Networking Academy

Programmability Webinar Series with DevNet

Session 7: Before, During, & After a Security Attack

Speaker: Krishan Veer

Hostess: Kara Sullivan

Jointly presented by DevNet & NetAcad

30 April, 2019

Welcome to the 7th session of the Programmability with Cisco DevNet webinar series

- Use the Q and A panel to ask questions.
- Use the Chat panel to communicate with attendees and panelists.
- A link to a recording of the session will be sent to all registered attendees.
- Please take the feedback survey at the end of the webinar.

The Webinar Series

Date	Topic
Oct'18	Networking with Programmability is Easy
Oct'18	A Network Engineer in the Programmable Age
Nov'18	Software Defined Networking and Controllers
Jan'19	Adding API Skills to Your Networking Toolbox
Feb'19	The New Toolbox of a Networking Engineer
Mar'19	Program Networking Devices using their APIs
Apr'19	Before, During, and After a Security Attack
May'19	Play with Linux & Python on Networking Devices
Jun'19	Automate your Network with a Bot

All Series Details can be Found @ http://bit.ly/devnet2

The Webinar Series – Raffle & Certificates

Raffle

- ✓ We will be raffling off a total of 15 Amazon gift cards in the amount of $25 US dollars at the end of this series.*
- ✓ 10 Amazon gift cards in the amount of $25 US dollars raffled off to everyone who participates in all of the live sessions
- ✓ 5 Amazon gift cards in the amount of $25 US dollars raffled off to everyone who participates in all of the sessions by either attending the live sessions or viewing/downloading the recording (can be a combination of the two in this raffle).

* Please note that this is a raffle and not everyone who qualifies will receive a gift card. There will be a total of 15 winners.

Certificate of Participation

- ✓ There will be an opportunity to sign up for a Certificate of Participation at the end of this series.
- ✓ To qualify, you must have participated in all sessions of the series.
- ✓ You can do this by attending the live sessions, viewing the recordings, or a combination of the two.
- ✓ Certificates will not be given out for individual sessions, but for the series as a whole.

cisco DEVNET

Before, During, and After a Malware Attack

Automate your workflow using APIs

April 2019

Krishan Veer

Technical Leader and Developer Advocate – Security

Cisco DevNet

Twitter: @veeratcisco

Agenda

- Overview
- FIREPOWER REST API
- Threat Grid API
- Umbrella Investigate API
- AMP for Endpoints API
- ISE REST API
- Workflow
- Demo

Overview

- Zero day Security Context
- Understanding RESTful APIs across the Cisco security products
- Leveraging APIs to create a stronger security workflows
- Making intelligence actionable
- Introduction to a very simple 0day workflow

Organisations are embracing **digital transformation**

But the move to digital business has increased exposure to attacks

of organizations not "fully aware" of the devices accessing their network

2/3

all IP traffic

21B

IoT devices

of all traffic will be encrypted

Threats are constantly evolving and getting smarter

Motivated and targeted adversaries

Increased attack sophistication

Insider threats

data breach averages

191 days time to detection

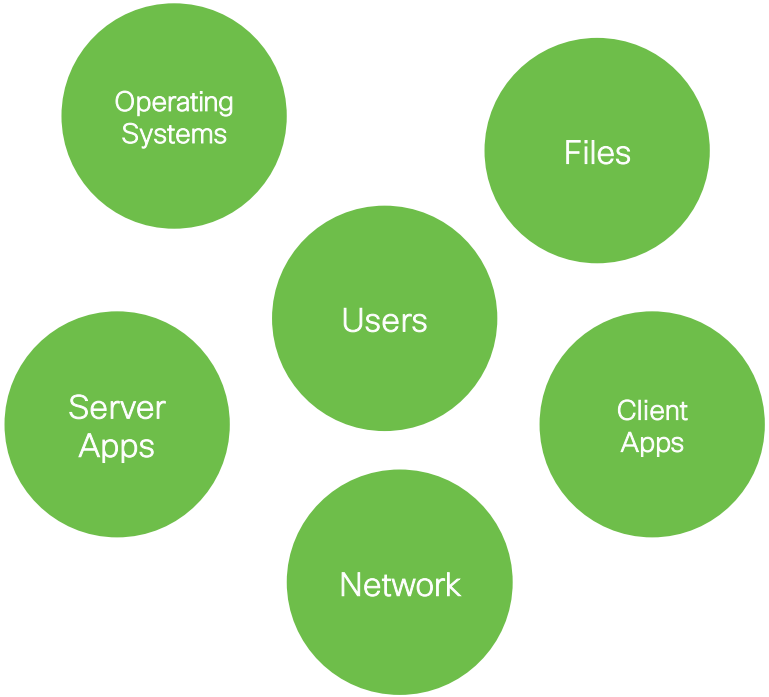
66 days time to contain

How do I start my defense!

Buy all Cisco security stuff!!!

Just Kidding... ☺

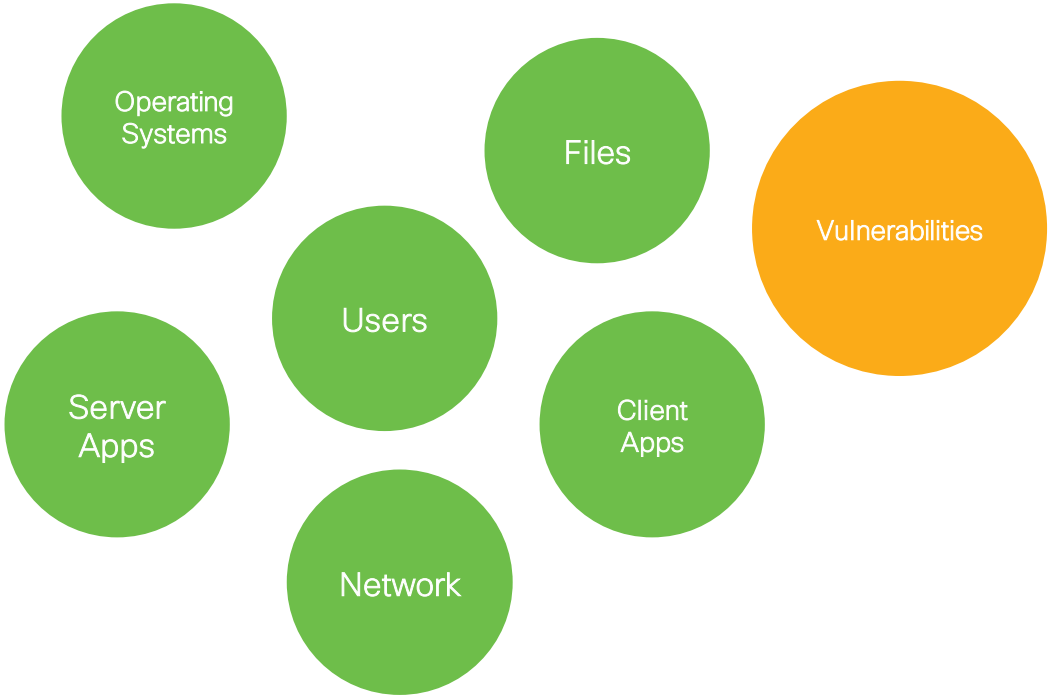
Know Your Network



Understand Its Weakness

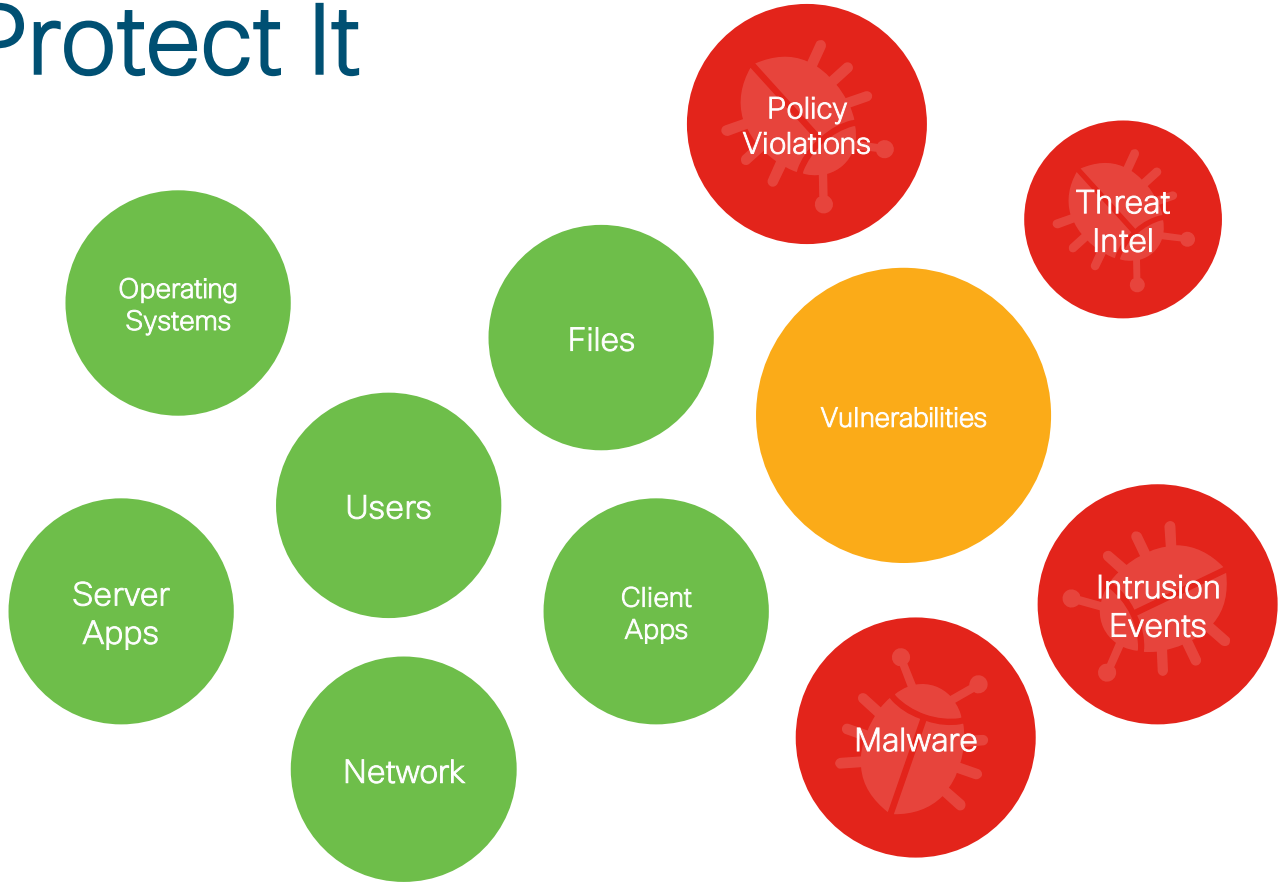
Hire Awesome Security Team!!!

Invest in People!!!



And Then Protect It

Give best tools
to your security
team!
&
Segment,
Segment,
Segment,
….
..
….
Segment



Don’t forget “Segment”….

Let's baseline terminology

Zero Day Attack

A zero-day attack hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

Zero Day worms

Zero Day Malware

Zero Day Virus

Zero-day = Unfixed Vulnerability + Working Exploit + External Knowledge

Developers have Zero time to fix the vulnerability

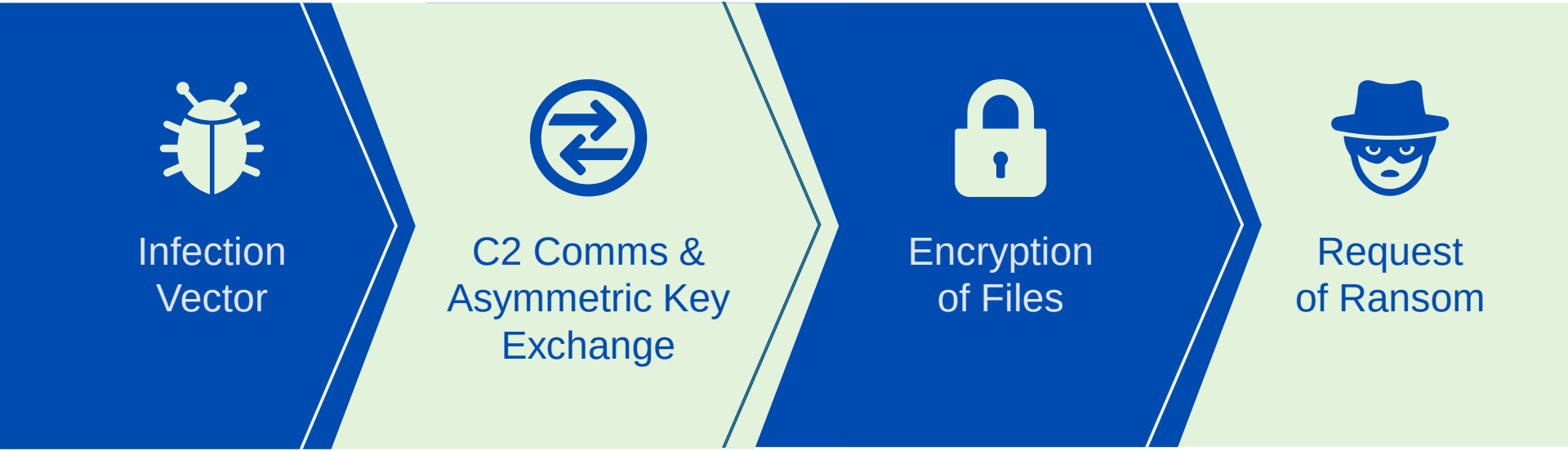
```
root@kali:~# nmap -sV -T5 192.168.110.153

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-06-26 21:35 EDT
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.20% done; ETC: 21:36 (0:00:25 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.110.153
Host is up (0.00029s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
443/tcp open   ssl/http Apache httpd
MAC Address: 00:0C:29:68:81:D6 (VMware)
```

> THE ATTACK!!!

```
root@kali:~# wpscan --url http://192.168.110.153/wp-login.php --wordlist=/root/Desktop/mrrobot/fsocity.dic --username elliot --wp-content-dir /wp-content

      WordPress Security Scanner by the WPScan Team
                      Version 2.8
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.110.153/wp-login.php/
[+] Started: Sun Jun 26 21:56:28 2016

[+] robots.txt available under: 'http://192.168.110.153/wp-login.php/robots.txt'
[!] The WordPress 'http://192.168.110.153/wp-login.php/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache
[+] Interesting header: SET-COOKIE: wordpress_test_cookie=WP+Cookie+check; path=/
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-POWERED-BY: PHP/5.5.29
[+] This site seems to be a multisite (http://codex.wordpress.org/Glossary#Multisite)

[i] WordPress version can not be detected

[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
  Brute Forcing 'elliot' Time: 00:02:54 <> (10000 / 858161)  1.16%  ETA: 04:06:  Brute Forcing 'elliot' Time: 00:02:54 <> (10001 / 858161)  1.16%  ETA:
```

Typical Ransomware Infection

- Problem: Enterprises can be taken hostage by malware that locks up critical resources



Ransomware frequently uses web and email

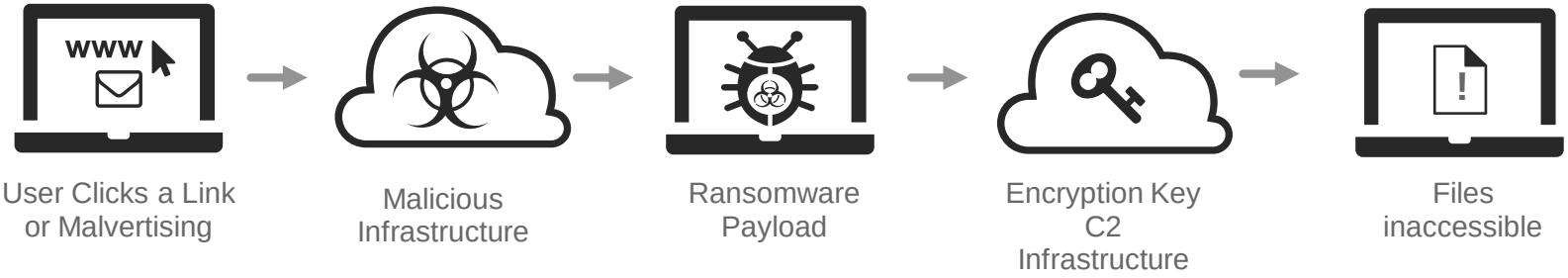
Ransomware takes control of targeted systems

Ransomware holds those systems ‘hostage’

Owner/company agrees to pay the ‘ransom’ (bitcoins) to free the system

How Ransomware Works–Most Variants Require All 5 Steps

WEB-BASED INFECTION



EMAIL-BASED INFECTION

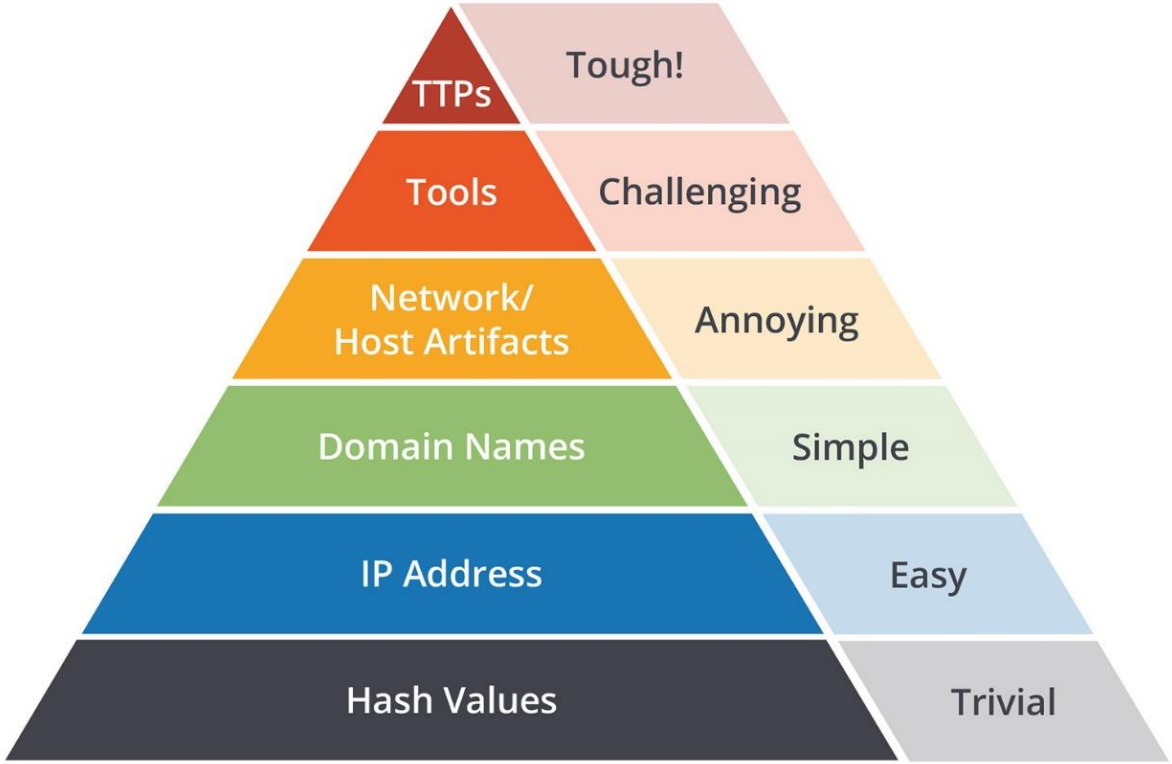
Most Ransomware Relies on C2 Callbacks

	Encryption Key				Payment MSG
NAME*	**DNS**	**IP**	**NO C2**	**TOR**	**PAYMENT**
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

*Top variants as of March 2016

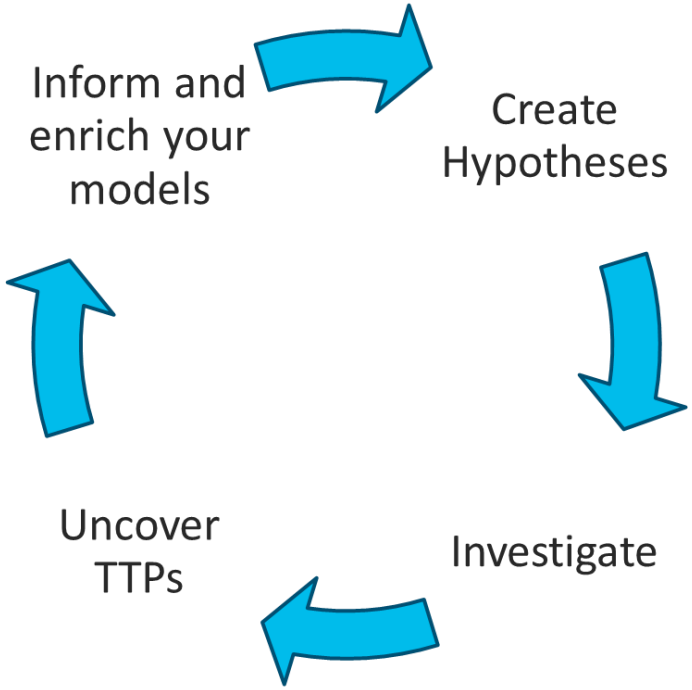
Detection/Hunt!!!

The Pyramid of pain… Hunt or Detect



Source: David J. Bianco, personal blog

The Loop… for detection and hunting

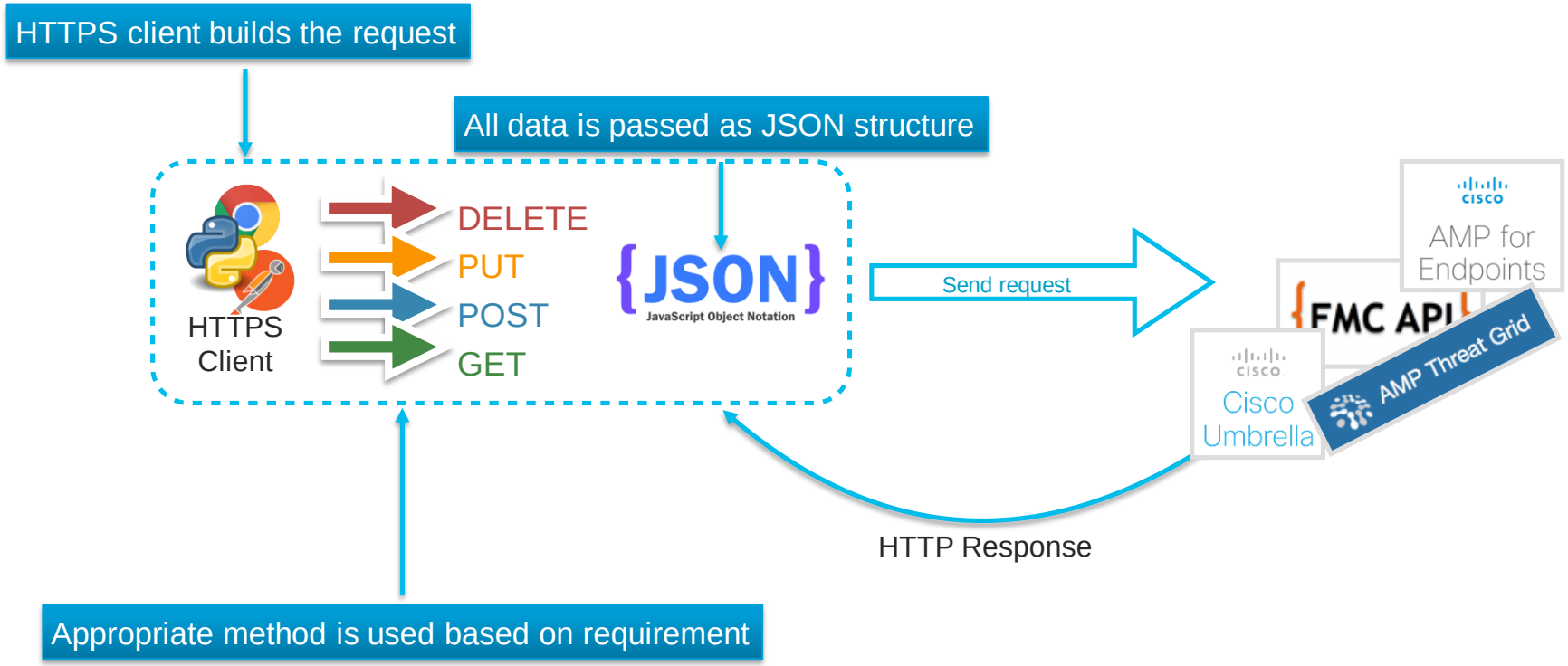


Source: Whitepaper - A framework for Cyber Threat hunting: By Sqrrl

Defense/Remediation

Goal

How REST API Works?



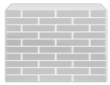
Cisco Firepower NGFW

Best of Breed

Threat-Focused stops vulnerability exploitation

High Availability

Intrusion Prevention



Firewall, VPN and Routing

Application Visibility and Control

Analytics and Visibility

Malware Protection

SSL Decrypt and Network Profiling

WWW

URL Filtering

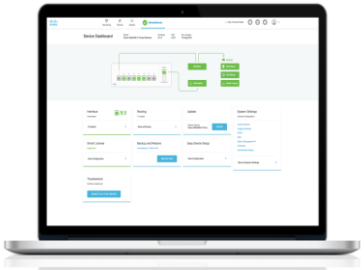
Identity-based Policy Control

Single OS + Single Management

Management Options

On-box

Firepower Device Manager

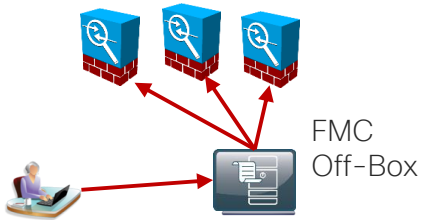


Enables easy on-box management of common security and policy tasks

Centralized

Firepower Management Centre

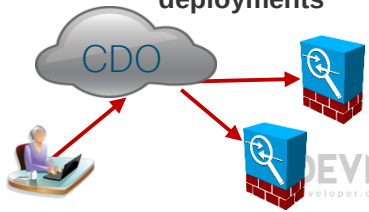
Enables comprehensive security administration and automation of multiple appliances



Cloud-based

Cisco Defence Orchestrator

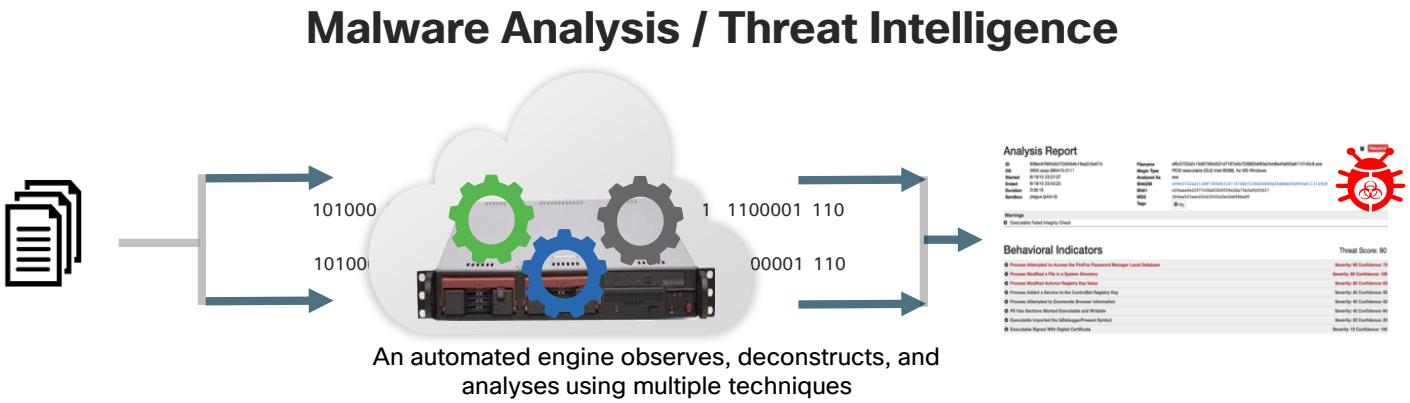
Enables centralised cloud-based policy management of multiple deployments



Firepower Management Centre (FMC) & (FDM) APIs

- Create, Read, Update, Delete
  - Objects
  - Policies
  - Interfaces
  - Devices
- Deployment

Threat Grid Overview

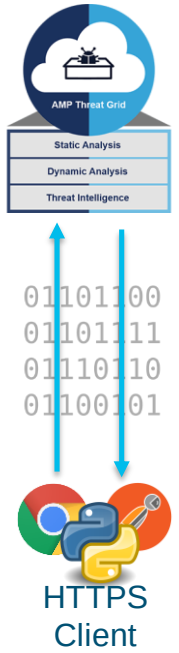


Malware Analysis
- Automated Analysis
  - Static
  - Dynamic
- Global Correlation

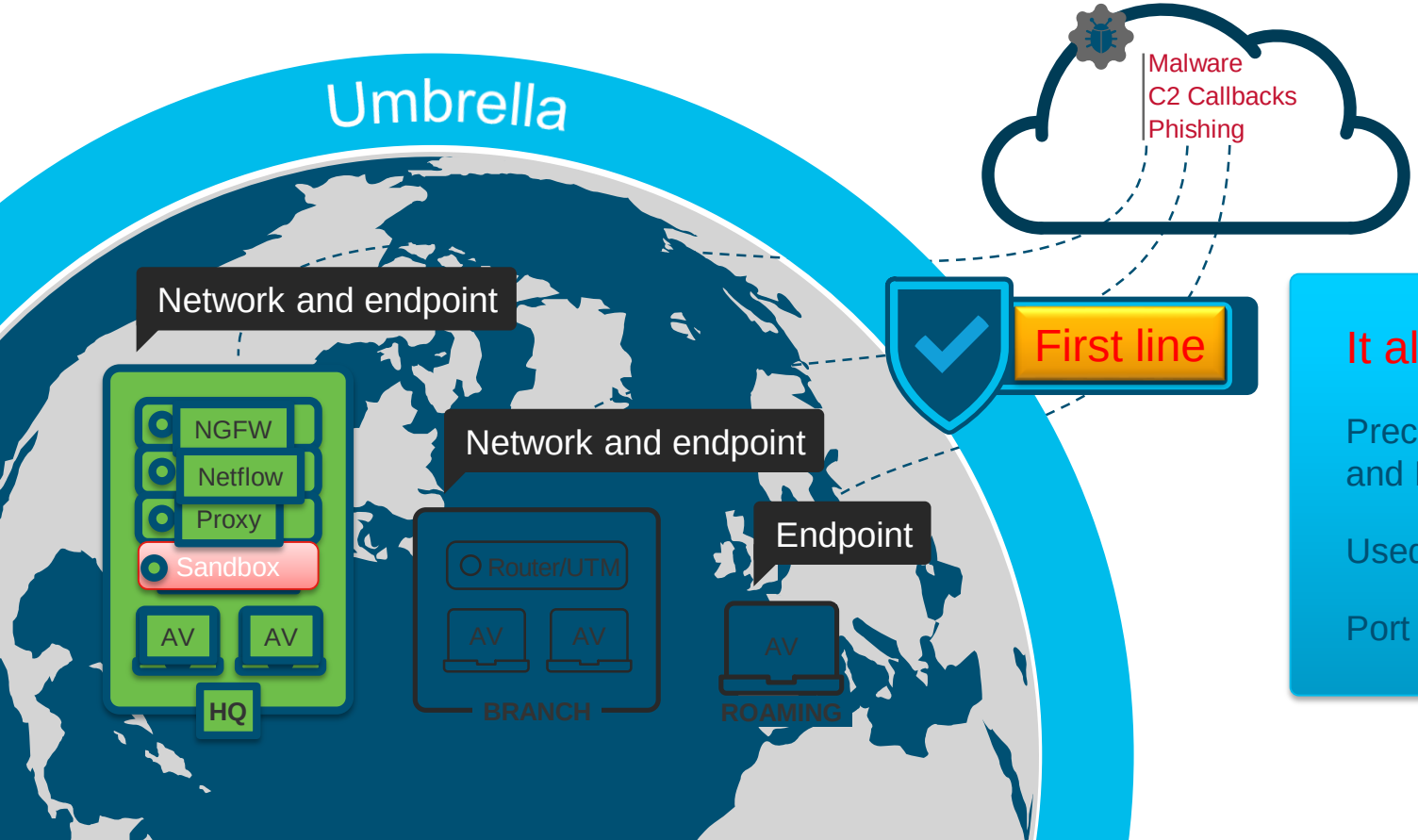
Threat Intelligence
- Threat Score
- Behaviour Indicators
- Observables
- Analysis Reports

Threat Grid

- Full featured API
- GET detailed reports for known/submitted files
- POST sample for dynamic analysis
- GET Threat Intelligence Feeds derived from collating sample data
- Account management



Where does Umbrella fit?



It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

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.

- Needed 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.*
  - *Determine co-occurring domains.*
  - *Find a historical record for this domain or IP address.*
  - *Query large numbers of domains quickly.*
  - *Add context to events in Splunk*.
- 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.
- Currently needed for Cisco Threat Response (this might change in the future).

Uncover the 1% with Cisco AMP for Endpoints

Stop Malware

Using multiple detection and protection mechanisms

Eliminate Blind Spots

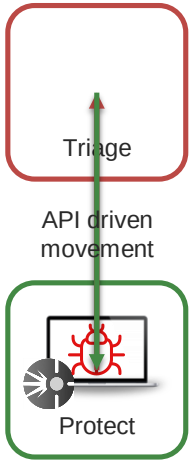
The network and endpoint, working together across all operating systems

Discover Unknown Threats

With proactive threat hunting

AMP for Endpoints – APIs

- Computer listing with connector details
- Move computers amongst groups
- Modify application black/whitelists
- Create and edit groups
- Gather filtered event data (custom reporting)



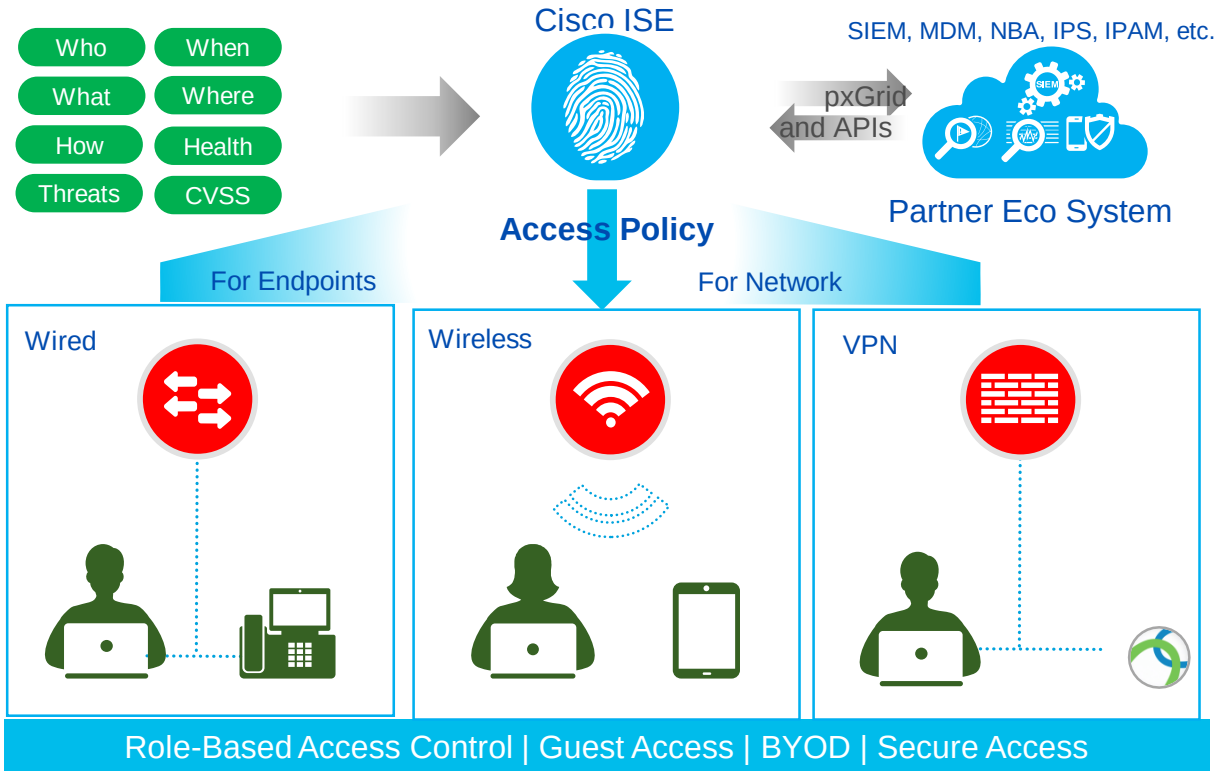
Cisco ISE and AnyConnect

Cisco ISE

Context-aware policy service, to control access and threats across wired, wireless, and VPN networks.

Cisco AnyConnect

Used for wired, wireless, and VPN access. Services include: Posture Assessment, Malware Protection, Web Security, Network Visibility and more



Talos -Powered Threat Intel

THREAT INTEL

1.5 MILLION
Daily Malware Samples

600 BILLION
Daily Email Messages

16 BILLION
Daily Web Requests

Honeypots

Open Source Communities

Vulnerability Discovery (Internal)

Product Telemetry

Internet-Wide Scanning

INTEL SHARING

Customer Data Sharing Programs

Service Provider Coordination Program

Open Source Intel Sharing

3rd Party Programs (MAPP)

Industry Sharing Partnerships (ISACs)

250+
Full Time Threat Intel Researchers

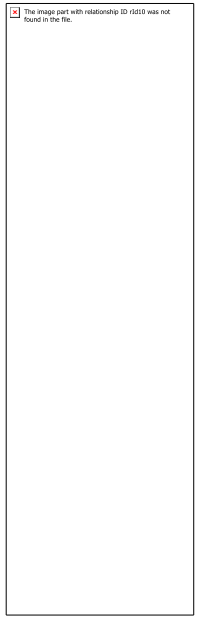
MILLIONS
Of Telemetry Agents

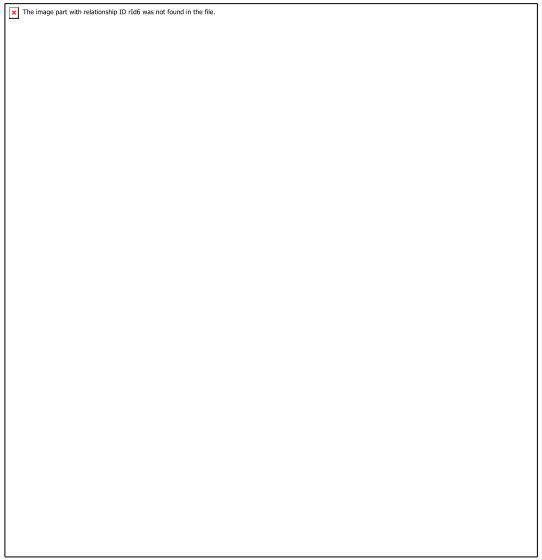
4
Global Data Centres

100+
Threat Intelligence Partners

1100+
Threat Traps

Mission



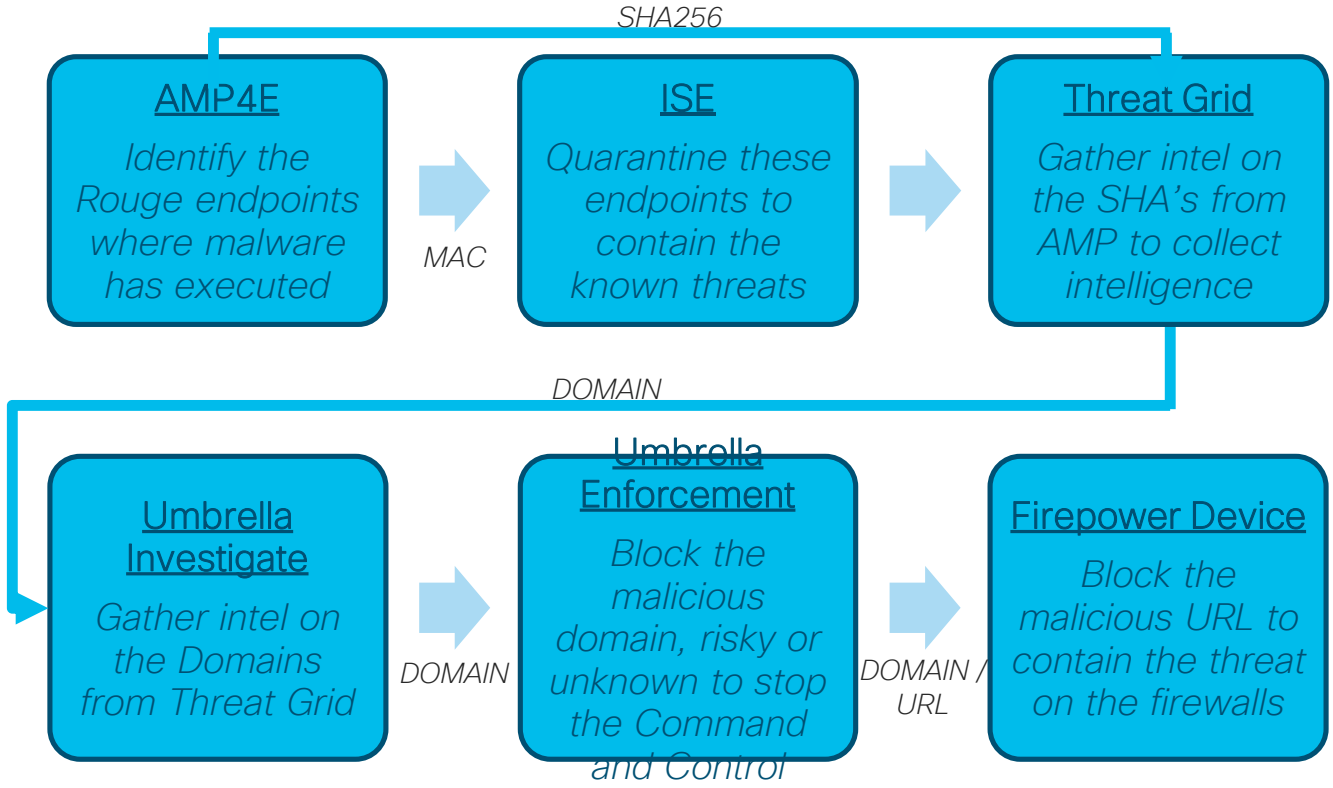


Automating the mitigation of a Zero Day Threat

We created a very simple workflow, using the Security APIs:

1. Identify the Rouge endpoints where malware has executed in our network using AMP for endpoints.
2. Use ISE to quarantine these endpoints to contain the known threats.
3. Use the AMP data to collect intelligence on the SHAs using Threat Grid.
4. Use Umbrella investigate to gather intelligence on the associated Domains and IPs found from Threat Grid.
5. Use Umbrella Enforcement to contain the threat and prevent the malware from executing, as it can't call home.
6. Use FDM APIs to enforce and contain the threat on the firewalls.

Zero-day threat investigation automation workflow



Prerequisite Checklist

- Python install with requests library
- ATOM or equivalent text editor
- Lets get coding….

Helpful Links

FMC API Guide

http://www.cisco.com/c/en/us/td/docs/security/firepower/620/api/REST/Firepower_REST_API_Quick_Start_Guide.html

Threat Grid API Guide

https://panacea.threatgrid.com/doc/main/api-getting-started.html

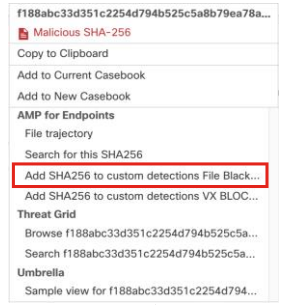
Umbrella Investigate Guide

https://docs.umbrella.com/developer/investigate-api/

AMP for Endpoints Guide

https://api-docs.amp.cisco.com/api_resources?api_host=api.amp.cisco.com&api_version=v1

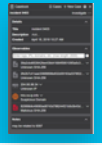
Cisco Threat Response: Workflow



1 Intel sources

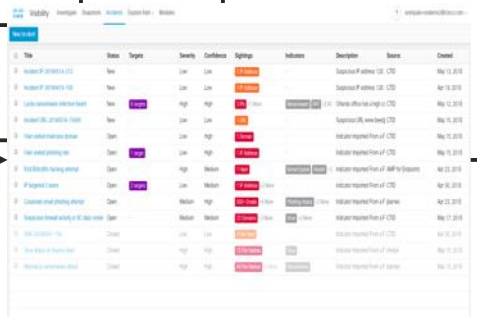
THREAT ROUNDUP

2 Casebook



3 Incidents

- NGFW
- AMP
- Stealthwatch



Threat Intelligence
What do you know about these observables (IP, Hash, URL, etc.)?

Threat Investigation
- Have we seen these observables?
- Which end-points interacted with the threat?

Virus Total

TALOS

ThreatGrid

AMP

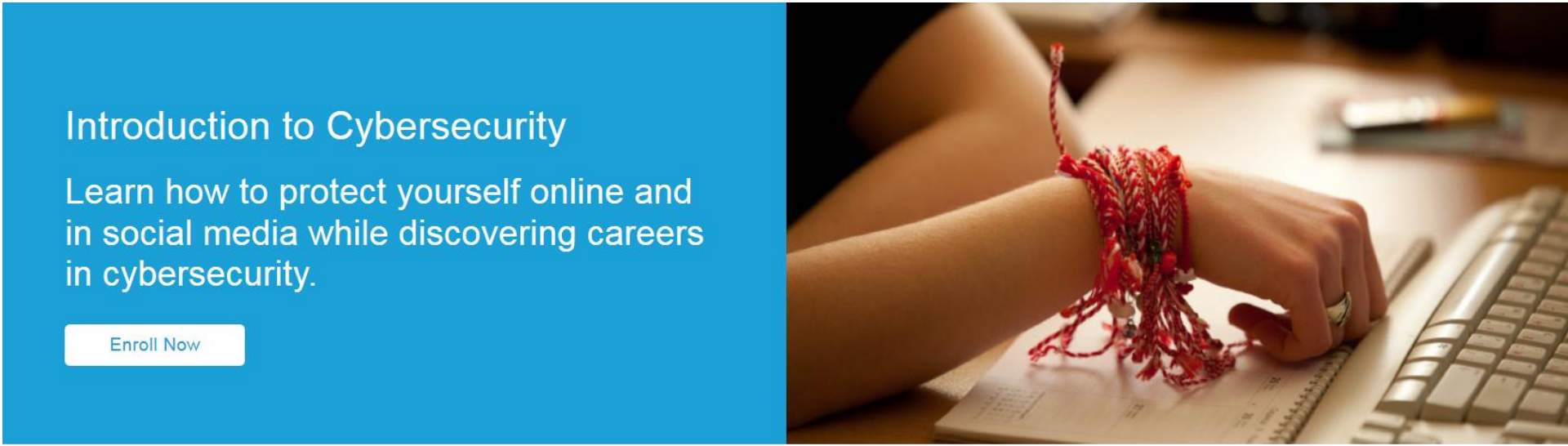
Umbrella

SMA

Stealth watch

NGFW

Intro to Cybersecurity Self-Enroll Course



You can enroll today to learn more @ http://bit.ly/introsecurity

The Webinar Series

Date	Topic
Oct'18	Networking with Programmability is Easy
Oct'18	A Network Engineer in the Programmable Age
Nov'18	Software Defined Networking and Controllers
Jan'19	Adding API Skills to Your Networking Toolbox
Feb'19	The New Toolbox of a Networking Engineer
Mar'19	Program Networking Devices using their APIs
Apr'19	Before, During, and After a Security Attack
May'19	Play with Linux & Python on Networking Devices
Jun'19	Automate your Network with a Bot

All Series Details can be Found @ http://bit.ly/devnet2

DEVNET

developer.cisco.com