Start Now 101 – Security Track

API is a foundation for modern security solutions

Oxana Sannikova, Security Programmability Lead
Global Security Architecture Team

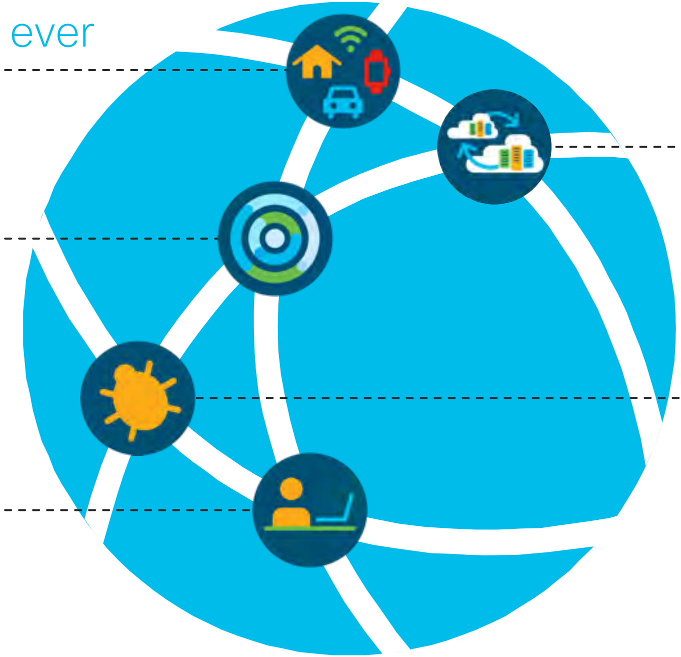
DEVNET-SEC

Today’s risk reality

More interconnected than ever

Continuous operations

Workers connecting everywhere



Multi-cloud reality

Automated and sophisticated threats

Customer Challenges

Too Many Point Products

Too Much Information

Too Much Effort

Too Little Time

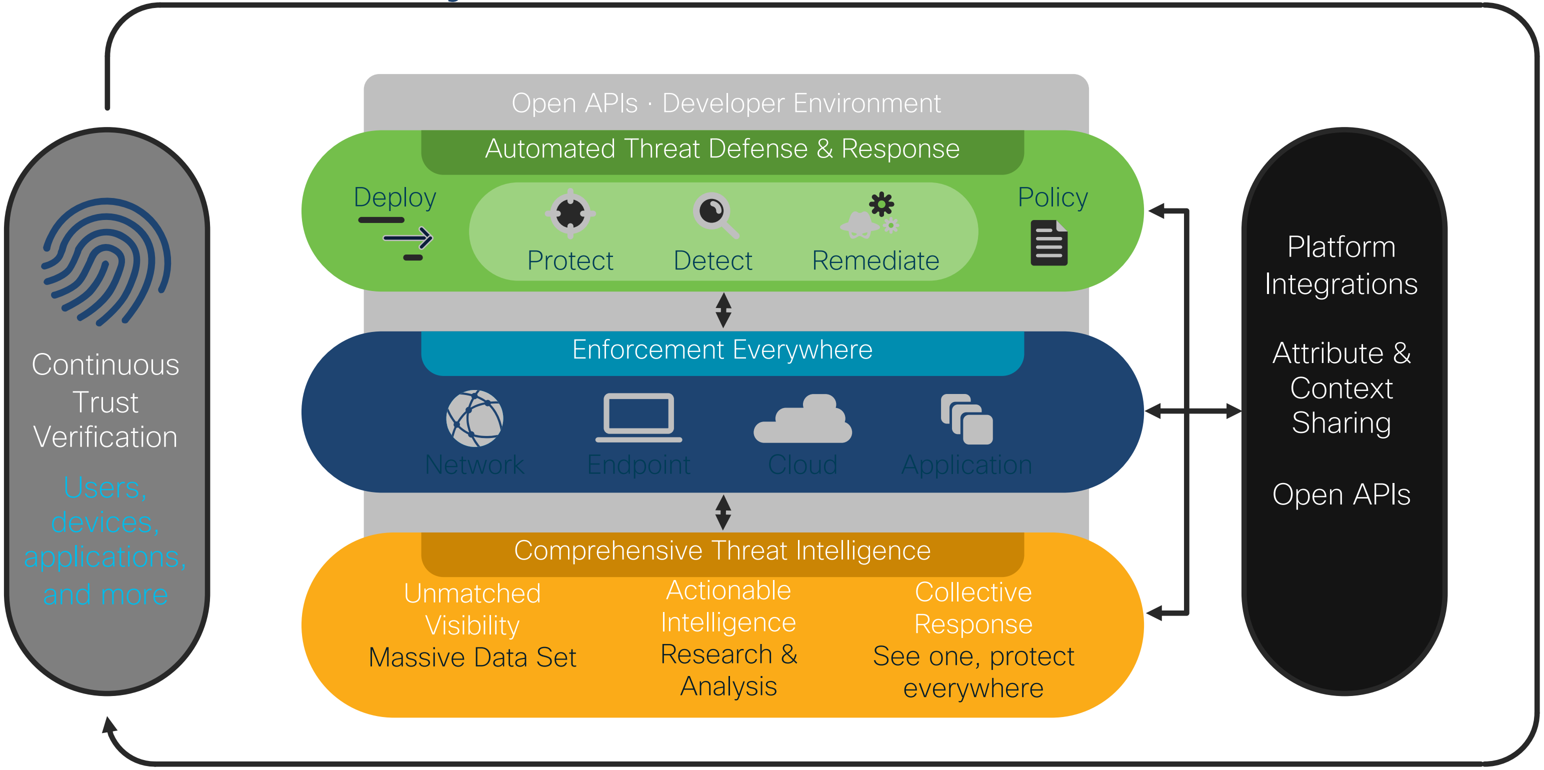
How to solve this?

Integration between security solutions

Automation of routine, non-cognitive tasks and policy automation

Goals:
- Increase Threat Prevention
- Decrease Time to Detect
- Reduce Time to Investigate
- Reduce Time to Remediate

Modern Security Architecture



Continuous Trust Verification

Users, devices, applications, and more

Open APIs · Developer Environment

Automated Threat Defense & Response

Deploy

Protect

Detect

Remediate

Policy

Enforcement Everywhere

Network

Endpoint

Cloud

Application

Comprehensive Threat Intelligence

Unmatched Visibility
Massive Data Set

Actionable Intelligence
Research & Analysis

Collective Response
See one, protect everywhere

Platform Integrations

Attribute & Context Sharing

Open APIs

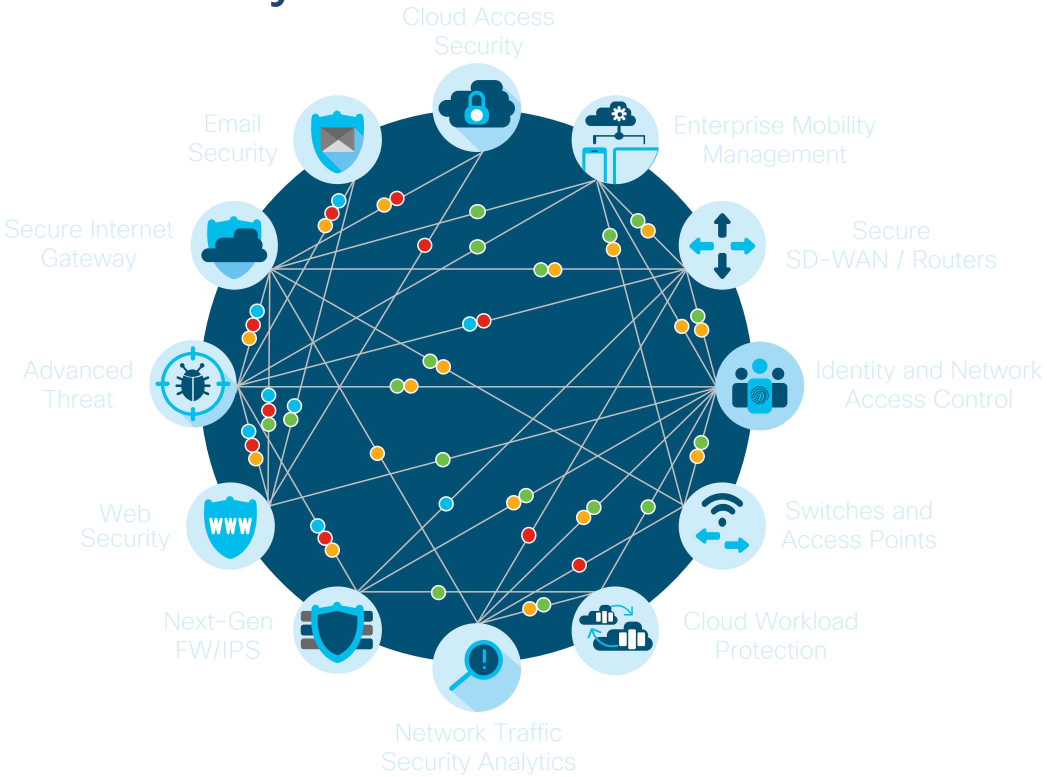
How Cisco Integrates Security

Threat Intel/Enforcement
Increased Threat Prevention

Event Visibility
Decreased Time to Detect

Context Awareness
Decreased Time to Investigate

Automated Policy
Decreased Time to Remediate


Cloud Access Security
Enterprise Mobility Management
Secure SD-WAN / Routers
Identity and Network Access Control
Switches and Access Points
Cloud Workload Protection
Network Traffic Security Analytics
Next-Gen FW/IPS
Web Security
Advanced Threat
Secure Internet Gateway
Email Security

World Full of ISE

DevNet Day - Security

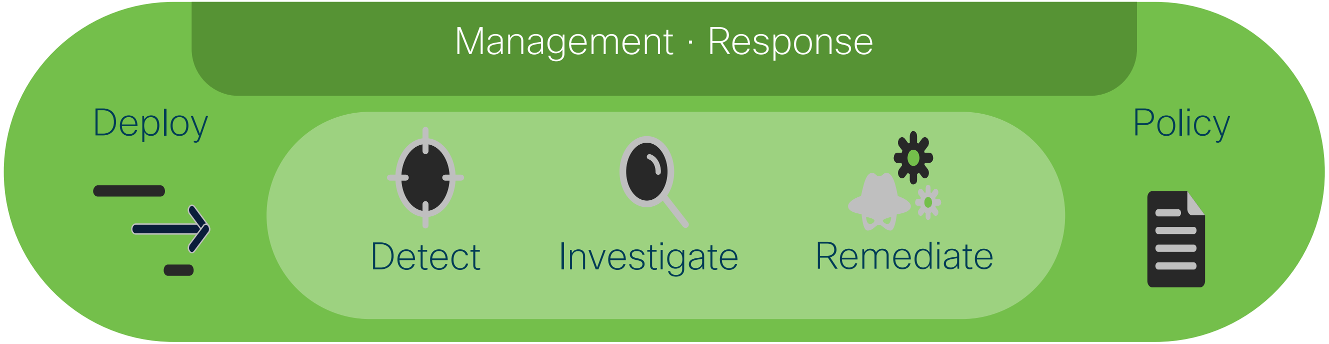
Gabriel Liechtman-Manor
Senior Software Engineer, Security Policy and Access
Session ID

CISCO Live!

CISCO

#CiscoLive | #DevNetDay

API as a foundation for modern security solutions



Thank you

Possibilities

#CiscoLive | #DevNetDay

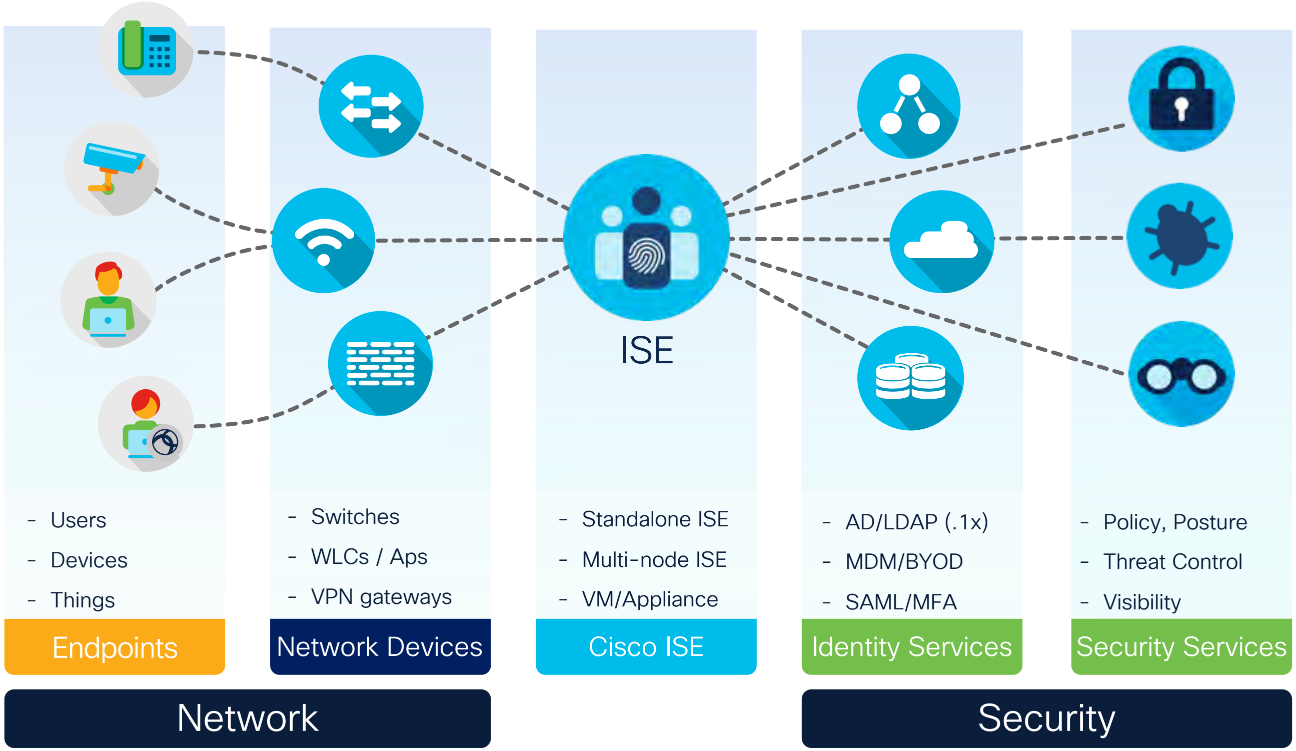
World Full of ISE

DevNet Day - Security

Gabriel Liechtman-Manor
Senior Software Engineer, Security Policy and Access

Session ID

ISE – The Bridge Between Network and Security



- Users
- Devices
- Things

Endpoints

- Switches
- WLCs / Aps
- VPN gateways

Network Devices

- Standalone ISE
- Multi-node ISE
- VM/Appliance

Cisco ISE

- AD/LDAP (.1x)
- MDM/BYOD
- SAML/MFA

Identity Services

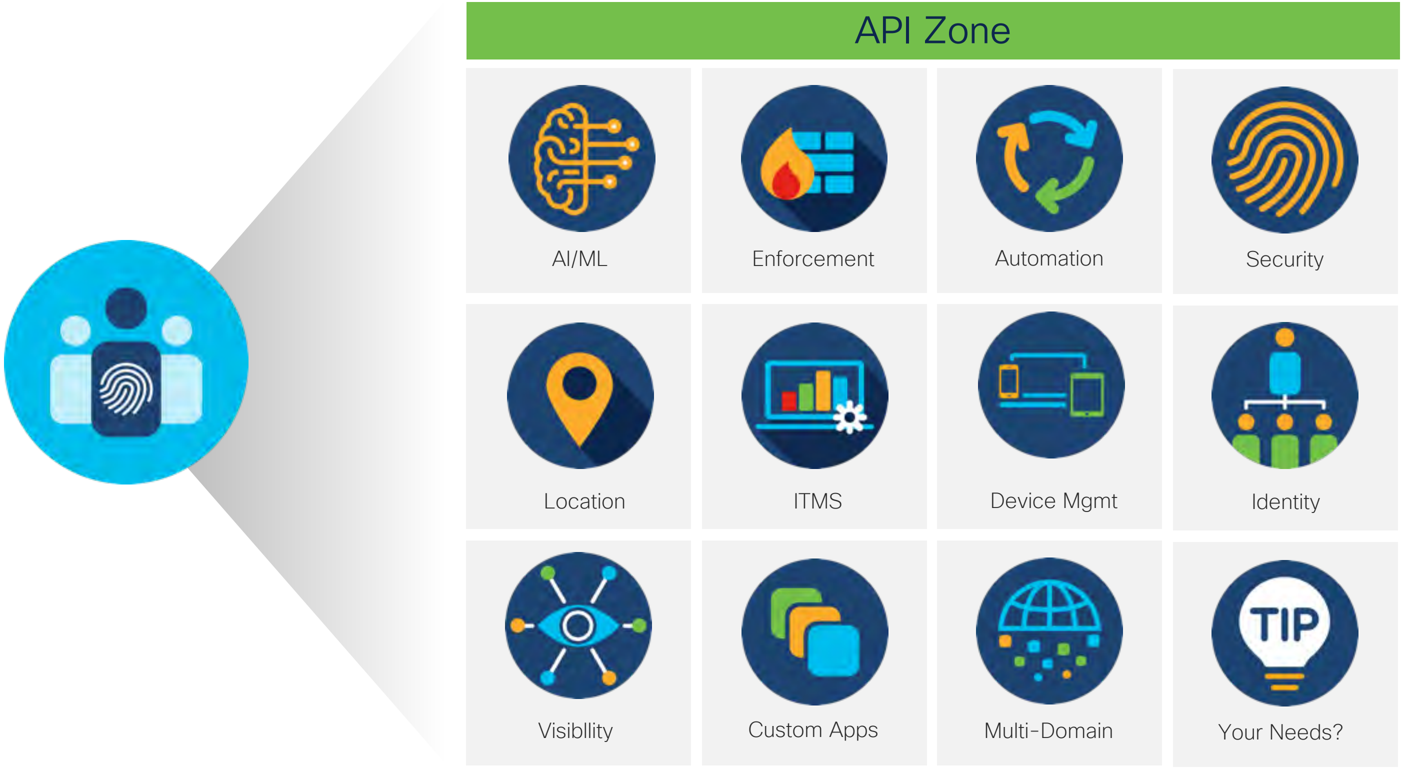
- Policy, Posture
- Threat Control
- Visibility

Security Services

Network

Security

ISE APIs – Kingdom of Creativity



API Zone

AI/ML

Enforcement

Automation

Security

Location

ITMS

Device Mgmt

Identity

Visiblity

Custom Apps

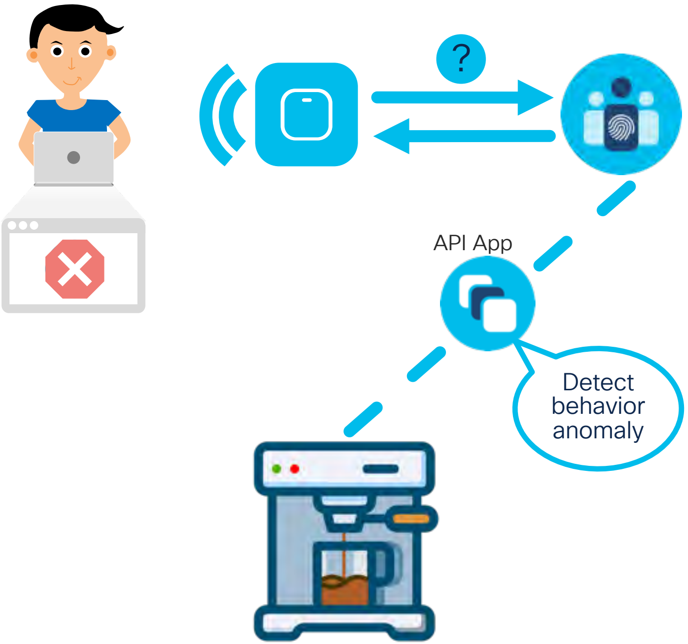
Multi-Domain

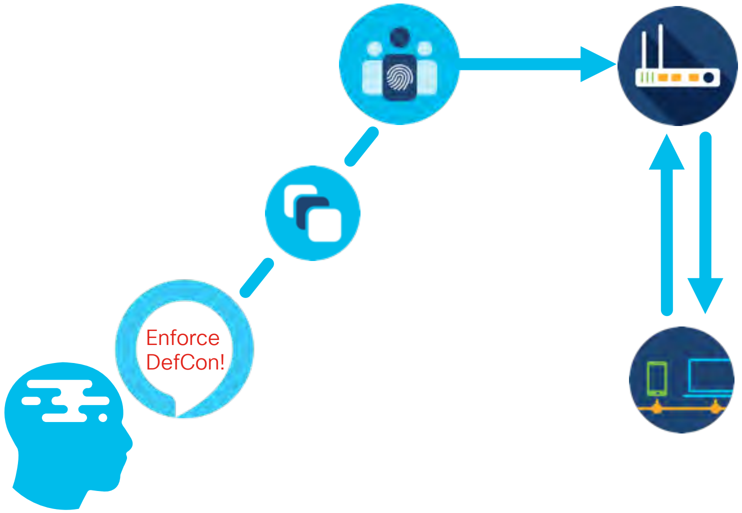
Your Needs?

Swiss Army Knife

ERS	PxGrid	MnT
Configuration, Orchestration, Automation	Context Exchange, Data Pub/Sub, Enforcement	Monitoroing, Troubleshooting, Discovery
HTTPS/REST	HTTPS/WebSocket	HTTPS/REST
ISE Admin/Sponsor	Certificate	ISE Admin

Create With No Limits





Solve a Real-World Challenges

100+ Product integrations

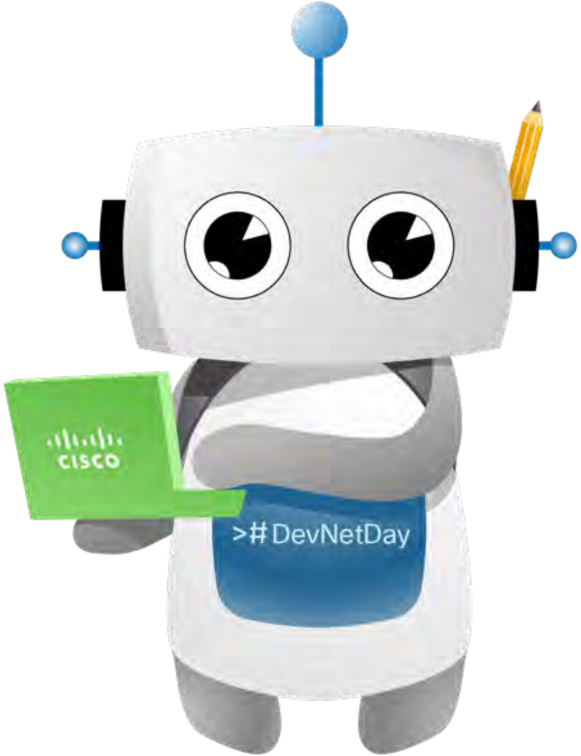
75+ Eco-system partners

Endless Use Cases

intelliment security
netskope
LogRhythm The Security Intelligence Company
FORTSCALE
exabeam
SECUREAUTH
CLAROTY
tenable
SOPHOS
DEMISTO
TRAPX SECURITY
McAfee
Cynerio
DIGITAL DEFENSE INCORPORATED
MEDIGATE
HanSight
IBM Radar
NETWORKS
SECURONIX
cisco
REDSHIFT NETWORKS
BlackRidge TECHNOLOGY
ZingBox
Huntsman
Attivo NETWORKS
NOZOMI NETWORKS
armis
RAPID7
splunk>
SAINT
Greenlight TECHNOLOGIES
SECURITY MATTERS
CYBER MDX
BAYSHORE
ThreatTrack
LiveAction
NetIQ
Check Point SOFTWARE TECHNOLOGIES LTD
Lumeta
SYNCURITY
CVU
illusive
LemonFish
endace
SIEMPLIFY
E8 SECURITY
Cwirex
Infoblox

Explore More

- Documentation
  - cs.co/ise-api
  - cs.co/pxgrid
  - cs.co/pxgrid-wiki
- Sandbox
  - https://devnetsandbox.cisco.com/RM/Topology



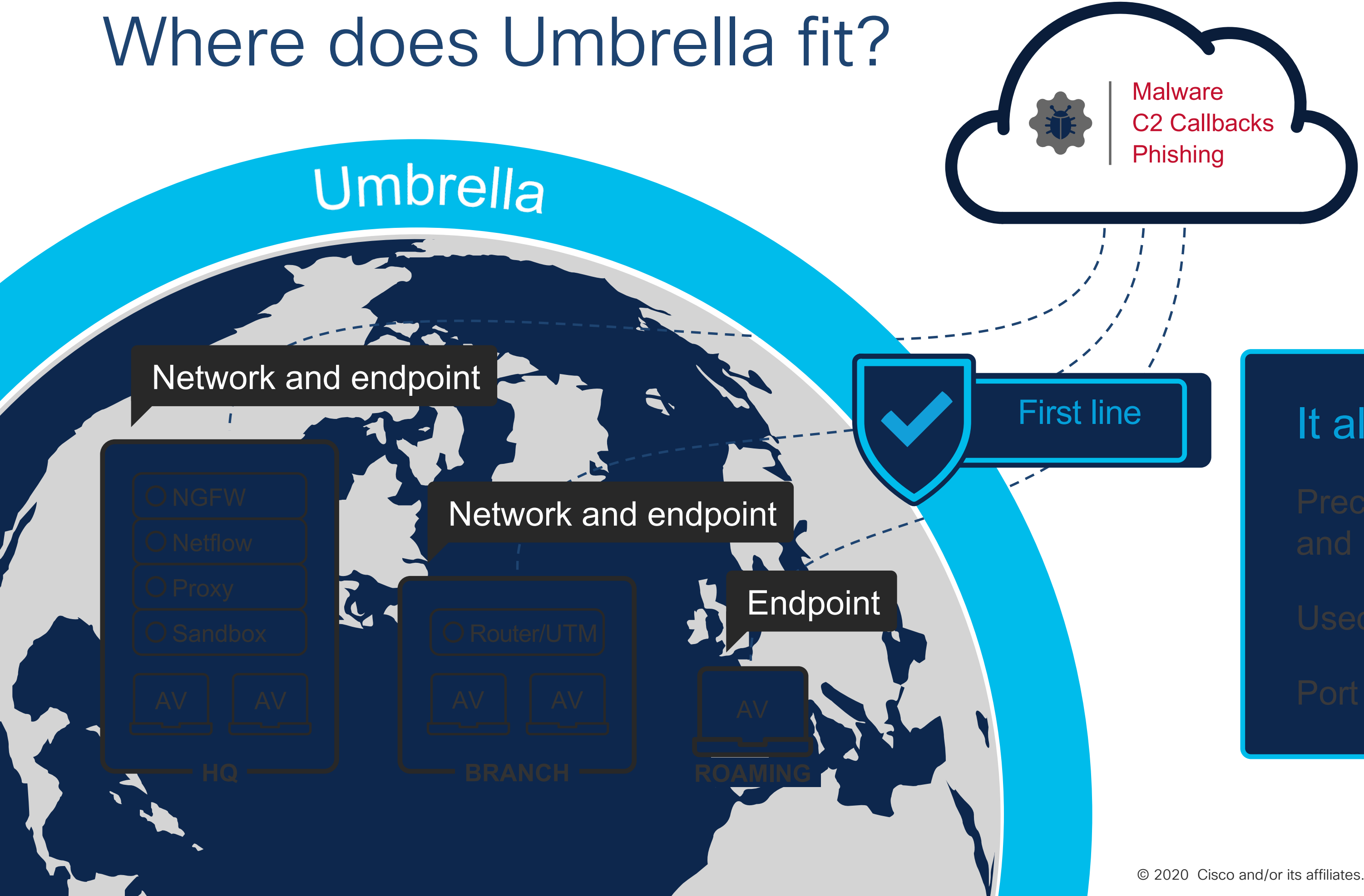
Thank you

Cisco Umbrella

Security Cisco Live Virtual DevNet Day

Krishan Veer Developer Advocate & Technical Leader
#veeratcisco

Where does Umbrella fit?



It all starts with DNS

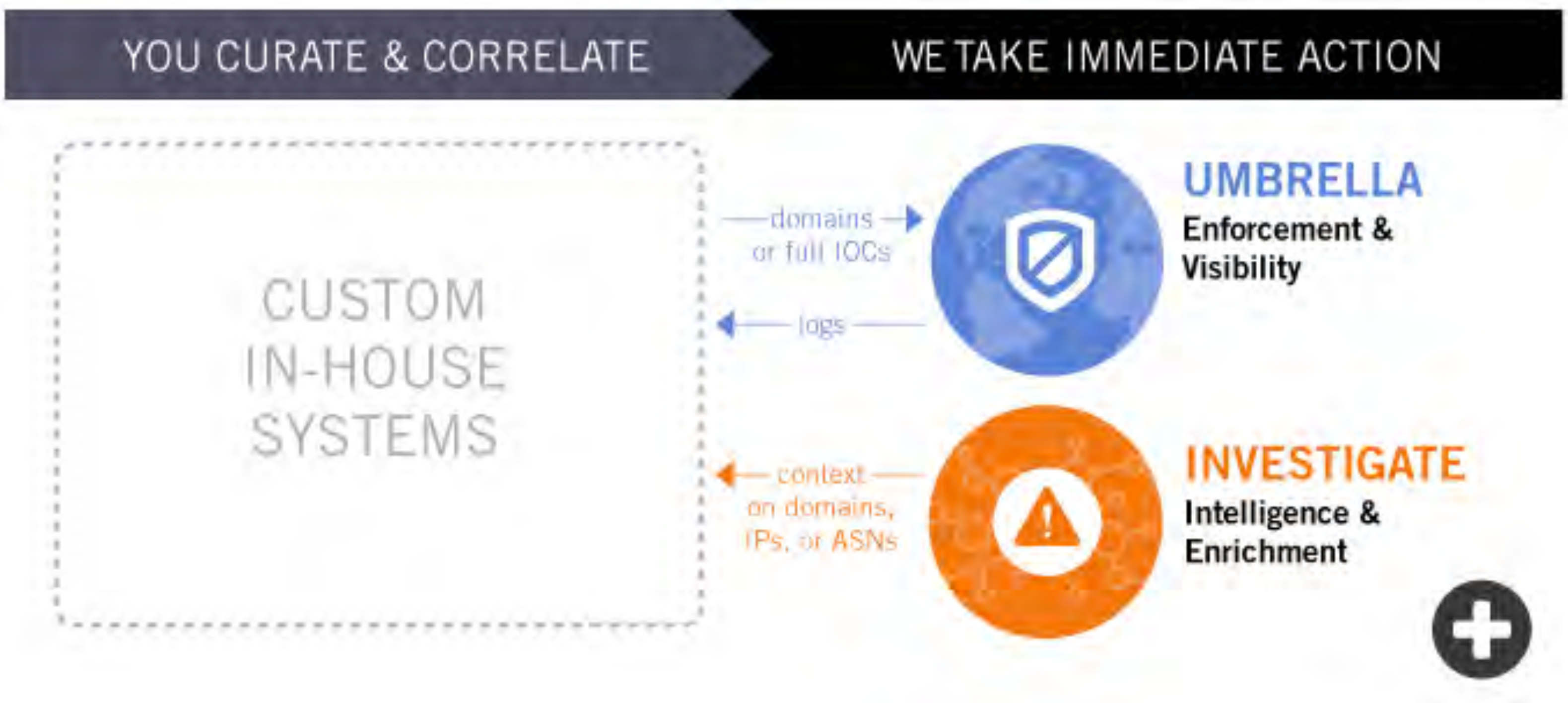
Precedes file execution and IP connection

Used by all devices

Port agnostic

Overview of Umbrella API’s

Umbrella API's



YOU CURATE & CORRELATE

WE TAKE IMMEDIATE ACTION

CUSTOM IN-HOUSE SYSTEMS

UMBRELLA

Enforcement & Visibility

INVESTIGATE

Intelligence & Enrichment

Umbrella Enforcement API Summary

Used with SIEM or Threat Intelligence Source to inject "events" and/or threat intelligence into their Umbrella environment.

These events or threat intelligence can be used in a custom integration with Umbrella to add additional domains to block.

Can be used to integrate SIEM or UTM with Umbrella. Existing integration with Splunk!

Up to 10 custom integrations possible with **Umbrella Platform Customers.**

Can be used for Cisco Threat Response!

Umbrella Investigate API Summary

Can be used to automate enrichment of context regarding an observable:

Check the security status of a domain, IP address or subset of domains.

Find a historical record for this domain or IP address.

Query large numbers of domains quickly.

The API is rate limited and are based on the tier of API access that was purchased and which endpoint is being requested.

Extra license needed on top of Umbrella Platform.

Can be used Cisco Threat Response (special license: UMB-INV-INT-API).

Other Umbrella API's

Reporting API

Included with all license packages!

API Endpoints:

- Most Recent Requests
- Top Identities
- Security Activity

Can be used for Cisco Threat Response!

Network Device Management API:

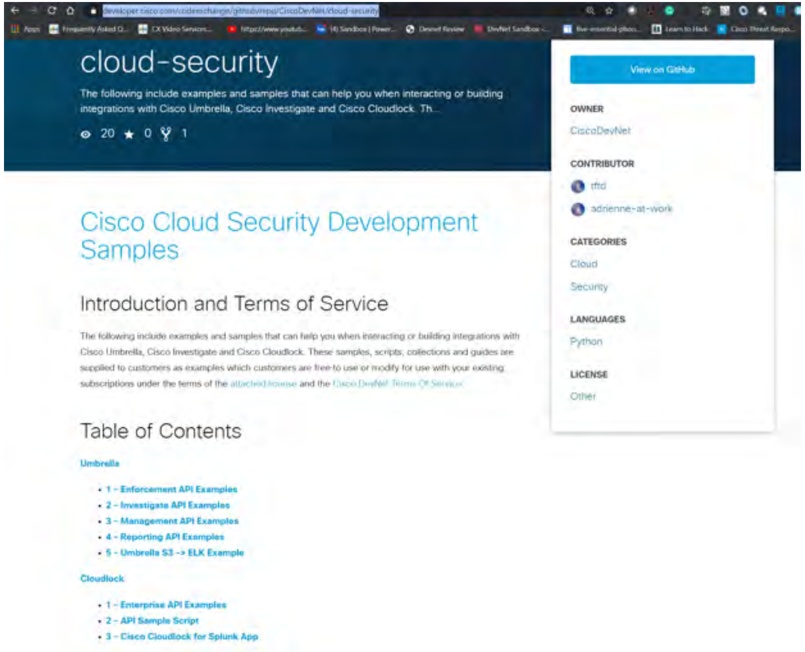
Allows you to register network devices as identities to the Umbrella dashboard.

Partner & Provider Console Reporting API:

This API is for MSP, MSSP, and Multi-Org Console administrators. It returns summary information that is available only in those Consoles.

Get Started…

Umbrella APIs



cloud-security

The following include examples and samples that can help you when interacting or building integrations with Cisco Umbrella, Cisco Investigate and Cisco Cloudlock. Th...

20 ★ 0 1

OWNER

CiscoDevNet

CONTRIBUTOR

tftd

adrienne-at-work

CATEGORIES

Cloud

Security

LANGUAGES

Python

LICENSE

Other

Cisco Cloud Security Development Samples

Introduction and Terms of Service

The following include examples and samples that can help you when interacting or building integrations with Cisco Umbrella, Cisco Investigate and Cisco Cloudlock. These samples, scripts, collections and guides are supplied to customers as examples which customers are free to use or modify for use with your existing subscriptions under the terms of the attached license and the Cisco DevNet Terms Of Service.

Table of Contents

Umbrella

- **1 – Enforcement API Examples**
- **2 – Investigate API Examples**
- **3 – Management API Examples**
- **4 – Reporting API Examples**
- **5 – Umbrella S3 -> ELK Example**

Cloudlock

- **1 – Enterprise API Examples**
- **2 – API Sample Script**
- **3 – Cisco Cloudlock for Splunk App**

Documentation

https://docs.umbrella.com/umbrella-api/docs/about-the-umbrella-api

Sample Code

https://developer.cisco.com/codeexchange/github/repo/CiscoDevNet/cloud-security

Learning Labs:

https://developer.cisco.com/learning/labs/tags/Security

Advanced Malware Protection and Threat Grid API’s

Security Cisco Live Virtual DevNet Day

Christopher van der Made
@Chrisco_DevNet

Thank you

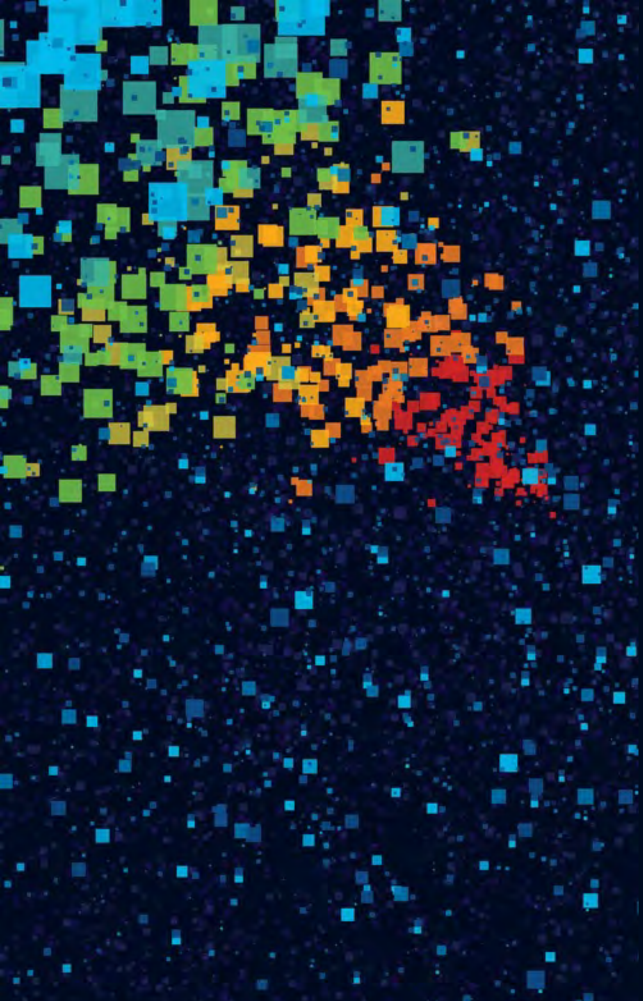
Possibilities

#CiscoLive | #DevNetDay

Security Management Appliance API’s

Security Cisco Live Virtual DevNet Day

Christopher van der Made
@Chrisco_DevNet



Agenda

- Intro to SMA
- Overview SMA API’s
- Example use cases
- Conclusion

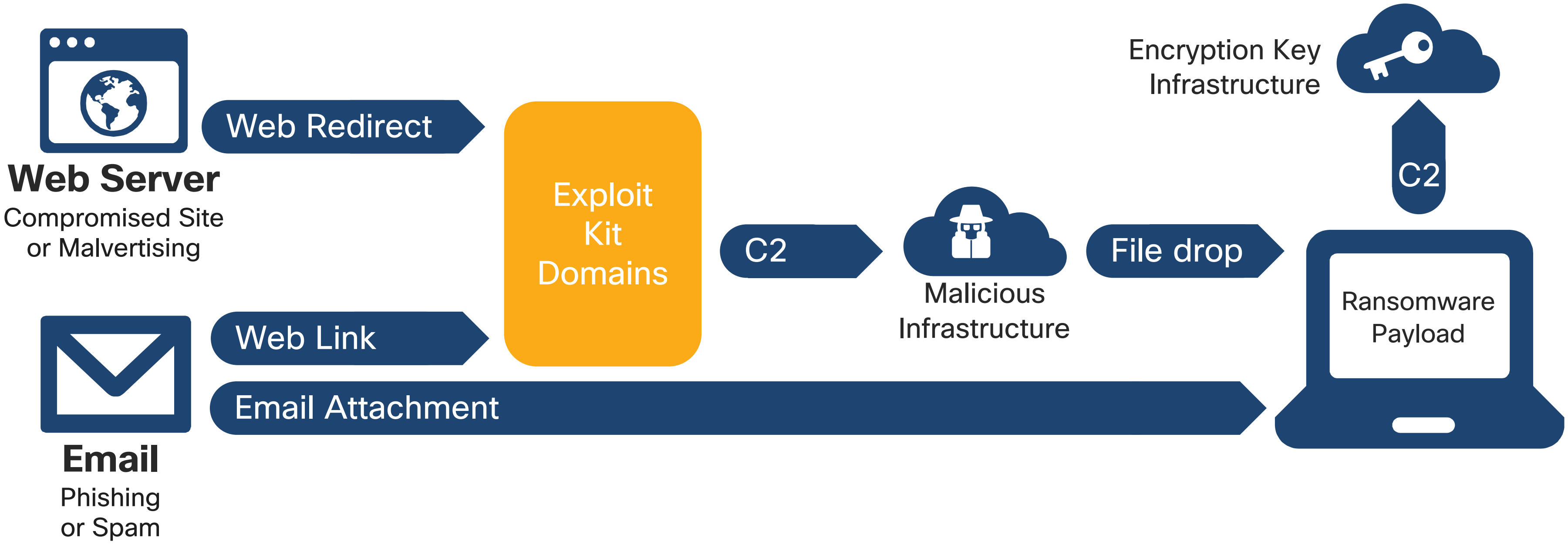
Intro to SMA

Did You Know?

Over 99%

of malware is sent by either web server or email

Ransomware Email and Web Delivery



Cisco Web Security Appliance Provides...

Integrations

Strong Effective Protection

Flexible Deployment

Cisco WSA

Granular Control

Detailed Reporting

1011010
10110 0
0 0110

Inbound and Outbound Protection

Inbound

Cisco Email Security with Advanced Malware Protection and Threat Grid

+

Cisco Advanced Phishing Protection

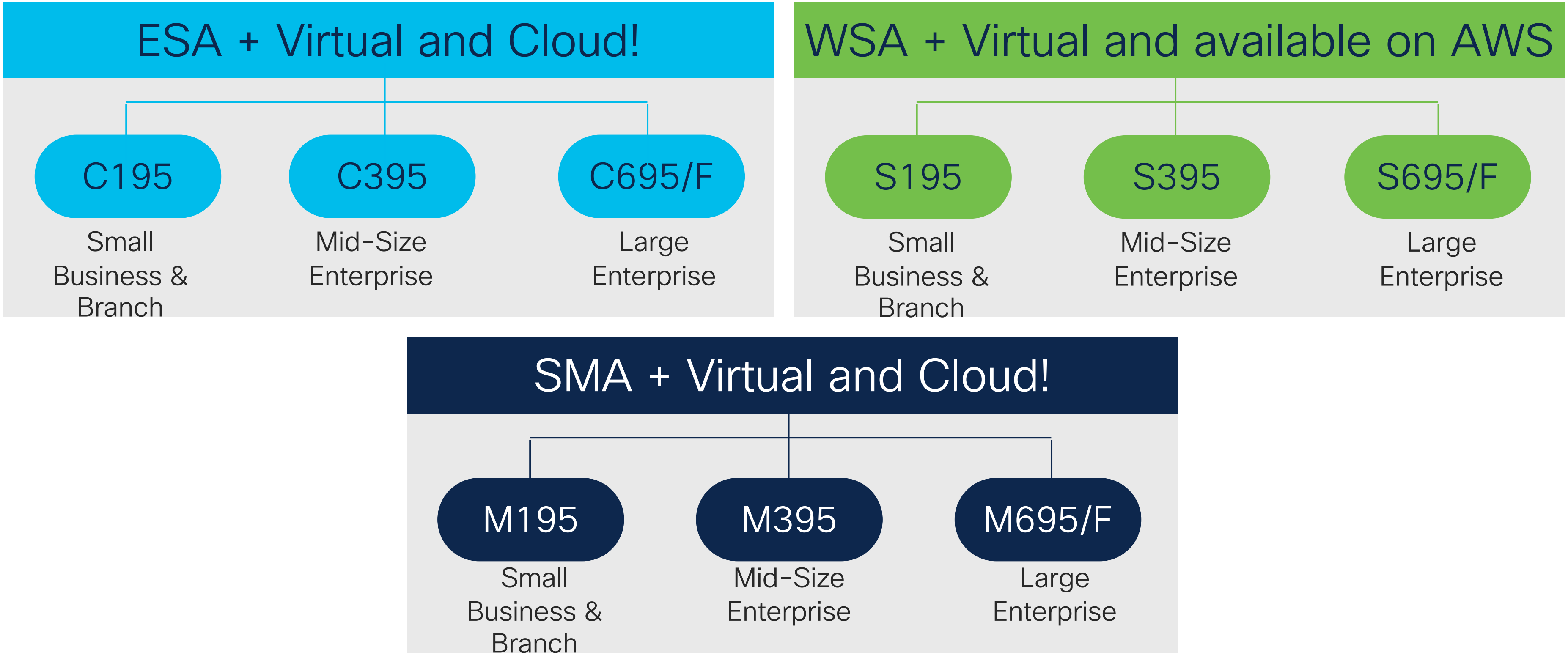
Outbound

Cisco Email Security with Data Loss Prevention and Encryption

+

Cisco Domain Protection

Cisco Content Security Product Family Tree



ESA + Virtual and Cloud!

- C195 – Small Business & Branch
- C395 – Mid-Size Enterprise
- C695/F – Large Enterprise

WSA + Virtual and available on AWS

- S195 – Small Business & Branch
- S395 – Mid-Size Enterprise
- S695/F – Large Enterprise

SMA + Virtual and Cloud!

- M195 – Small Business & Branch
- M395 – Mid-Size Enterprise
- M695/F – Large Enterprise

Overview SMA API’s

Overview SMA API’s

- Email related API’s:
    - Reporting API
    - Message Tracking API
    - Quarantine API
- Web related API’s:
    - Reporting API
    - Web tracking API

Example use cases

Example Use Cases SMA API’s

- Email:
  - Searching for Messages and Message Details
  - Rejected Connections
  - DLP Details
  - AMP Details
  - Deleting or releasing messages from Quarantine
  - Adding, Editing, and Appending Safelist and Blocklist Entries
- Web:
  - Layer 4 monitor details
  - Retrieving web usage for a particular user or for all users using filters

Conclusion

References

- Guide to SMA API's: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12.html
- Guide to ESA API's: https://www.cisco.com/c/en/us/td/docs/security/esa/esa_all/esa_api/esa_api_12-0/b_ESA_API_Getting_Started_Guide_12-0/b_ESA_API_Getting_Started_Guide_chapter_00.html

Thank you

Possibilities

#CiscoLive | #DevNetDay

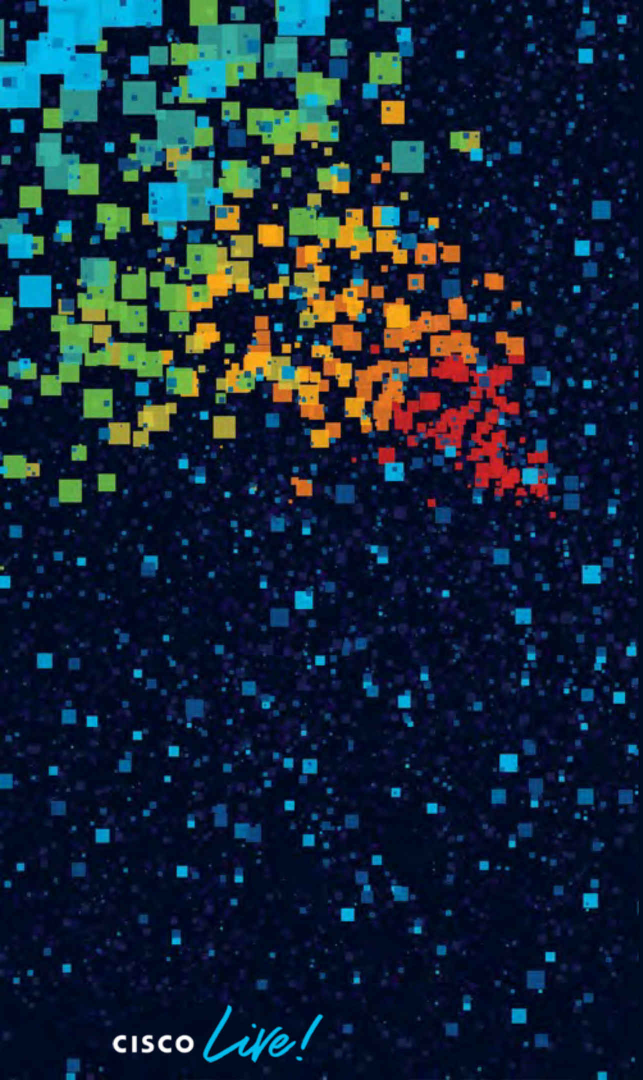
Possibilities

#CiscoLive | #DevNetDay

Security Management Appliance API’s

Security Cisco Live Virtual DevNet Day

Christopher van der Made
@Chrisco_DevNet



Agenda

- Intro to SMA
- Overview SMA API’s
- Example use cases
- Conclusion

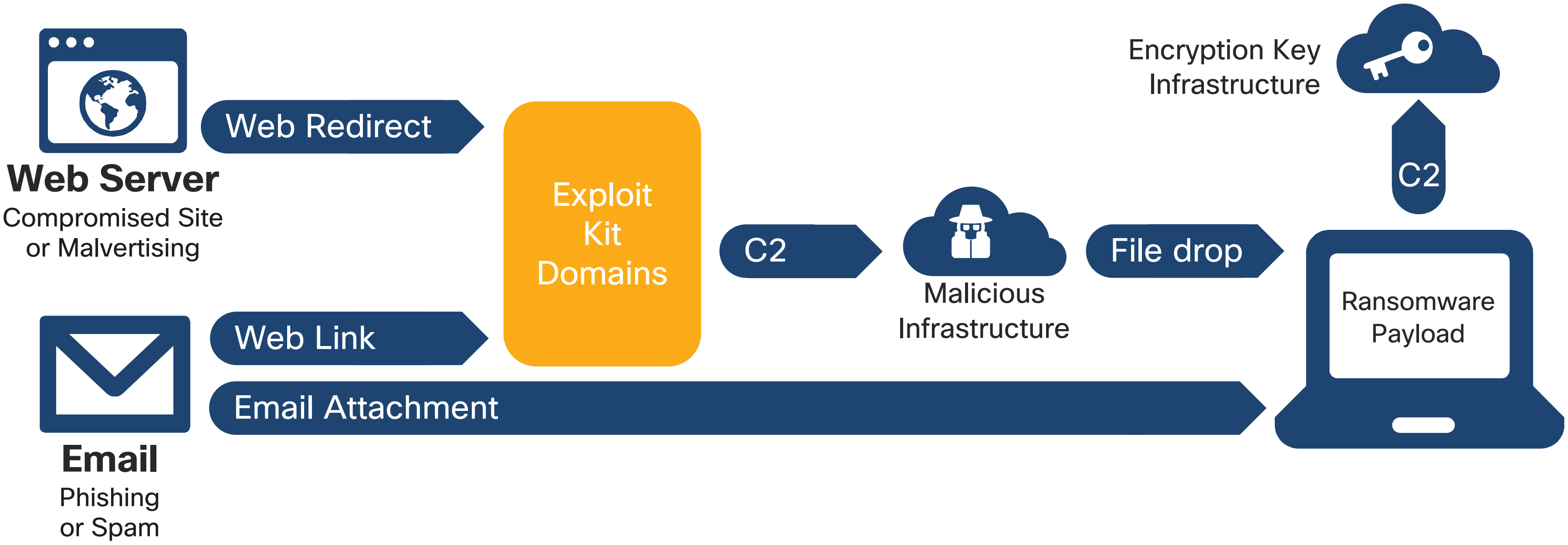
Intro to SMA

Did You Know?

Over 99%

of malware is sent by either web server or email

Ransomware Email and Web Delivery



Cisco Web Security Appliance Provides...

Integrations

Strong Effective Protection

Flexible Deployment

Cisco WSA

Granular Control

Detailed Reporting

Inbound and Outbound Protection

Inbound

Outbound

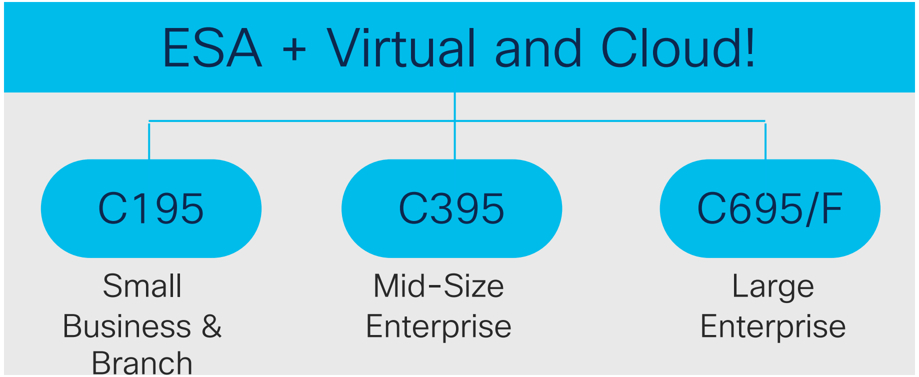
Cisco Email Security with Advanced Malware Protection and Threat Grid

Cisco Advanced Phishing Protection

Cisco Email Security with Data Loss Prevention and Encryption

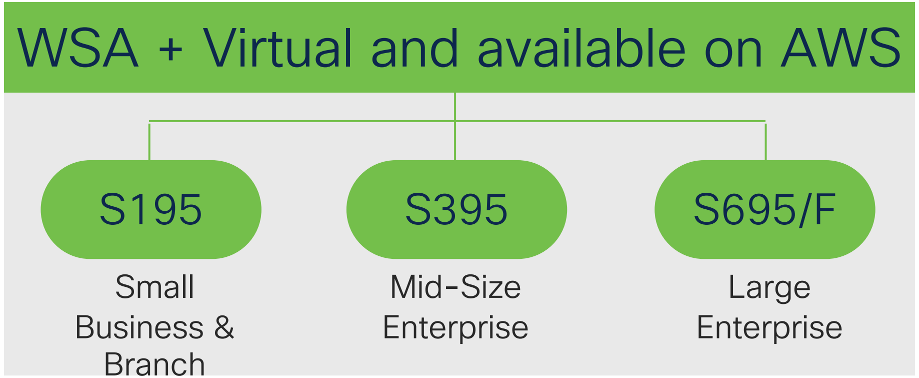
Cisco Domain Protection

Cisco Content Security Product Family Tree



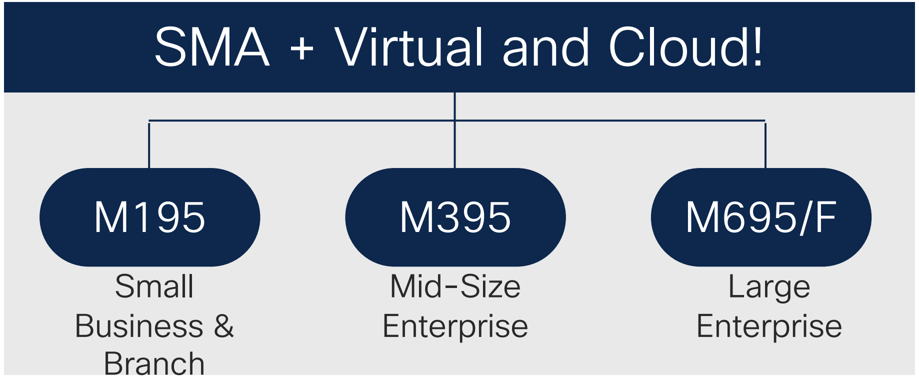
ESA + Virtual and Cloud!

- C195 – Small Business & Branch
- C395 – Mid-Size Enterprise
- C695/F – Large Enterprise



WSA + Virtual and available on AWS

- S195 – Small Business & Branch
- S395 – Mid-Size Enterprise
- S695/F – Large Enterprise



SMA + Virtual and Cloud!

- M195 – Small Business & Branch
- M395 – Mid-Size Enterprise
- M695/F – Large Enterprise

Overview SMA API's

Overview SMA API’s

- Email related API’s:
  - Reporting API
  - Message Tracking API
  - Quarantine API
- Web related API’s:
  - Reporting API
  - Web tracking API

Example use cases

Example Use Cases SMA API’s

- Email:
  - Searching for Messages and Message Details
  - Rejected Connections
  - DLP Details
  - AMP Details
  - Deleting or releasing messages from Quarantine
  - Adding, Editing, and Appending Safelist and Blocklist Entries
- Web:
  - Layer 4 monitor details
  - Retrieving web usage for a particular user or for all users using filters

Conclusion

References

- Guide to SMA API's: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12.html
- Guide to ESA API's: https://www.cisco.com/c/en/us/td/docs/security/esa/esa_all/esa_api/esa_api_12-0/b_ESA_API_Getting_Started_Guide_12-0/b_ESA_API_Getting_Started_Guide_chapter_00.html

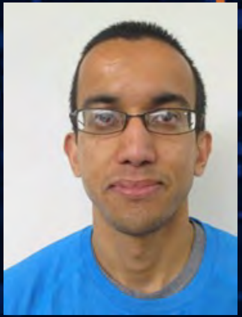
Thank you

Possibilities

#CiscoLive | #DevNetDay

Jared Smith
Principal Engineer

Firepower & Firepower APIs



Yatish Joshi
Technical Leader
@tryjoshi

Next Generation Firewall

- Industry Leading Next Generation Firewall

Key Features

- VPN
- Threat Protection
- TLS Decryption
- Identity
- Talos Threat Intelligence

NGFW Management

Firepower Management Center

- Multi-device
- Full functionality (Netops + SecOps)
- On-premise
- UI/REST API

Cisco Defense Orchestrator

- Multi-device
- Cloud
- UI/REST API

Firepower Device Manager

- Single Device
- On-Premise
- UI/REST API

Coexist
NetOps Focus
Simple SecOps

Firepower Threat Defense (FDM)

Session Overview:

- Introduction Firepower Threat Defense
- Introduction to Firepower Threat Defense REST API
- Demo Ansible
- Demo Import/Export API

Firepower Management Center (FMC)

Session Overview:

- Introduction to Firepower Management Center
- Features and capabilities
- Threat detection
- Firepower APIs

Stealthwatch APIs

DevNet Day

Kyle Winters
Technical Marketing Engineer, CX Technology & Transformation Group
@kyle_m_winters

Thank you

Stealthwatch APIs

Kyle Michael Winters – Technical Marketing Engineer
@kyle_m_winters

What is Cisco Stealthwatch?

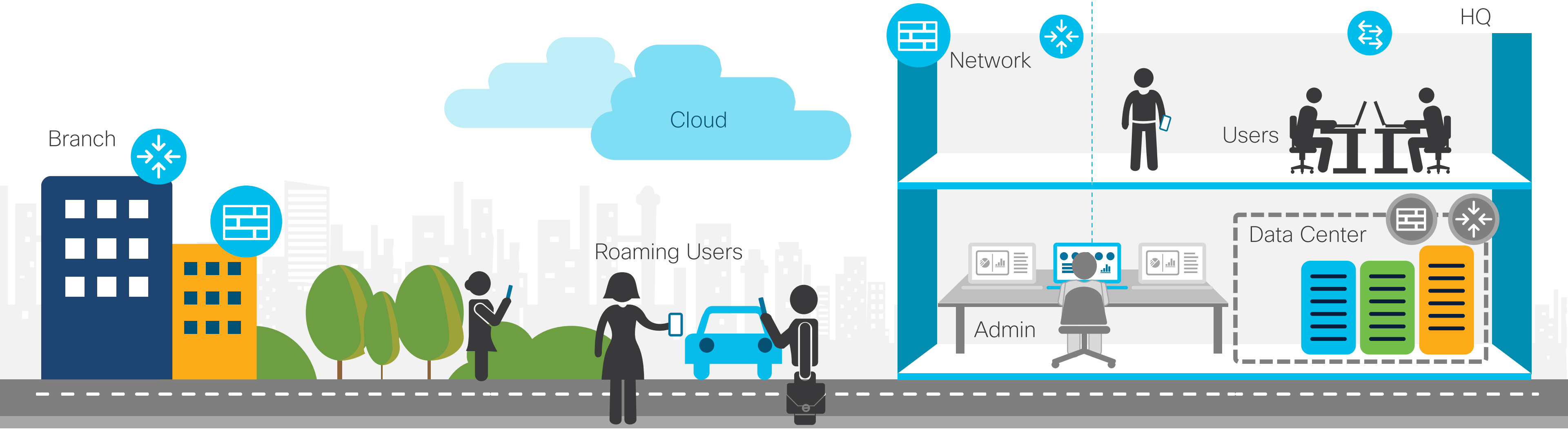
KNOW every host

SEE every conversation

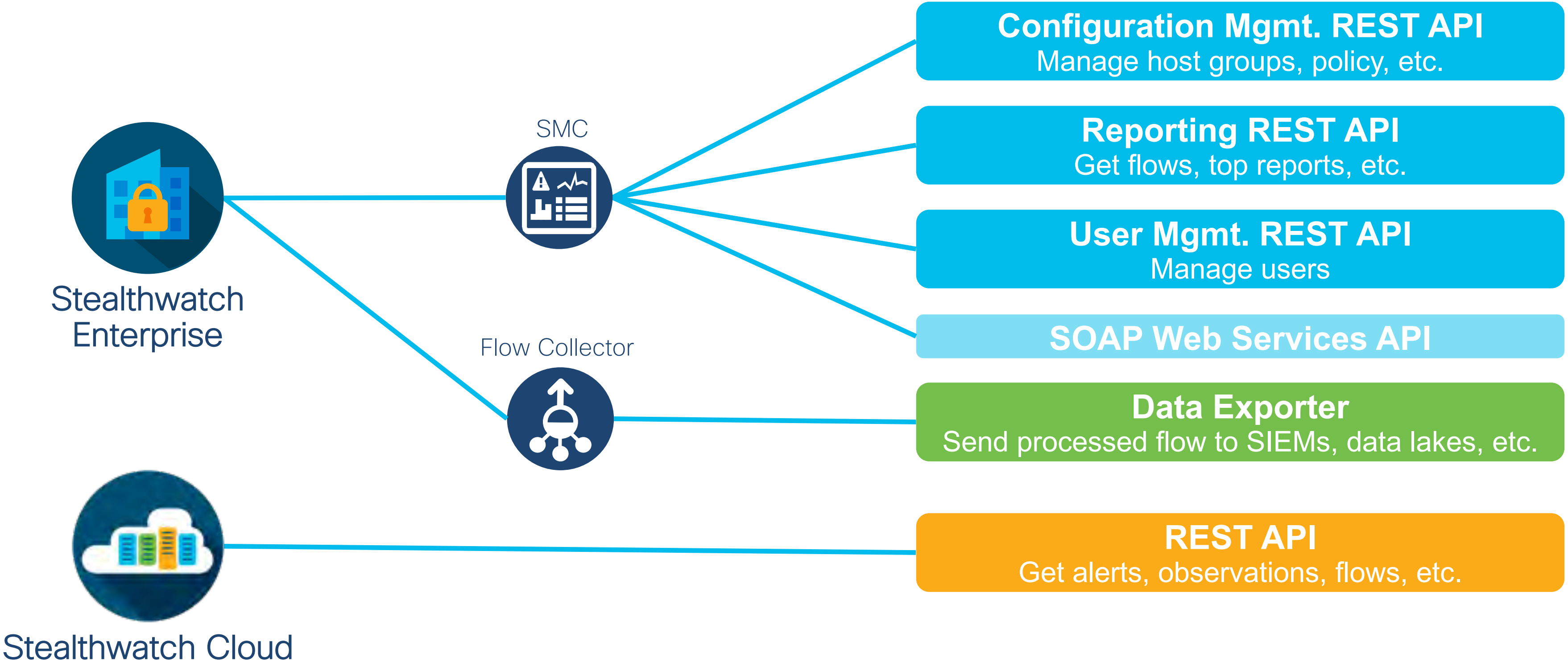
Understand what is **NORMAL**

Be alerted to **CHANGE**

Respond to **THREATS** quickly



Stealthwatch API Capabilities



Configuration Mgmt. REST API
Manage host groups, policy, etc.

Reporting REST API
Get flows, top reports, etc.

User Mgmt. REST API
Manage users

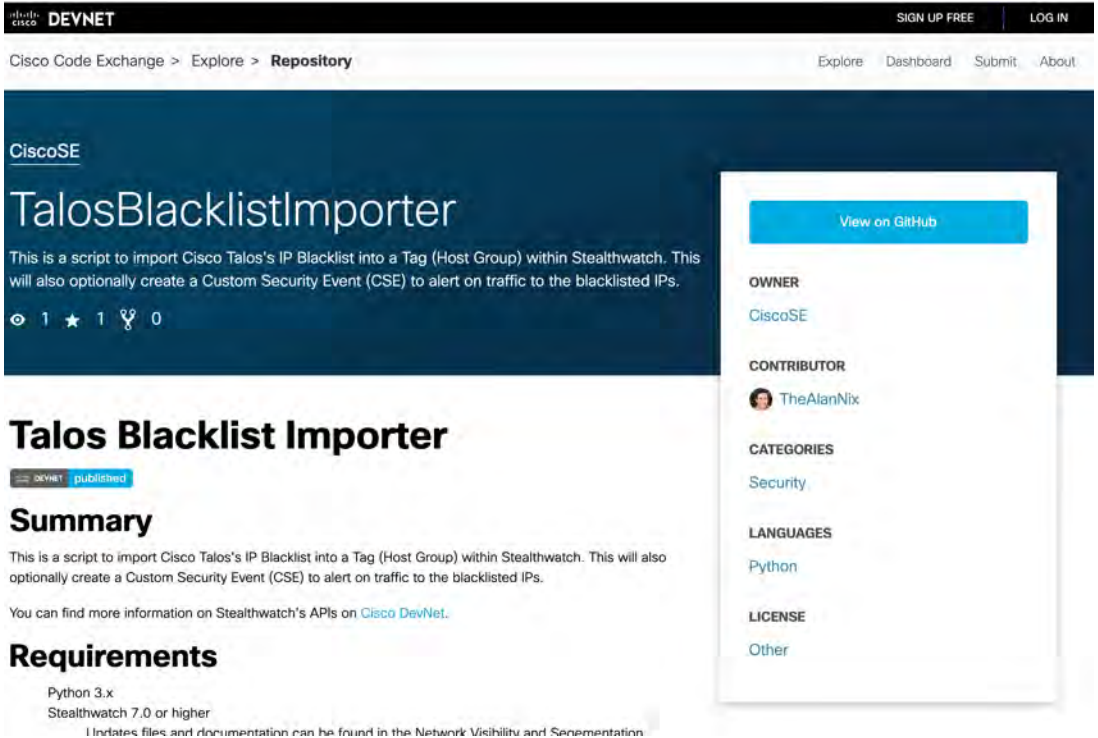
SOAP Web Services API

Data Exporter
Send processed flow to SIEMs, data lakes, etc.

REST API
Get alerts, observations, flows, etc.

Demo: Talos Blacklist Importer

- Imports the IP Blacklist from Cisco Talos into a Stealthwatch host group (tag)
- Creates a Custom Security Event (CSE) to alert on traffic with Blacklisted IP (Optional)
- Available through DevNet, hosted on GitHub, and free to use



Cisco Code Exchange > Explore > **Repository**

CiscoSE

TalosBlacklistImporter

This is a script to import Cisco Talos's IP Blacklist into a Tag (Host Group) within Stealthwatch. This will also optionally create a Custom Security Event (CSE) to alert on traffic to the blacklisted IPs.

◉ 1 ★ 1 ⑂ 0

OWNER
CiscoSE

CONTRIBUTOR
TheAlanNix

CATEGORIES
Security

LANGUAGES
Python

LICENSE
Other

Talos Blacklist Importer

DEVNET published

Summary

This is a script to import Cisco Talos's IP Blacklist into a Tag (Host Group) within Stealthwatch. This will also optionally create a Custom Security Event (CSE) to alert on traffic to the blacklisted IPs.

You can find more information on Stealthwatch's APIs on Cisco DevNet.

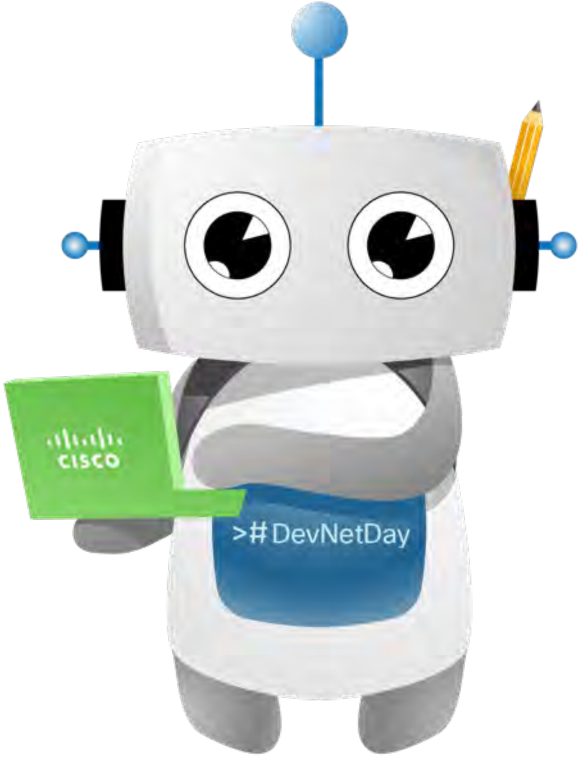
Requirements

Python 3.x
Stealthwatch 7.0 or higher
Updates files and documentation can be found in the Network Visibility and Segmentation

Explore More

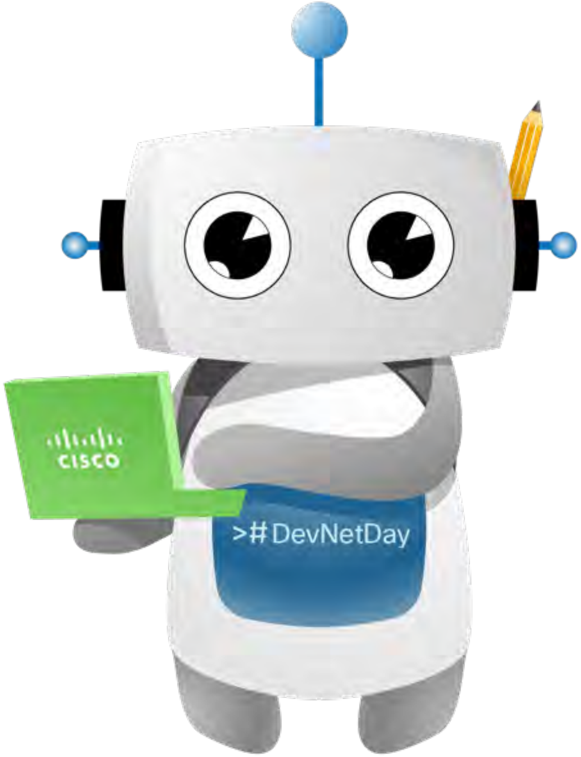
developer.cisco.com/stealthwatch

- Extensive APIs provided by Stealthwatch are now easily accessible on DevNet:
  - Stealthwatch Enterprise REST API documentation
  - Stealthwatch Cloud REST API documentation
- Additional resources to help developers get started:
  - Code Exchange for Stealthwatch for sample scripts, postman collections, and useful scripts and software capabilities
  - Cisco Stealthwatch API Forum specifically for API developers to ask and answer questions related to Stealthwatch APIs
  - DevNet Stealthwatch Enterprise Sandbox to test API capabilities in a 24x7 lab environment
  - Stealthwatch Cloud Free 60-day Trial to test API capabilities in a demo environment



Explore More

- Learn more about Stealthwatch API capabilities at Cisco Live US 2020!
    - Coming in July: *DEVNET-2008 - Using Stealthwatch APIs to Integrate, Automate, and Orchestrate*



Thank you

DevNet Security Certification

Krishan Veer Developer Advocate, Technical Leader – Security
@ Cisco CX
#veeratcisco

Introducing Cisco's expanded certification suite

Cisco Certification Program offerings launched Feb. 24, 2020

	Associate Level	Specialist Level	Professional Level	Expert Level
Engineering	CISCO CERTIFIED CCNA	CISCO CERTIFIED SPECIALIST	CISCO CERTIFIED CCNP	CISCO CERTIFIED CCIE
Software	CISCO CERTIFIED DEVNET Associate	CISCO CERTIFIED DEVNET SPECIALIST	CISCO CERTIFIED DEVNET Professional	Future Offering CISCO CERTIFIED DEVNET Expert

How our program is evolving

Associate Level

CISCO CERTIFIED CCNA

One Exam

CISCO CERTIFIED DEVNET Associate

One Exam

Specialist Level

CISCO CERTIFIED SPECIALIST

One Exam:
Every written proctored exam (except CCNA) = Cisco Certified Specialist

CISCO CERTIFIED DEVNET SPECIALIST

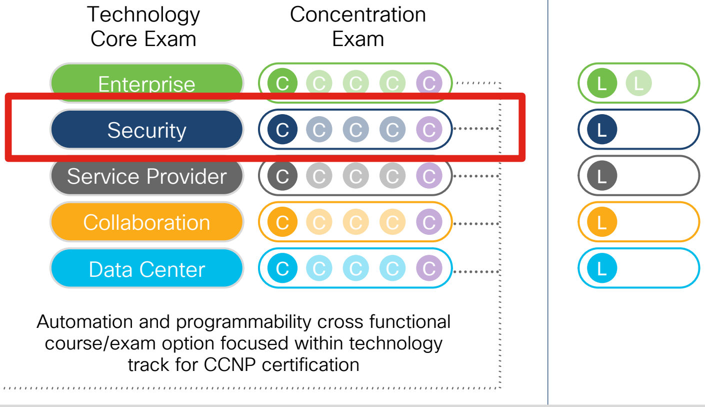
CISCO CERTIFIED DEVNET SPECIALIST

One Exam:
Every DevNet written, proctored exam (except Cisco Certified DevNet Associate) = Cisco Certified DevNet Specialist

Professional Level

CISCO CERTIFIED CCNP

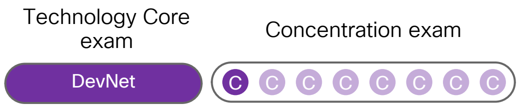
Two Exams:
1 concentration exam and 1 technology core in any order, but from the same track



Automation and programmability cross functional course/exam option focused within technology track for CCNP certification

CISCO CERTIFIED DEVNET Professional

Two Exams:
1 DevNet core and 1 concentration exam in any order, but from the DevNet track



Expert Level

CISCO CERTIFIED CCIE

Lab Exam

1 technology core and 1 CCIE lab in same track

CISCO CERTIFIED DEVNET Expert

Future Offering

Future offering

Training for new job roles
DevSecOps Engineer

Professional certification

CCNP Security

Technology concentrations

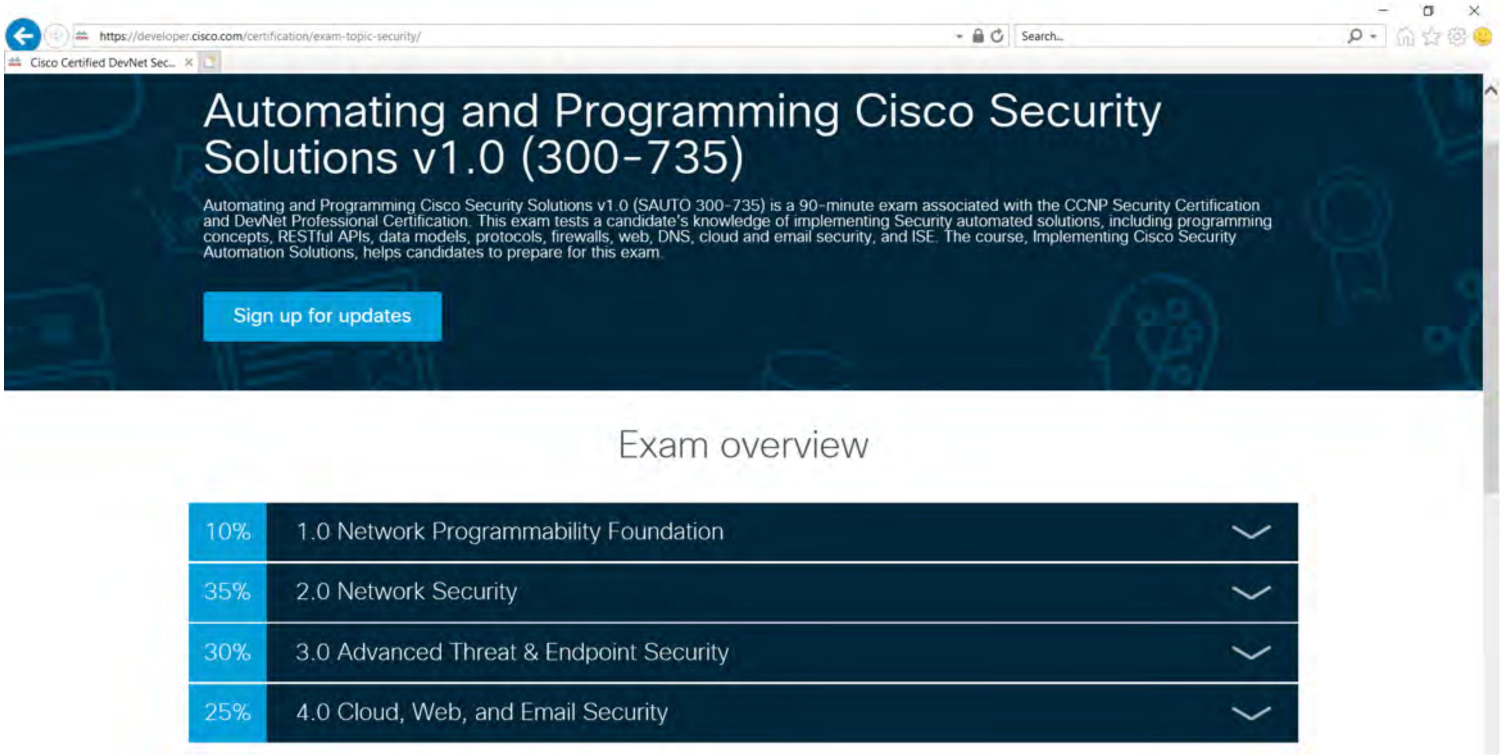
Cisco Specialist: Security
Automate security operations

Cisco DevNet Specialist: DevOps
Securely deploy applications

Cisco DevNet Specialist: Webex
Build chat bots for alerting and monitoring

Find more information on DevNet, CLN, Cisco.com

Find learning lab and sandbox offerings to start learning journey



https://developer.cisco.com/certification/exam-topic-security/
Search...
Cisco Certified DevNet Sec...

Automating and Programming Cisco Security Solutions v1.0 (300-735)

Automating and Programming Cisco Security Solutions v1.0 (SAUTO 300-735) is a 90-minute exam associated with the CCNP Security Certification and DevNet Professional Certification. This exam tests a candidate's knowledge of implementing Security automated solutions, including programming concepts, RESTful APIs, data models, protocols, firewalls, web, DNS, cloud and email security, and ISE. The course, Implementing Cisco Security Automation Solutions, helps candidates to prepare for this exam.

Exam overview

10%	1.0 Network Programmability Foundation
35%	2.0 Network Security
30%	3.0 Advanced Threat & Endpoint Security
25%	4.0 Cloud, Web, and Email Security

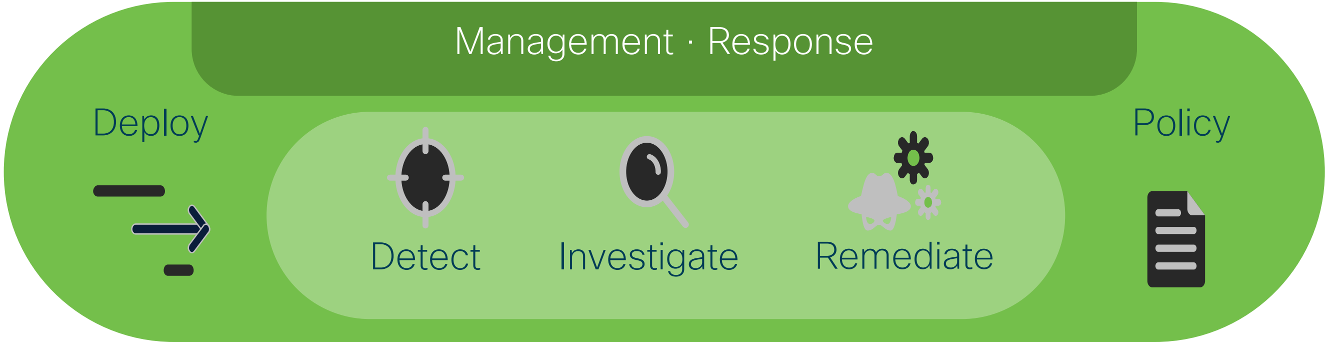
developer.cisco.com/certification cisco.com/nextlevel

Your Next Steps

3 things you can do today to start getting ready

1. Register with DevNet at developer.cisco.com/certification
2. Review the Exam Topics and learn what skills you will need to prepare for certification
3. Find the DevNet learning labs, videos and sandboxes that align to your learning goals

API as a foundation for modern security solutions



Management · Response

Deploy

Detect

Investigate

Remediate

Policy