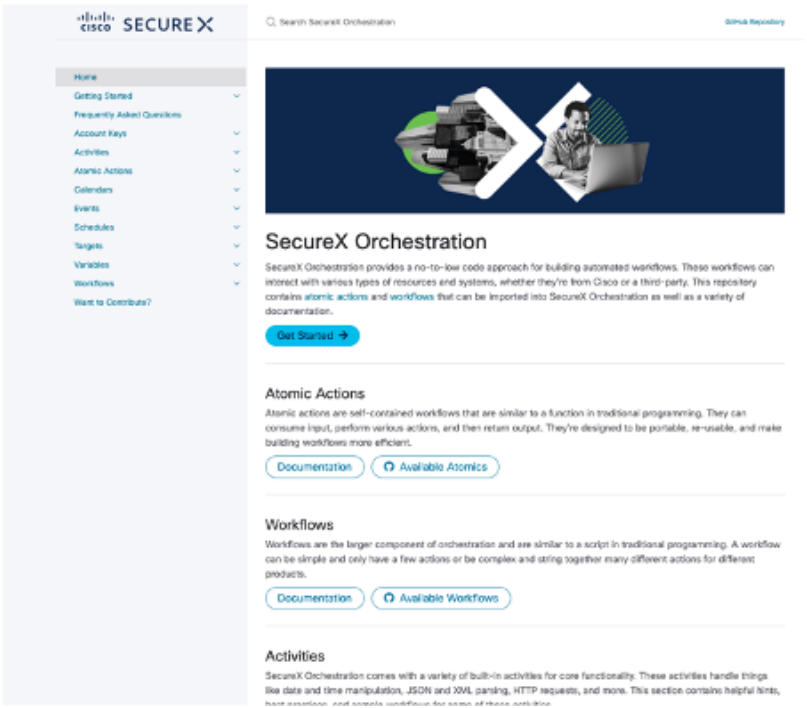
Orchestration Content

https://cs.co/SXO_repo



Documentation

https://cs.co/SXO_docs



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Документация

https://cs.co/SXO_docs

- Широкий набор информации про оркестрацию включая:
  - Как начать работать
  - Концепции и терминология
  - Руководства для различных примеров
  - Документация процессов

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

2

Готовые Workflows

Варианты использования

Product	Workflow Name
Adaptive Security Appliance	AWS VPN Capacity Expansion
Adaptive Security Appliance	Microsoft Online Split Tunnel Configuration
Defense Orchestrator	Microsoft Online Object Group Update
Multiple	Phishing Investigation
Orbital	CVE Hunt to ServiceNow Incident
Stealthwatch Cloud	Quarantine AWS Instances from Alerts
Talos	Get New Blog Posts
Talos	SolarWinds Investigation

and more…

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Обучающие примеры

- Condition Block
- Date and Time
- Execute Python Script
- For Each Loop
- HTTP Request
- JSONPath Query
- Parsing Nested JSON
- Response Workflows
- Tables
- Target Groups
- While Loop
- XPath Query

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Phishing Investigation Workflow

- Проблема:
  - Клиенты хотят автоматизировать расследование подозрительных email, о которых сообщают пользователи в их рабочей среде.
- Решение:
  - Процесс SecureX Orchestration, который мониторит новые сообщения в почтовом ящике и расследует каждое прибывающее письмо.
  - Находки документируются в Threat Response и уведомления отправляются соответствующим людям после завершения расследования.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Phishing Investigation Workflow

Расследование

- Email Body и Headers
- Attachments

Документирование

- Casebook
- Incident
- Sighting

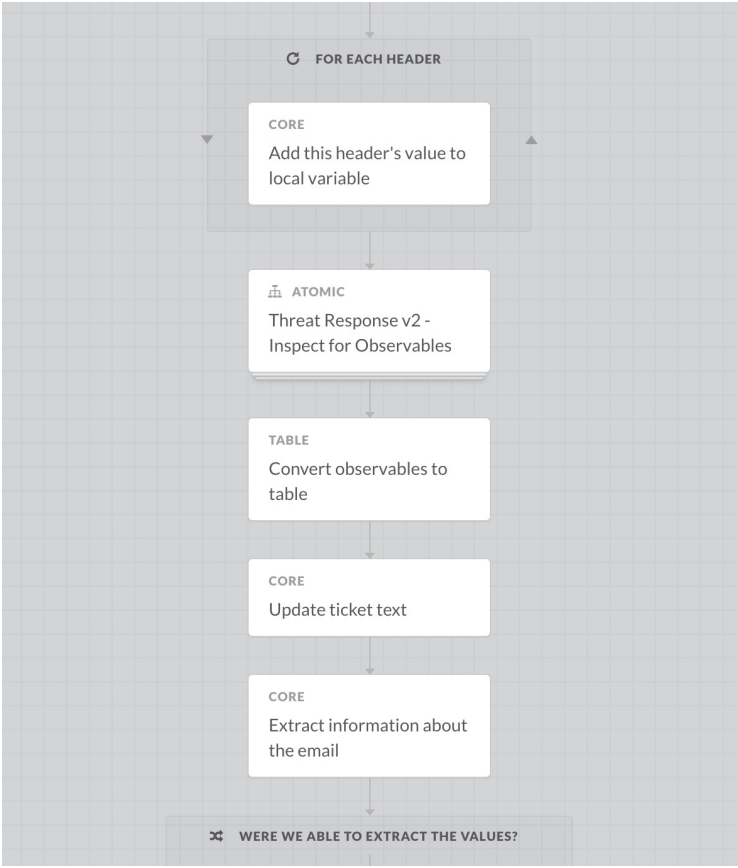
Уведомление

- Webex Teams
- Email

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

1 Расследование

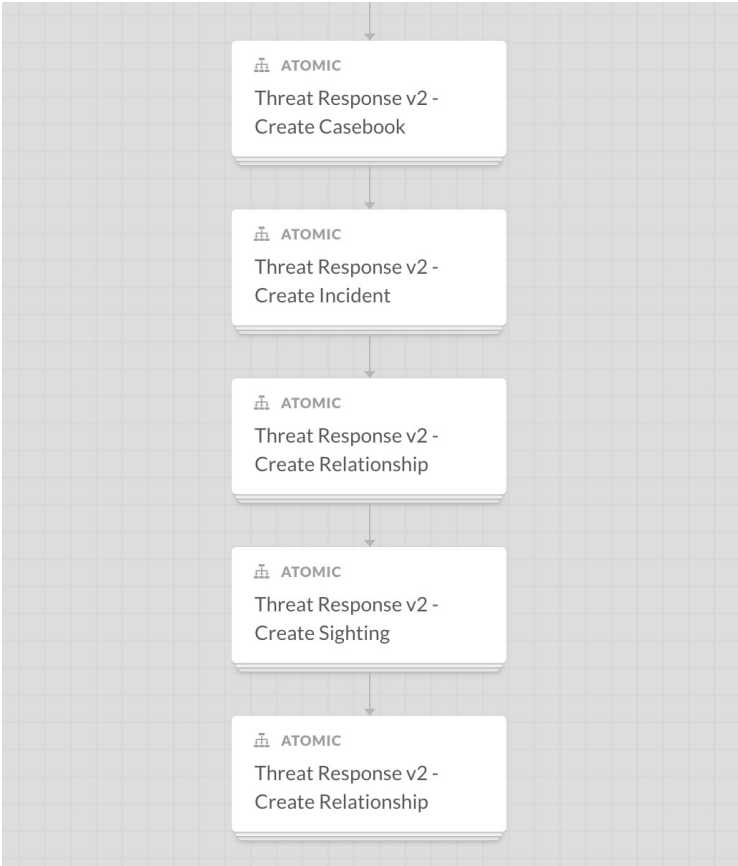
- Извлечение наблюдений
  - Email Body и Headers
- Получение диспозиции
  - Clean, Suspicious, Malicious, etc.
- Анализ в Threat Grid
  - Сокращенные URLs
  - Вложенные файлы
    - PDFs, Microsoft Office Documents, etc.



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

2 Документирование

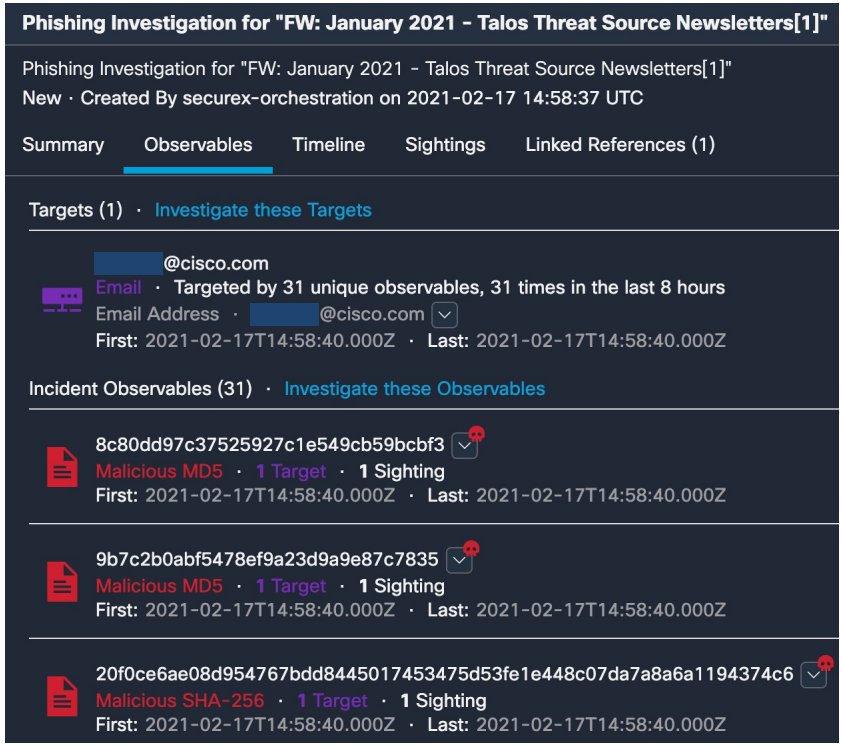
- Threat Response
  - Casebook
    - Observables
  - Incident
  - Sighting
    - Observables
    - Target



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

2 Документирование

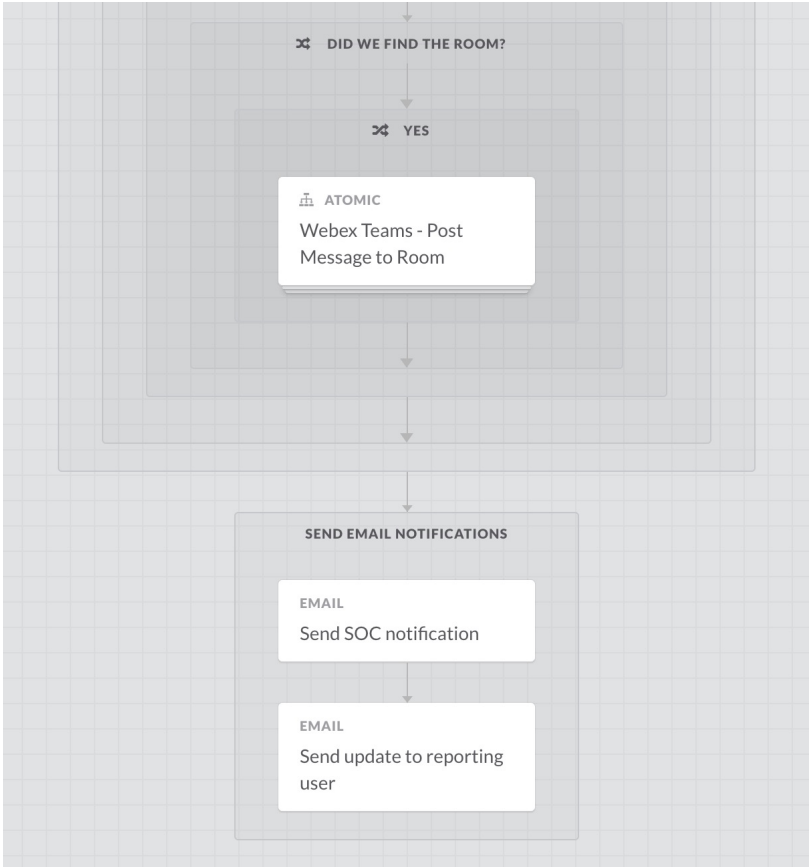
- Threat Response
  - Casebook
    - Observables
  - Incident
  - Sighting
    - Observables
    - Target



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

3 Notify

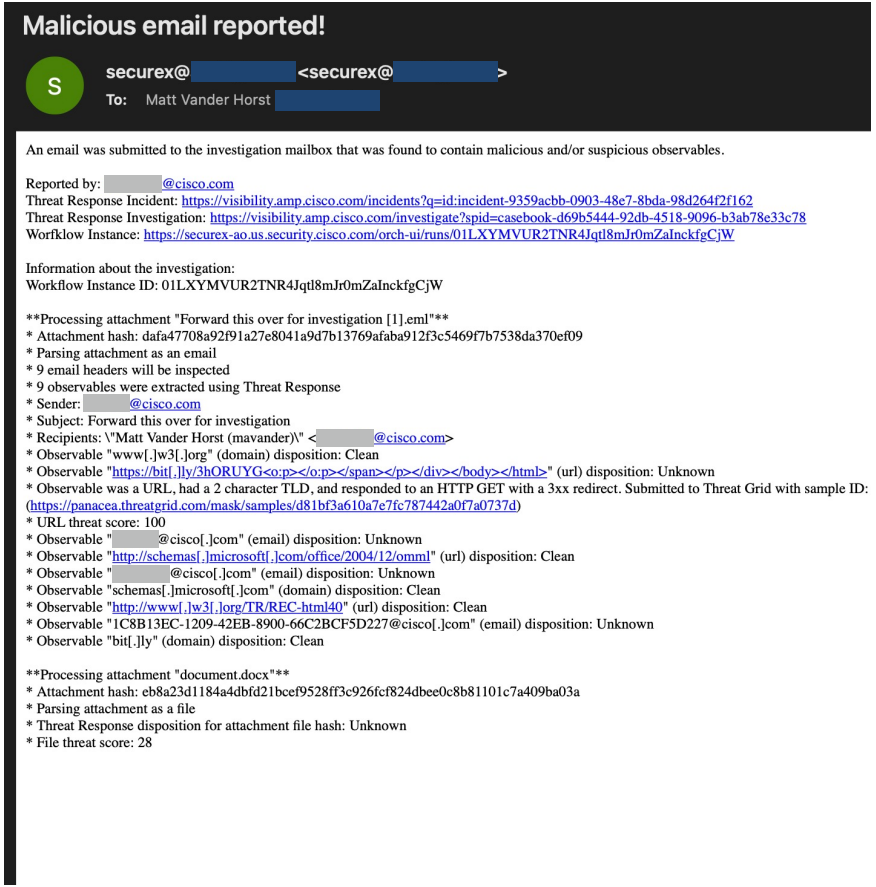
- Webex Teams
- Email
  - Security Operations
  - End User



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

3 Уведомление

- Webex Teams
- Email
  - Security Operations
  - End User



Malicious email reported!

S

securex@ [redacted] <securex@ [redacted] >

To: Matt Vander Horst [redacted]

An email was submitted to the investigation mailbox that was found to contain malicious and/or suspicious observables.

Reported by: [redacted]@cisco.com
Threat Response Incident: https://visibility.amp.cisco.com/incidents?q=id:incident-9359acbb-0903-48e7-8bda-98d264f2f162
Threat Response Investigation: https://visibility.amp.cisco.com/investigate?spid=casebook-d69b5444-92db-4518-9096-b3ab78e33c78
Worfklow Instance: https://securex-ao.us.security.cisco.com/orch-ui/runs/01LXYMVUR2TNR4Jqtl8mJr0mZaInckfgCjW

Information about the investigation:
Workflow Instance ID: 01LXYMVUR2TNR4Jqtl8mJr0mZaInckfgCjW

Processing attachment "Forward this over for investigation [1].eml"
* Attachment hash: dafa47708a92f91a27e8041a9d7b13769afaba912f3c5469f7b7538da370ef09
* Parsing attachment as an email
* 9 email headers will be inspected
* 9 observables were extracted using Threat Response
* Sender: [redacted]@cisco.com
* Subject: Forward this over for investigation
* Recipients: \"Matt Vander Horst (mavander)\" <[redacted]@cisco.com>
* Observable "www[.]w3[.]org" (domain) disposition: Clean
* Observable "https://bit[.]ly/3hORUYG<o:p></o:p></p> </body></html>" (url) disposition: Unknown
* Observable was a URL, had a 2 character TLD, and responded to an HTTP GET with a 3xx redirect. Submitted to Threat Grid with sample ID: (https://panacea.threatgrid.com/mask/samples/d81bf3a610a7e7fc787442a0f7a0737d)
* URL threat score: 100
* Observable "[redacted]@cisco[.]com" (email) disposition: Unknown
* Observable "http://schemas[.]microsoft[.]com/office/2004/12/omml" (url) disposition: Clean
* Observable "[redacted]@cisco[.]com" (email) disposition: Unknown
* Observable "schemas[.]microsoft[.]com" (domain) disposition: Clean
* Observable "http://www[.]w3[.]org/TR/REC-html40" (url) disposition: Clean
* Observable "1C8B13EC-1209-42EB-8900-66C2BCF5D227@cisco[.]com" (email) disposition: Unknown
* Observable "bit[.]ly" (domain) disposition: Clean

Processing attachment "document.docx"
* Attachment hash: eb8a23d1184a4dbfd21bcef9528ff3c926fcf824dbee0c8b81101c7a409ba03a
* Parsing attachment as a file
* Threat Response disposition for attachment file hash: Unknown
* File threat score: 28

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ресурсы

- GitHub Repository
  https://cs.co/SXO_repo
- Documentation
  https://cs.co/SXO_docs
- Video Playlist
  https://cs.co/SXO_videos
- Cisco DevNet
  https://developer.cisco.com

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Сбор данных из блогов безопасности

- Проблема:
  - Клиенты хотят автоматизировать процесс процесс проверки индикаторов компрометации, которые поступают их других источников кибераналитики.
- Решение:
  - Процесс SecureX Orchestration, который мониторит веб ресурсы и RSS потоки и проверяет индикаторы компрометации, которые там находятся.
  - Находки документируются в Threat Response и уведомления отправляются соответствующим людям после завершения расследования.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Анализ отчетов кибераналитиков

https://youtu.be/E_Sq4VdFKcg?t=6278

Rapid Threat Containment. Блокировка IP на NGFW

- Проблема:
  - Клиенты хотят с одной стороны ускорить и упростить процесс блокировки подозрительных адресов на NGFW, с другой стороны обезопасить его и снизить вероятность ложных срабатываний.
- Решение:
  - Процесс SecureX Orchestration, получает на вход необходимый адрес, отправляет запрос на подтверждение локальному аналитику и после утверждения автоматически его добавляет в необходимые списки блокировки на любых NGFW.
  - Процесс автоматически завершается и документируется .

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Rapid Threat Containment

https://youtu.be/E_Sq4VdFKcg?t=6887

Заключение

SecureX тренинг

Глобальные threat hunting workshops

Вы можете запросить виртуальные классы для того, чтобы пройти обучение на реальных атаках

Использует варианты использования SecureX

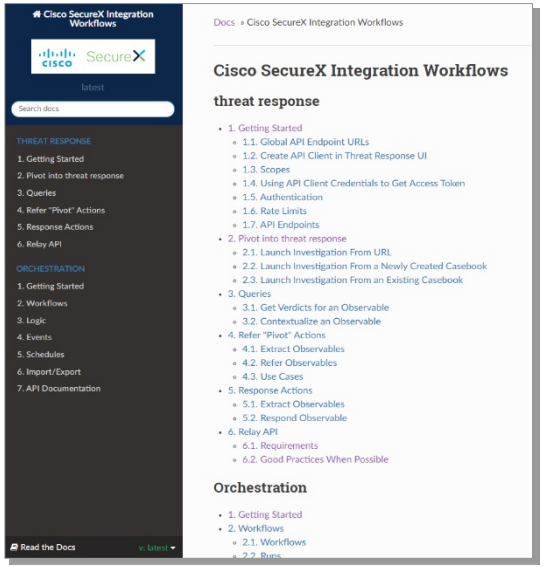
Узнайте, как защититься от злоумышленников с помощью платформы SecureX

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ресурсы

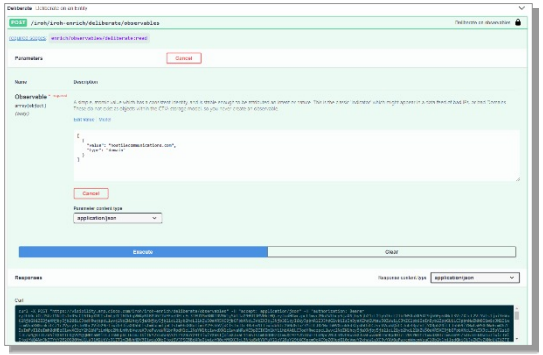
Документация интеграции

cs.co/SecureX_integration_workflows



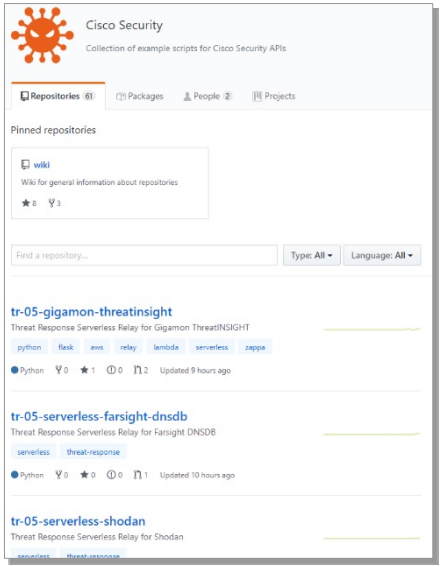
UI документы

github.com/threatgrid/ctim/tree/master/doc



GitHub

github.com/CiscoSecurity

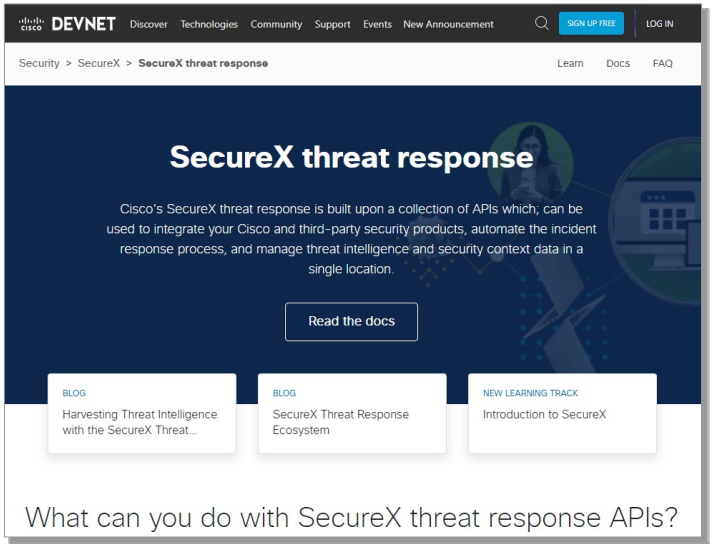


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ресурсы SecureX threat response

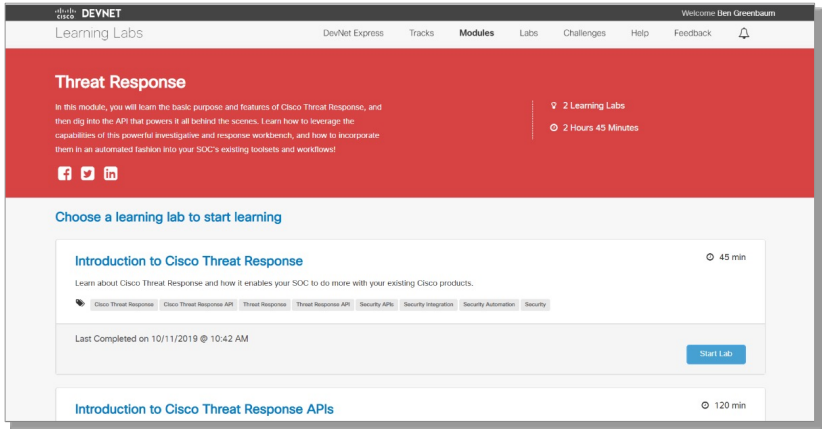
DevNet

- developer.cisco.com/threat-response/
- cs.co/SecureX_integration_workflows



DevNet learning labs

- cs.co/CTR-API-labs

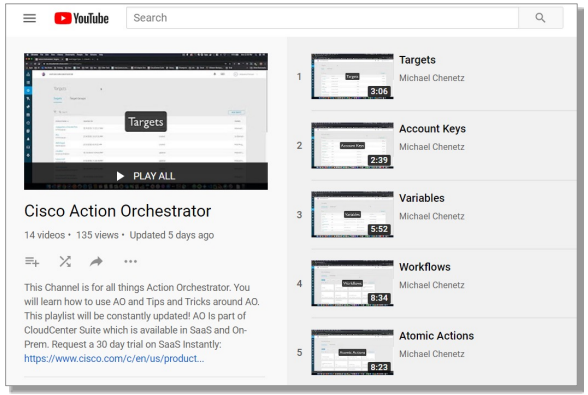


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ресурсы SecureX orchestration

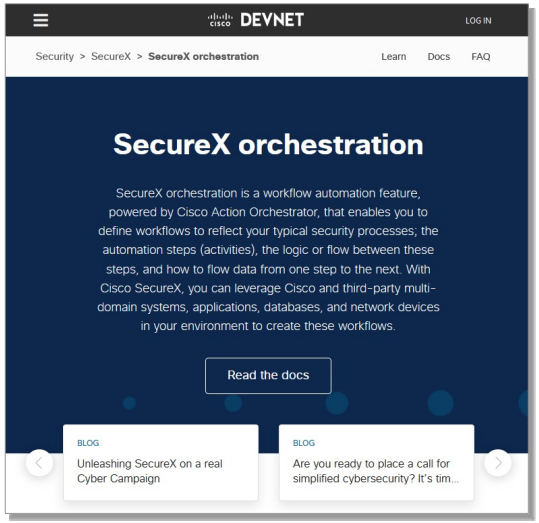
Videos

cs.co/AOvideos



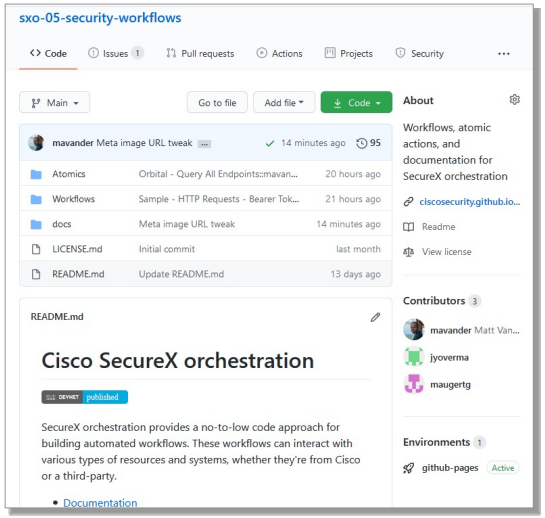
DevNet

developer.cisco.com/securex/orchestration



GitHub

github.com/CiscoSecurity



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you