
Say hello
to the future.
Cisco Connect 2019
Bangkok, Thailand. 26 March 2019
#CiscoConnectTH

From Chasing Alerts to Hunting Threats

What makes an Effective SOC is Evolving

Nadhem Al-Fadan, PhD

SOC and IR Services, Cisco

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

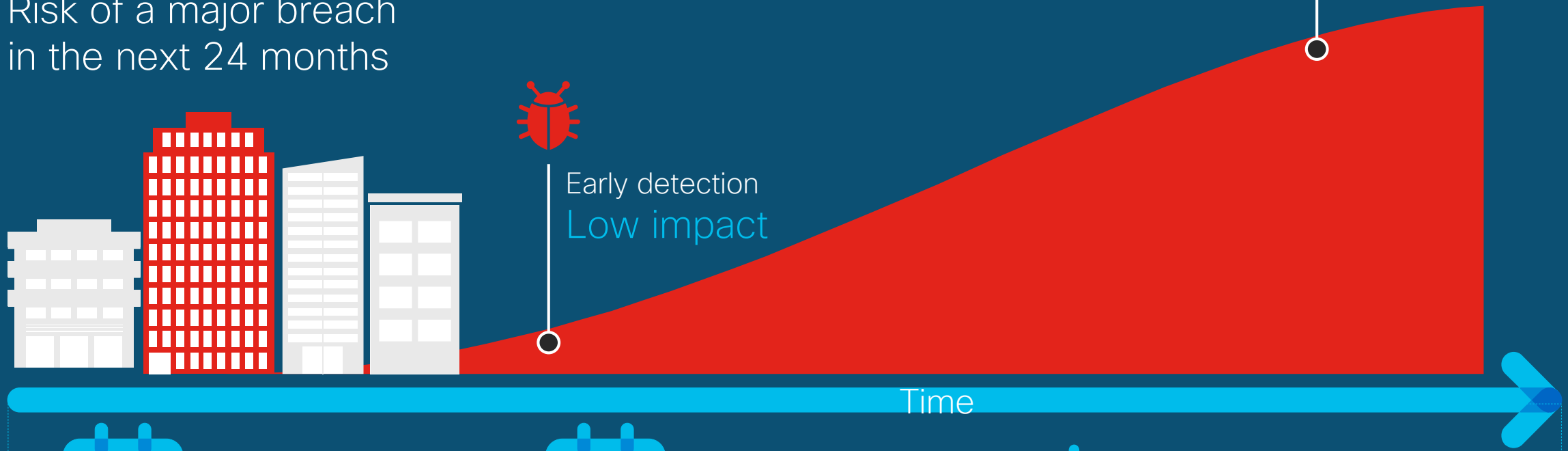
Unable to keep pace with current threats.

*according to Cybersecurity Ventures, 2017

And time is a critical factor

1 in 4

Risk of a major breach
in the next 24 months



197 DAYS

Industry average detection time for a breach

69 DAYS

Industry average time to contain a breach

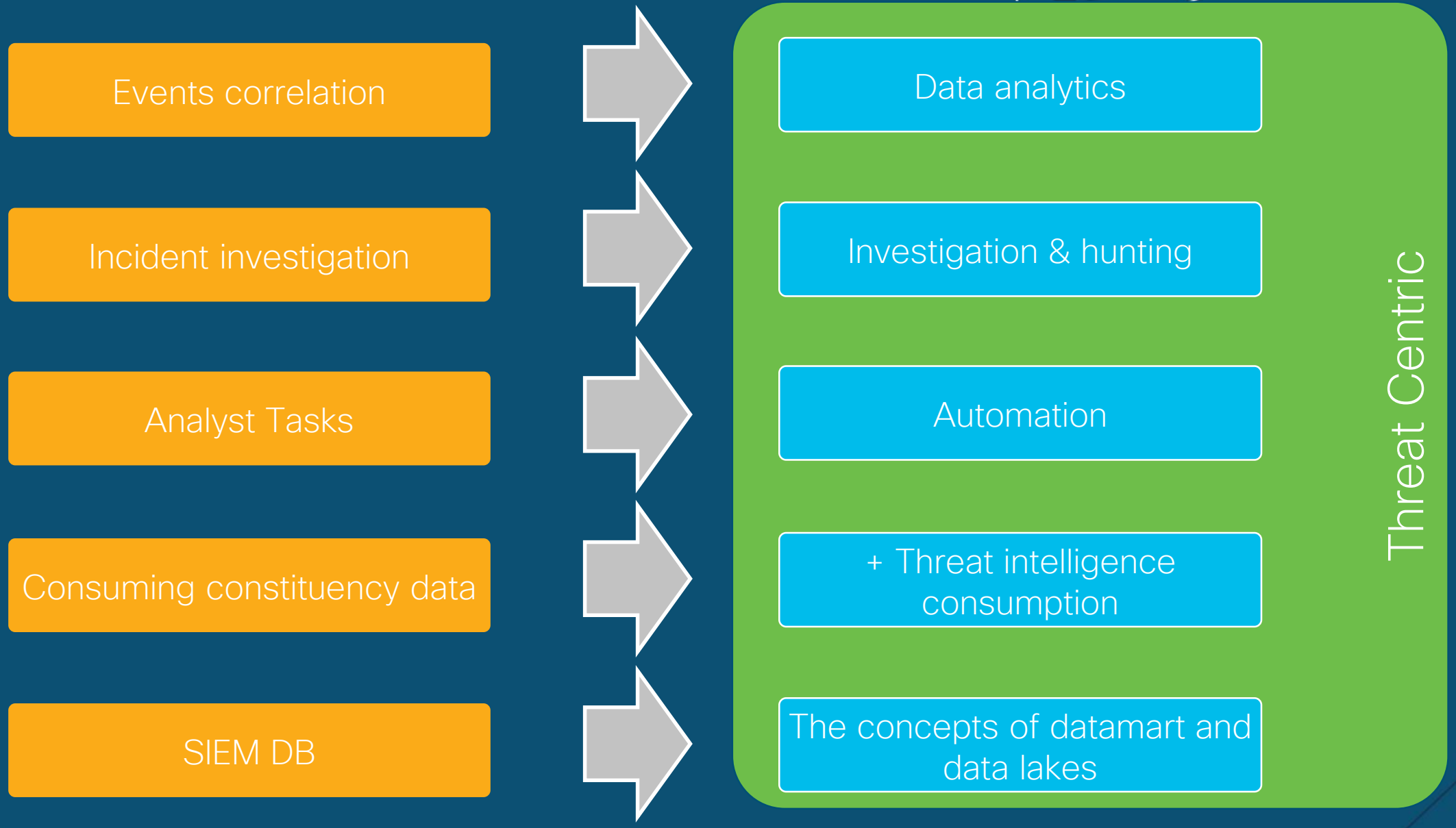
$3.86M

Average cost of a data breach

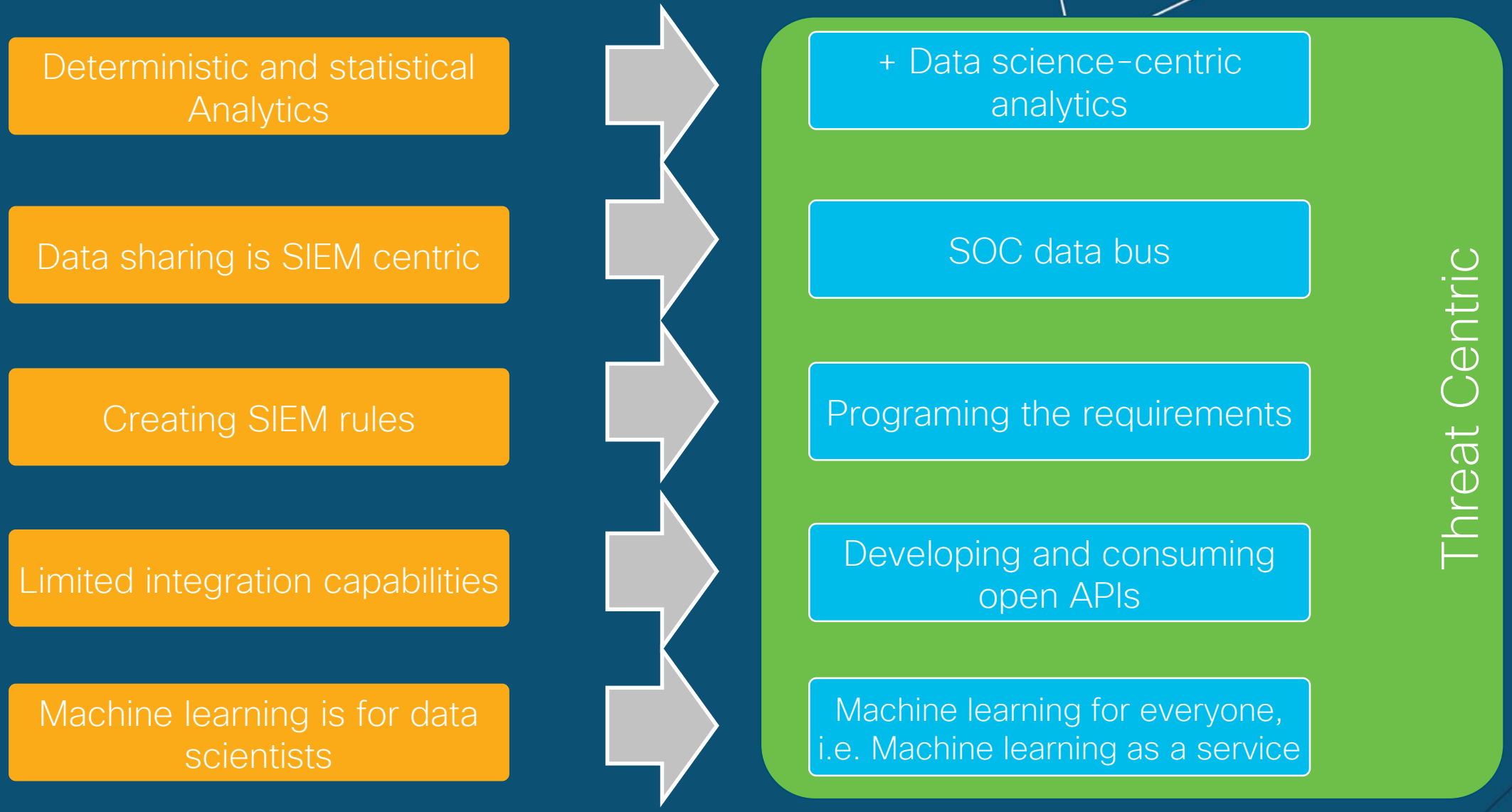
Source: Ponemon 2018 Cost of a Data Breach Study

SOC – What is Changing?

SOC – What is Changing?



SOC – What is Changing?



Beyond Basic SOC Service

Advanced Threat Intelligence

Automation

Advanced Security Analytics

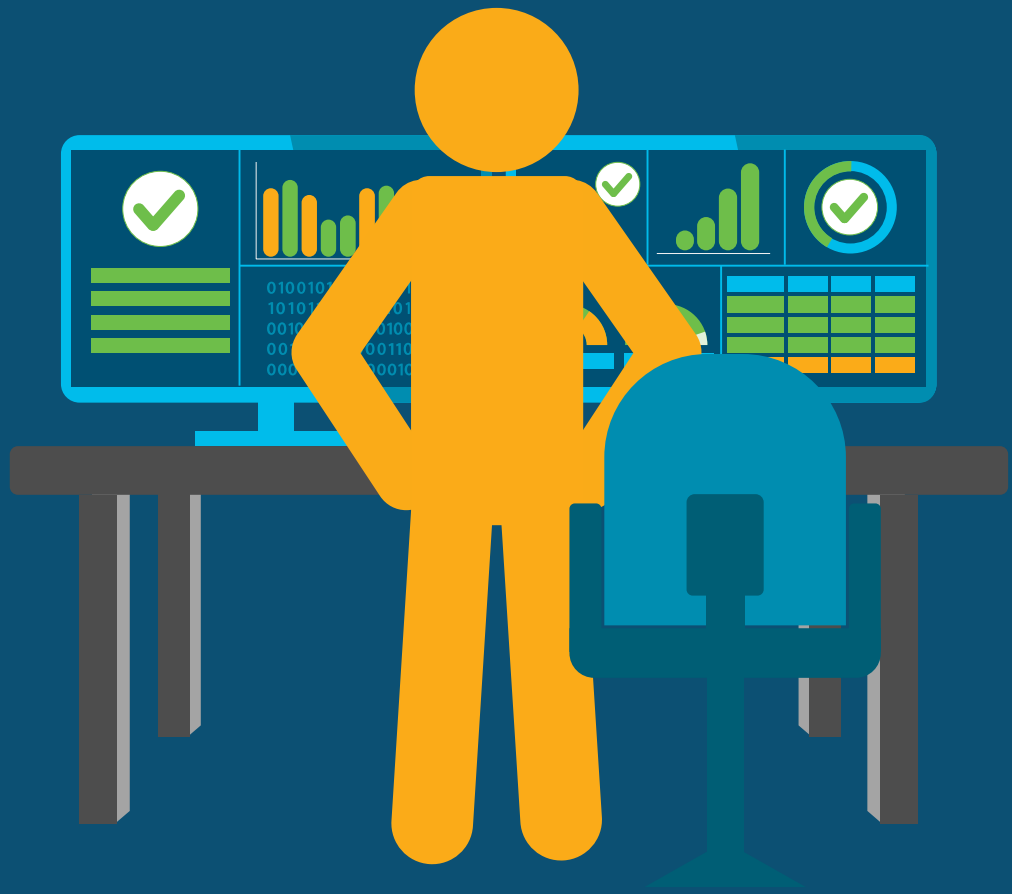
Advanced Reporting: KPIs, KRIs

Advanced Case Management

Threat Hunting and Deception

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



Respond faster!

Expand

visibility across your entire attack surface

Reduce

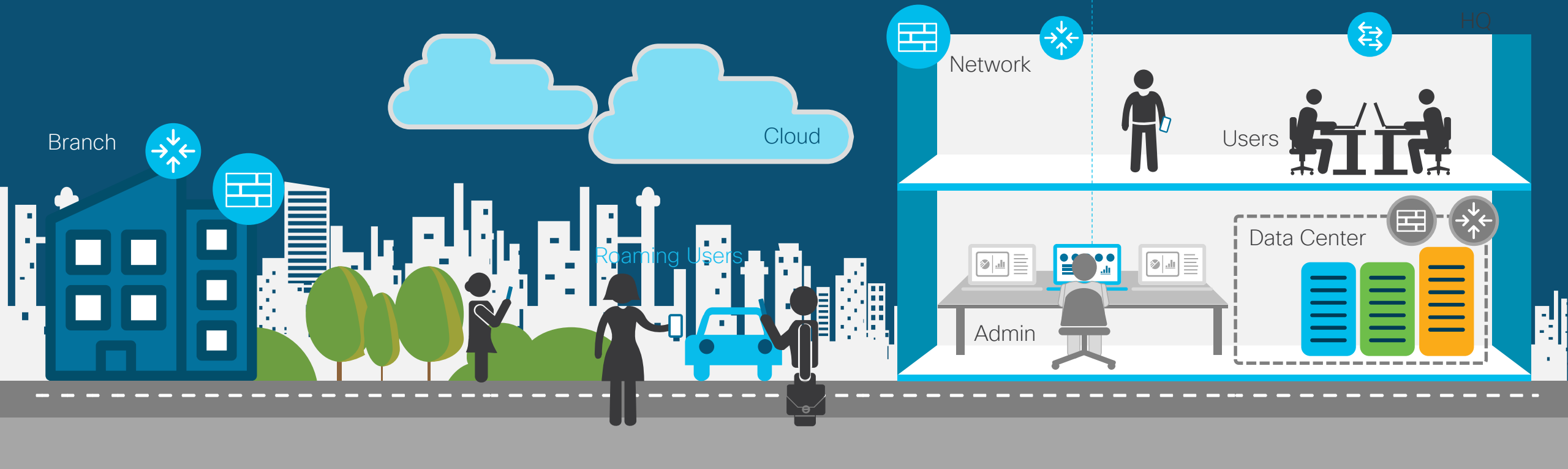
massive data sets to get to the critical alerts that matter

Accelerate

response capabilities

You can't respond to what you can't see

- **KNOW** every host
- **SEE** every communication
- Understand what is **NORMAL**
- Be alerted to **CHANGE**
- Respond to **THREATS** quickly



SOC Architecture

Evaluate, build and maintain a successful SOC with Cisco SOC Advisory Services

Strategy

based on desired outcomes

Architecture and design

using preferred operational model

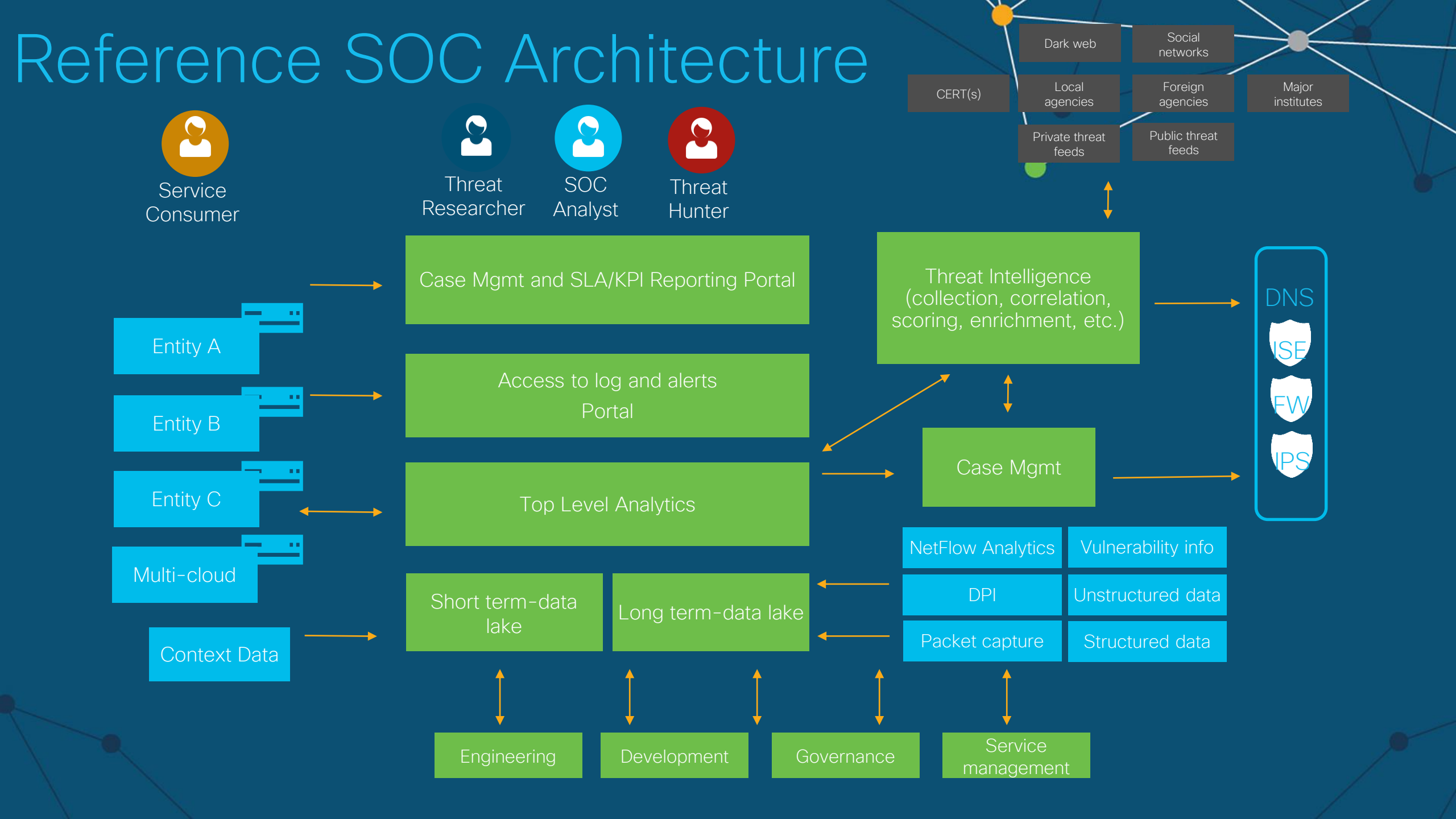
Assessments and Testing

to ensure effectiveness

Planning

to guide development

Reference SOC Architecture



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

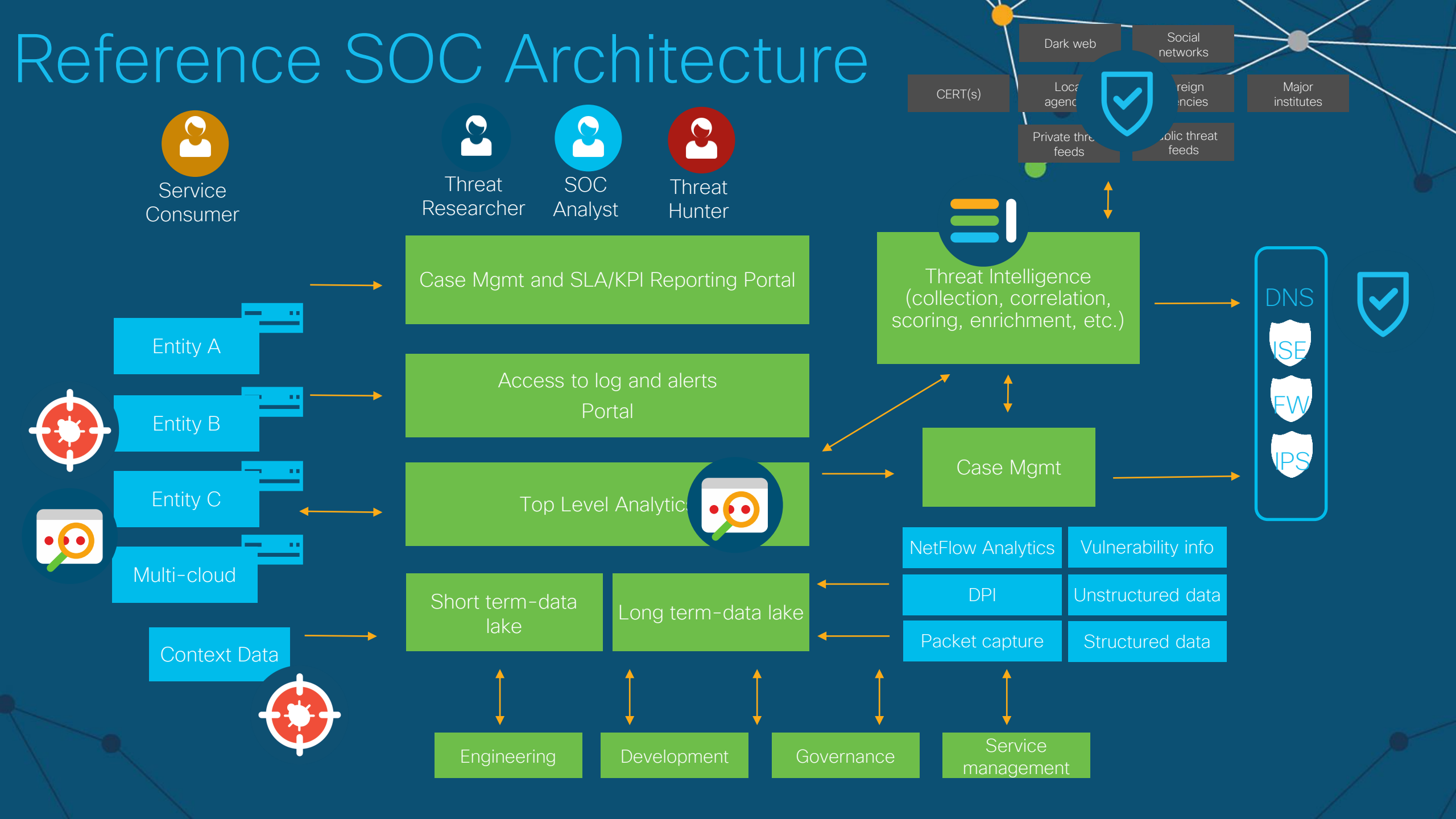
AMP for Endpoints and Threat Grid

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

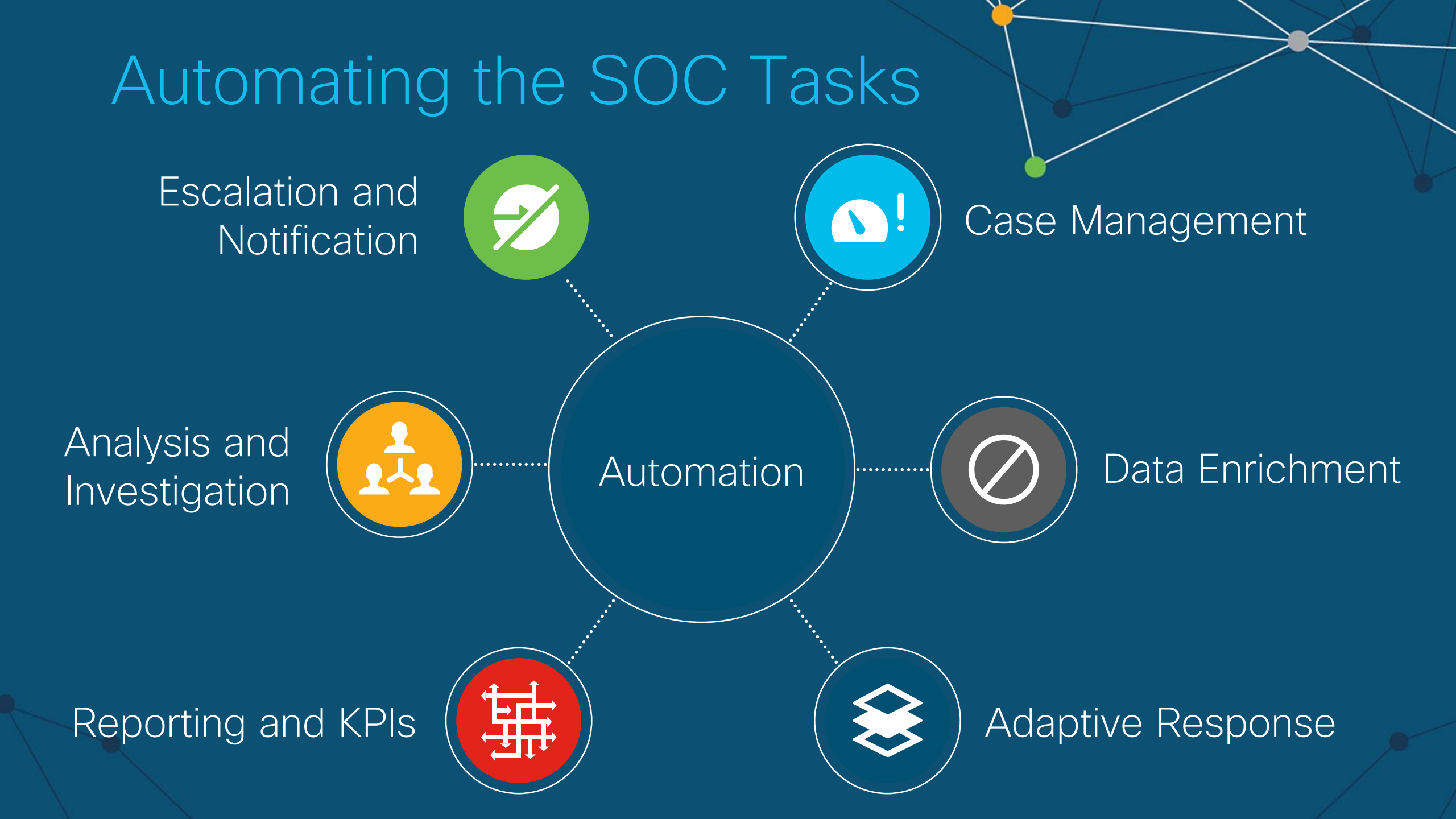
Reference SOC Architecture



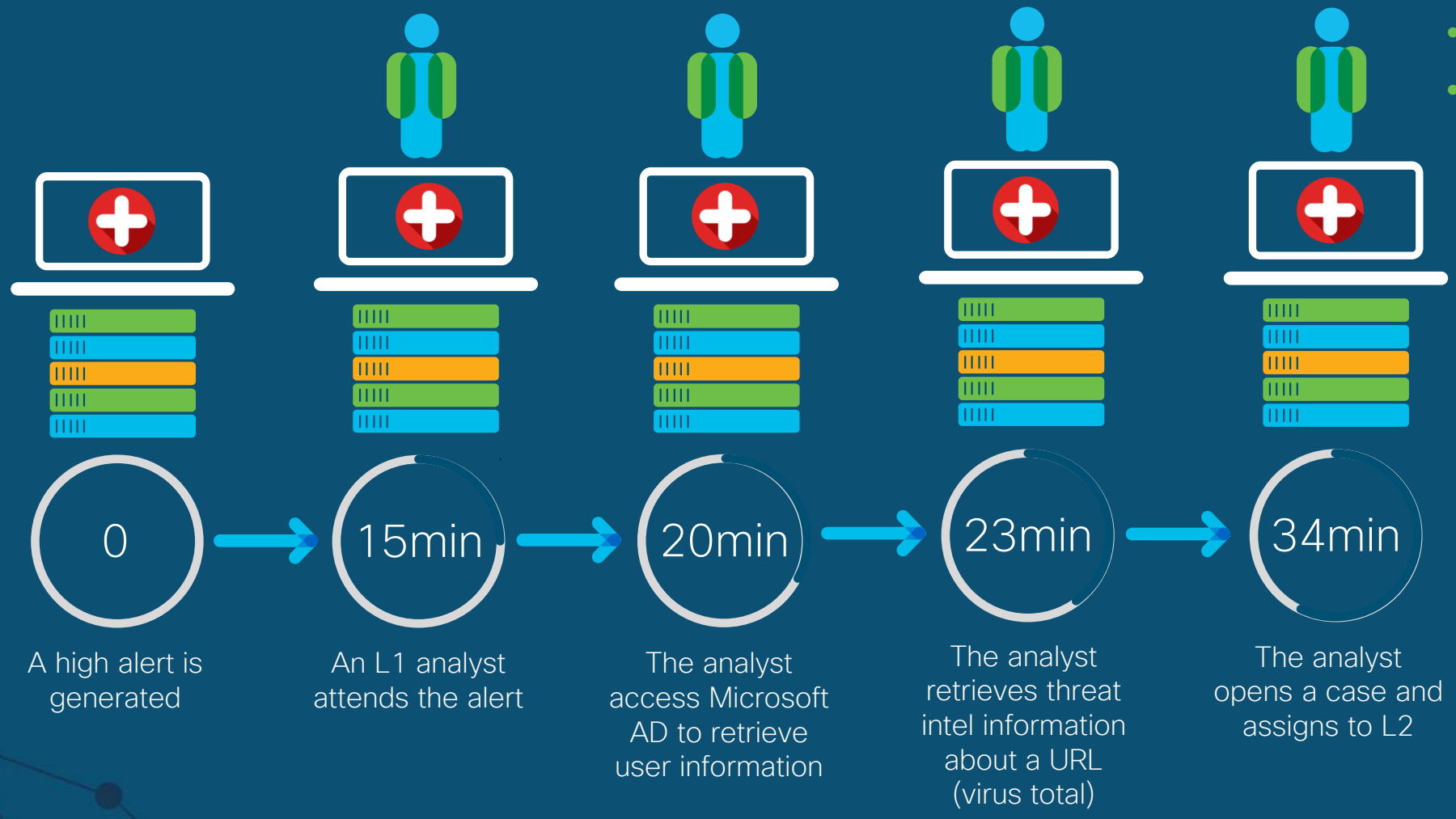
Why is automation critical in today's SOC?

Automation of the SOC aims to streamlines a series of time consuming, repetitive, manual tasks into cohesive and automated playbooks.

Automating the SOC Tasks



A Customer Test – One Process



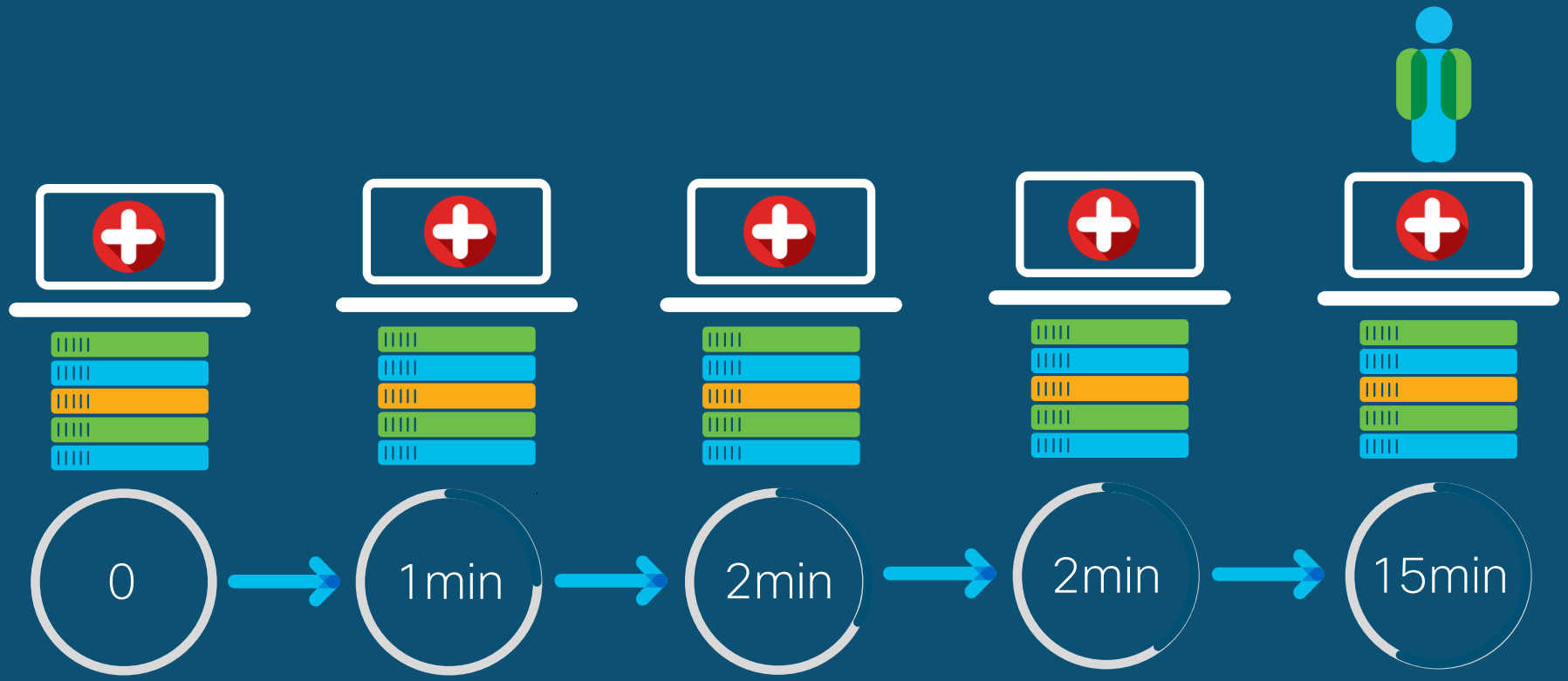
What was involved?

- Four dashboards!
- Copy and paste!
- Other alerts were getting generated simultaneously!

What if?

- What if we can save 10 minutes per alert?
- How many alerts can we optimize?
- How many analysts per shift?
- How many shifts per day?

Automating “this” Process



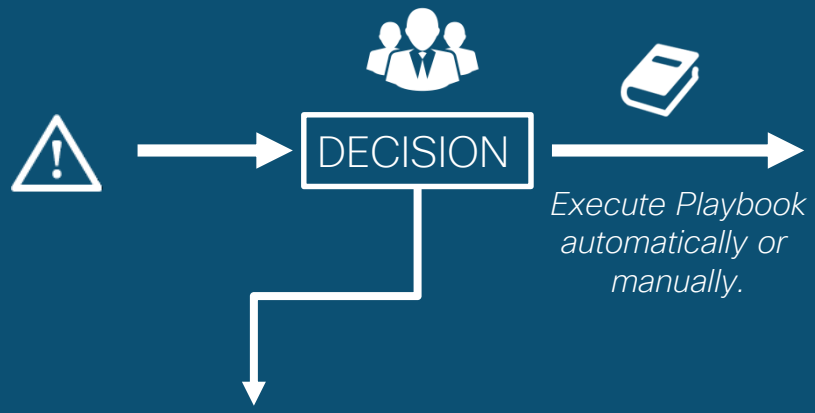
What was involved?

- One dashboard
- No copy and paste
- Time to triage and analyze is optimized

CREATE AND EXECUTE

PLAYBOOKS

TO RUN COURSES OF ACTIONS FOR YOU SECURITY TEAM WITH A SIMPLE CLICK



Execute Playbook automatically or manually.

Gain relevant data through orchestration of other tools in your network.

What is threat hunting and why it is important?

Proactive vs reactive

Hunters go out and look for intruders before any alerts are generate

Human-centric vs tool-centric

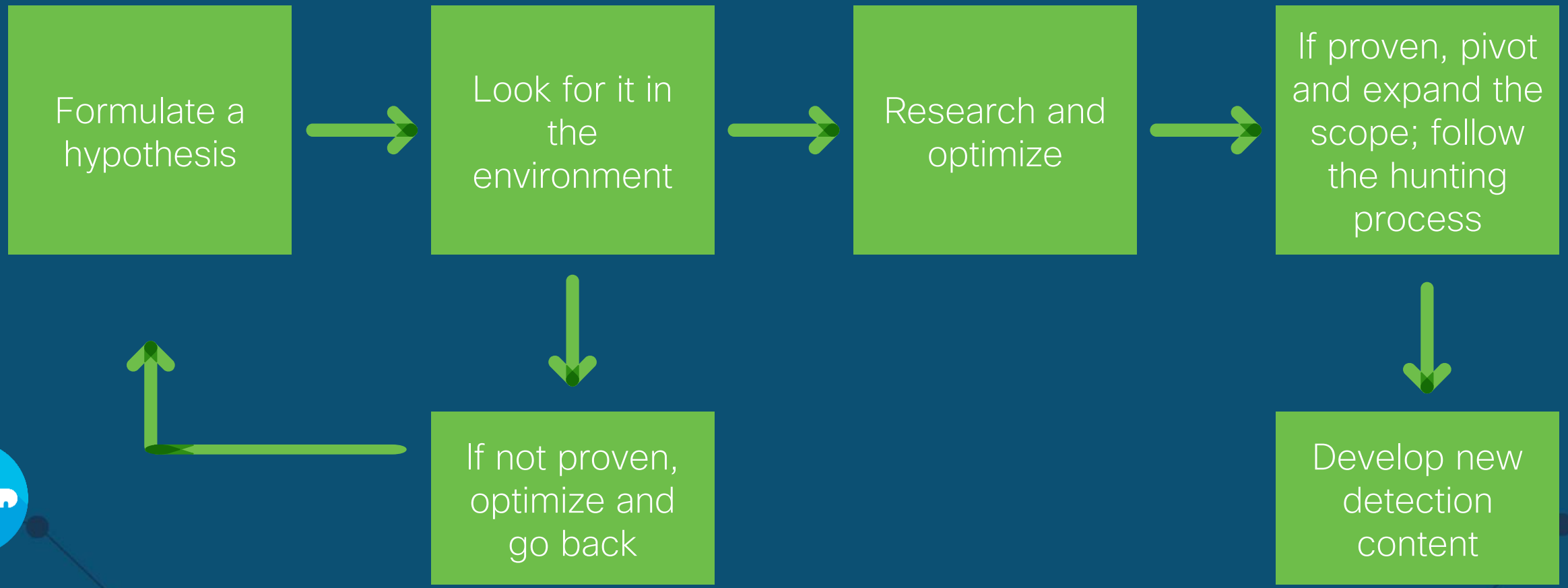
Starts with “a what-if question”, followed by an initial lead/clue, but then hunters take many twists and turns

Hunters do not follow rules, but can have a loose methodology

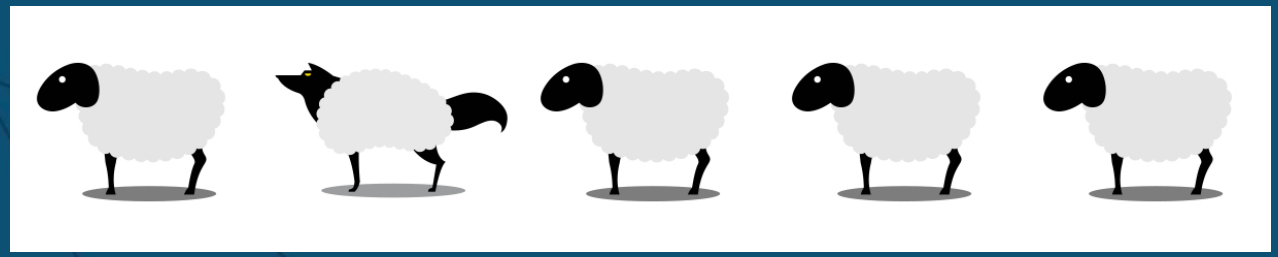
Initial steps can be scripted,
scheduled and automated!


Hunters are hungry for “big” data!

Threat Hunting – A Loose Methodology



Deception for Better Detection and Hunting



Focused on Internal Compromises

- Nothing superficial!
- Identify attacker lateral movement and reconnaissance activity targeting production-critical systems
- Embedded (deep) within the applications. Examples:
  - AD admin accounts (honey) with hashes available on systems in the network
  - SQL admin accounts (honey) with (honey) tables access
  - etc.
- Deception should be linked with detection, hunting and response.
- The practice should be heavily governed!
- Possible source of “light” threat intelligence (IOCS and TTPs)
- Link that with the broad threat intelligence (ex. decoy documents leaking outside the organization detected through TI or decoy documents calling home!)

What if?

About Us

The Cisco Security Incident Response Services team is comprised of an international ensemble of seasoned cyber security professionals possessing extensive experience in a variety of disciplines such as computer crime investigations, incident response, malware analysis, threat intelligence and more.

Comprised of selectively recruited consultants

International team of experts with diverse backgrounds

Ability to reach across the Cisco enterprise

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

A Winning Combination

Seasoned Investigators

+

TALOS

Deep Telemetry During an incident

Law Enforcement Interaction

Reverse Engineer Malware

Signature Creation

Deep & Dark Web Research

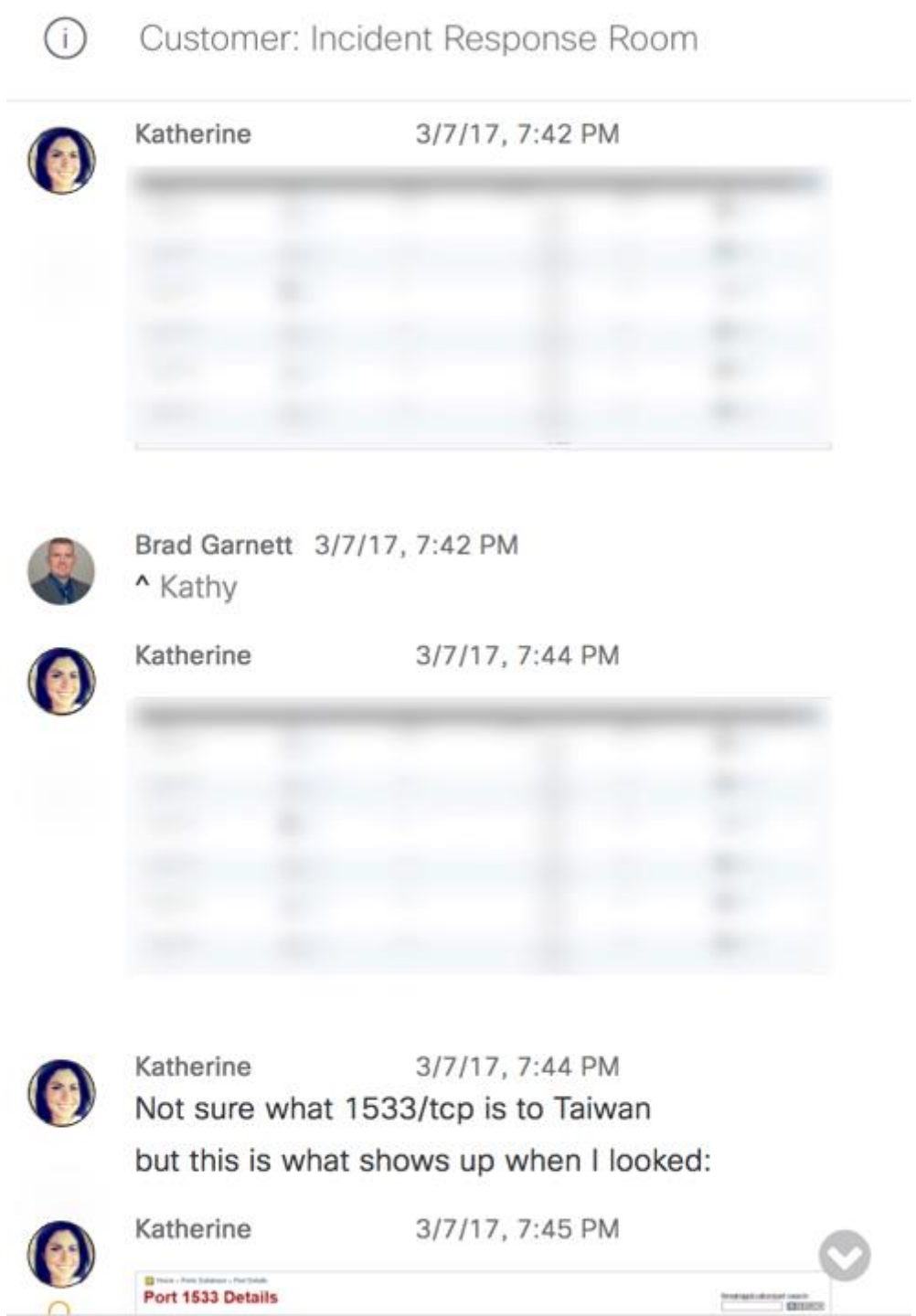
350+
Full Time Threat Intel Researchers

MILLIONS
Of Telemetry Agents

4
Global Data Centers

100+
Threat Intelligence Partners

1100+
Threat Traps



Collaboration

On-Demand

Cisco Collaboration technology allows for real time and coordination communication across organizations


Say hello
to the future.
Cisco Connect 2019
Bangkok, Thailand. 26 March 2019
#CiscoConnectTH