Cisco Connect 2019

Philippines, Manila . 11 Apr 2019

#CiscoConnectPH

Empowering Defenders With Cisco Threat Response

Lewis Tan *CISSP, OPST*

SecOps Asean + Korea

An incident comes in...

Your HR department has been targeted with a phishing campaign

Administrative assistant to the VP of HR inadvertently opens the email attachment

The attacker gains access and control to the admin's system, that has access to servers containing sensitive employee data

Admin notices that their system has slowed down considerably and creates a ticket with the IT Help desk

Help desk performs initial investigation and is unable to resolve the issue, and sends the incident to the SOC team

Punycode with Phishing

Rolex	rolęx.com	xn--rolx-nu5a.com
Rolex	rołex.com	xn--roex-11a.com
Ryanair	ryanaır.de	xn--ryanar-t9a.de
Singapore Airlines	sıngaporeair.com	xn--sngaporeair-zzb.com
Spar	spar.com	xn--spa-nxb.com
Starbucks	starbucks.com	xn--starucks-hpd.com
Waitrose	waıtrose.com	xn--watrose-sfb.com

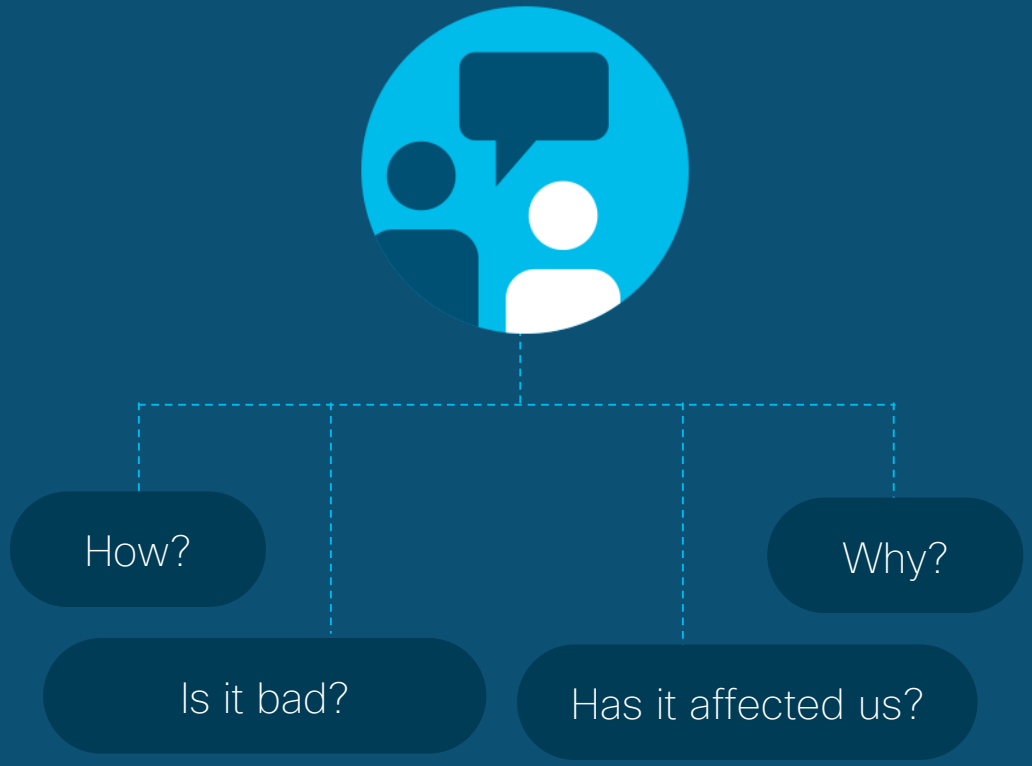
Lots of questions to be answered… and fast!

1. Do we care about this threat?
2. What departments and machines have been infected with this specific file?
3. Who was patient 0?
4. Are there any related attacks or attack components we need to be concerned with?
5. How can we block this attack, and prevent potential future attacks?

Security must work together

But too often it doesn't...

Security Operations



Technologies and Intelligence

- **Threat Intel**
- Endpoint Security
- SIEM
- **Next-Gen IPS**
- Malware Detection
- Secure Internet Gateway
- Email Security
- Web Security
- Third party Sources
- Network Analytics
- Next-Gen Firewall
- Identity Management

Security challenges go deeper than technology

2 million cybersecurity positions are projected to go unfilled by 2019*

SOCs are understaffed

Overwhelmed with alerts from disparate security products

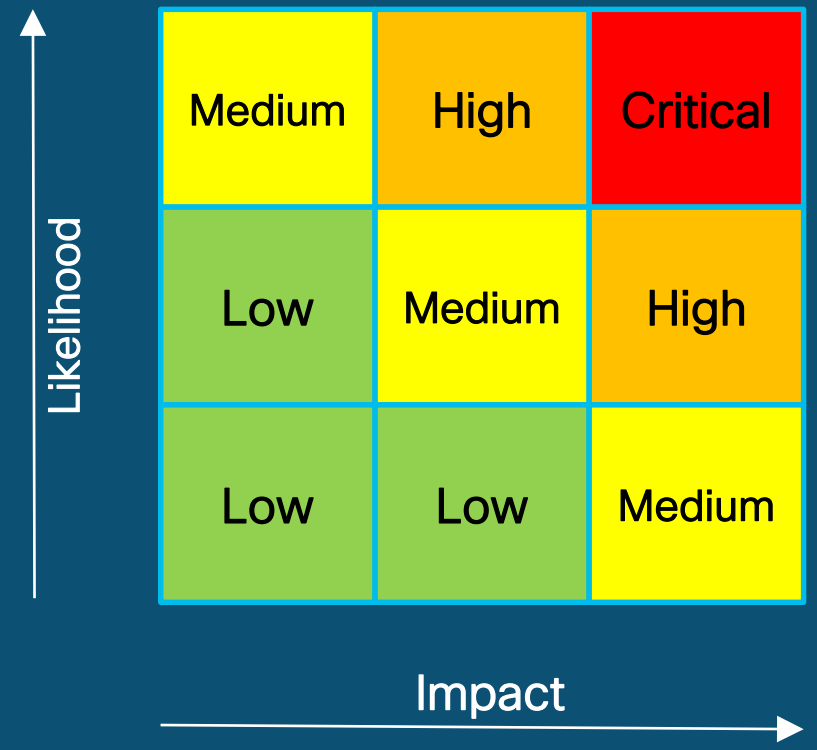
Unable to keep pace with current threats.

*according to Cybersecurity Ventures, 2017

Find the unknowns

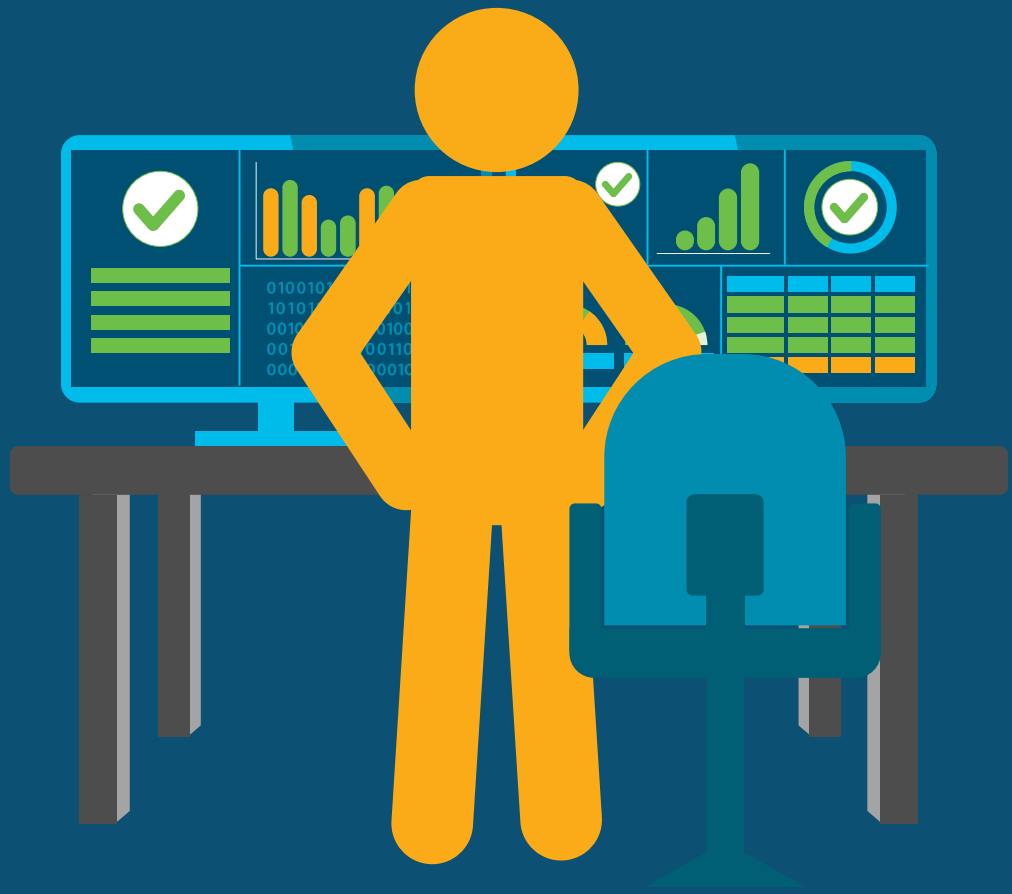
- Where do you start?
- Which tool do I use?
- What information do I need?
- How do I connect the dots?

Identify the risks



We believe security systems should empower your people to investigate and respond to threats faster

- Automation should reduce the burden on the SOC
- Alerts should be relevant and prescriptive
- Security products and threat intel should all work together



Visibility + Analytics enable faster response

Contextual network-wide, internet-wide, endpoint visibility

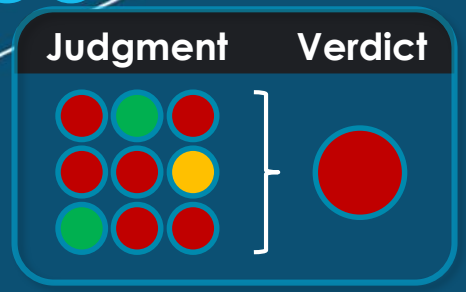
Predictive threat analytics

- Behavioral modeling
- Machine learning
- Global threat intelligence

Automated detection and response

- Unknown threats
- Insider threat
- Encrypted malware
- Policy violations

Introducing Cisco Threat Response



Cisco TALOS
Threat Intel

TALOS

AMP ProtectDB
(File Reputation)

VirusTotal

3rd Party
Threat
Intel

Umbrella
DNS-Layer
Intel

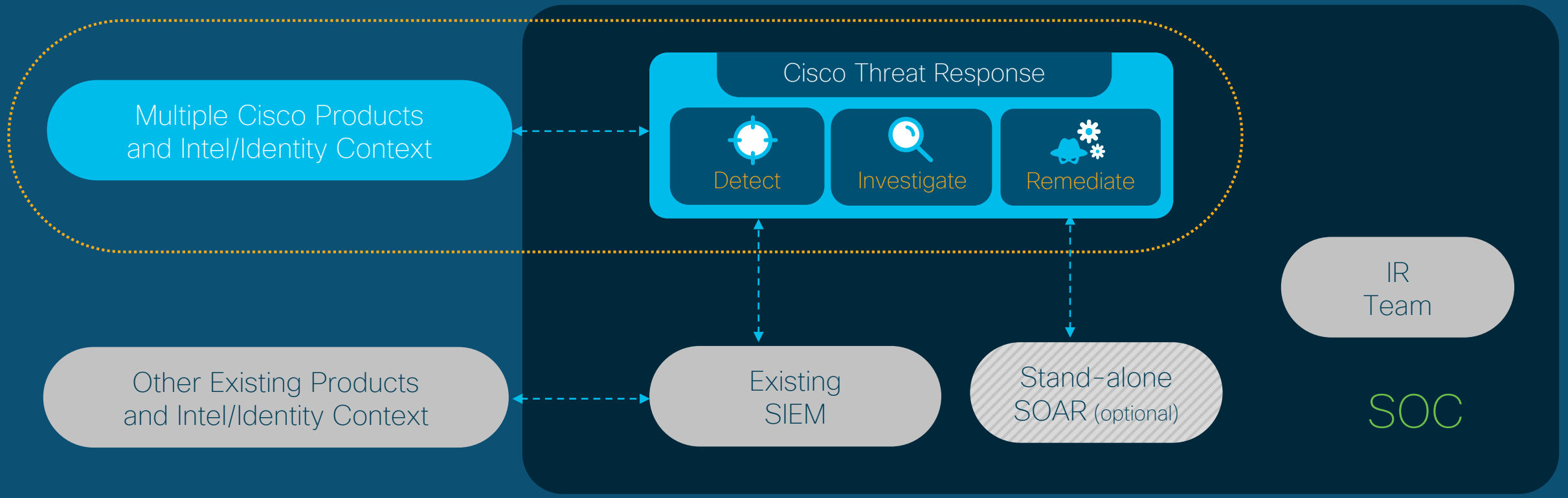
Visibility

AMP Global
Intelligence

Cisco Threat Response DEMO

Cisco Threat Response in your SOC

Complements your existing investments and supports your IR team



Cisco Threat Response for everyone

Scales with the changing needs of your organization

Commercial Organizations

and State and Local Governments

- Small security team
- Limited SIEM deployment
- Leverage full stack with API

Large Enterprises

and Large Government Agencies

- Security Operations Center
- Extensive SIEM deployment
- APIs across the stack is key

Managed Security Service Providers

- Security Operations Center
- Multi-tenant SIEM deployment
- APIs across the stack is key

Cisco Threat Response is included

...with select Cisco Security product licenses

You're already entitled to Threat Response if you have...

- Cisco AMP for Endpoints
- Cisco Threat Grid
- Cisco Umbrella
- Cisco Email Security
- Cisco NGFW/ NGIPS with AMP for Networks

Not a customer yet?

Request your free trial of Cisco AMP for Endpoints... and try both solutions right now!

www.cisco.com/go/amp

www.cisoc.com/go/threatgrid

www.cisco.com/go/umbrella

www.cisco.com/go/emailsecurity

www.cisco.com/go/ngfw

Cisco Threat Response in the classroom

Threat Hunting Workshops educate your team with real-world scenarios

161 global workshops

...already held from May-July 2018
with even more happening now

Features Cisco Threat Response

... and integrations with Cisco security products and threat intelligence

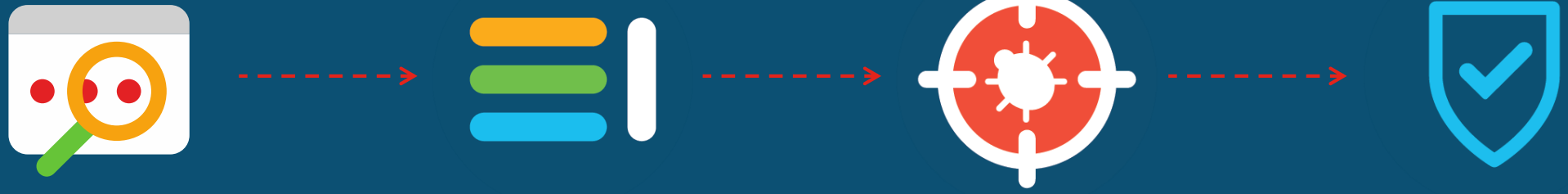
Cisco Threat Response

Learn more about Cisco Threat Response at
cisco.com/go/threatresponse

Security That Works Together

Let Cisco help you respond *faster!*

Accelerate your SOC with Cisco Security technologies



Stealthwatch

immediately raises the alarm by pinpointing malicious network activities, and helps to understand the scope of the attack

Cisco Threat Response

brings together intelligence from different sources to present a single view of the what, where, when and how of the threat

AMP for Endpoints and Threat Grid

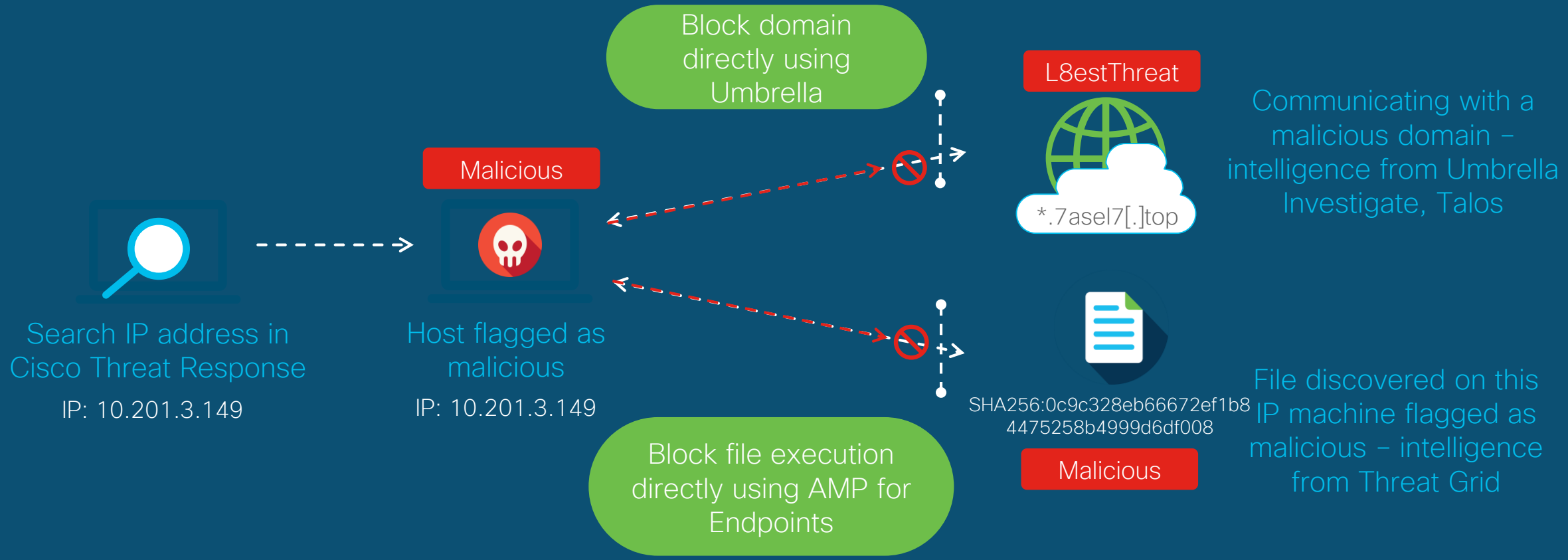
automatically flags the file as malicious with deep malware analysis, and prevents it from spreading

Umbrella Investigate

identifies the malicious domain callback, and associated infrastructure in order to prevent future attacks by the entity

Respond even faster: With security that works together

Using Cisco Threat Response



Prepare earlier so you can respond faster using Cisco Incident Response Services

Retainer

Annual Subscription

Dedicated Seasoned Consultants

Offer may include:

- Emergency Response
- Proactive Threat Hunting
- IR Readiness Assessments
- Table Top Exercises

Access to Included Tools:

- AMP for Endpoints
- Umbrella
- Stealthwatch
- Threat Grid

Proactive

Proactive Threat Hunting

IR Readiness Assessment

Table Top Exercise

IR Plans & Playbooks

Emergency

Emergency Incident Response
-contact with your dedicated senior IR pro within 4 hrs
-deploy within 24 hrs

Data breach, exfiltration, malware, ransomware, and more

We help you recover

Cisco Protected

- 60 day AMP, SW, Umbrella licenses
- Monthly check-ins with responders
- Proactive services to be **ready** and **resilient**

Questions & Answers

Cisco Connect 2019

Philippines, Manila . 11 Apr 2019

#CiscoConnectPH