
CISCO
You make possible

Threat Hunting Using APIs

Krishan Veer
Security Developer Advocate
Twitter: veeratcisco

DEVNET-2638

Barcelona | January 27-31, 2020

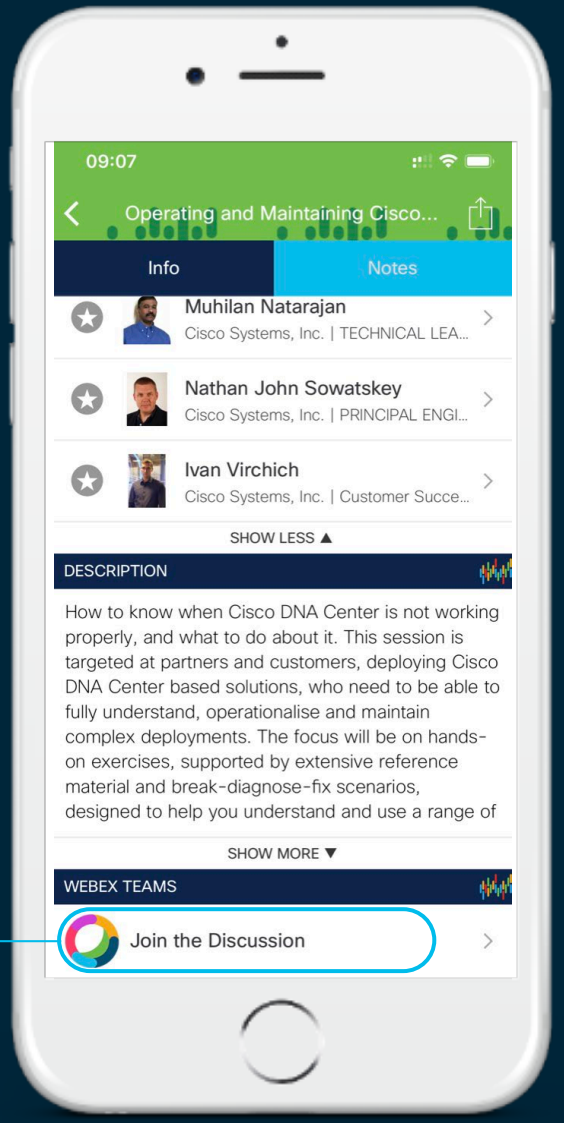
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

- Introduction to threat hunting
- Pyramid of pain
- Hunting File hashes
- Hunting IPs
- Hunting Domains
- Network and Host Artifacts
- Tools & TTPs
- Cisco Threat Response CTR

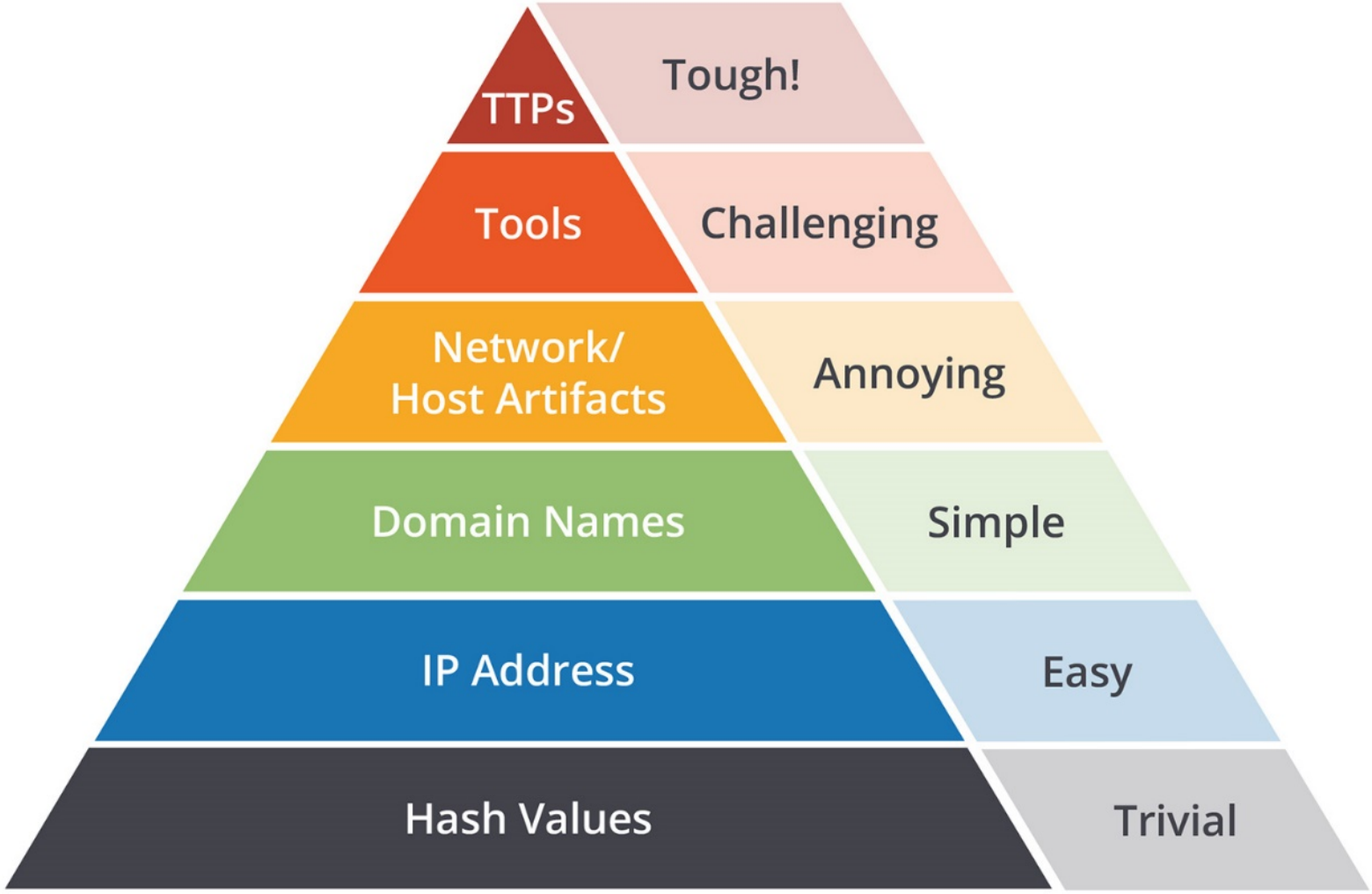
Threat Hunting

The process of proactively and iteratively searching through environments to detect and isolate previously unknown threats and breaches.

Why Do I Care?

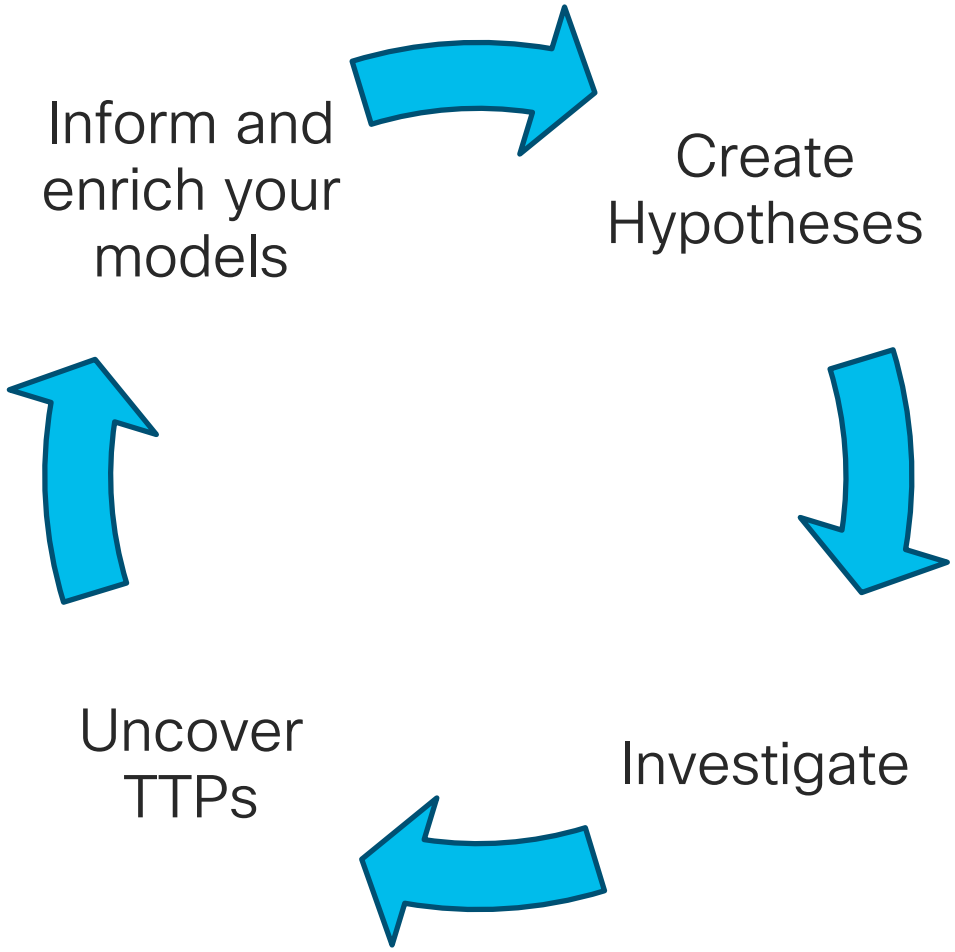
- Awesome new Career Path
- Proactively hunt threats Not just incident response
- Non stop fun!

The Pyramid of pain...



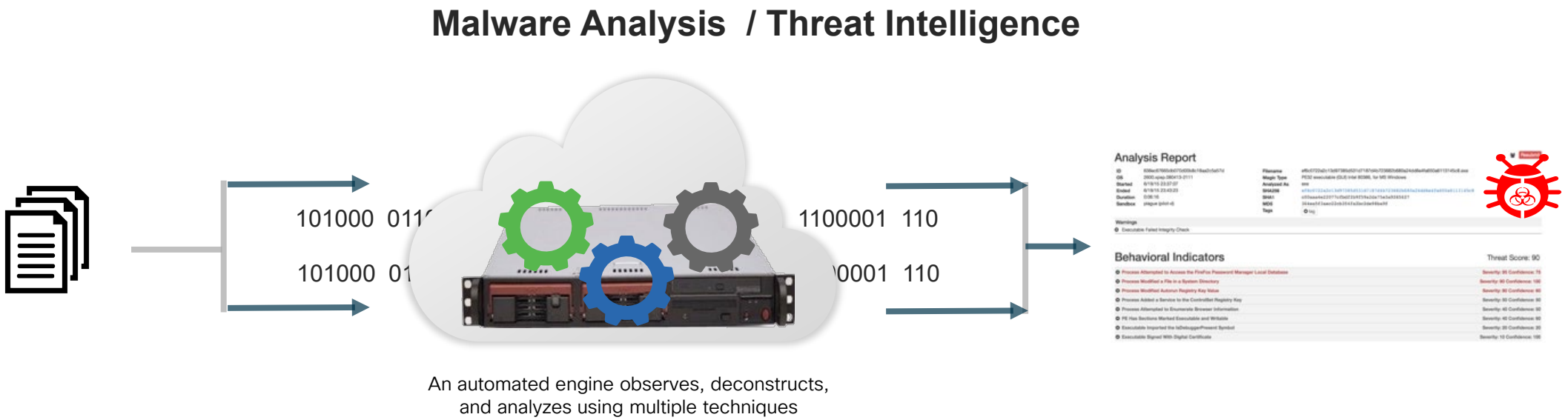
Source: David J. Bianco, personal blog

The Hunting Loop...



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

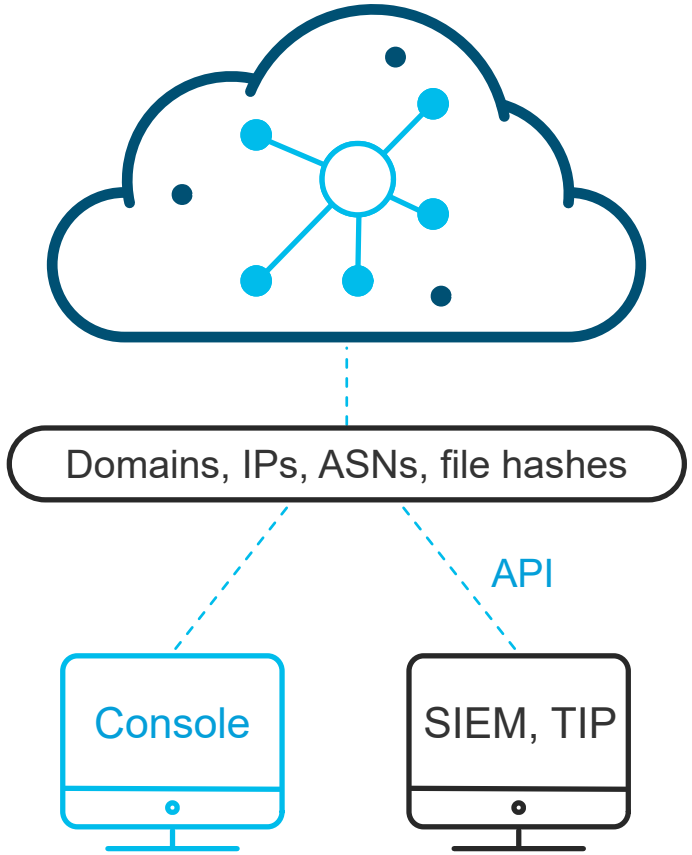
Threat Grid Overview



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

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

Cisco Umbrella Investigate: a powerful way to uncover threats



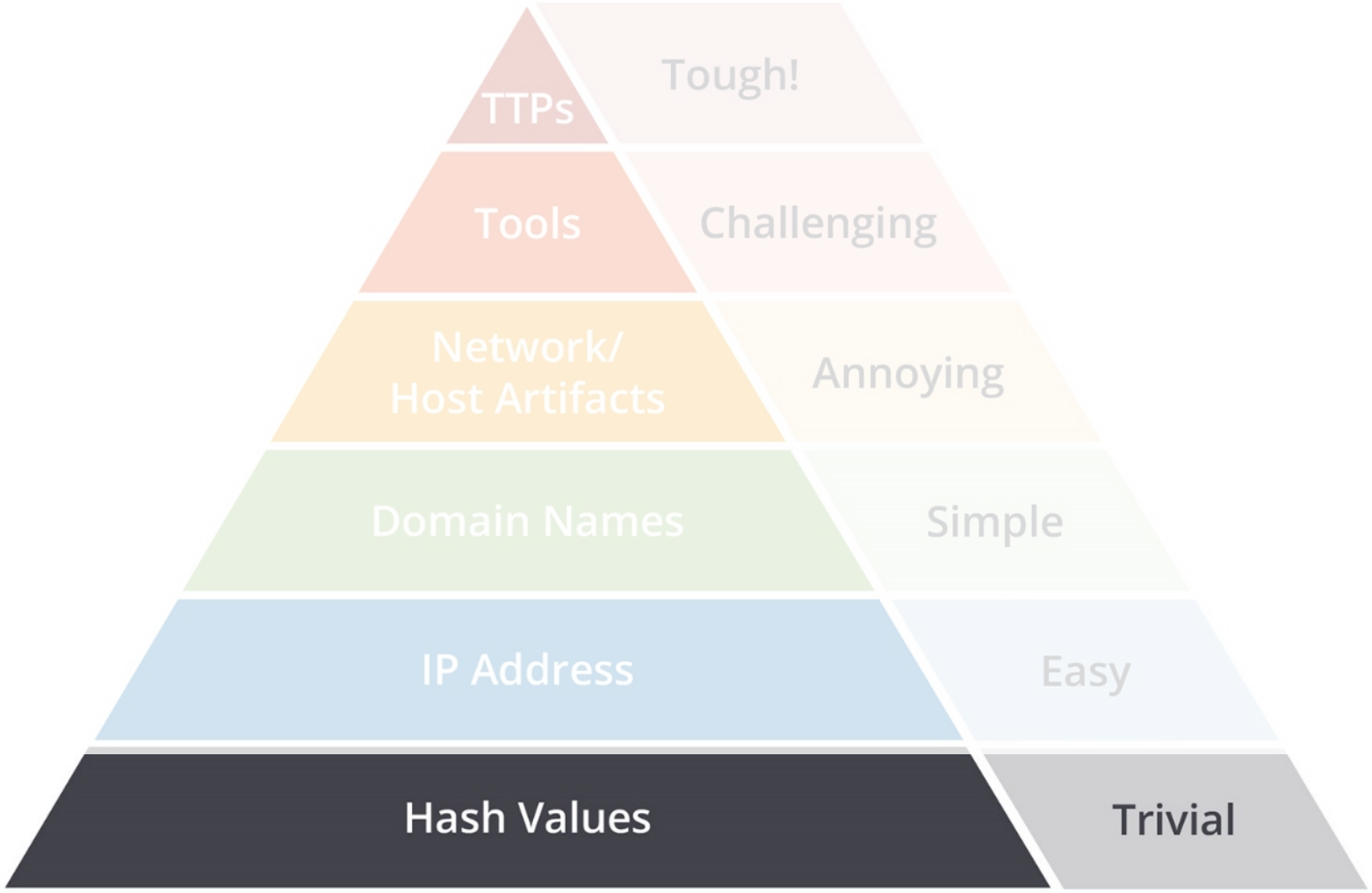
Key points

Intelligence about domains, IPs, and malware

Live graph of DNS requests and other contextual data

Correlated against statistical models

Enrich security data with global intelligence



Source: David J. Bianco, personal blog

File hash

SHA:

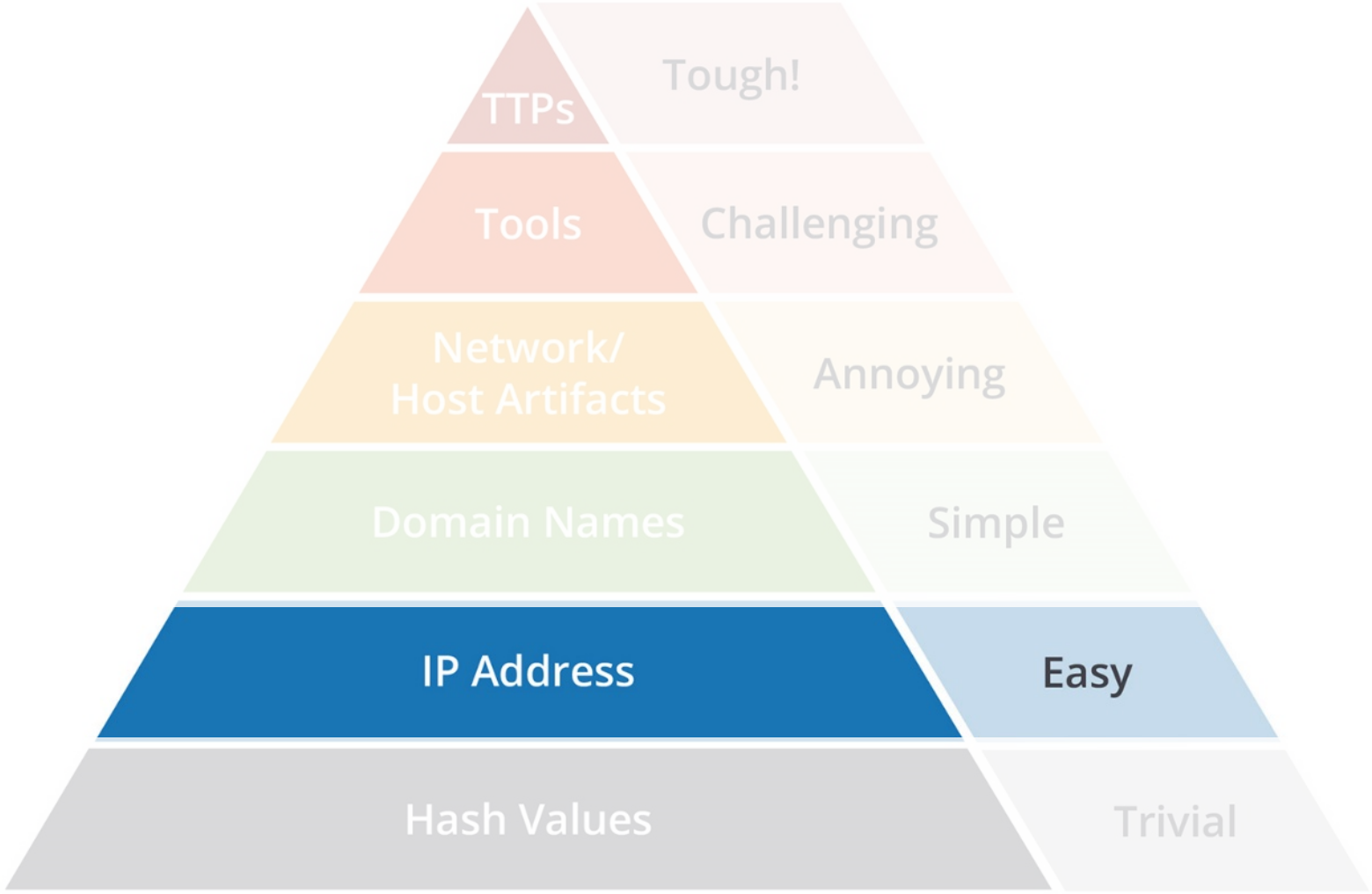
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370

Intelligence :

- Cisco Umbrella
- Cisco Threat Grid
- *VirusTotal*

Let’s see what this File hash represents



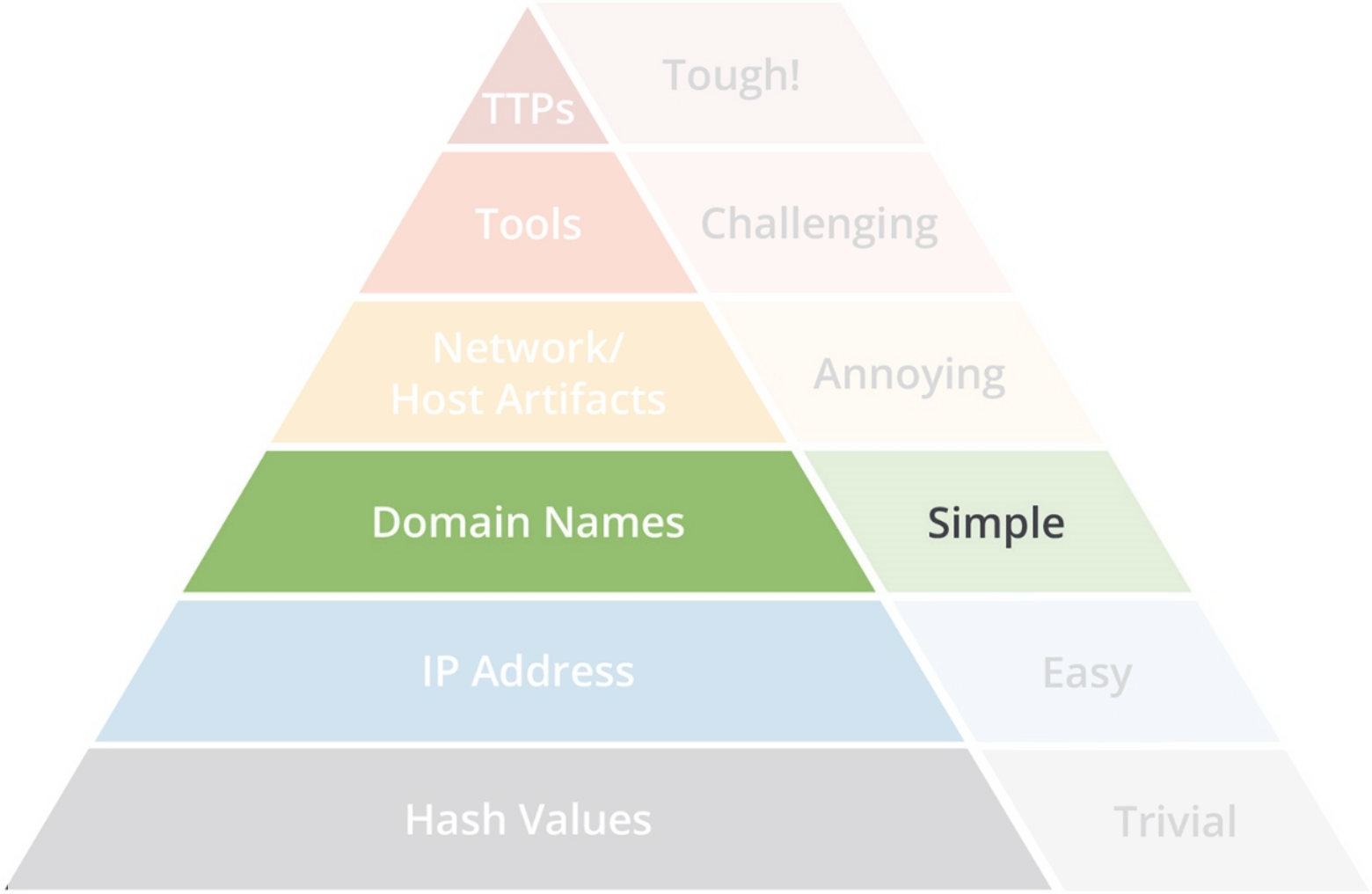
Source: David J. Bianco, personal blog

IP Address

193.23.244.244

Intelligence:

- Cisco Umbrella Investigate
- TOR
- VirusTotal
- Cisco Threat Grid



Source: David J. Bianco, personal blog

Domain

tourindia.in

Internetbadguys.com

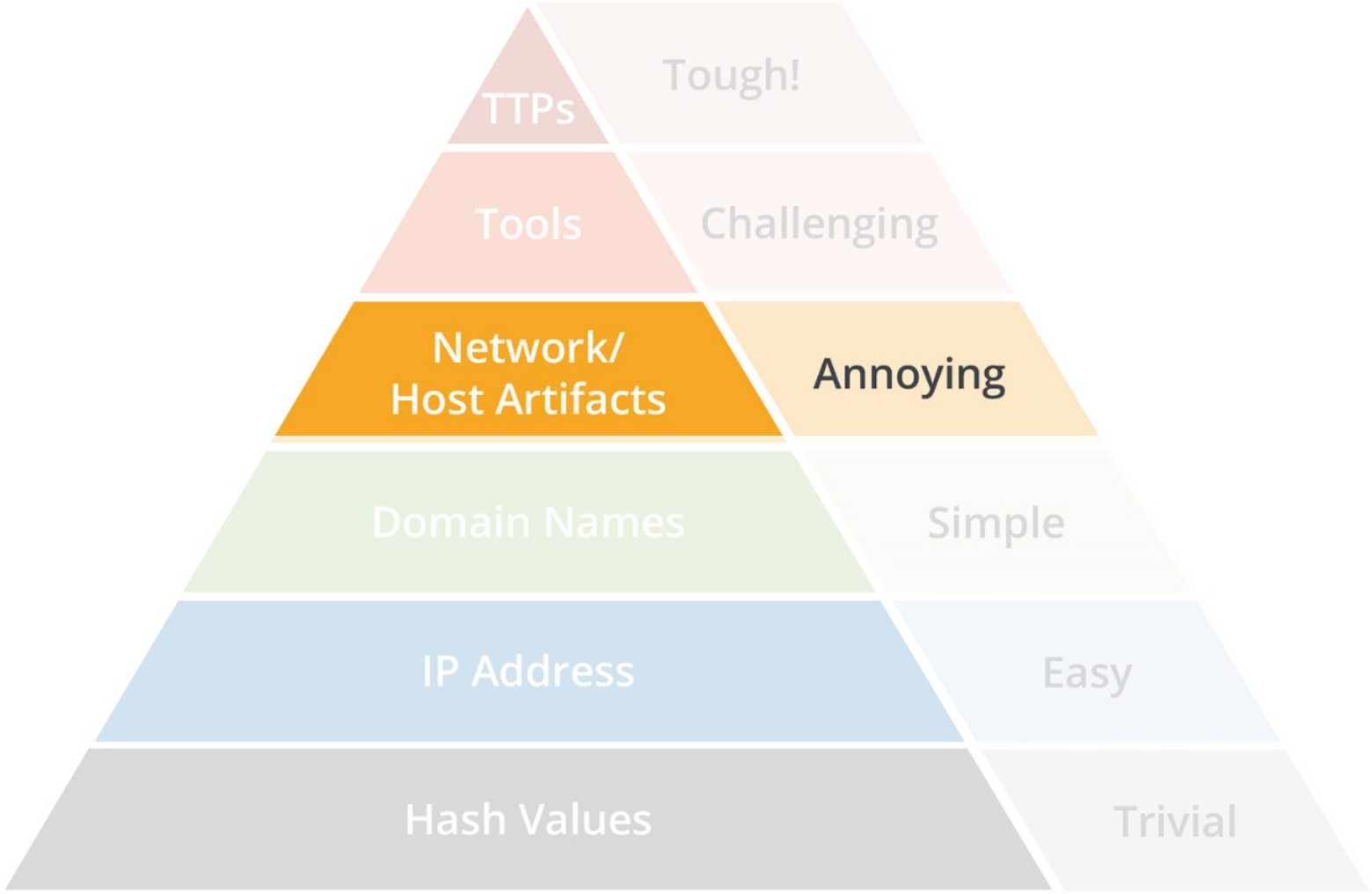
ysearch.com

xxlvbrloxvriy2c5.onion

Tools:

Cisco Umbrella Investigate

Cisco Threat Grid



Source: David J. Bianco, personal blog

Network and Host Artifacts

Pay attention to the listening ports utilizing

TCP/UDP ports such as SMTP, HTTP, FTP and proxy servers

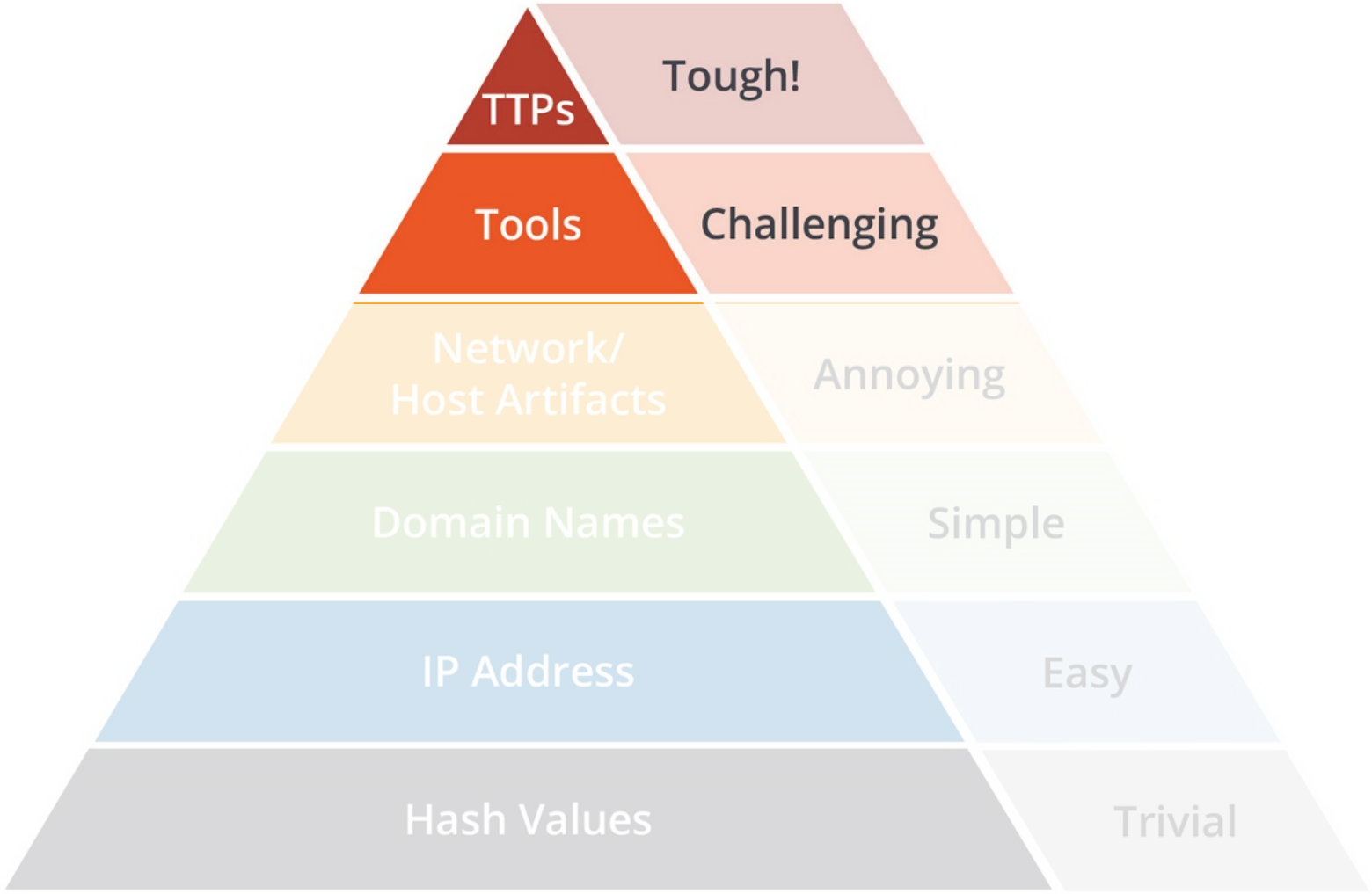
Pay attention to the Registry, Disk, Memory

Trigger Points: **Network**

- Unusual outbound network traffic
- Geographical irregularities w.r.t traffic
- Heartbeat or Beacon behavior

Trigger Points: **Hosts**

- Too much sudden high privilege activities
- Too many reads from valuable assets dbs
- Suspicious registry changes
- Too many system file changes



Source: David J. Bianco, personal blog

Tactics, Techniques and Procedures TTPs)

Characterize the how and what of adversary behavior (what they are doing and how they are doing it).

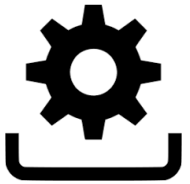
Understanding the Attackers MO

Social Engineering

Weaponization

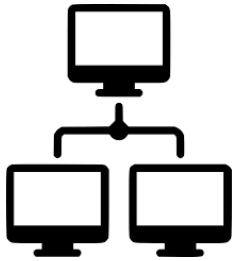
Delivery

Exploits



Install

Command & Control



Move
Laterally

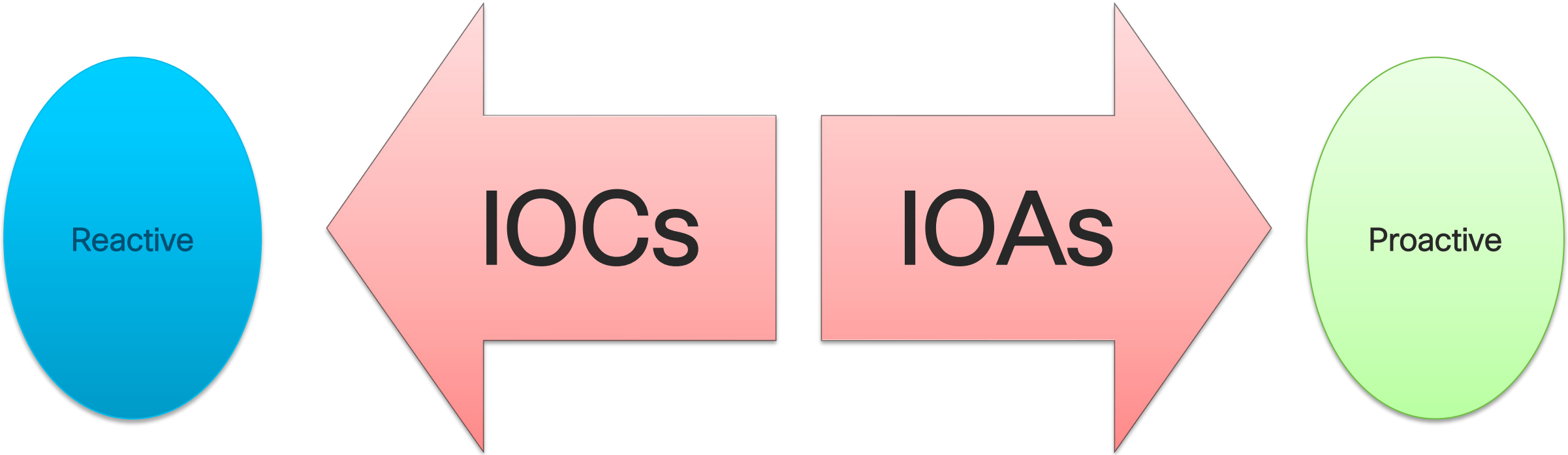
Mirai TTPs

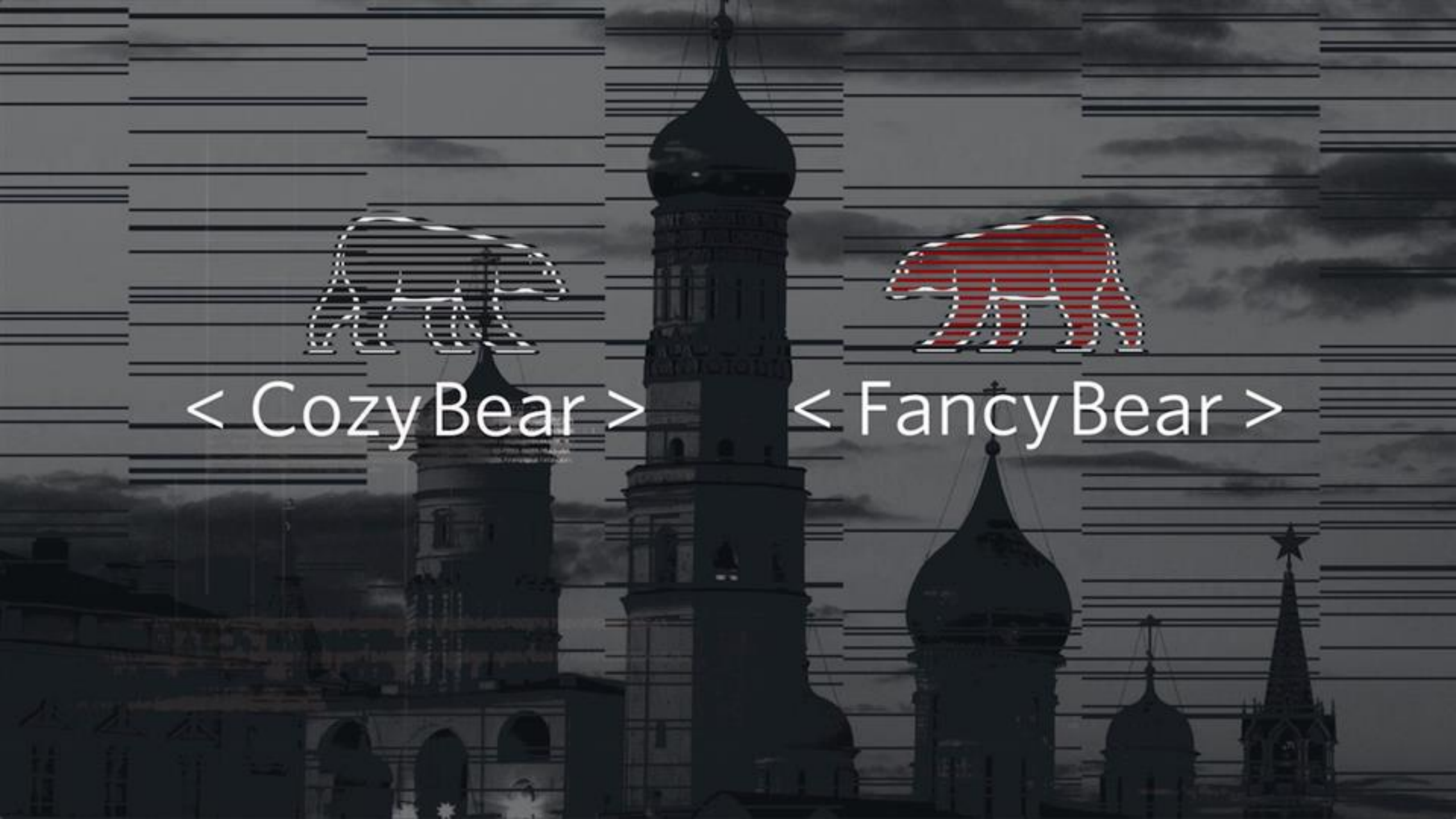
- Exploit IOT devices exclusively using zero day exploits.
- Discover unsecure IOT devices with IP scans continuously.
- Escape scrutiny of GE, DOD, HP, USPS by skipping their network.
- Massive DDOS attacks against targets. Ex. Minecraft servers, Rutgers etc.
- House cleaning: Get rid of all competing botnets.

OCEAN'S ELEVEN

THEY'RE HAVING SO MUCH FUN IT'S ILLEGAL

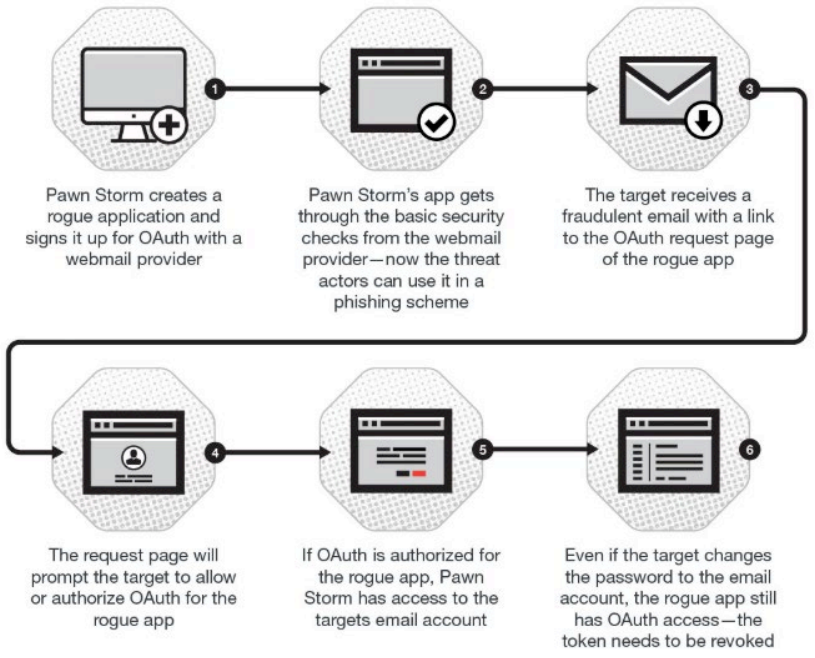
IOCs vs IOAs

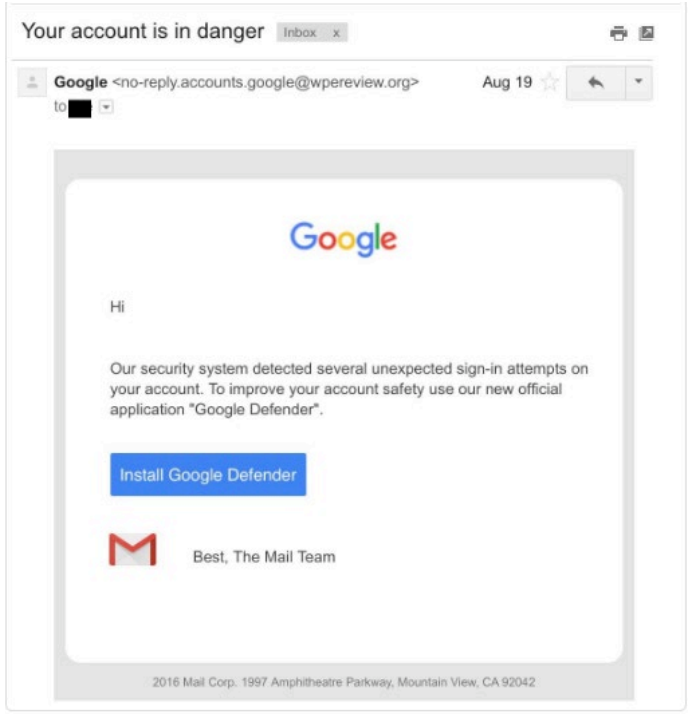


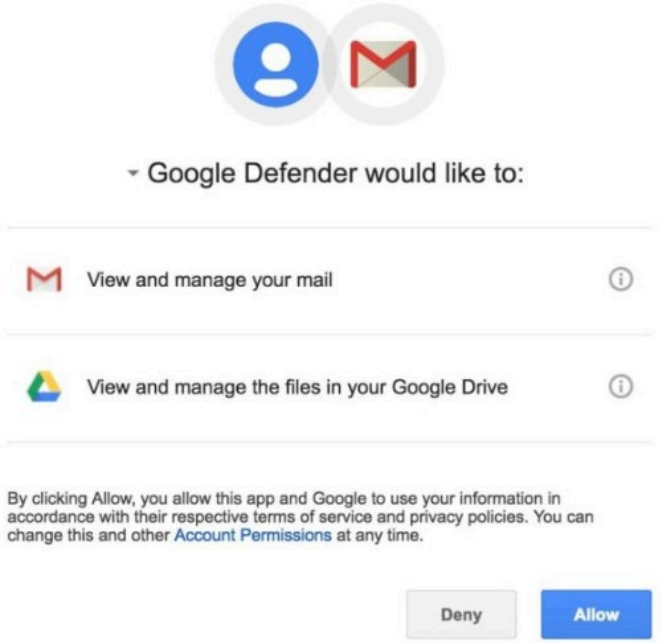

< CozyBear >
< FancyBear >

DNC Network Hack

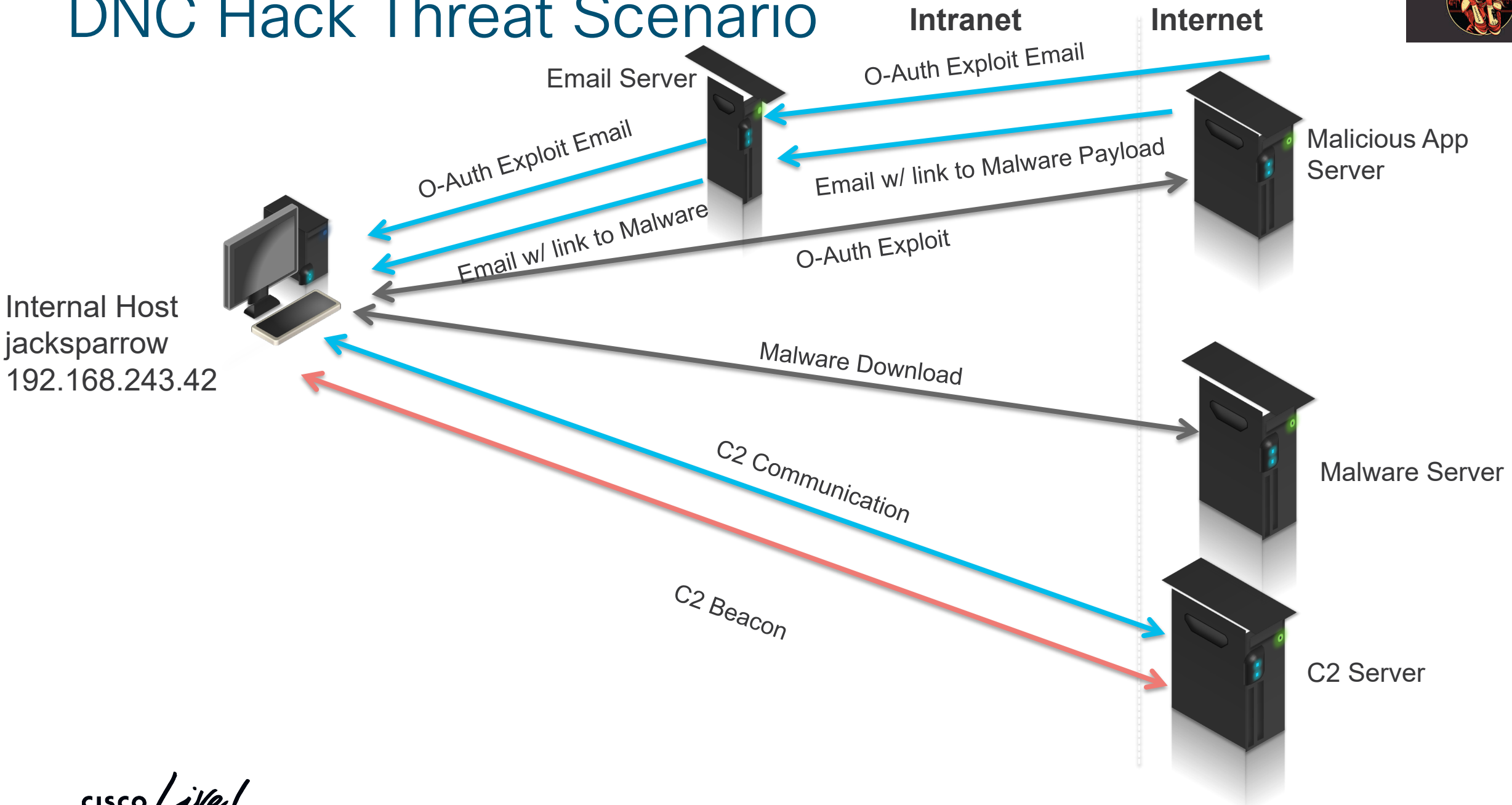
- Fancy Bear (a.k.a Pawn Storm or APT 28) and Cozy Bear (APT 29)
- Combination of Oauth Exploitation and Malware Infection





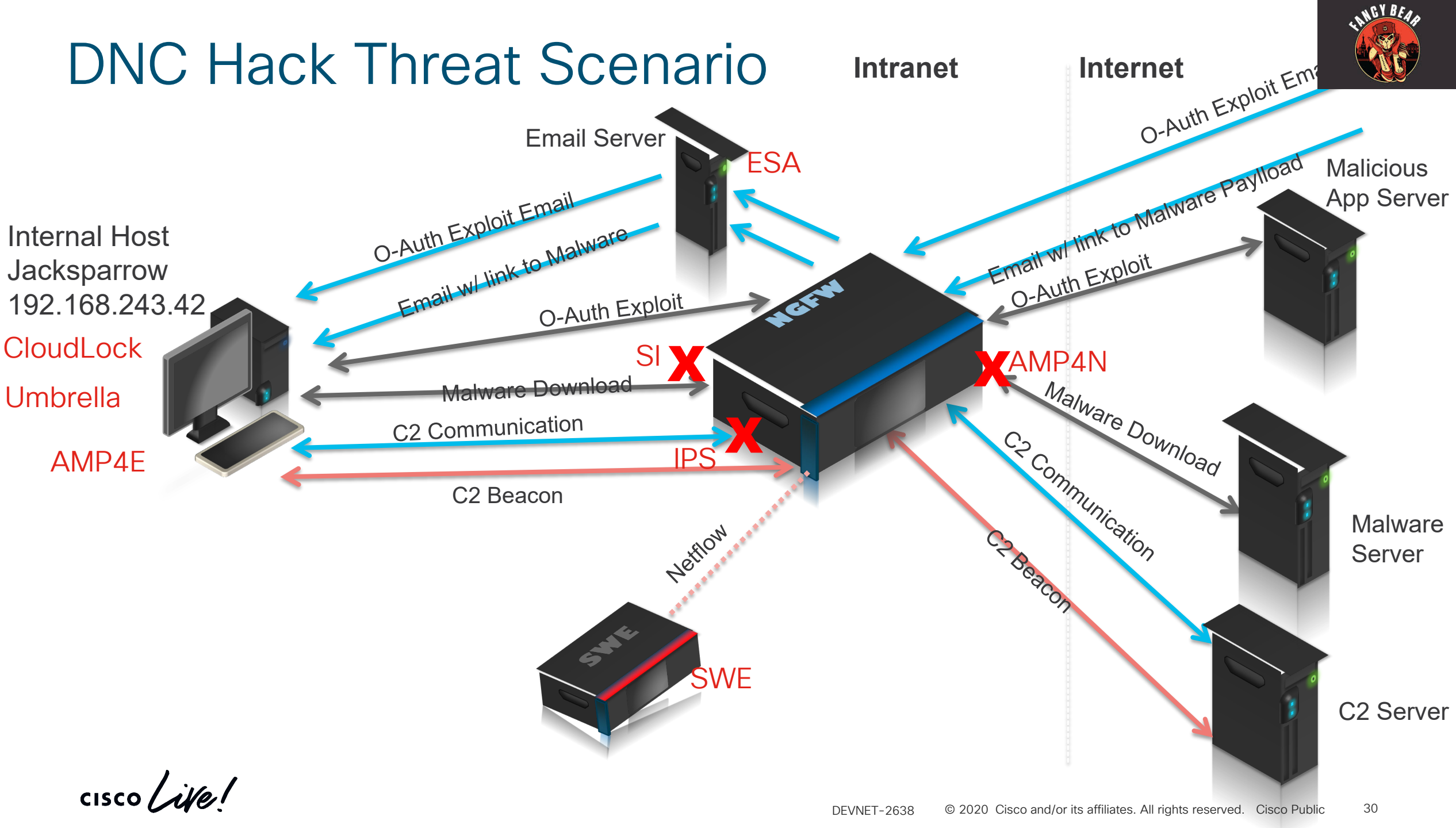


DNC Hack Threat Scenario



Cisco Threat Response

DNC Hack Threat Scenario



SecOps

EPP

NGIPS

DNS Security

Etc

File Analysis

Domain reputation

IP reputation

Etc

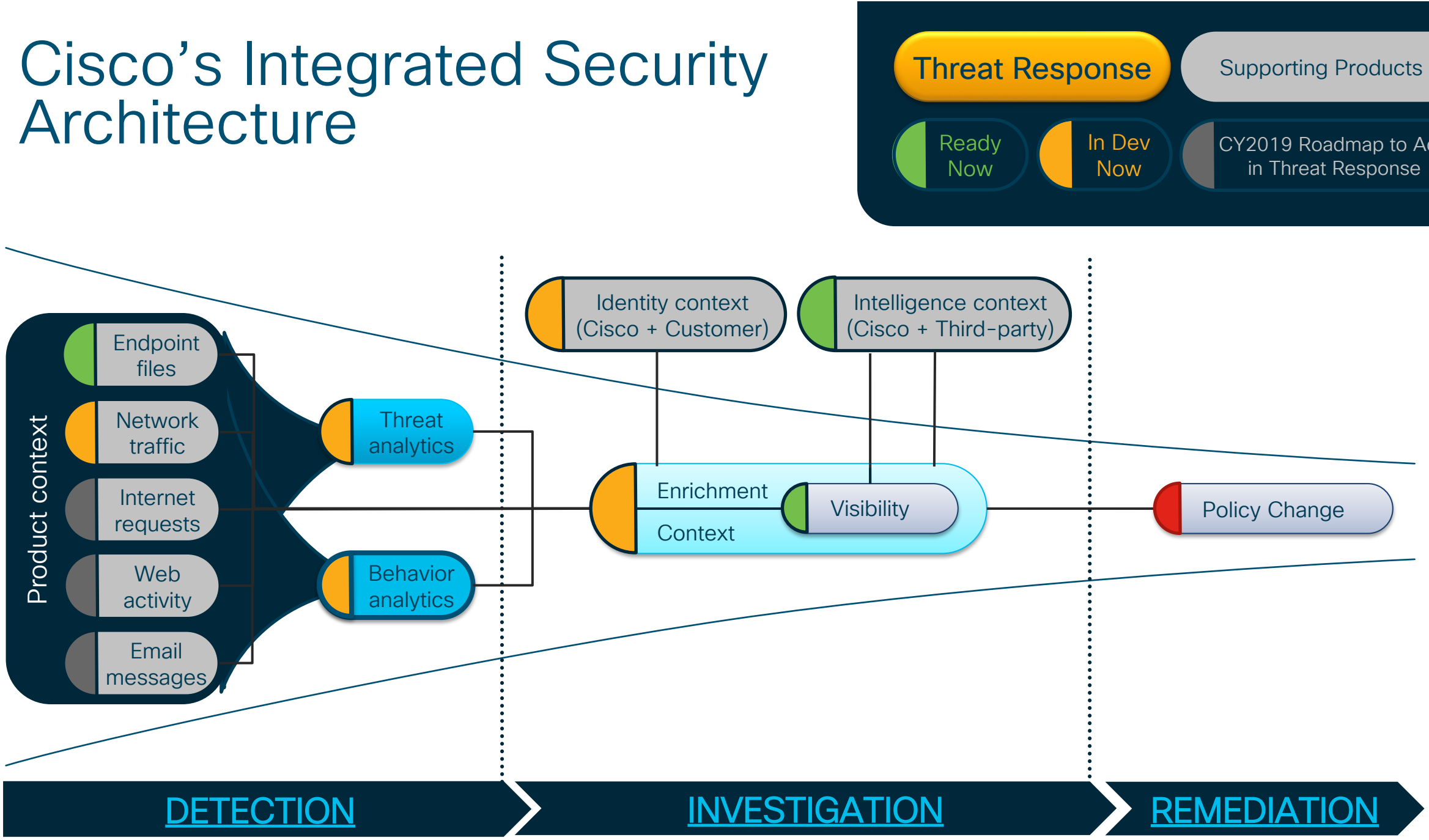
EPP logs

NGIPS logs

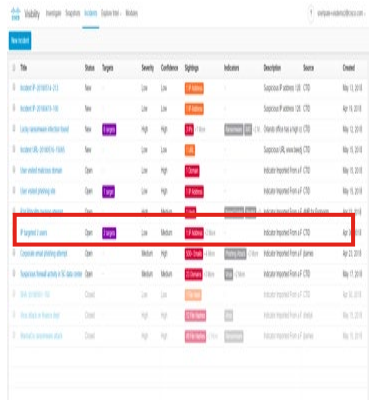
DNS logs

Etc

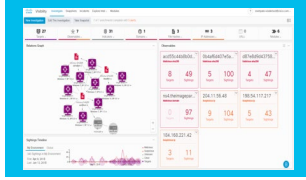
Cisco's Integrated Security Architecture



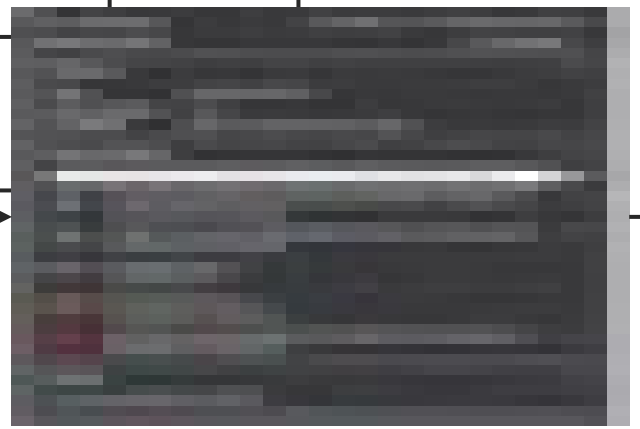
Cisco Threat Response: Workflow

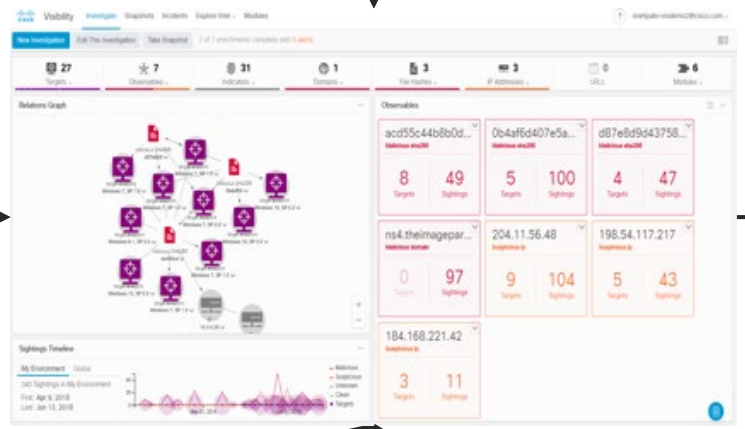


1 Intel sources



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

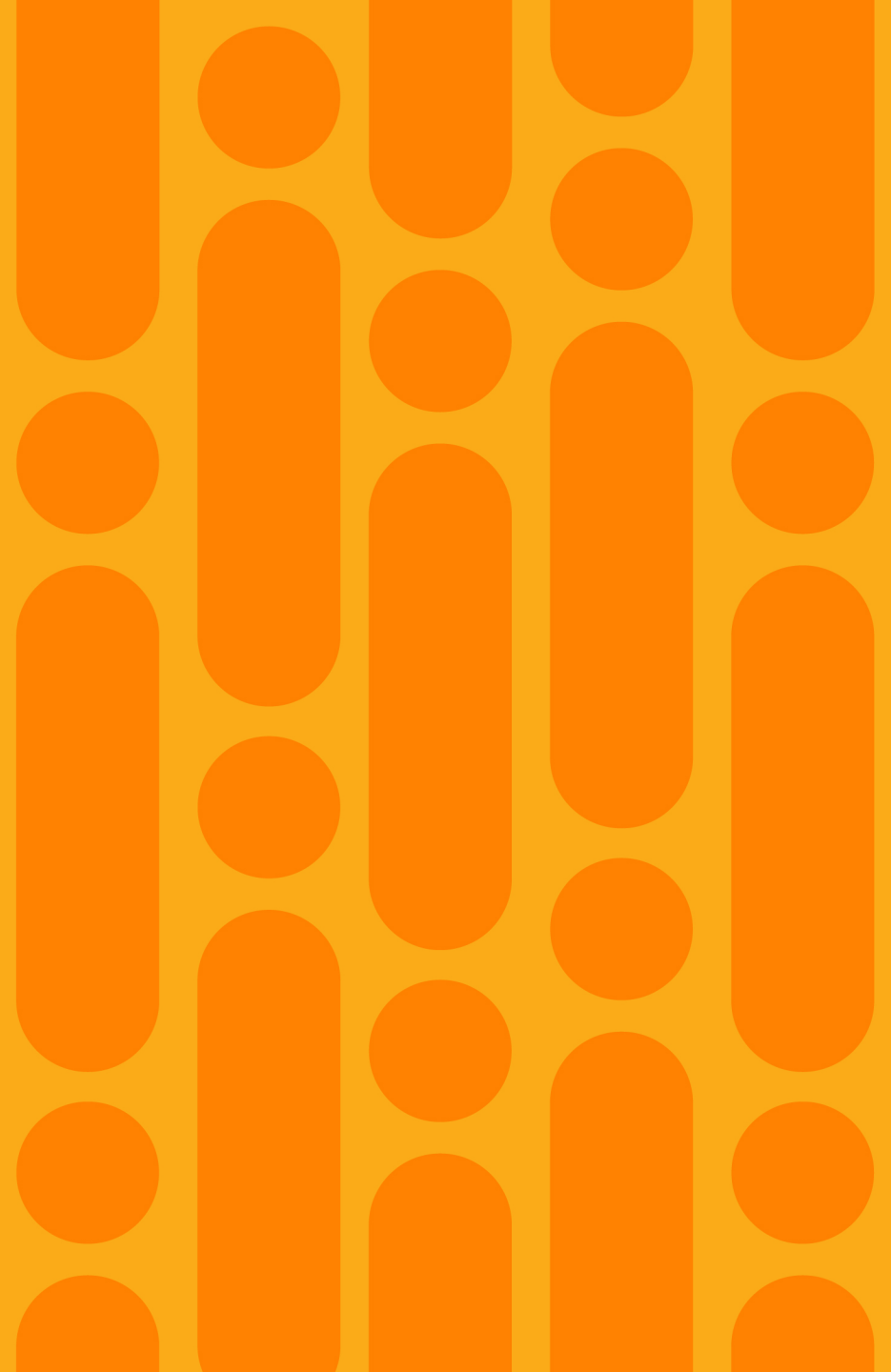
DEMO CTR

Things to remember

- Be a detective – Question everything
- Automation! Automation! Automation!
- *There is always a way --- **James Bond!*** Yes! be prepared with a Strategy
- Use new tools (Analytics, Big Data, ML/AI ...etc.)

- But the best resources every ORG has is People!!!

Happy Hunting!!!



Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the
Cisco campus

Walk-in labs

Meet the engineer
1:1 meetings

Related sessions


Thank you
cisco Live!

You make **possible**