



Cognitive Threat Analytics Demo Script

October, 2016

CONTENTS

CONTENTS	1
1.0 Preface	3
2.0 Introducing the solution.....	3
3.0 Enabling CTA	4
3.1 CTA incidents in AMP console	6
3.2 Pivoting to CTA dashboard	6
3.3 Analyzing CTA events in AMP	7
3.3 Analyzing CTA events in AMP	10
4.0 Summary.....	14

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR INFORMATION.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPS WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

All contents are Copyright © 2016 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1.0 Preface

The following script is the talk track to give a proper demonstration of Cognitive Threat Analytics (CTA) using both the AMP console and the CTA portal. We have included screen shots to walk you through enabling CTA in AMP, as well as the demonstration itself. A video of the demonstration is available here:

<https://sharevideo.cisco.com/#/videos/58cb9941-3e86-4089-ad46-04c5dd899a06>

2.0 Introducing the solution

Today's malware is more evasive than ever. With the industry average time to detection of 200 days, you need to be quicker to catch threats that have bypassed your existing security controls. Cisco has now integrated Cisco Cognitive Threat Analytics with Cisco Advanced Malware Protection for Endpoints, to reduce that time to detection from months and days to minutes and seconds.

Cisco Cognitive Threat Analytics, or Cisco CTA, is a cloud-based software as a service (SaaS) security offering that turns an existing web proxy—such as Cisco Cloud Web Security (CWS), Cisco Web Security Appliance (WSA), or Blue Coat ProxySG—into a security sensor that analyzes traffic for command and control communications. Analyzing over 10 billion web requests per day, Cisco CTA finds breached devices infected with malware that have managed to bypass your traditional security controls. These breached devices will be operating inside your organization's environment, creating a major threat to your business through the potential loss of important and sensitive data.

Cisco CTA has additional benefits over traditional security products that require an agent or connector to function. Cisco CTA analyzes all web traffic across all devices throughout the network, providing security teams with threat intelligence into BYOD and the ever-expanding set of IoT devices such as printers and TVs.

Cisco Advanced Malware Protection for Endpoints, also known as AMP for Endpoints, is an endpoint prevention, detection, and response tool that continuously monitors, analyzes, and records all file and executable activity on endpoints, even after an initial inspection. It provides deep visibility into file activity and processes, and their interactions across all endpoints on the network, regardless of file disposition. With a few clicks from AMP's browser-based management console, a file and any associated processes can be blocked from executing on all endpoint's across the network.

Integrating Cisco CTA into Cisco AMP for endpoints, correlates the detailed endpoint data from Cisco AMP with threat focused outbound web communications discovered in Cisco CTA. The result? Cisco AMP for Endpoints is now seeing about 30% more breaches & infections thanks to this integration. Furthermore, Cisco AMP for endpoints provides the context for those breaches & infections detected by Cisco CTA.

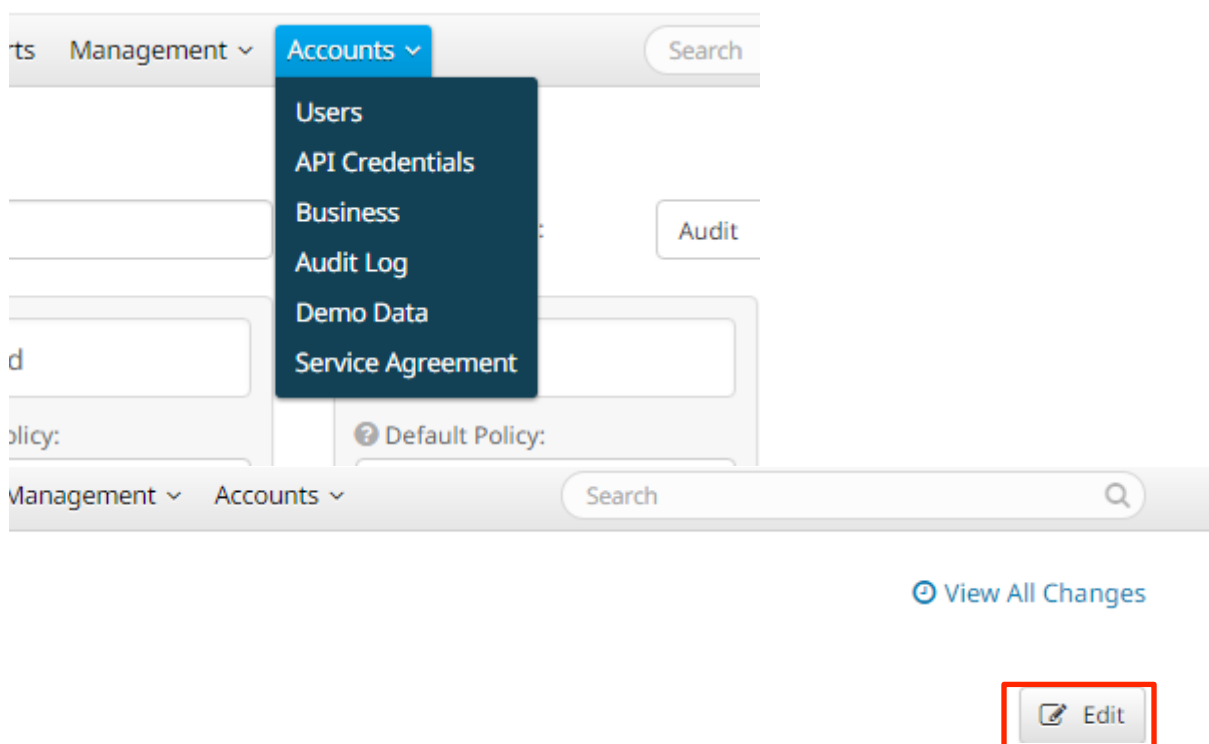
To give the field simple to use demonstration capability, the standard demo data in Cisco AMP now includes results from the Cisco CTA integration.

3.0 Enabling CTA

Cisco CTA is available for all Cisco AMP for Endpoints customers – meaning that any customer, new or existing can leverage Cisco CTA to get more value out of their existing Cisco AMP for endpoints investment. Cisco CTA has fast become an integral & essential part of the Cisco AMP story which underpins the Cisco Security Architecture.

The integration between Cisco AMP for endpoints and Cisco CTA is extremely simple to manage & execute. As I am about to demonstrate, enabling Cisco CTA on Cisco AMP for endpoints does not require anything more than simply enabling it in settings and it's provisioning is fully automated.

First we enable Cisco CTA simply by clicking a button on the Business page.



Here you click on Enable. After a couple of seconds, CTA is added to Cisco AMP for endpoints:

Cisco Cognitive Threat Analytics

Cognitive Threat Analytics Integration: Disabled

Enable

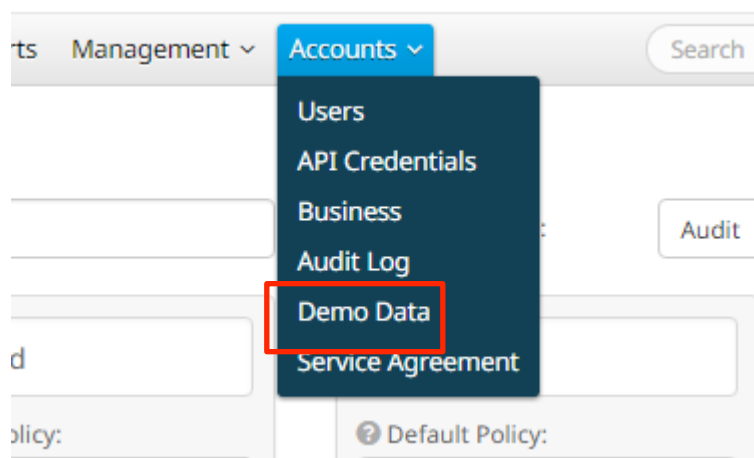
Configure

? [Learn More About CTA](#)

Required next steps

- For **Cisco WSA** or **BlueCoat ProxySG** - choose "Configure" to walk through a wizard that will help you configure CTA for ingesting logs
- For **Cisco CWS** please contact [Support](#) to link your existing account to your AMP for Endpoints business.

You can showcase the Cisco CTA integration using the standard Demo Data functionality found within Cisco AMP for Endpoints.



Let's have a look the demo data with Cisco CTA integration enabled.

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by will add computers and events to your Cisco AMP for Endpoints Con Detections and Events displays behave when malware is detected. D because of the severity of some of the Demo Data malware it may o

To include Cognitive Threat events in your Demo Data enable Cogni you will need to Refresh it to see Cognitive Threat events.

Refresh Demo Data

Disable Demo Data

3.1 CTA incidents in AMP console

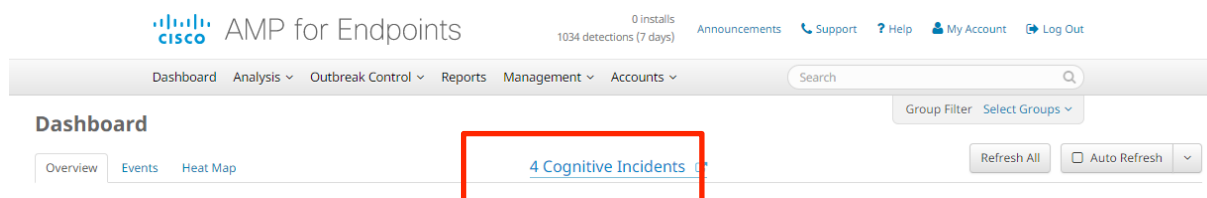
As you would expect, Cisco CTA detects breaches & infections, so Cisco CTA findings are shown in the IOC section of the dashboard.

In general, Cisco AMP for endpoints provides specific information about known files and Malware on each individual endpoint. Cisco CTA is different in this respect as it is designed to detect both known and unknown infections and provides detailed information about the whole threat campaign operating within the network. Cisco CTA displays this contextual threat information within the Cisco AMP for Endpoints dashboard, in the form of additional endpoint indicators of compromise and a list of active infections prioritized by risk.

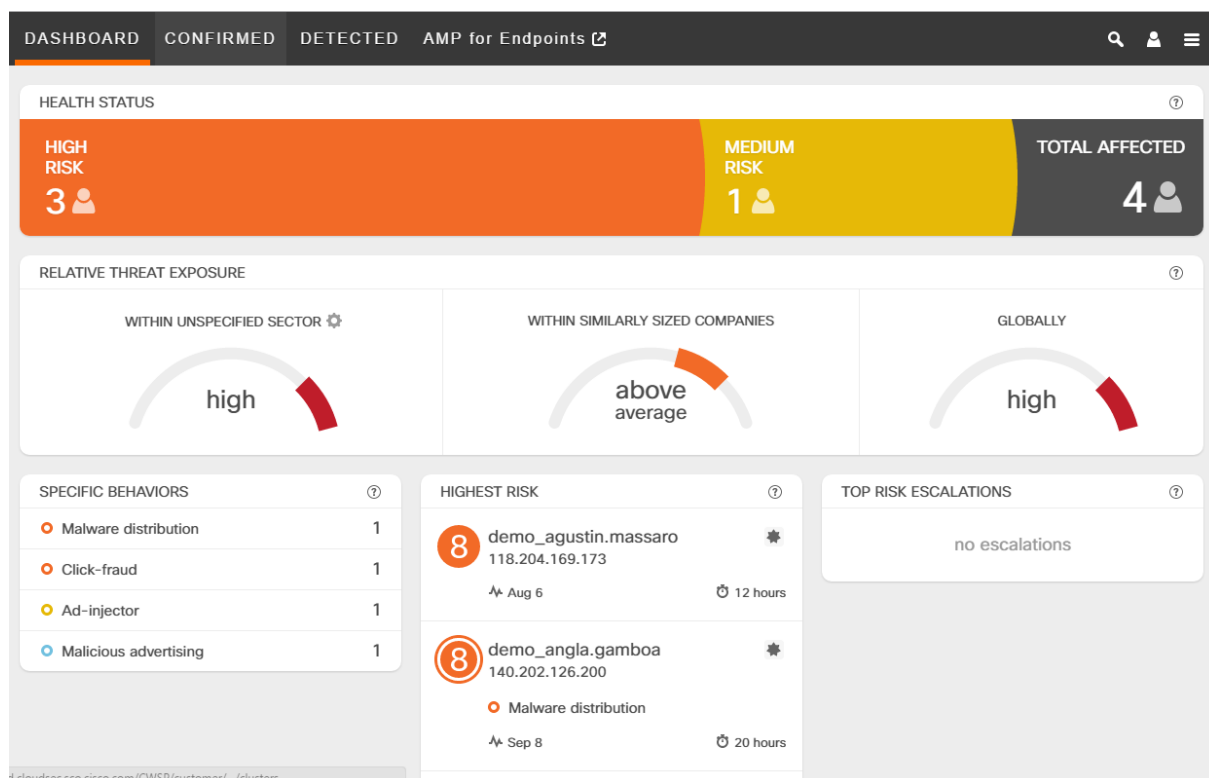
For enhanced detailed information about specific threats detected by Cisco CTA, we can click through the link on the Cisco AMP for Endpoints dashboard which redirects us to the Cisco CTA Dashboard.

3.2 Pivoting to CTA dashboard

The Cisco CTA dashboard provides us with a high-level overview of the security stance of the company as a whole and provides us with answers to the high level questions security teams get asked including “how secure are we?”, “what threats are affecting our network today?” and “how healthy is our network?”



The CTA Dashboard shows the highest risk incidents that require immediate attention. The Cisco CTA dashboard also allows us to make direct comparisons about the threats faced by our organization and those of a similar size within the same field or vertical. Cisco CTA achieves this by benchmarking both the number and risk of incidents as well as profiling your organization’s network size. It then compares the results to trends measured across Cisco’s entire customer base.








To see how results from Cisco CTA are correlated with Cisco AMP for endpoints lets go back to the Cisco AMP Console.

(close the window, back to AMP Console)

3.3 Analyzing CTA events in AMP

Cisco CTA detections are automatically shown in the IOC section in the Cisco AMP for endpoints Dashboard as they represent active infections.

Indications of Compromise		
Demo_Cta		Mark Resolved
Threat Detected , Potential Dropper Infection , Cognitive Threat		
Demo_TeslaCrypt		Mark Resolved
Threat Detected , Executed malware , Potential Dropper Infection		
Demo_Dyre		Mark Resolved
Threat Detected , Executed malware		
Demo_ZAccess		Mark Resolved
Threat Detected , Potential Dropper Infection , Java compromise , Executed malware		
Demo_CozyDuke		Mark Resolved
Threat Detected , Executed malware		

As you click on the device name, you will see the events from both Cisco AMP for endpoints and Cisco CTA that relate to this specific infected computer. Clicking the Event Type takes you straight to the relevant portion of the Device Trajectory within Cisco AMP for Endpoints. Clicking the computer name brings up all relevant Events for that device.

(click Demo_Cta IoC)

The presence of the Cisco CTA detection means that malware was not completely prevented from running and is currently active within our environment. Thanks to the integration between Cisco AMP for endpoints and Cisco CTA, we can look into the trajectory to reveal those remaining active malware components – and block them with Cisco AMP for endpoints.

Cognitive Threat Analytics Demo Script

Overview Events Heat Map 4 Cognitive Incidents

Filter: (New) Select a Filter

Event Type All Event Types + Group All Groups +

Filters X Computer: 828ef78f-f12f-42f2-a6da-ac5a4672e794

Sort Time

Not Subscribed Reset Save Filter As...

Demo_Cta Cognitive Threat Analytics detected CTA.malware.salinity communicating from 140.202.126.200	Cognitive Threat	2016-09-08 13:32:30 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 22:54:05 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 22:44:00 UTC
Demo_Cta detected winfeqy.exe as W32.B7B28E855B-100.SBX.VIOC	Quarantine: Not Seen	2016-09-07 21:13:04 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 19:38:56 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 19:33:58 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 18:54:05 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 18:44:00 UTC

276 total events 20 / page 1 of 14 Export to CSV

Let's expand a Cisco CTA Event and take a look at the details within. All of the important information is summarized here. This includes any command and control channels, URLs and malicious activities detected on this endpoint.

Demo_Cta Cognitive Threat Analytics detected CTA.malware.salinity communicating from 140.202.126.200	Cognitive Threat	2016-09-08 13:32:30 UTC
--	------------------	-------------------------

Cognitive Threat	Detection	CTA.malware.salinity
Connector Info	Category	malware
Comments	Local IP Addresses	140.202.126.200
	Remote IP Addresses	119.59.104.21 181.88.192.62 192.185.190.9 202.163.115.10 52.28.249.128
	Activities	salinity (severity: 9) salinity (severity: 8) anomalous http (severity: 8) malware distribution (severity: 8)
	URL Samples	http://www.bijibali.com/images/logof.gif?14f03da=153688822 http://paktexileindustries.com/images/logos.gif?14eea67=131694186 http://patagonia-ambient.com.ar/logos.gif?14ef489=87806500 http://www.ktscc.org/logo.gif?14f04e4=21955812 http://inspiringgemsshop.com/images/logo.gif?14f04d4=197602164 http://inspiringgemsshop.com/images/logo.gif?16f34d2=96260936 http://paktexileindustries.com/images/logos.gif?16f1b5e=192469744 http://patagonia-ambient.com.ar/logos.gif?16f2580=96245248 http://www.bijibali.com/images/logof.gif?16f33b9=168454671 http://www.ktscc.org/logo.gif?16f34e2=192522000 http://patagonia-ambient.com.ar/logos.gif?2f17744=345653980 http://www.ktscc.org/logo.gif?2f187bf=345683513 http://www.bijibali.com/images/logof.gif?2f18696=148149186 http://paktexileindustries.com/images/logos.gif?2f16d22=148129638 http://inspiringgemsshop.com/images/logo.gif?2f187a0=493833280

Run Scan Device Trajectory Management

Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 22:54:05 UTC
Demo_Cta detected multiple infected files	Multiple Infections	2016-09-07 22:44:00 UTC

Clicking the small arrow takes us to the individual Incident within the Cisco CTA portal.

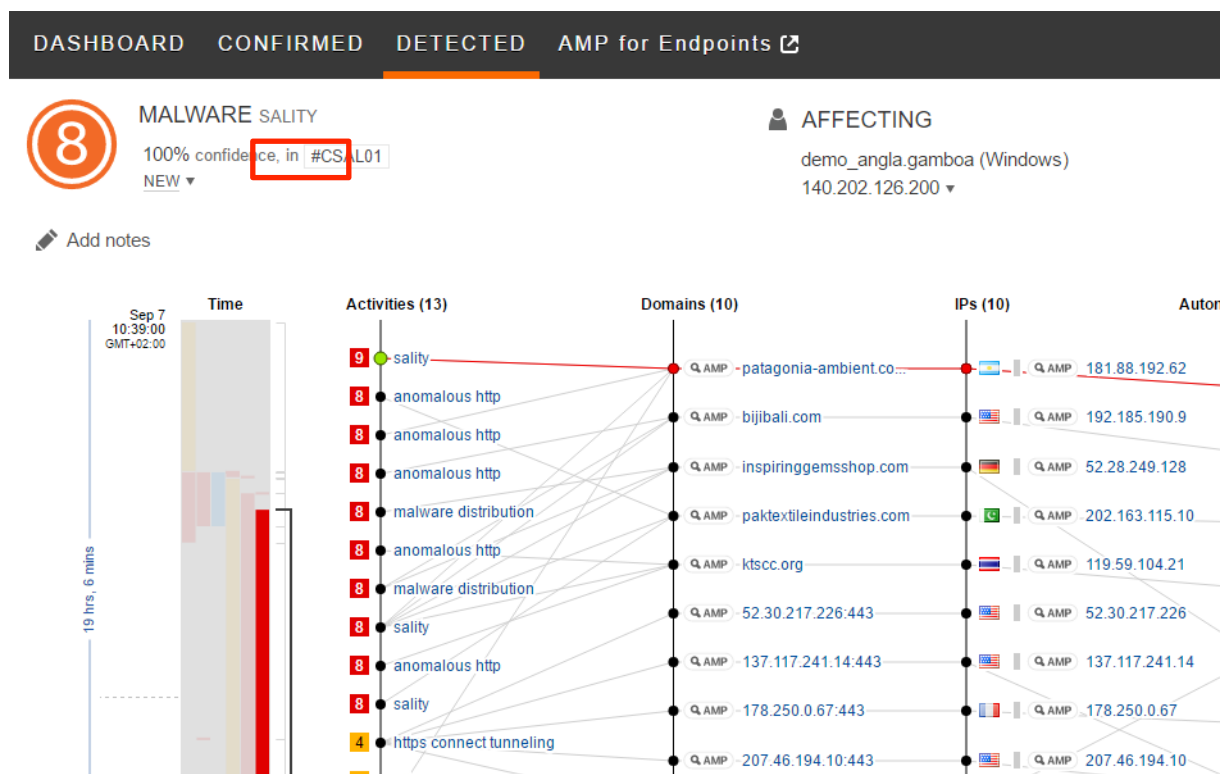
Demo_Cta Cognitive Threat Analytics detected CTA.malware.sality communicating from 140.202.126.200		
Cognitive Threat	Detection	CTA.malware.sality
Connector Info	Category	Open event detail in Cognitive Threat Analytics
Comments	Local IP Addresses	140.202.126.200
	Remote IP Addresses	119.59.104.21 181.88.192.62 192.185.190.9 202.163.115.10 52.28.249.128

3.3 Analyzing CTA events in AMP

As Cisco CTA tracks entire threat campaigns, in most cases we can quickly see who the attacker is, what techniques are in use and how to eradicate such infection by simply reviewing the associated campaign. This helps tremendously with prioritization and scoping. Here we can see all of the individual connections that CTA has detected that correspond to the threat over time. Cisco Cognitive Threat Analytics is designed to detect Command and Control channels which are used by Malware.

We can see that Cisco Cognitive Threat Analytics has classified the communication channels into several different categories, with severity 9 being the highest threat. We can see that the many different communication activities are going to various URLs and IPs located around the world. These URLs and IPs are hosted on a variety of different autonomous systems, showing the global nature of this threat.

Looking at the bottom of the screen, you can see a detailed list of all the detected requests, URLs and files that have been downloaded as well as the amount of traffic that has been transferred during this incident. The amount of traffic transferred can be an indicator of whether data theft has been a part of this attack.



(Click the cluster label #CSAL01 to get to the confirmed incident section)

We can now go over to the confirmed threat page to understand detailed information about this threat campaign:

1. We can see immediately what risk this threat presents – This threat has a risk score of 8 out of 10 and Cisco Cognitive Threat Analytics has a confidence level of 100% that it knows what it is.
2. We can see the number of affected users as well as the infection history; in this case it is a Single user in our organisation that has been infected.
3. The threat description written here in plain English, clearly states that the Sality botnet resides in memory, disables anti-virus and is designed to communicate with a command and control infrastructure. The recommended response to this threat is to wipe any infected machines.
4. The Occurrence data tells us that this threat has been within our organisation for 20 hours and the date it was first seen.
5. Here is the Global Benchmark – We can see that this campaign is quite well spread throughout the world, affecting 50+ users in 30+ companies. This information is useful as it can indicate a potential targeted attack, which we would need to prioritise.

Cognitive Threat Analytics Demo Script

The screenshot shows the CTA dashboard with the following sections:

- Navigation Bar:** DASHBOARD, CONFIRMED, DETECTED, AMP for Endpoints.
- Threat Summary:**
 - #CSAL01:** 100% confidence.
 - AFFECTING:** 1 user, Windows; 50+ users in 20+ companies.
 - OCCURRENCE:** 20 hours; Sep 7 - Sep 8.
- Add notes:** A red box highlights a note: "Threat related to the Salty botnet which is dynamic, modular, and resilient. Resides in memory and attempts to disable antivirus solutions. Spreads by infecting existing files in network shares. Command-and-control communication can be established through HTTP or using peer-to-peer communication. Generally classified as a high-risk threat. Perform a full scan of the infected device for the record and then reimaging the device."
- AFFECTED USERS:** 1 user affected by this threat during the last 45 days with unresolved incidents. User: demo_angla.gamboa.
- INFECTION HISTORY:** Number of users exhibiting malicious behaviors during the 44 days before yesterday. A bar chart shows active infections over time, with a peak on Sep 4.
- Threat Details List:**
 - #CMST01: 8 risk, last seen Aug 6, 2016 for 6 hours.
 - #CSAL01: 8 risk, last seen Sep 8, 2016 for 20 hours.
 - #CAMZ02: 7 risk, last seen Aug 6, 2016 for 9 hours.
 - #CSPF01: 4 risk, last seen Aug 6, 2016 for 9 hours.

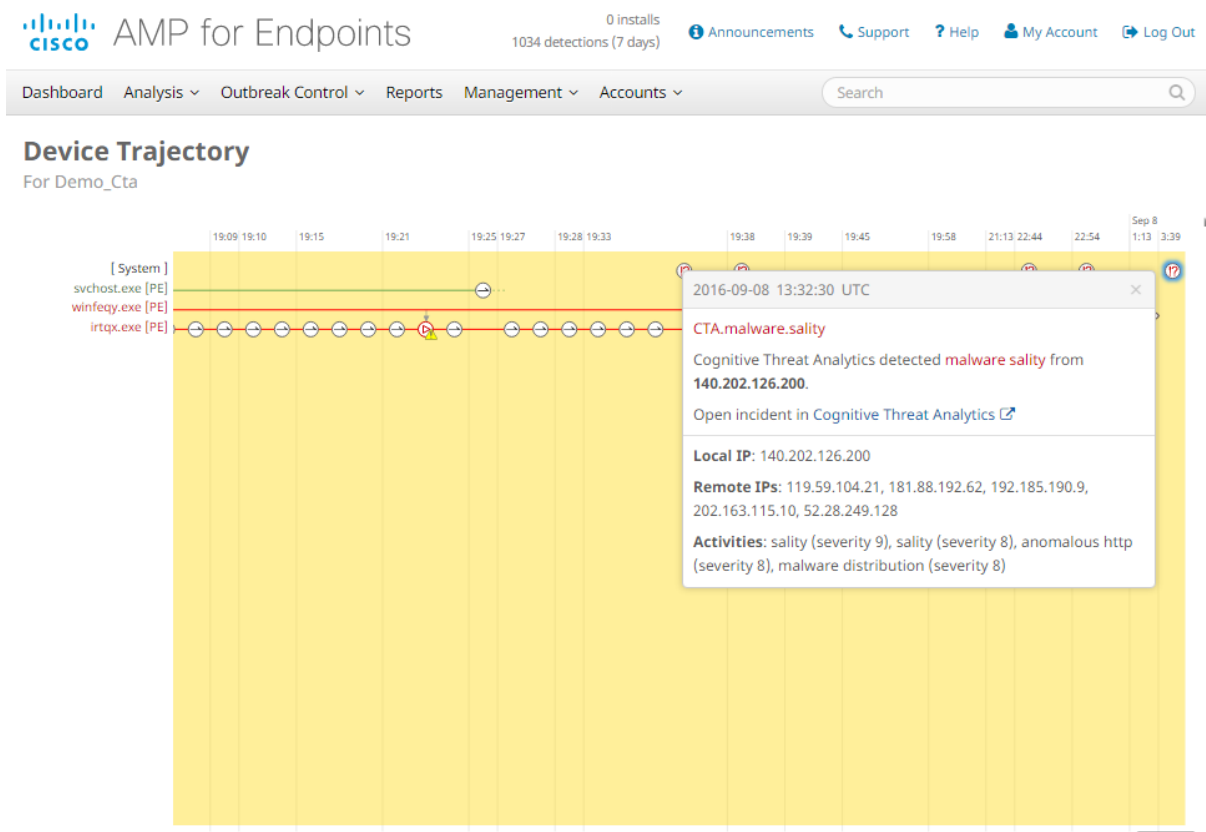
(Close CTA tab, go back to AMP and click the trajectory button on the CTA Event)

Now that we understand that this threat is serious with the loss of data very real through the attacker's command and control infrastructure, we need to stop it in its tracks. We will need to go back to the Cisco AMP for endpoints console to perform the actions needed to eradicate it, by blocking any malicious binaries associated with it.

The screenshot shows the Cisco AMP for Endpoints console with the following sections:

- Navigation Bar:** Overview, Events, Heat Map. 4 Cognitive Incidents.
- Filter:** (New) Select a Filter.
- Event Type:** All Event Types.
- Group:** All Groups.
- Filters:** Computer: 828ef78f-f12f-42f2-a6da-ac5a4672e794.
- Sort:** Time.
- Buttons:** Not Subscribed, Reset, Save Filter As...
- Event Details:**
 - Demo_Cta:** Cognitive Threat Analytics detected CTA.malware.sality communicating from 140.202.126.200.
 - Cognitive Threat:** Detection: CTA.malware.sality.
 - Connector Info:** Category: Open event detail in Cognitive Threat Analytics.
 - Comments:** Local IP Addresses: 140.202.126.200.

Looking at the Salty threat in AMP for endpoints, we need to click on the device trajectory button in the AMP for endpoints console.

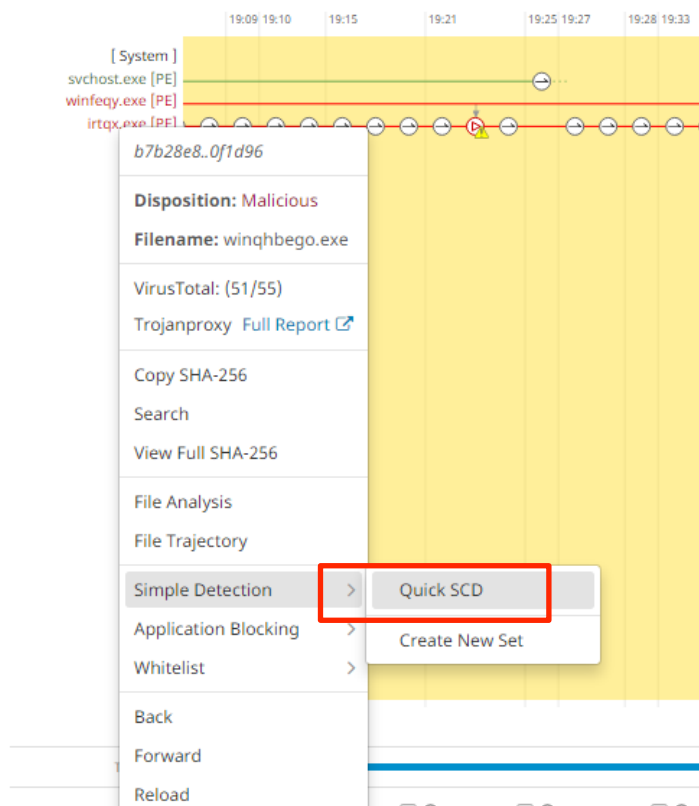


The highlighted yellow bar, shows us the span of the Cisco CTA detection. The icon provides us with information about file activity specifically related to the Sality infection on the endpoint. The power of Cisco AMP is in its ability to selectively block specific files associated with an infection, everywhere in the environment where Cisco AMP for Endpoints is installed. We will use the standard Simple Detection to do that to prevent Sality from running on the infected endpoint.

(right-click on *irtqx.exe*, select Simple Detection and Quick SCD)

Device Trajectory

For Demo_Cta



By blocking the files, we are stopping the malicious binaries that were participating in the command and control activity, thus blocking attackers from remotely stealing our sensitive data.

4.0 Summary

In cases such as these, Cisco's likely recommendation would be to reimage any infected machines to ensure that they are free from any remaining malicious artifacts. For widespread persistent and repeating infections, a root cause analysis using Cisco AMP for Endpoints can be a better course of action. Cisco AMP for Endpoints can reveal the initial attack vector and block files and processes fixing any widespread vulnerabilities and preventing them from being exploited in further attacks.

We have demonstrated how a Cisco integrated security architecture can vastly reduce the time to detection and how quickly we can remediate both known and unknown threats simply at the click of a button.