White paper
Cisco Public

Cisco Threat Response

Supporting Intelligence-Driven Incident Response and Threat Hunting

Abstract

The intended audience of this paper are security analysts that are involved with incident response and already using or considering using cyber threat intelligence in their operations.

This paper will describe Cisco Threat Response, a new security tool from Cisco that improves the ability of security operations teams, primarily threat hunters and incident responders, to find and respond to threats within their infrastructure. It does so by combining global and local threat intelligence and context from Cisco and 3rd parties. We will examine the F3EAD model of threat intelligence-driven response, and show how Cisco Threat Response aids the performance of each of the phases therein.

Contents

Cybersecurity operations can be defined as those functions which include incident monitoring, detection, response, coordination, computer network defense tool engineering, operation and maintenance. (Zimmerman, 2014)

Introduction to Cisco Threat Response

At the heart of cybersecurity operations are the men and women responsible for monitoring and defending the environment against cyber threats. The goal is to mitigate and control the cyber threat before it becomes an incident that affects the normal course of operation of an entity. These are the primary users of cybersecurity operations tools.

It therefore becomes important for us to always be grounded in the contextual user experience across the functions that are performed in the cyber security operations center. To complicate the contextual user experience further, there are multiple security tools in the operations center –the implication being multiple vendors and interfaces that may or may not be integrated.

Cisco Threat Response was built to support network operations teams and help incident responders understand threats on their network -by gathering, combining, and correlating threat intelligence available from the Cisco Talos Intelligence group, other Cisco products, and third parties with their own organization's recorded network and security data.

Each source of either global or local intelligence is provided by a module. Some of the threat intelligence modules are provided by default; others need to be added and configured by the user. Typically,in these cases, users provide the linkage between their deployments or subscriptions and the Cisco Threat Response portal via an API key. When referring to this flexibility of the Cisco Threat Response service, think of this as a Bring-Your-Own-API model. To integrate with Cisco Threat Response, a user provides the API key(s) of the services they wish to integrate.

In short, Cisco Threat Response brings together threat intelligence,and local security context and control, into one place for the security analyst. The next two sections will describe how and from where each of these is provided.

Threat Intelligence

Several Threat Intelligence modules are provided by default as part of Cisco Threat Response. Others are optional and can be added and configured with the appropriate API keys for the integrated services.

Talos Intelligence

Cisco Threat Response contains a Talos Intelligence enrichment module that requires no manual configuration. Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. These teams are supported by unrivaled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers, products and services. Talos defends Cisco customers against known and emerging threats, discovers new vulnerabilities in common software, and interdicts threats in the wild before they can further harm the internet at large. Talos maintains the official rule sets of Snort.org,ClamAV, and SpamCop, in addition to releasing many open-source research and analysis tools. Talos was formed by combining SourceFire's Vulnerability Research Team, the Cisco Threat Research and Communications group, and the Cisco Security Applications Group. Their combined expertise is backed by a sophisticated infrastructure, and Cisco's unrivaled telemetry of data that spans across networks, endpoints, cloud environments, virtual systems, and daily web and email traffic. Talos utilizes its extensive threat intelligence to make the internet safer for everyone.

AMP File Reputation

Cisco's Advanced Malware Protection File Reputation database houses billions of file hashes and dispositions, and is also known as AMP Protect DB. This is the database that drives the powerful file reputation capabilities behind all AMP-enabled products. It is integrated by default with Cisco Threat Response.

AMP Global Intelligence

AMP Global Intelligence is another Advanced Malware Protection dataset, curated from dozens of independent data sources. While initially implemented for use by the AMP platform, Cisco Threat Response is also able to leverage this powerful collection by default. AMP Global Intelligence includes intelligence from Threat Grid and other Cisco and third-party intelligence sources.

Threat Grid

Threat Grid is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment. In the integration with Cisco Threat Response, Threat Grid is a reference module which can enrich information presented in the Cisco Threat Response graph. With an active Threat Grid portal subscription, security analyst scan optionally configure this module to allow for pivoting into the Threat Grid portal to gather additional intelligence about file hashes, IPs, domains and URLs in Threat Grid's knowledge store.

Umbrella Investigate Threat Intelligence

Cisco Threat Response includes Umbrella Investigate as an enrichment module for observations. Umbrella Investigate was built in order to predict, identify, and investigate the internet origin of attacks. Umbrella Investigate leverages data mining and algorithmic classification techniques such as machine learning, graph theory, anomaly detection, and temporal patterns in combination with contextual search, visualization, and scoring. *Note: In the Cisco Threat Response interface, the Umbrella Investigate Module has an enrichment and a response action. For the enrichment action, an Umbrella Investigate API key is not needed with Cisco Threat Response. For the response action, an Umbrella Platform API key is required.*

VirusTotal

VirusTotal inspects items with over 70 antivirus (AV) scanner and URL/domain blacklisting services, in addition to a myriad of tools to extract signals from the submitted content. In the incident response process, it allows users to query a URL, IP address, domain or file hash to gain additional context from the AV scanners and services as to the threats associated with the sample.

Users may register for a free Virus Total account, and receive an API key. This optional module allows users with an API key to have Threat Response use it on their behalf to include VirusTotal query results in any investigation.

The other half of the Cisco Threat Response equation is local security context –what is happening on your network. This is also provided via an assortment of modules, all optional and easily configured by the user via API Keys.

Local Security Context and Control

Advanced Malware Protection (AMP) for Endpoints

A core part of the endpoint security platform, AMP for Endpoints is deployed as a preventative and investigative tool supporting detection and/or response functions for Windows, MacOS, Linux, Android and iOS devices.

When operating AMP for Endpoints, security analysts are able to perform the following incident response functions:

- Search endpoint telemetry by file, host name, URL, IP address, device name, user name and others.
- Block files on Windows, MacOS and Linux platforms by a Simple Custom Detection (SCD) –which comprises one or more SHA 256 hashes of the desired file to be block. Should that file hash be found on any endpoint with the above Operating System, it will be deleted immediately without user intervention.
- Create lists of APKs that, if seen by AMP for Android, will generate warnings on the Android device that prompt users to remove those unwanted applications.
- Apply application safe-lists and block-lists based on the SHA-256 hash of the executable.
- Perform advanced custom detections based on various kinds of user-written signatures.

Cisco Threat Response supports AMP for Endpoints as an integration module that allows security analysts to:

- Enrich investigations with relevant AMP events and local context.
- Block and unblock file hashes directly from the Cisco Threat Response interface.

Cisco Umbrella Platform

This is Cisco's recursive Domain Name Service (DNS) that offers users preventative controls and investigative tools offering protection against known sites that pose cybersecurity risks. Using the Umbrella Platform in the incident response process, the Umbrella portal allows security analysts to:

- Search DNS queries by internal network identities, domains,URLs and IPs.
- Block domains that are may not currently be known to be malicious.
- Enforce the blocking and unblocking of domains via an API.

Cisco Threat Response supports the Umbrella Platform as a response module–with the ability to block and unblock domains directly in Cisco Threat Response. While Umbrella provides both global threat intelligence, and local context and control, all these functions are handled by a single Umbrella module.

Cisco Threat Response in the Incident-response and Intelligence Cycle

Introduction to F3EAD

Recommended reading to understand how intelligence fits into the incident response process is Intelligence-Driven Incident Response by Scott J. Roberts and Rebekah Brown. Published by O'Reilly Media, Inc. ISBN: 978-1-491-93494-4

Threat Intelligence and Incident Response are both mature disciplines, each with many defined models and frameworks for adoption and operation, to help guide practitioners. Let's examine some representative models and see how best to tie them together into a useful framework for threat hunting.

The Incident Response cycle can be summarized as Preparation, Identification, Containment, Eradication, Recovery and Post-Incident Activity. (Cichonski, Millar, Grance, & Scarfone, 2012) Figure 1 illustrates the Incident Response cycle.

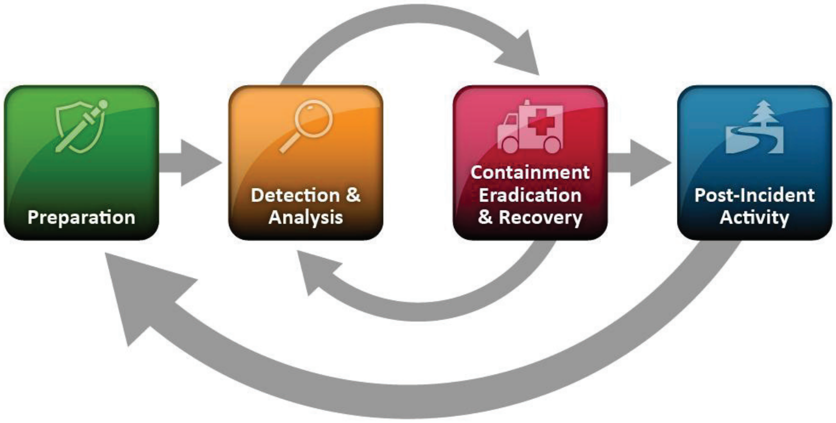


Figure 1: Incident Response Cycle – Source: NIST SP800-61r2

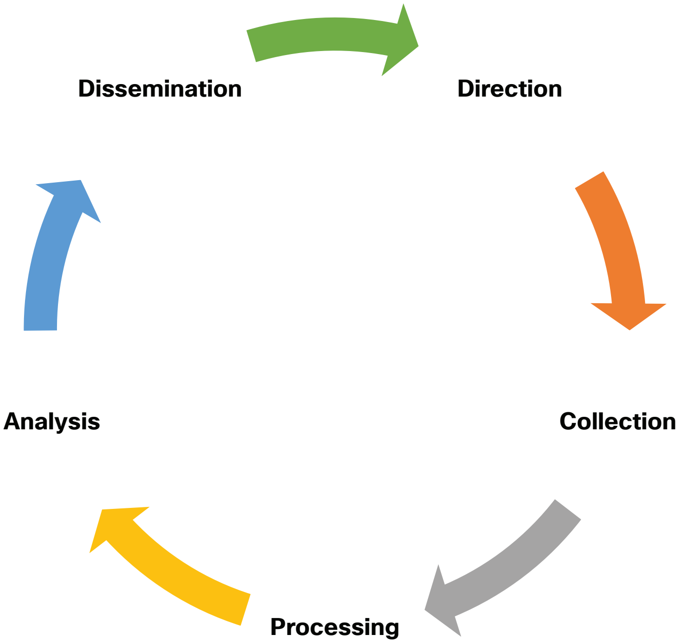


Figure 2: The Intelligence Cycle.

The Intelligence cycle can be summarized as Direction, Collection, Processing, Analysis and Dissemination. (The United States Intelligence Community, 2018) Figure 2 illustrates the Intelligence cycle.

One of the models that can be applied to Cyber Threat Hunting is F3EAD – pronounced "feed". F3EAD combines elements of the Incident Response cycle and the Intelligence cycle.

In the application of the model to cybersecurity incident response, it consists of the following phases:

Find: This stage determines the threats that the hunters will address. This information can come from many sources including private and third-party intelligence feeds. This phase is analogous to the Preparation phase of the Incident Response cycle.

Fix: In this phase, the cybersecurity defenders will work to locate the telemetry involved with the intelligence identified in the prior phase. This phase is analogous to the Identification phase of the Incident Response cycle.

Finish: This is when the cybersecurity defenders takes decisive action against the actor, going through the Containment, Mitigation and Eradication phases of the Incident Response cycle.

Find, Fix and Finish are the Incident Response portions of the F3EAD model. The following phases are involved with the Intelligence portions of the F3EAD model.

Exploit: This is the Collection phase of the Intelligence cycle. It could involve using the evidence from the Finish phase that may be useful to the defenders. Any indicators of compromise, malware samples and common vulnerabilities and exposure identifiers are amongst pieces of information that will be collected in this phase.

Analyze: The objective during this phase is to develop the information collected. The development of this information will help paint a bigger picture of the initial observable or indicator with the goal of gaining deeper understanding of the extent of the threat so that actors and associated indicators can be detected, mitigated and remediated.

Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

Cisco Threat Response supports security analysts to perform intelligence-driven incident response.

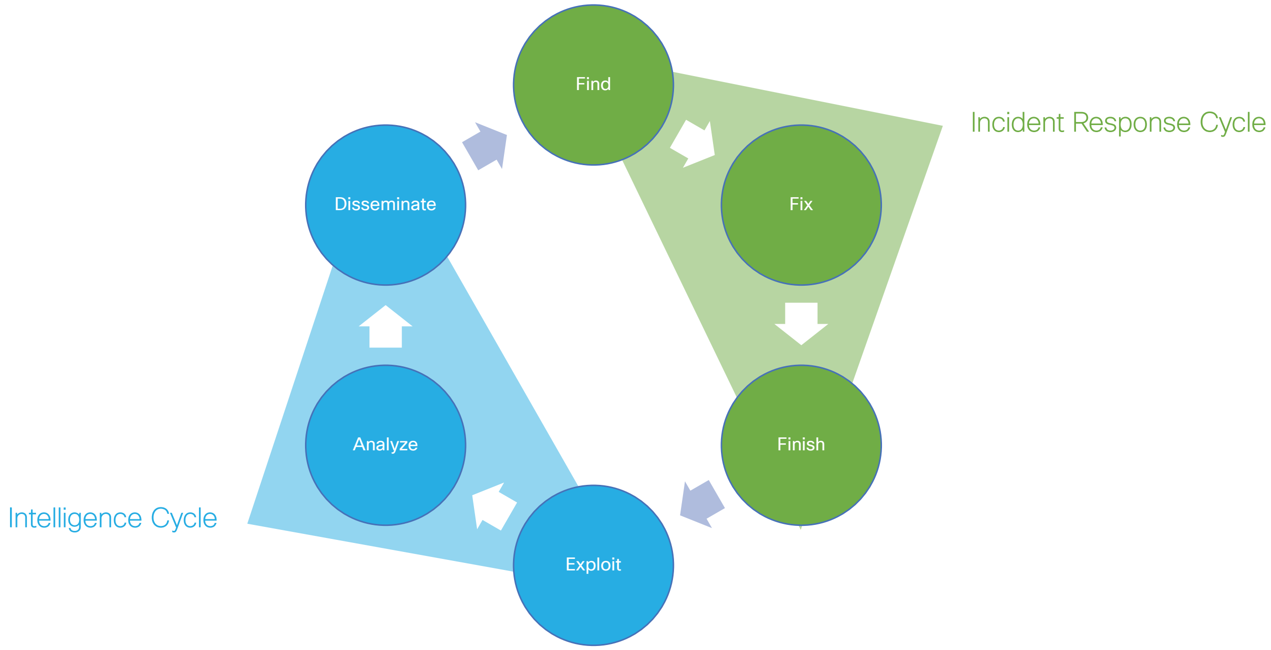


Figure 3: F3EAD Model

Applying the F3EAD model and Cisco Threat Response to a real-world case

Consider an industry bulletin from a trusted group that advises organizations to look for certain pieces of information. For the purpose of this paper, consider the bulletin to be a Malware Analysis Report (MAR) issued by the United States Computer Emergency Readiness Team, US-CERT.

"DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity."

Please review the details here: https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

Find

Your organization may deem the US-CERT to be a knowledgeable and trusted source of information and that your team should act on bulletins issued by said entity and are prepared to act on this intelligence. In the Incident Response cycle, this is your Preparation. Information has been disseminated. You and your team are consumers of this information.

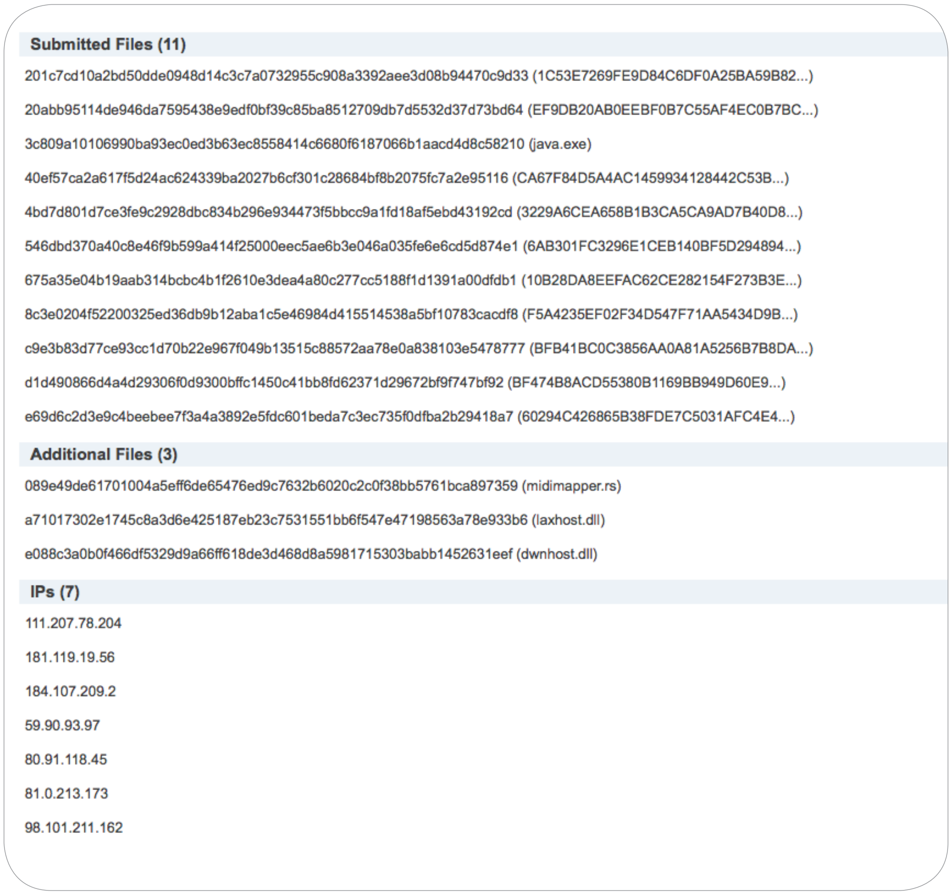
Fix

The Fix phase of the F3EAD model focuses on searching for and attempting to locate any telemetry associated with this information identified in the Find phase.

Cisco Threat Response allows defenders to copy indicators directly from a source (without edits) and paste that directly into the Investigate window. The benefit here is one of speed saving analysts time to format and edit indicators.

The analyst can paste this directly into the Investigate console of Cisco Threat Response.

Figure 5 shows the indicators being pasted into the Cisco Threat Response Investigate console.



Submitted Files (11)

201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33 (1C53E7269FE9D84C6DF0A25BA59B82...)

20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64 (EF9DB20AB0EEBF0B7C55AF4EC0B7BC...)

3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210 (java.exe)

40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116 (CA67F84D5A4AC1459934128442C53B...)

4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd (3229A6CEA658B1B3CA5CA9AD7B40D8...)

546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1 (6AB301FC3296E1CEB140BF5D294894...)

675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1 (10B28DA8EEFAC62CE282154F273B3E...)

8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8 (F5A4235EF02F34D547F71AA5434D9B...)

c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777 (BFB41BC0C3856AA0A81A5256B7B8DA...)

d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92 (BF474B8ACD55380B1169BB949D60E9...)

e69d6c2d3e9c4beebee7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7 (60294C426865B38FDE7C5031AFC4E4...)

Additional Files (3)

089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359 (midimapper.rs)

a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6 (laxhost.dll)

e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef (dwnhost.dll)

IPs (7)

111.207.78.204

181.119.19.56

184.107.209.2

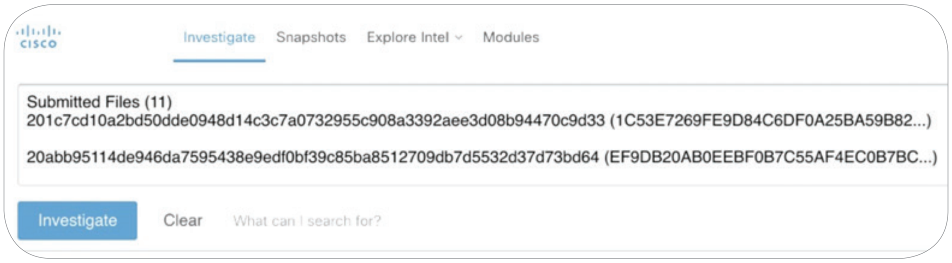
59.90.93.97

80.91.118.45

81.0.213.173

98.101.211.162

Figure 4: HIDDENCOBRA TYPEFRAME indicators



Submitted Files (11)
201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33 (1C53E7269FE9D84C6DF0A25BA59B82...)

20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64 (EF9DB20AB0EEBF0B7C55AF4EC0B7BC...)

Figure 5: Investigate Console of Cisco Threat Response

Cisco Threat Response queries all configured Modules and returns that data to the user in a graph. Figure 6 illustrates the first half of the results graph being returned from the initial search.

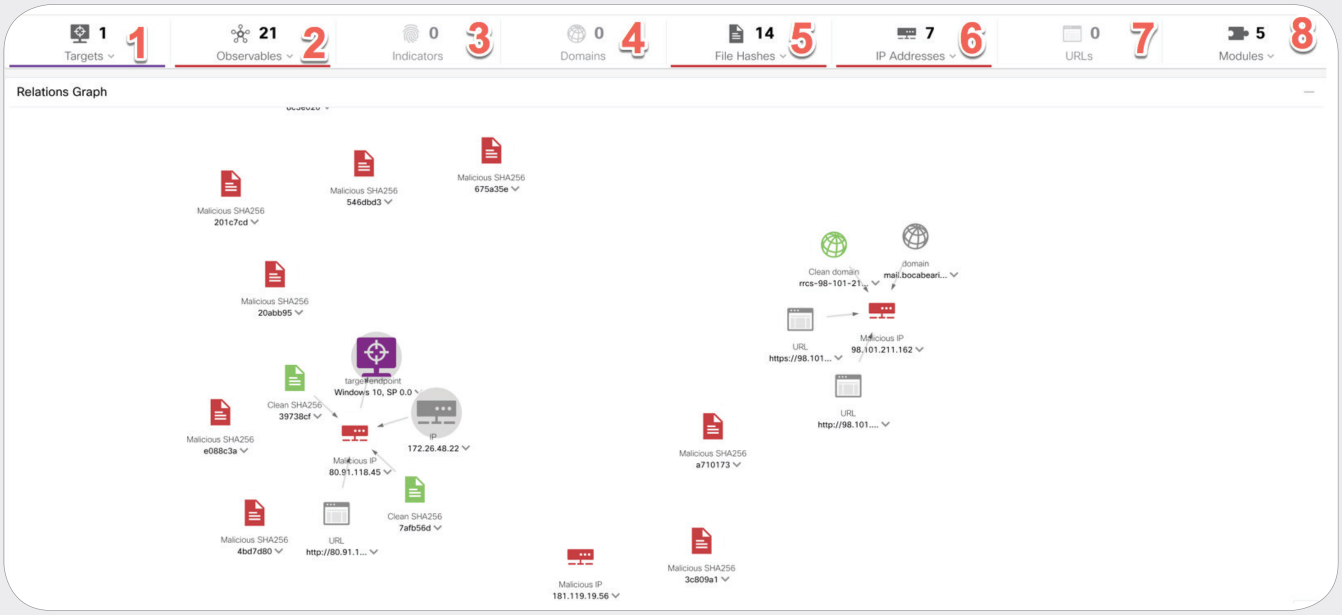
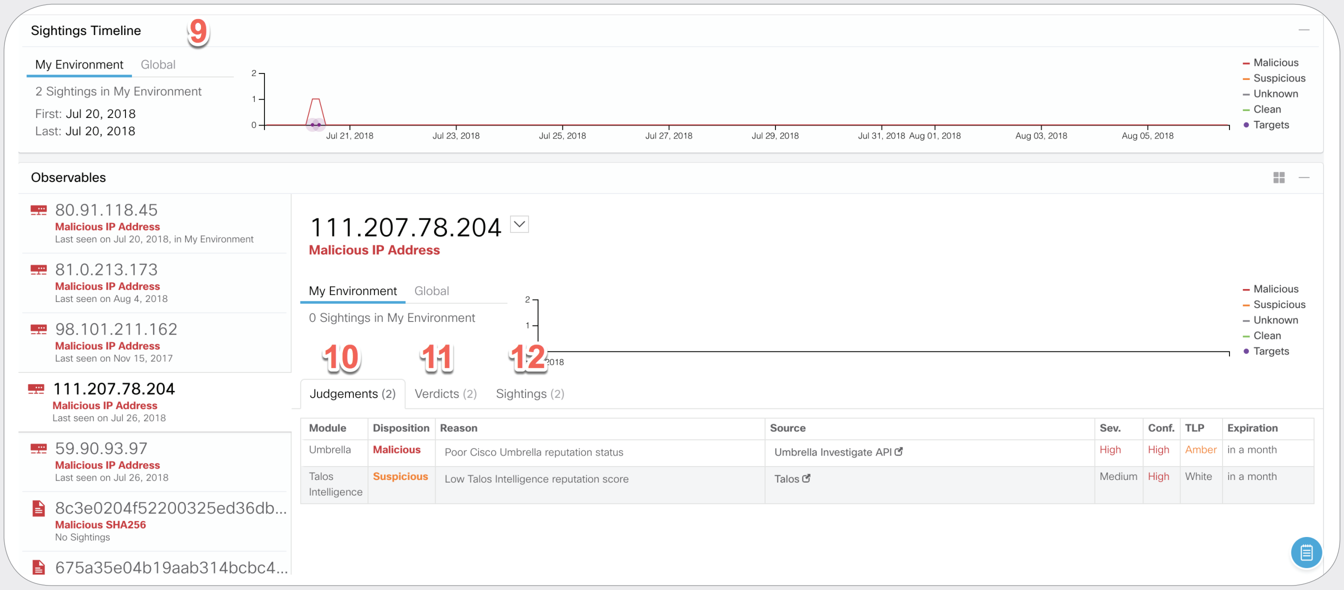


Figure 6: First half of results graph of Cisco Threat Response. (Red numbers added in for reference)

From this section of the graph, you can see:

1. Targets: A Target represents the device, identity, or resource that a threat has targeted. A Target is identified by one or more Observables. When known, a type, operating system, and other metadata is recorded as well. Targets are always part of a local Sighting.
2. Observables: Cisco Threat Response supports the quick investigation of cyber Observables, which might be domain names, IP addresses, file hashes, PKI certificate serial numbers, and even specific devices or users. These observables are extracted from the input text, and counted here. The first thing that Cisco Threat Response does with an observable is determine its disposition, by aggregating what is known about that observable from the various enrichment modules that have been configured. The disposition tells us whether the observable is: Clean, Malicious, Suspicious, Common, Unknown. These dispositions are signaled intuitively by color throughout the interface.
3. Indicators: An Indicator describes a pattern of behavior or a set of conditions which indicate malicious behavior. Some indicators are more indicative than others of malicious behavior, so knowing exactly which bad behaviors an observable
   (such as a domain or an IP address) are exhibiting can help an incident responder decide what to do next.
4. Domains: In the Domains section, Cisco Threat Response will show any domains that were extracted from the Investigate console input. The dispositions of the domains are reflected here.
5. File Hashes: Cisco Threat Response will show the file hashes that were extracted from the Investigate console input. The dispositions of the hashes are reflected here.
6. IP Addresses: Cisco Threat Response will show the IP addresses that were extracted from the Investigate console input. The dispositions of the IP addresses are reflected here.
7. URLs: Cisco Threat Response will show URLs that were extracted from the Investigate console input. The dispositions of the URLs are reflected here.
8. Modules: Cisco Threat Response uses integration modules to integrate with Cisco security products and third-party tools. Integration modules can provide enrichment and response capabilities.

The second half of the graph showing sighting timelines and observables is shown in Figure 7.



Sightings Timeline

My Environment Global

2 Sightings in My Environment

First: Jul 20, 2018
Last: Jul 20, 2018

Observables

80.91.118.45
Malicious IP Address
Last seen on Jul 20, 2018, in My Environment

81.0.213.173
Malicious IP Address
Last seen on Aug 4, 2018

98.101.211.162
Malicious IP Address
Last seen on Nov 15, 2017

111.207.78.204
Malicious IP Address
Last seen on Jul 26, 2018

59.90.93.97
Malicious IP Address
Last seen on Jul 26, 2018

8c3e0204f52200325ed36db...
Malicious SHA256
No Sightings

675a35e04b19aab314bcbc4...

111.207.78.204
Malicious IP Address

My Environment Global

0 Sightings in My Environment

Judgements (2) Verdicts (2) Sightings (2)

Module	Disposition	Reason	Source	Sev.	Conf.	TLP	Expiration
Umbrella	Malicious	Poor Cisco Umbrella reputation status	Umbrella Investigate API	High	High	Amber	in a month
Talos Intelligence	Suspicious	Low Talos Intelligence reputation score	Talos	Medium	High	White	in a month

Figure 7: Second half of results graph of Cisco Threat Response showing Sightings Timelines and Observables. (Red numbers added in for reference)

From this section of the graph, you can find:

9. Sightings Timeline: This is a timeline of the sightings that have been seen in the local and global environment.

10. Judgements: A Judgement associates a disposition with a cyber observable, and is valid for an explicit span of time. Judgements can optionally be related to Indicators, providing further insight as to why a specific disposition was associated with that observable.

11. Verdicts: A Verdict indicates the most recent and most relevant disposition for a given cyber observable from each reporting system, as well as the Judgement from which the verdict was derived.

12. A Sighting is a record of the appearance of a cyber observable at a given date and time. Sightings can optionally be related to Indicators, providing threat intelligence context about the observable.

From the graph, we can see that we have a target in our environment that has been affected by the intelligence investigated. Figure 8 shows the graph relationship around the observable that affects a target.

From this view, the analyst can tell:

- Host with IP 172.26.48.22 has connected to malicious IP 80.91.118.45
- Two programs with clean dispositions made the connection to malicious IP 80.91.118.45
- There is a URL hosted at that malicious IP.

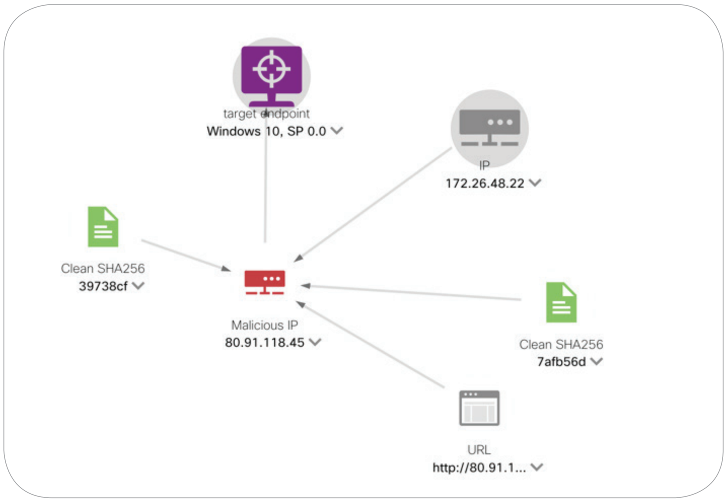


Figure 8: Graph showing the relationships between the observable, the target, the URL, the file hashes and IP addresses.

Continuing to unravel the thread further, the analyst is afforded point and click capability to determine the programs associated with those clean file hashes. Note, these file hashes were not part of the original intelligence that was pasted into the Cisco Threat Response Investigate console.

At the AMP for Endpoints Console, the analyst can see:

- The first time the file was seen.
- The last time the file was seen.
- The entry point into the environment.
- The file name associated with that hash is putty.exe or putty[1].exe
- The current disposition of the file is Clean.
- The IP and port the file connected to.
- The file location.
- The applications that downloaded the file into the environment.

Figures 10 - 13 shows the File Trajectory displayed by AMP for Endpoints.

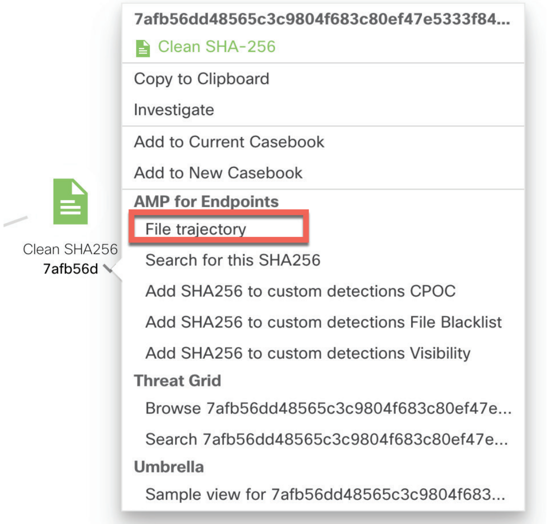
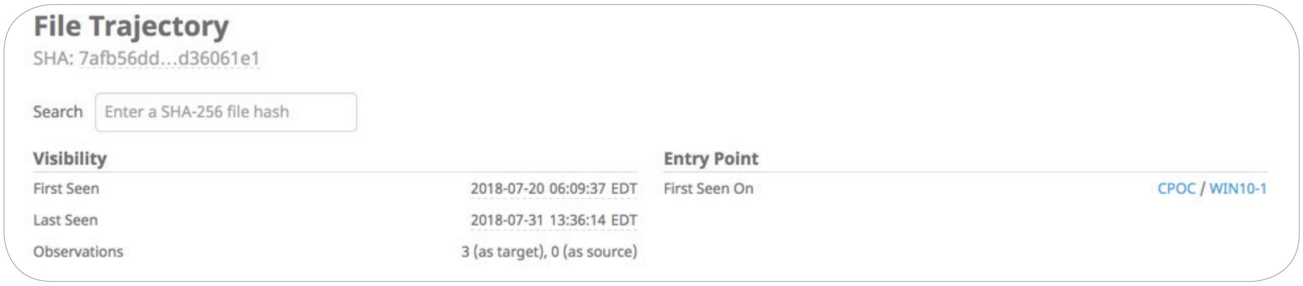

Clean SHA256
7afb56d
7afb56dd48565c3c9804f683c80ef47e5333f84...
Clean SHA-256
Copy to Clipboard
Investigate
Add to Current Casebook
Add to New Casebook
AMP for Endpoints
File trajectory
Search for this SHA256
Add SHA256 to custom detections CPOC
Add SHA256 to custom detections File Blacklist
Add SHA256 to custom detections Visibility
Threat Grid
Browse 7afb56dd48565c3c9804f683c80ef47e...
Search 7afb56dd48565c3c9804f683c80ef47e...
Umbrella
Sample view for 7afb56dd48565c3c9804f683...

Figure 9: Pivot menu on file hash showing the ability to get to File trajectory via AMP for Endpoints.



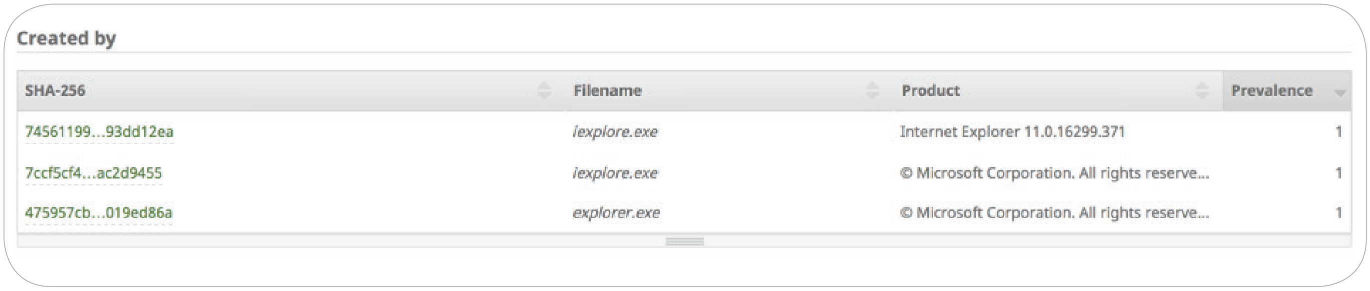
File Trajectory

SHA: 7afb56dd...d36061e1

Search: Enter a SHA-256 file hash

Visibility		Entry Point	
First Seen	2018-07-20 06:09:37 EDT	First Seen On	CPOC / WIN10-1
Last Seen	2018-07-31 13:36:14 EDT		
Observations	3 (as target), 0 (as source)		

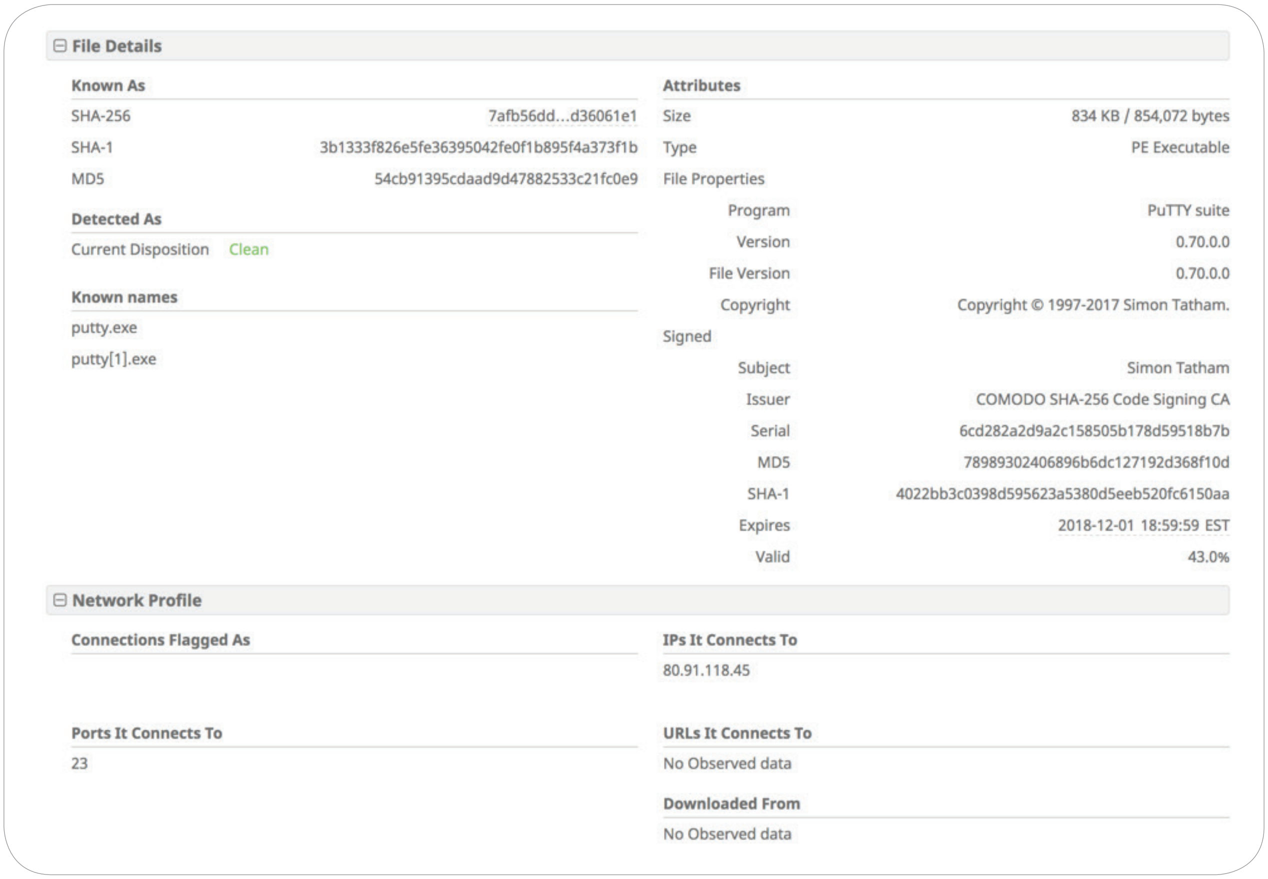
Figure 10: AMP for Endpoint File Trajectory Entry Point



Created by

SHA-256	Filename	Product	Prevalence
74561199...93dd12ea	*iexplore.exe*	Internet Explorer 11.0.16299.371	1
7ccf5cf4...ac2d9455	*iexplore.exe*	© Microsoft Corporation. All rights reserve...	1
475957cb...019ed86a	*explorer.exe*	© Microsoft Corporation. All rights reserve...	1

Figure 11: AMP for Endpoint File Trajectory “Created by” section showing the parent file that retrieved the current file hash being investigated.



⊟ **File Details**

Known As

SHA-256	7afb56dd...d36061e1
SHA-1	3b1333f826e5fe36395042fe0f1b895f4a373f1b
MD5	54cb91395cdaad9d47882533c21fc0e9

Detected As

Current Disposition Clean

Known names

putty.exe

putty[1].exe

Attributes

Size		834 KB / 854,072 bytes
Type		PE Executable
File Properties		
	Program	PuTTY suite
	Version	0.70.0.0
	File Version	0.70.0.0
	Copyright	Copyright © 1997-2017 Simon Tatham.
Signed		
	Subject	Simon Tatham
	Issuer	COMODO SHA-256 Code Signing CA
	Serial	6cd282a2d9a2c158505b178d59518b7b
	MD5	78989302406896b6dc127192d368f10d
	SHA-1	4022bb3c0398d595623a5380d5eeb520fc6150aa
	Expires	2018-12-01 18:59:59 EST
	Valid	43.0%

⊟ **Network Profile**

Connections Flagged As

IPs It Connects To

80.91.118.45

Ports It Connects To

23

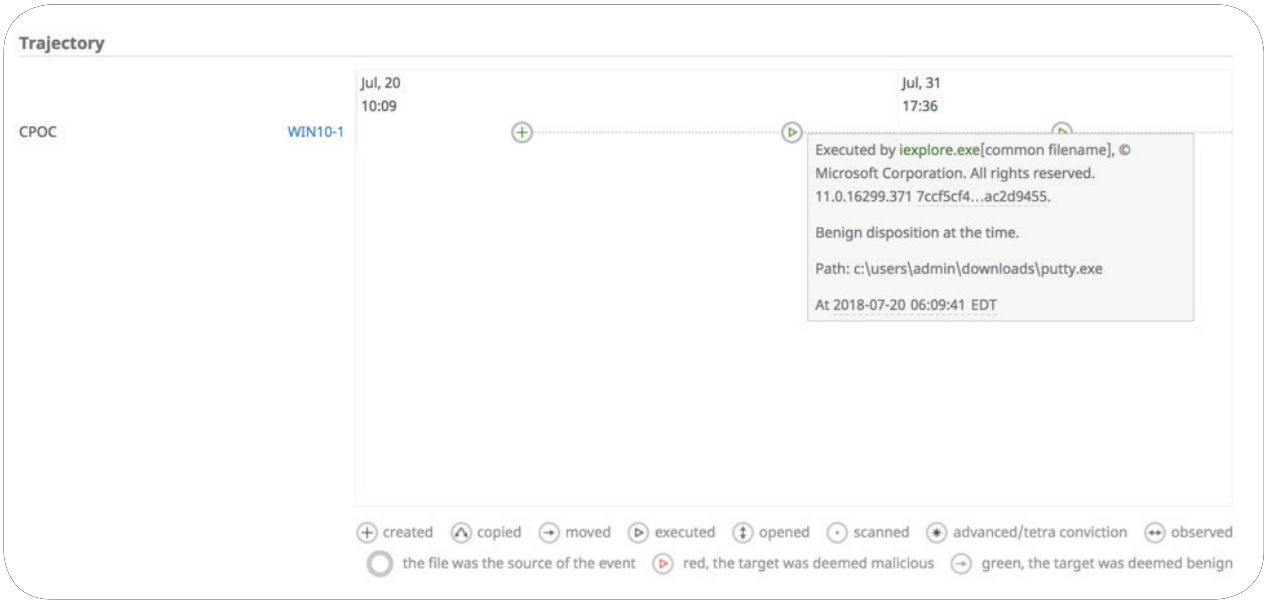
URLs It Connects To

No Observed data

Downloaded From

No Observed data

Figure 12: AMP for Endpoints File Details and Network Profile



Trajectory
CPOC
WIN10-1
Jul, 20
10:09
Jul, 31
17:36
created
copied
moved
executed
opened
scanned
advanced/tetra conviction
observed
the file was the source of the event
red, the target was deemed malicious
green, the target was deemed benign

Executed by iexplore.exe[common filename], © Microsoft Corporation. All rights reserved. 11.0.16299.371 7ccf5cf4...ac2d9455.

Benign disposition at the time.

Path: c:\users\admin\downloads\putty.exe

At 2018-07-20 06:09:41 EDT

Figure 13: AMP for Endpoints File trajectory showing location.

At this point, the analyst has used the intelligence from the Find phase to help set the case to decide as to what the subsequent courses of action should be, based on organizational policy. Those courses of action could include blocking the source IP, blocking the destination IP, blocking both the source and destination IP or placing those programs under lockdown so that they cannot be executed. Next phases depend on organizational policy and IR capability.

Finish

Cisco Threat Response allows security analysts to issue domain blocks and file hash blocks directly via the pivot menus if the approved organizational course of response is determined to be one of those actions.

Figures 14 and 15 shows the ability of Cisco Threat Response to respectively block a file hash and domain.

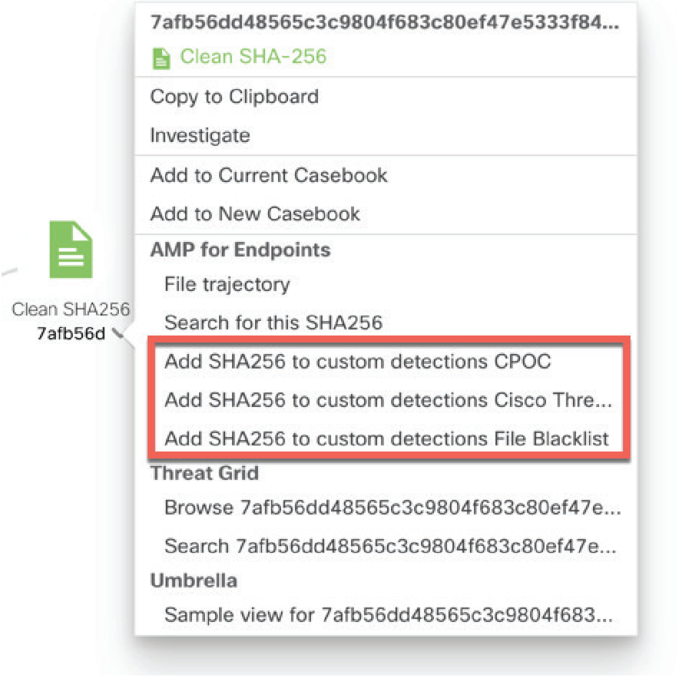

Clean SHA256
7afb56d
7afb56dd48565c3c9804f683c80ef47e5333f84...
Clean SHA-256
Copy to Clipboard
Investigate
Add to Current Casebook
Add to New Casebook
AMP for Endpoints
File trajectory
Search for this SHA256
Add SHA256 to custom detections CPOC
Add SHA256 to custom detections Cisco Thre...
Add SHA256 to custom detections File Blacklist
Threat Grid
Browse 7afb56dd48565c3c9804f683c80ef47e...
Search 7afb56dd48565c3c9804f683c80ef47e...
Umbrella
Sample view for 7afb56dd48565c3c9804f683...

Figure 14: Cisco Threat Response adding a file hash to a Simple Custom Detection in AMP for Endpoints via API integration.

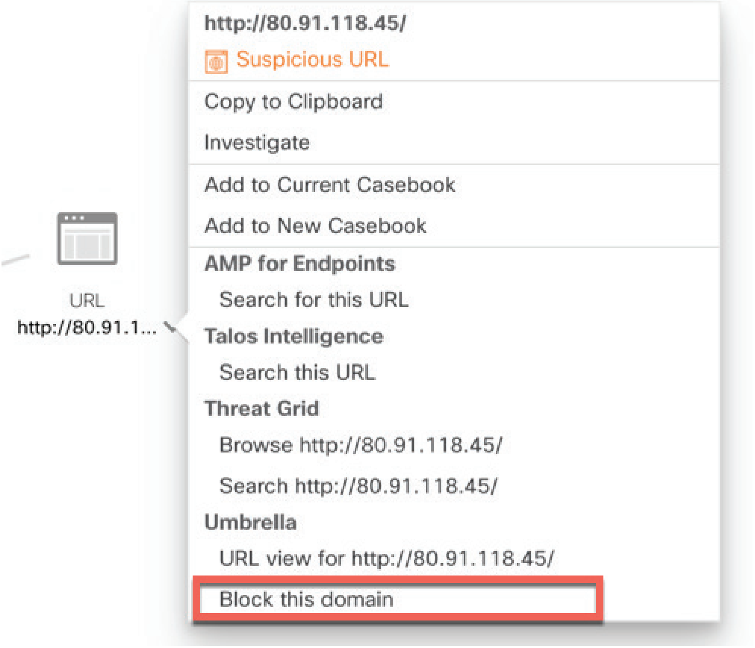


Figure 15: Cisco Threat Response ability to block a domain in Cisco Umbrella Platform via Enforcement API integration.

The security analyst can now move into the intelligence part of the F3EAD model.

Exploit

In the Exploit phase, the analyst develops data that resulted from the incident response. The results graph included pieces of information that we did not have awareness of before – the new information was not part of our Investigate input from the US-CERT bulletin. Figures 16, 17 and 18 show additional information for a malicious IP indicator that was found by Cisco Threat Response.

In this example – exploiting the IP intelligence, the analyst is able to:

- Link additional domains to the initial malicious IP indicator.
- Link additional URLs to the initial malicious IP indicator.

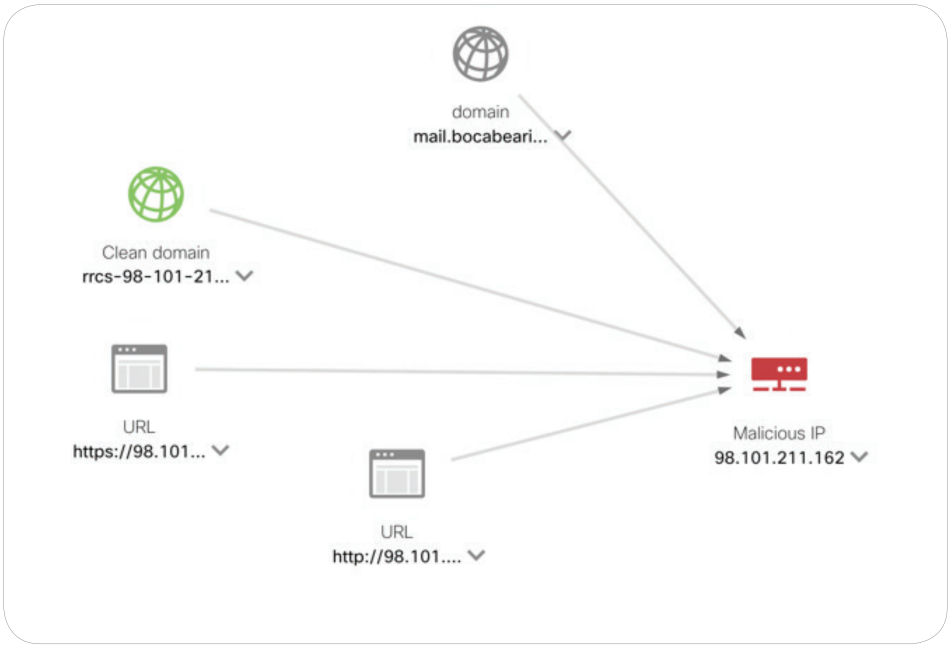


Figure 16: Enrichment data for malicious IP. Information not known before.

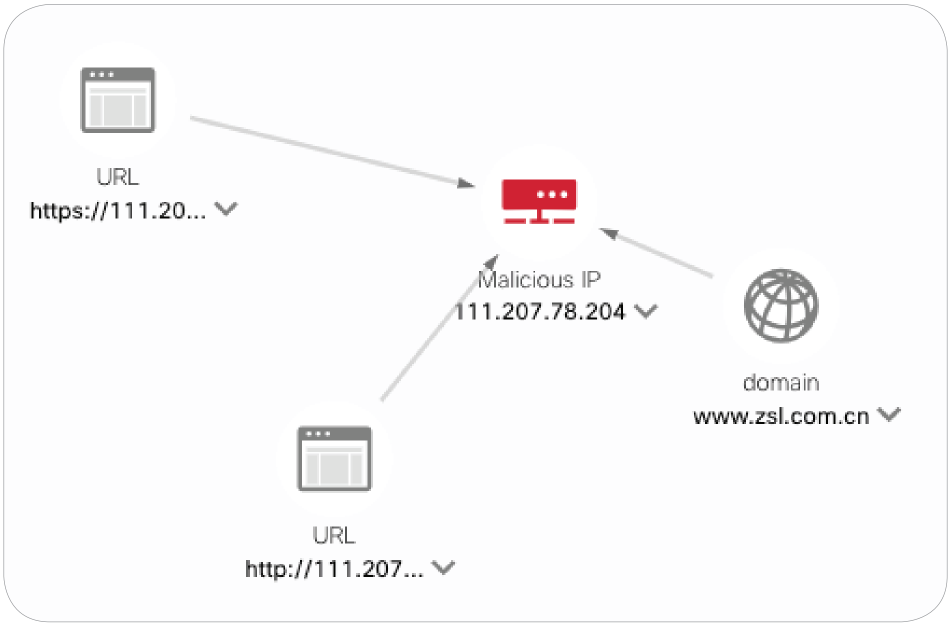


Figure 17: Enrichment data for malicious IP. Information not known before.

Another piece of gathered intelligence that Cisco Threat Response allows the security analyst to exploit, are the targets that were identified. The target identification returned a few pieces of information. Figure 19 shows the Target observable for the above scenario. The analyst is presented with the:

- Machine Host name
- Machine MAC address
- Machine IP
- AMP Computer GUID

With this information, the analyst can choose to place that host in focus to get additional context about that host.

Analyze

The Analyze phase develops the previously exploited evidence to see if additional information can be gathered. Malware analysis in sandboxes or gloveboxes (Cisco Threat Grid is considered a glovebox where analysts can interact with the malware sample) may be a process that security teams will choose to utilize during the Analyze phase. This is the phase where the investigators and cyber threat hunters go down the rabbit-hole to see what is at the other end. The work and deliverables in this phase attempts to develop a bigger picture so that the threat can be detected and mitigated.

Cisco Threat Response allows security analysts and cyber threat hunters to gain access to additional context to help analyze the additional pieces of information that may have been uncovered.

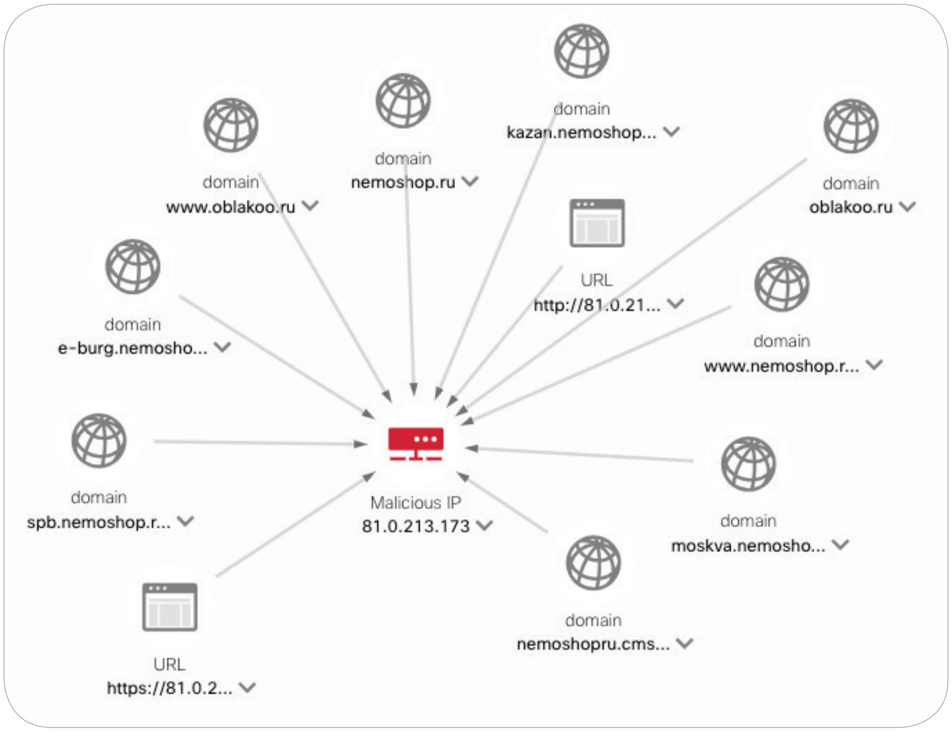
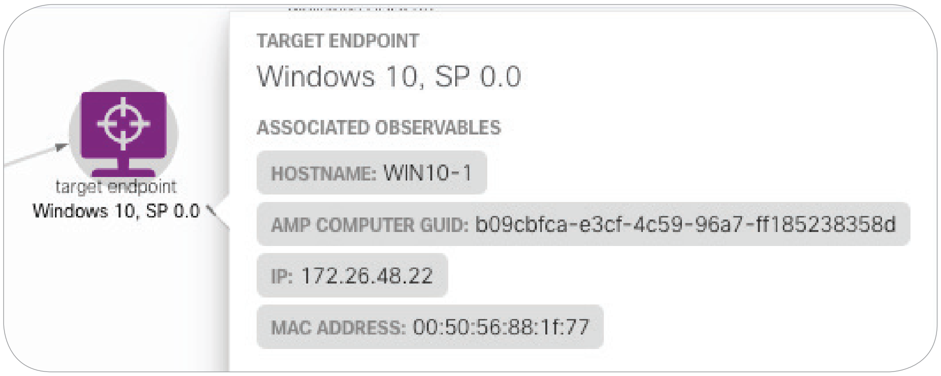


Figure 18: Enrichment data for malicious IP. Information not known before.



TARGET ENDPOINT

Windows 10, SP 0.0

ASSOCIATED OBSERVABLES

HOSTNAME: WIN10-1

AMP COMPUTER GUID: b09cbfca-e3cf-4c59-96a7-ff185238358d

IP: 172.26.48.22

MAC ADDRESS: 00:50:56:88:1f:77

Figure 19: Cisco Threat Response Target Identification

Using Figure 18 as a reference point, we see additional domains that have resolved to the malicious IP. Let's work with one of those domains displayed, www[dot]nemoshop[dot]ru

Cisco Threat Response allows the analyst to analyze this domain using Talos Intelligence, Threat Grid and Umbrella.

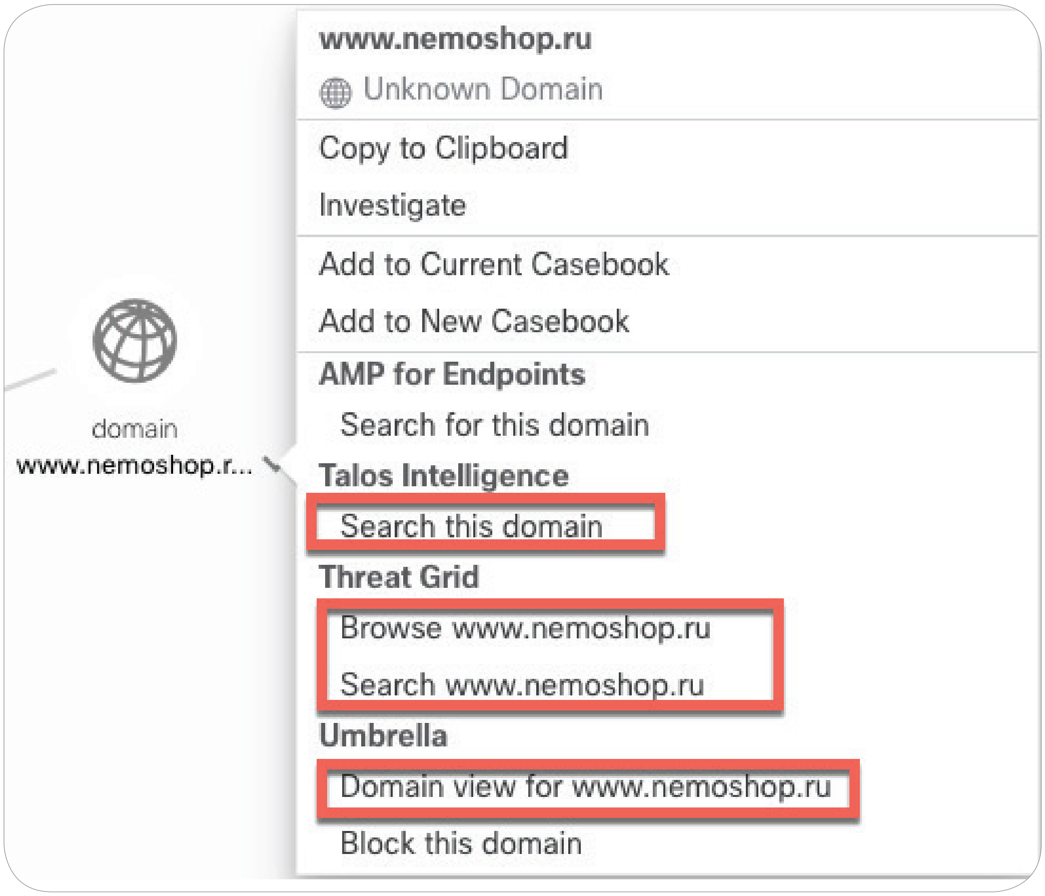
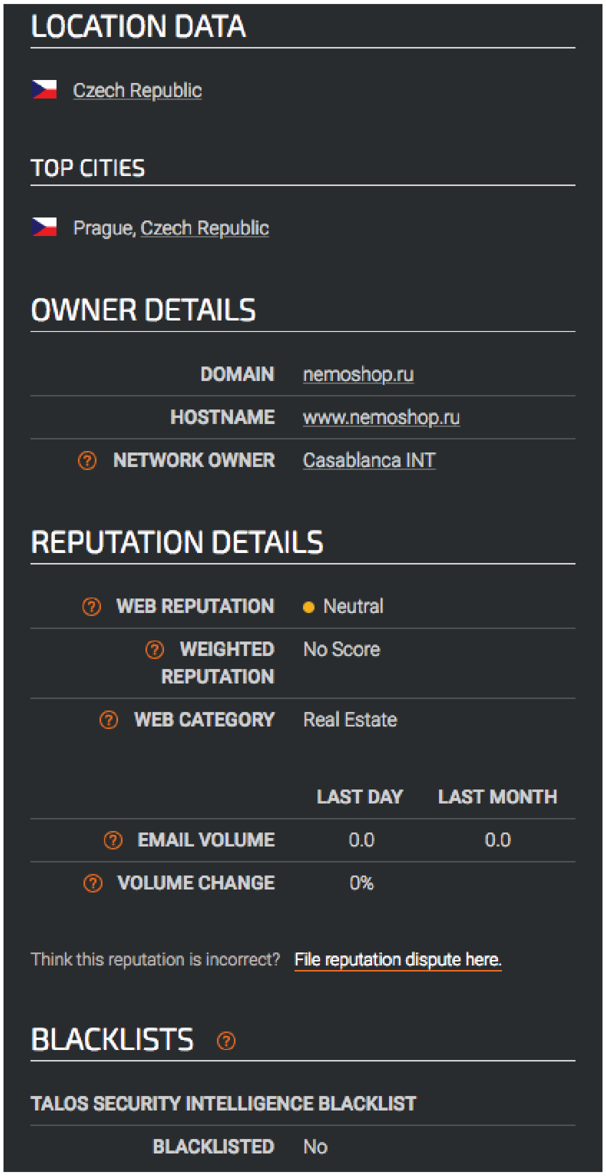


Figure 20: Cisco Threat Response supporting the Analyze function of F3EAD

With a single click, the analyst is able to gain tactical insight into the domain.

Figures 21 through 23 show the various responses from the configured Modules.



LOCATION DATA

Czech Republic

TOP CITIES

Prague, Czech Republic

OWNER DETAILS

DOMAIN	nemoshop.ru
HOSTNAME	www.nemoshop.ru
NETWORK OWNER	Casablanca INT

REPUTATION DETAILS

WEB REPUTATION	● Neutral
WEIGHTED REPUTATION	No Score
WEB CATEGORY	Real Estate

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

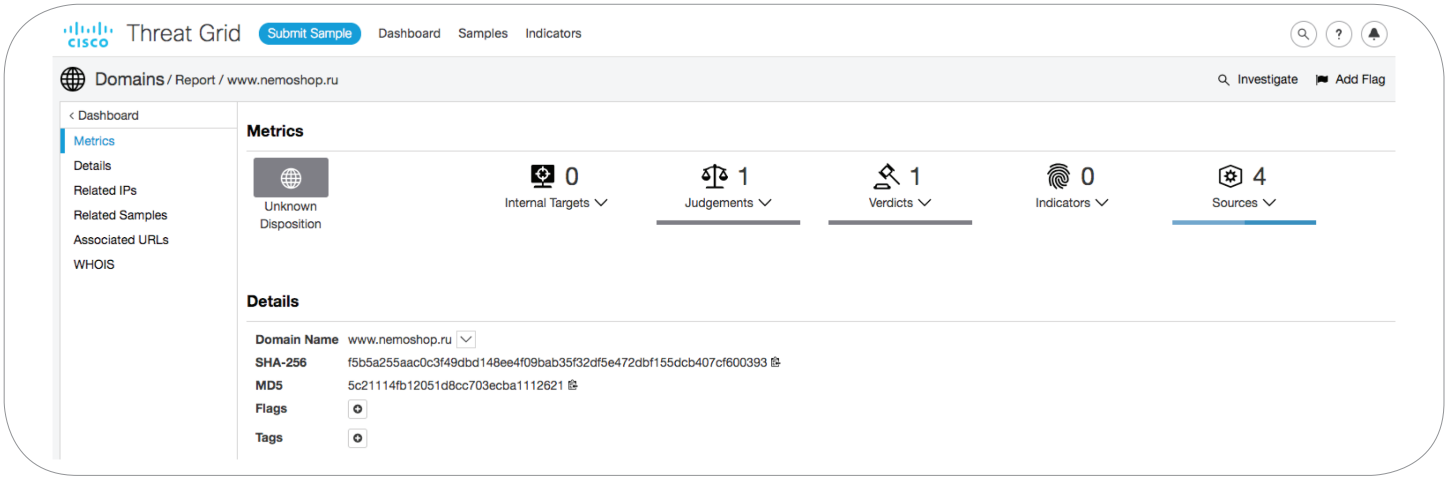
Think this reputation is incorrect? File reputation dispute here.

BLACKLISTS

TALOS SECURITY INTELLIGENCE BLACKLIST

BLACKLISTED	No

Figure 21: Talos Intelligence data results for the domain.



Metrics

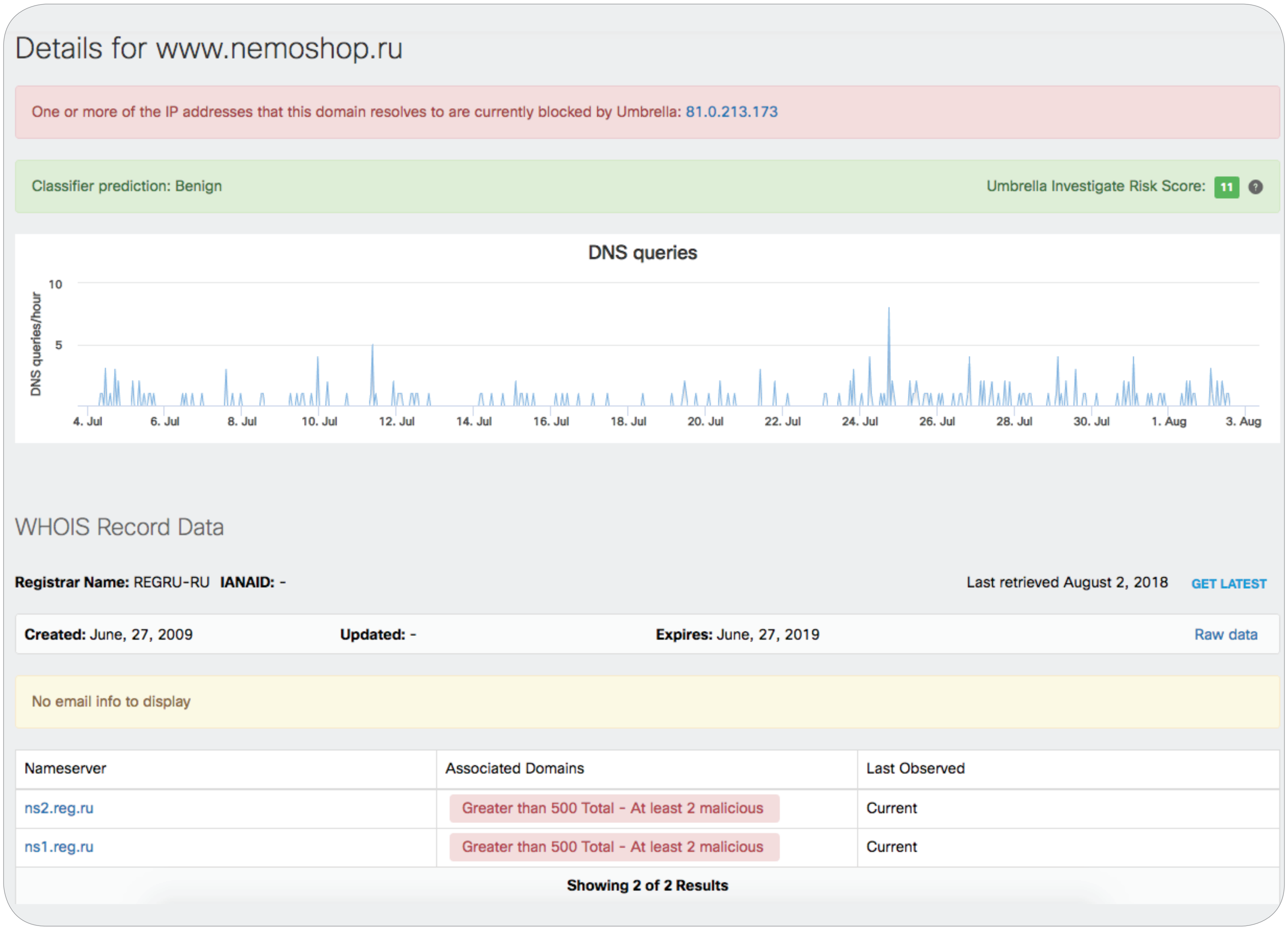
Unknown Disposition

0	1	1	0	4
Internal Targets	Judgements	Verdicts	Indicators	Sources

Details

Domain Name	www.nemoshop.ru
SHA-256	f5b5a255aac0c3f49dbd148ee4f09bab35f32df5e472dbf155dcb407cf600393
MD5	5c21114fb12051d8cc703ecba1112621
Flags	⊕
Tags	⊕

Figure 22: Browsing Threat Grid results for the domain.



Details for www.nemoshop.ru

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 81.0.213.173

Classifier prediction: Benign

Umbrella Investigate Risk Score: 11

WHOIS Record Data

Registrar Name: REGRU-RU **IANAID:** -

Last retrieved August 2, 2018 GET LATEST

Created: June, 27, 2009 **Updated:** - **Expires:** June, 27, 2019 Raw data

No email info to display

Nameserver	Associated Domains	Last Observed
ns2.reg.ru	Greater than 500 Total - At least 2 malicious	Current
ns1.reg.ru	Greater than 500 Total - At least 2 malicious	Current

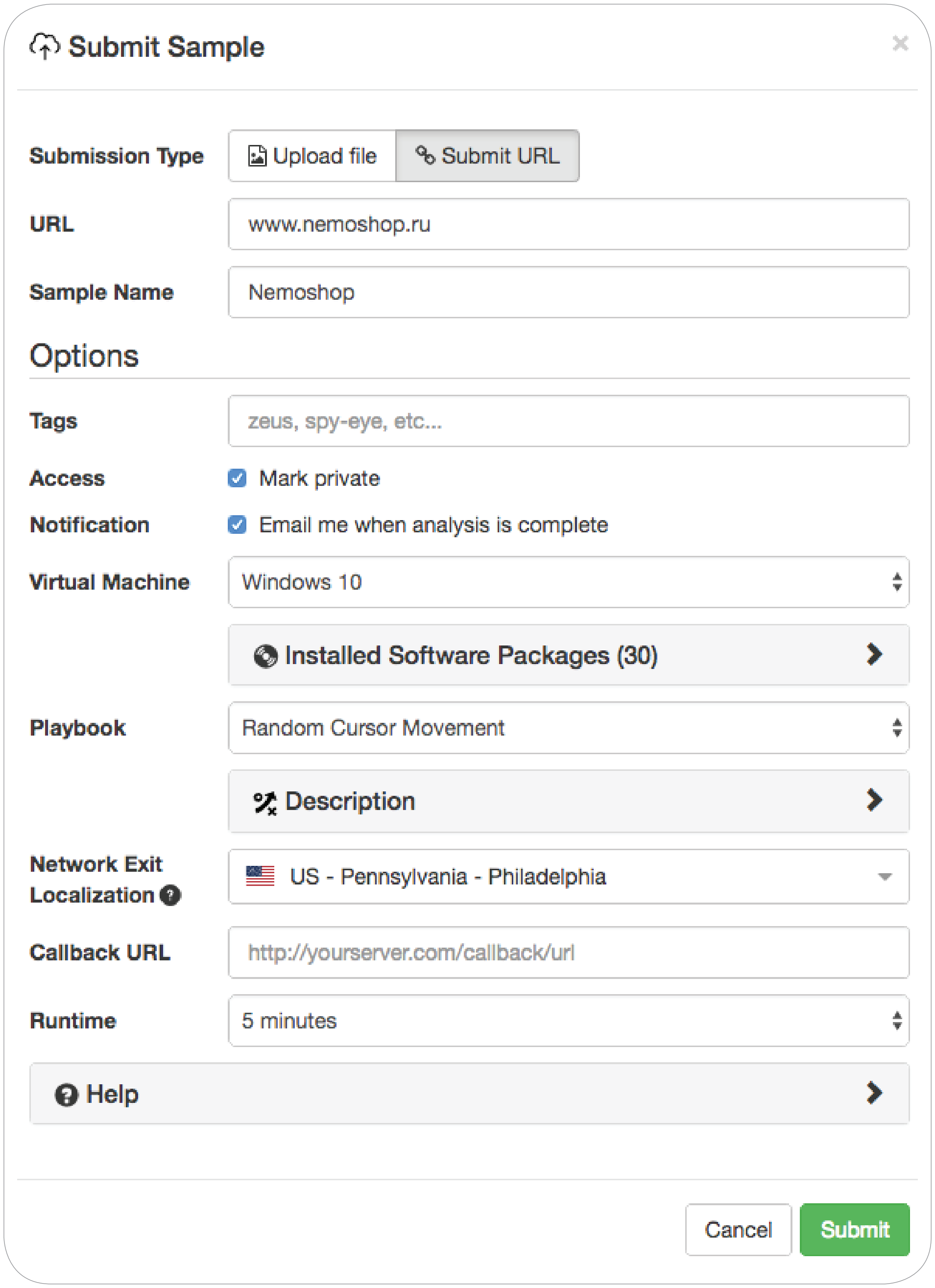
Showing 2 of 2 Results

Figure 23: Umbrella results for the domain.

To go a step deeper into the analysis of this particular domain, Cisco Threat Grid allows the analyst to detonate the URL in a glovebox to perform deeper analysis.

Figure 24 illustrates the submission of the URL into the Threat Grid glovebox.

If the analyst elects to have an email notification sent, figure 25 shows a representation of the email content.



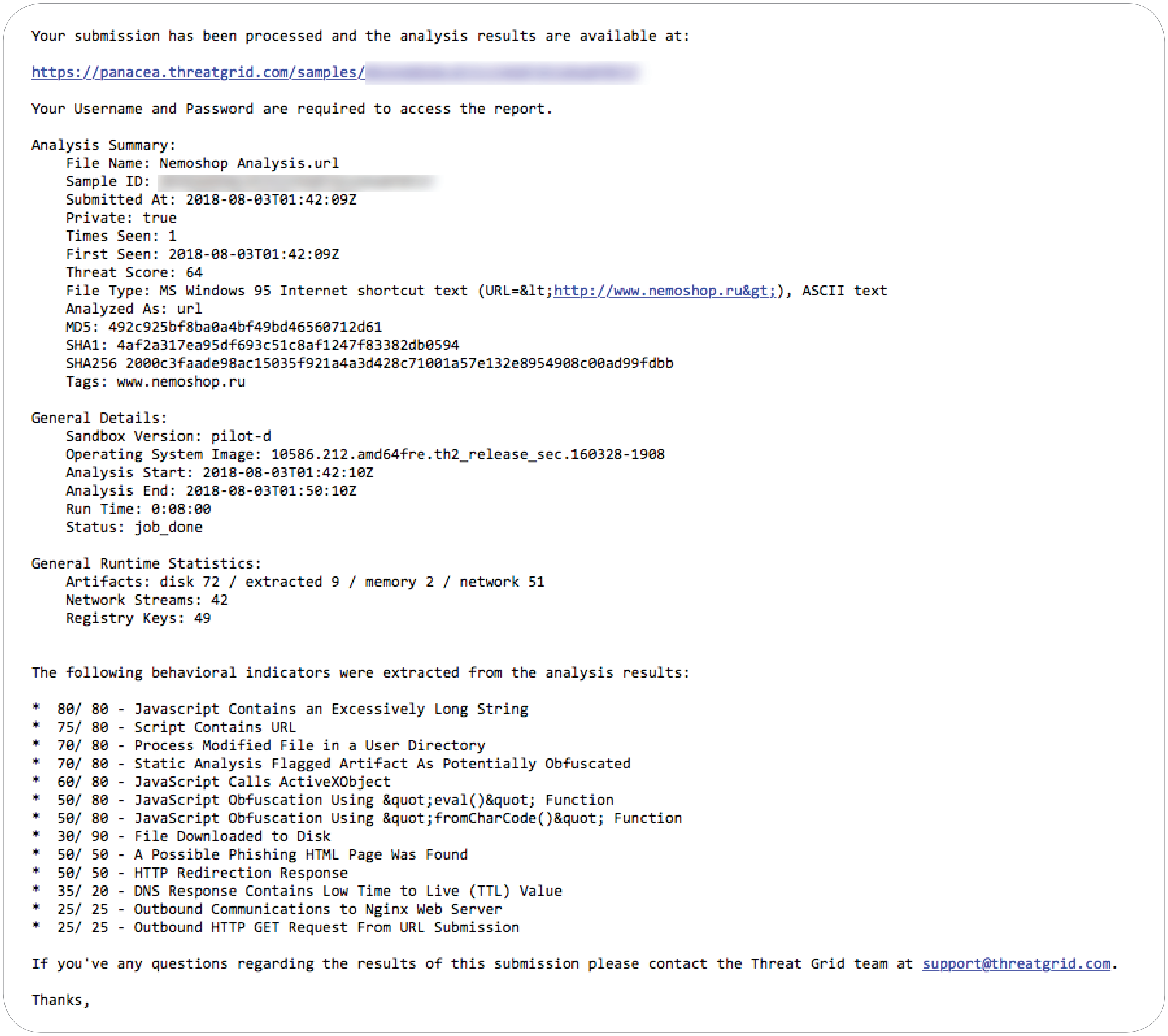
Submit Sample

Submission Type	Upload file / Submit URL
URL	www.nemoshop.ru
Sample Name	Nemoshop

Options

Tags	zeus, spy-eye, etc...
Access	☑ Mark private
Notification	☑ Email me when analysis is complete
Virtual Machine	Windows 10
	Installed Software Packages (30)
Playbook	Random Cursor Movement
	Description
Network Exit Localization	US - Pennsylvania - Philadelphia
Callback URL	http://yourserver.com/callback/url
Runtime	5 minutes

Figure 24: URL submission to Threat Grid

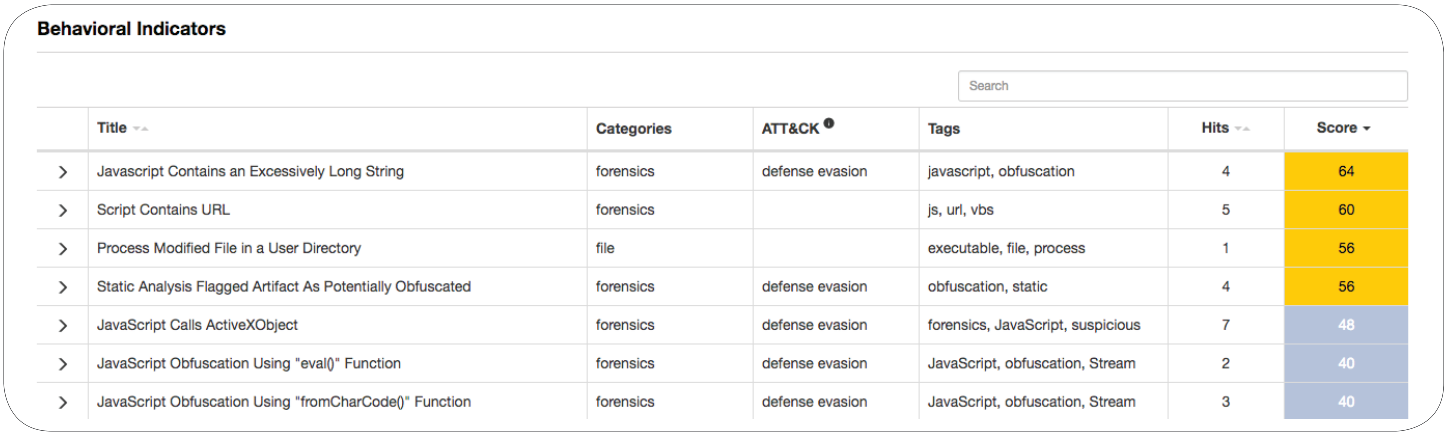


```
Your submission has been processed and the analysis results are available at:

https://panacea.threatgrid.com/samples/[redacted]

Your Username and Password are required to access the report.

Analysis Summary:
    File Name: Nemoshop Analysis.url
    Sample ID: [redacted]
    Submitted At: 2018-08-03T01:42:09Z
    Private: true
    Times Seen: 1
    First Seen: 2018-08-03T01:42:09Z
    Threat Score: 64
    File Type: MS Windows 95 Internet shortcut text (URL=&lt;http://www.nemoshop.ru&gt;), ASCII text
    Analyzed As: url
    MD5: 492c925bf8ba0a4bf49bd46560712d61
    SHA1: 4af2a317ea95df693c51c8af1247f83382db0594
    SHA256 2000c3faade98ac15035f921a4a3d428c71001a57e132e8954908c00ad99fdbb
    Tags: www.nemoshop.ru

General Details:
    Sandbox Version: pilot-d
    Operating System Image: 10586.212.amd64fre.th2_release_sec.160328-1908
    Analysis Start: 2018-08-03T01:42:10Z
    Analysis End: 2018-08-03T01:50:10Z
    Run Time: 0:08:00
    Status: job_done

General Runtime Statistics:
    Artifacts: disk 72 / extracted 9 / memory 2 / network 51
    Network Streams: 42
    Registry Keys: 49


The following behavioral indicators were extracted from the analysis results:

*  80/ 80 - Javascript Contains an Excessively Long String
*  75/ 80 - Script Contains URL
*  70/ 80 - Process Modified File in a User Directory
*  70/ 80 - Static Analysis Flagged Artifact As Potentially Obfuscated
*  60/ 80 - JavaScript Calls ActiveXObject
*  50/ 80 - JavaScript Obfuscation Using &quot;eval()&quot; Function
*  50/ 80 - JavaScript Obfuscation Using &quot;fromCharCode()&quot; Function
*  30/ 90 - File Downloaded to Disk
*  50/ 50 - A Possible Phishing HTML Page Was Found
*  50/ 50 - HTTP Redirection Response
*  35/ 20 - DNS Response Contains Low Time to Live (TTL) Value
*  25/ 25 - Outbound Communications to Nginx Web Server
*  25/ 25 - Outbound HTTP GET Request From URL Submission

If you've any questions regarding the results of this submission please contact the Threat Grid team at support@threatgrid.com.

Thanks,
```

Figure 25: Threat Grid email notification when sample analysis is completed.

On the Threat Grid console, in addition to being able to see Network Stream, File Activity, Registry Activity, Mutex, Memory Related, Thread Events and Process Creation metrics, the analyst is now also presented with information about MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) metrics for the sample.

Figure 26 shows the ATT&CK classification for the behavioral indicators.



Behavioral Indicators

	Title	Categories	ATT&CK	Tags	Hits	Score
>	Javascript Contains an Excessively Long String	forensics	defense evasion	javascript, obfuscation	4	64
>	Script Contains URL	forensics		js, url, vbs	5	60
>	Process Modified File in a User Directory	file		executable, file, process	1	56
>	Static Analysis Flagged Artifact As Potentially Obfuscated	forensics	defense evasion	obfuscation, static	4	56
>	JavaScript Calls ActiveXObject	forensics	defense evasion	forensics, JavaScript, suspicious	7	48
>	JavaScript Obfuscation Using "eval()" Function	forensics	defense evasion	JavaScript, obfuscation, Stream	2	40
>	JavaScript Obfuscation Using "fromCharCode()" Function	forensics	defense evasion	JavaScript, obfuscation, Stream	3	40

Figure 26: Threat Grid sample analysis results showing ATT&CK classification.

Analysts continue to analyze information to prepare for organizing the output deliverables utilizing Cisco and third-party tools. Cisco Threat Response facilitates rapid analysis utilizing AMP for Endpoints, Threat Grid, Talos Intelligence and Umbrella.

Disseminate

The Disseminate phase is where Security Teams create deliverables that are useful to team members and to external organizations.

Cisco Threat Response supports the Dissemination phase with two powerful features, Snapshots and Casebooks.

Snapshots support analysts by allowing them to preserve snapshots of their investigations so that they may review it as a team as they organize and gather their data for publication.

A snapshot saves the current investigation and graph for subsequent retrieval and analysis. A unique identifier is created upon snapshot creation and analysts can provide a name for the snapshot as well as a description.

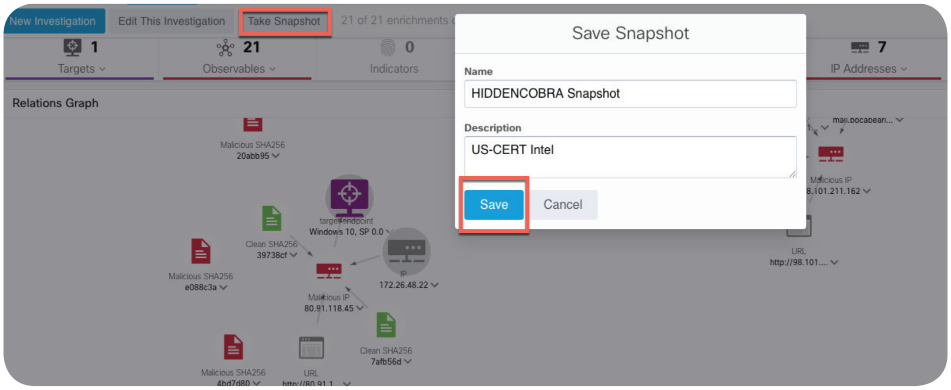
Snapshots can be shared among users in the same organization, to communicate the state of a hunt and/or investigation at a point in time.

Cisco Threat Response Casebooks are analogous to an analyst's notebook. It is constructed with APIs hosted in and data stored within the Cisco Threat Response platform. Casebooks are available via multiple landing pages in Cisco's Security portfolio. Initially, Casebooks are available via Cisco Threat Response, Threat Grid and AMP for Endpoints. Regardless of which product a Casebook is created in, it will be available and editable via the others. In this way, your case notes can follow you across the integrated suite.

Casebooks allow analysts to:

- Gather observables in groups.
- Assign a name and description to the casebook.
- Add/Remove/Update notes concerning the hunt or IR process.
- Add and remove observables to and from the casebook.
- Immediately see dispositions of observables added.
- Execute actions from Casebook.
- Investigate all observables at once with a single click.

In supporting these functions in Casebooks, Cisco Threat Response greatly enhances the agility of incident responders and threat hunters to share their knowledge as they work in this phase of the F3EAD model.

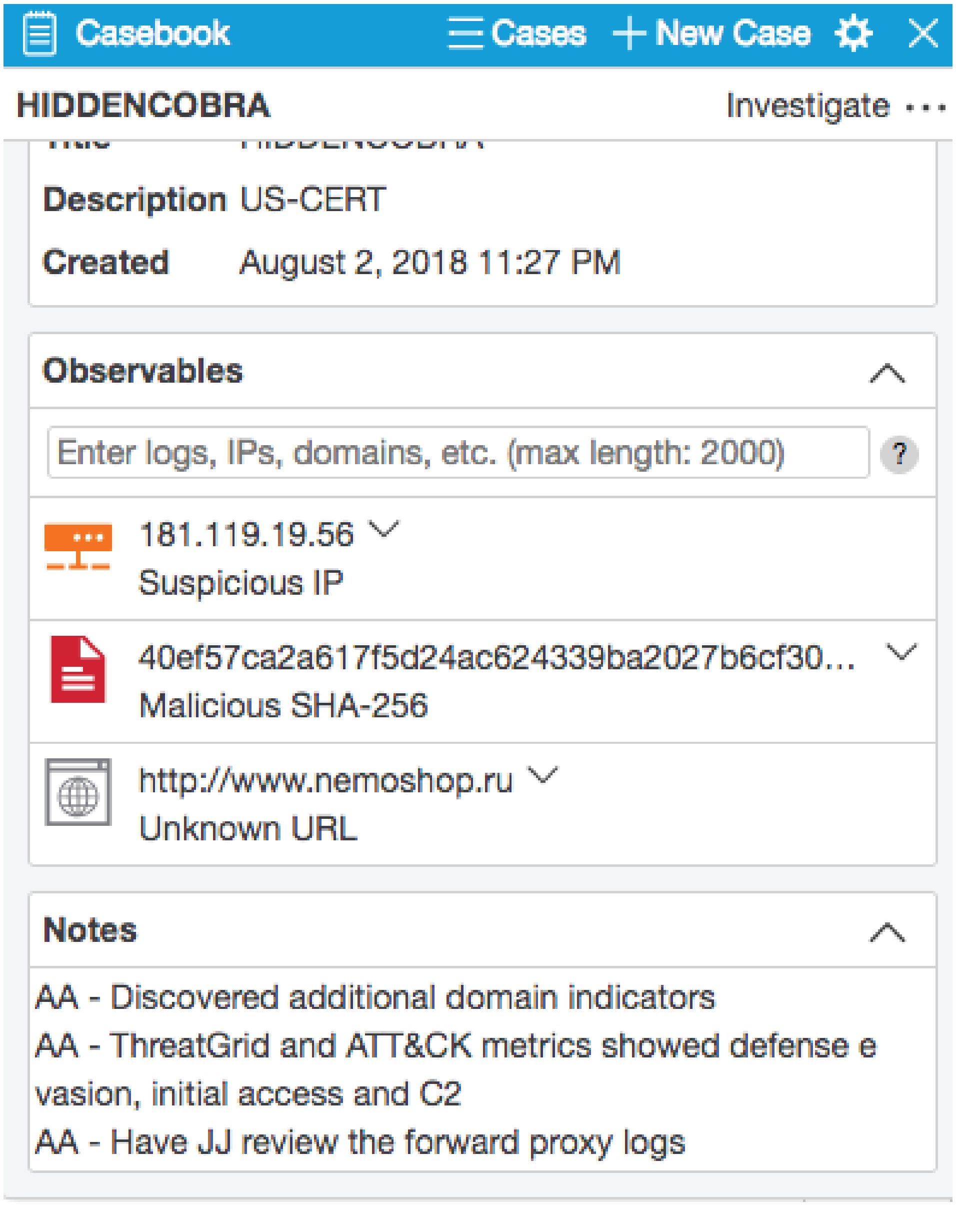


Save Snapshot

Name: HIDDENCOBRA Snapshot

Description: US-CERT Intel

Figure 27: Cisco Threat Response Snapshot



HIDDENCOBRA

Description US-CERT

Created August 2, 2018 11:27 PM

Observables

181.119.19.56
Suspicious IP

40ef57ca2a617f5d24ac624339ba2027b6cf30…
Malicious SHA-256

http://www.nemoshop.ru
Unknown URL

Notes

AA - Discovered additional domain indicators
AA - ThreatGrid and ATT&CK metrics showed defense e vasion, initial access and C2
AA - Have JJ review the forward proxy logs

Figure 28: Cisco Threat Response Casebook

Conclusion

In summary, Cisco Threat Response supports security analysts in their intelligence-driven incident response process by:

- Increasing their ability to see and identify threats in their environment.
- Correlating detections from multiple sources to help prioritize incidents.
- Enriching detections with threat intelligence and user, device, and data context to reduce false positives and highlight exactly where they're affected.
- Automating and orchestrating response actions to reduce remediation time.

Summary of Cisco Threat Response supporting processes in the F3EAD model

F3EAD Process	Cisco Threat Response Support 1
Find	Cisco Talos and other Intelligence
Fix	Cisco Threat Response Investigate
Finish	Cisco Threat Response Pivot and Action
Exploit	Cisco Threat Response Pivot
Analyze	Cisco Threat Response Pivot
Disseminate	Cisco Threat Response Snapshots and Casebooks

[1] Cisco Threat Response Casebooks are available through the entire lifecycle of the incident response and cyber threat hunt.

Works Cited

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer Security Incident Handling Guide. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

The United States Intelligence Community. (2018, August). How Intelligence Works. Retrieved from Intelligence Careers: https://www.intelligencecareers.gov/icintelligence.html

Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Center.
The MITRE Corporation.