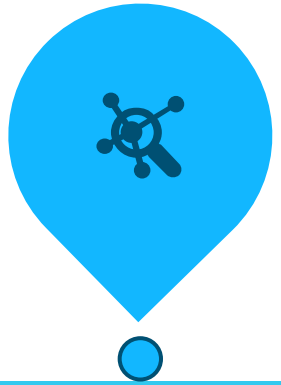
Stay ahead of the game: automate your threat hunting workflows

Christopher van der Made
Developer Advocate Security
Today

Updated May 2017

There is simply too much information and threat intelligence out there for SOC analysts to (consciously) consume. We need to automate as much as possible and provide bitesize cases to them.

Cyber Security Challenges



Too Many Point Products

Too Much Information

Too Much Effort

Too Little Time

How to solve this?

Integration between security solutions

Automation of routine, non-cognitive tasks and policy automation

Goals:

- Increase Threat Prevention
- Decrease Time to Detect
- Reduce Time to Investigate
- Reduce Time to Remediate

APIs for Configuration/Management

- Migration
- Bootstrapping
- Dynamic Provisioning
- Initial Configuration
- Monitoring/System Analytics
- Routine Configuration Change/Mgmt.

Goal:
Eliminate tedious, non-cognitive, time consuming tasks to free up IT sec experts so they can focus on higher priority tasks

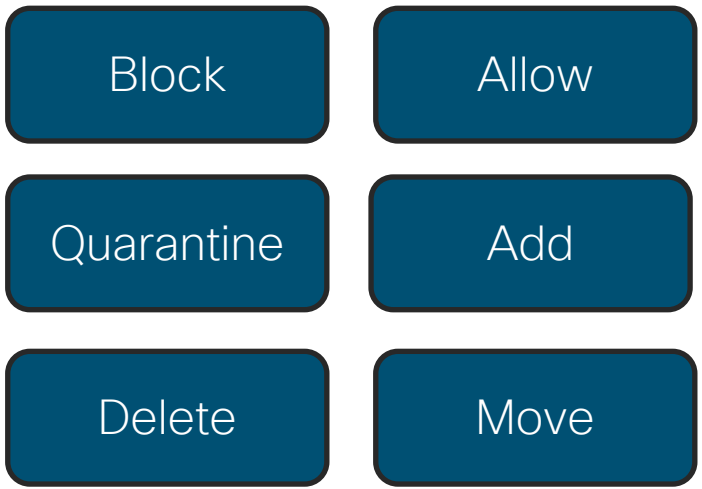
APIs for Data Manipulation & Sharing: Import/Export

Data internal to the network
(Identity, Context Awareness, Event Visibility, Threat Intel)

Data external to the network
(Threat Intel, Analytics)

Goal:
Detect Threats already in the network. Make data collection faster and more efficient. Correlate data from all attack vectors/security systems.

APIs to Perform Actions: Automated Policy to Prevent/React to Threats



Goal:
Implement protections faster than the threat can spread and progress in the network.

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

Agenda

- **Introduction to Threat Hunting**
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

Introduction to Threat Hunting


Sako

Threat Hunting:

"The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."

Types of Hunts

1 Intelligence-Driven

Atomic Indicators

- Low-hanging fruit hunts
- Known threats
- Security controls bypass

2 TTP-Driven

Behavioral & Compound Indicators

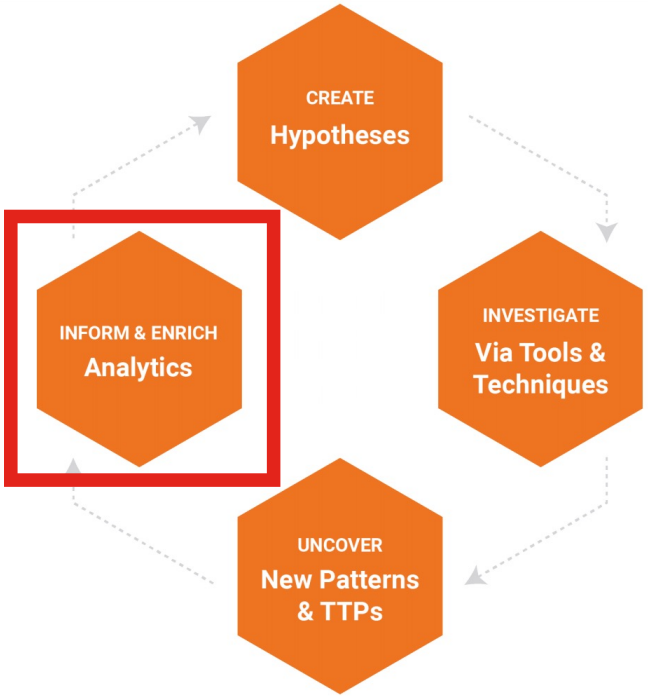
- TTP's: tactics, techniques, procedures
- Methodologies used by advanced attackers
- Systematic approach for discovering unknowns

3 Anomaly-Driven

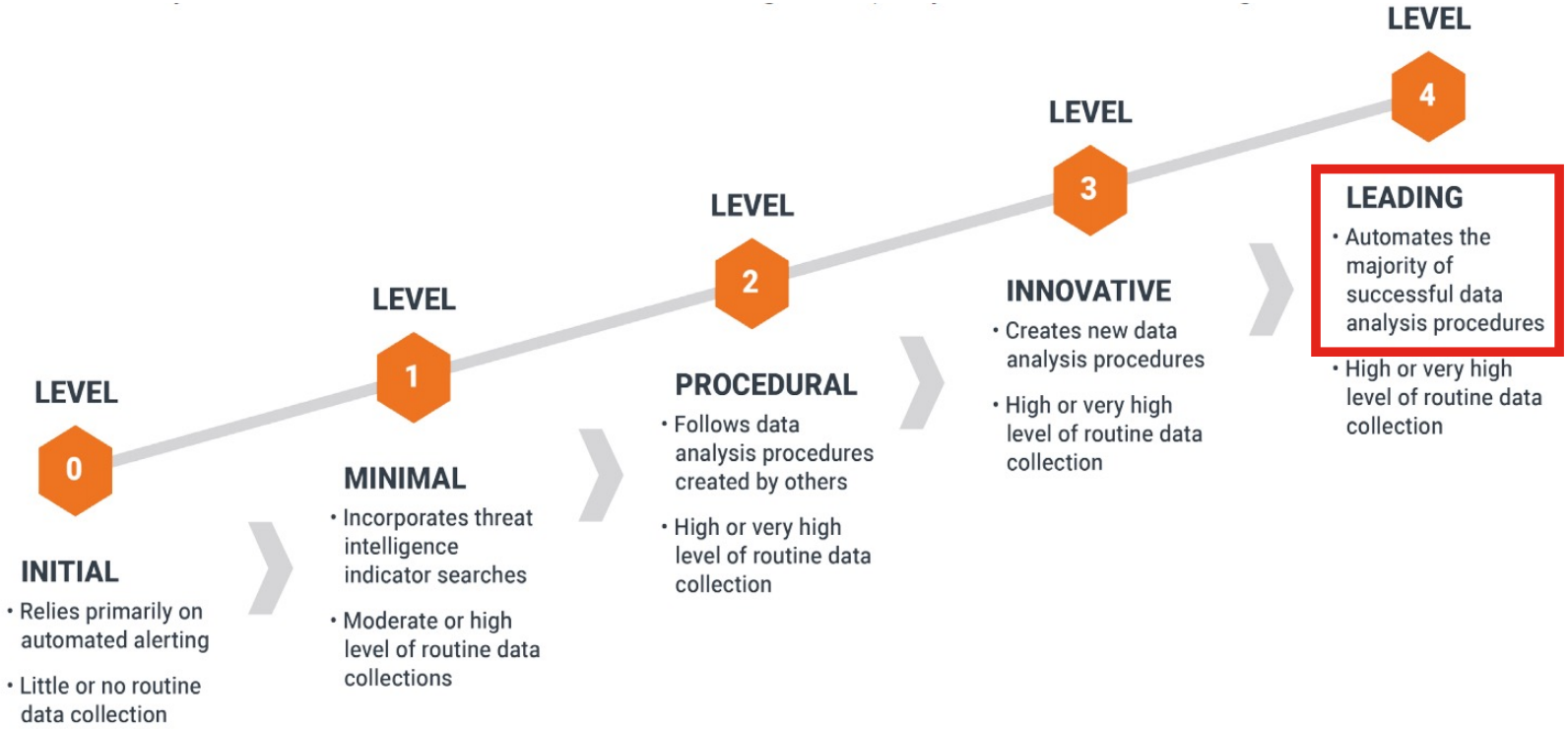
Generic Behaviors

- Low-prevalence artifacts
- Outlier behaviors
- Unknown threat leads

The Hunting Loop



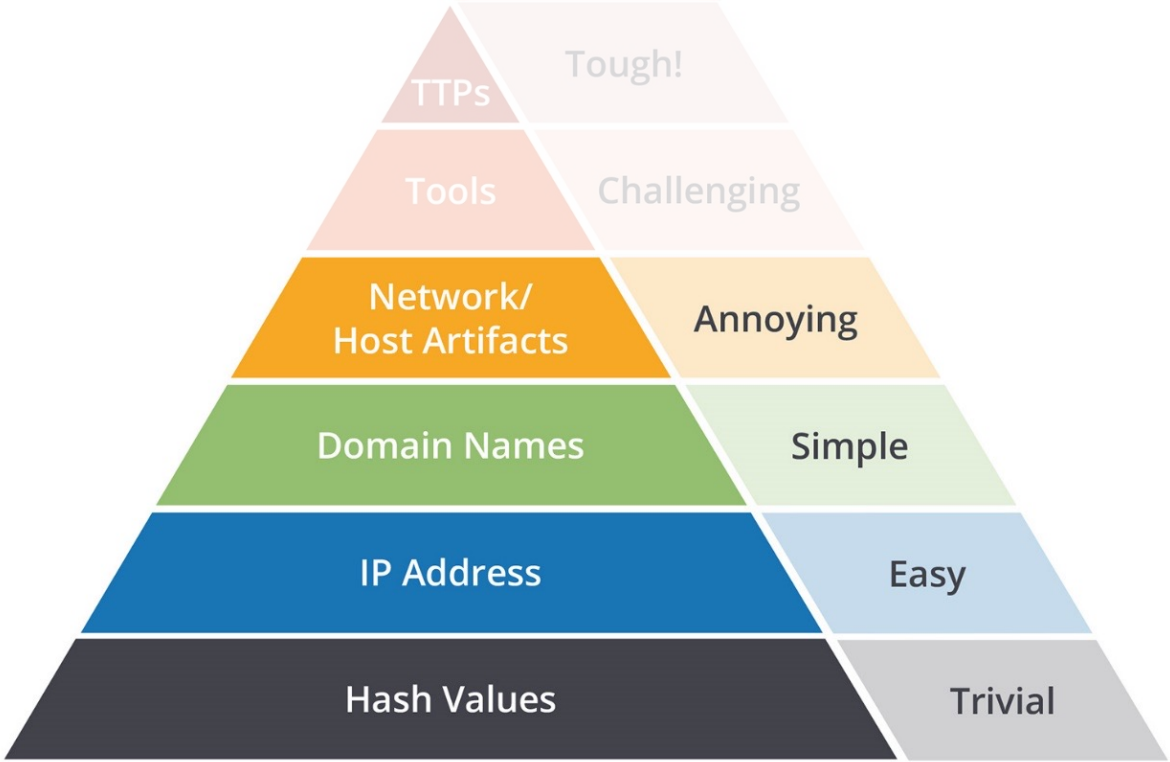
Source: "A framework for Cyber Threat hunting" by Sqrrl



On-Demand Hunting

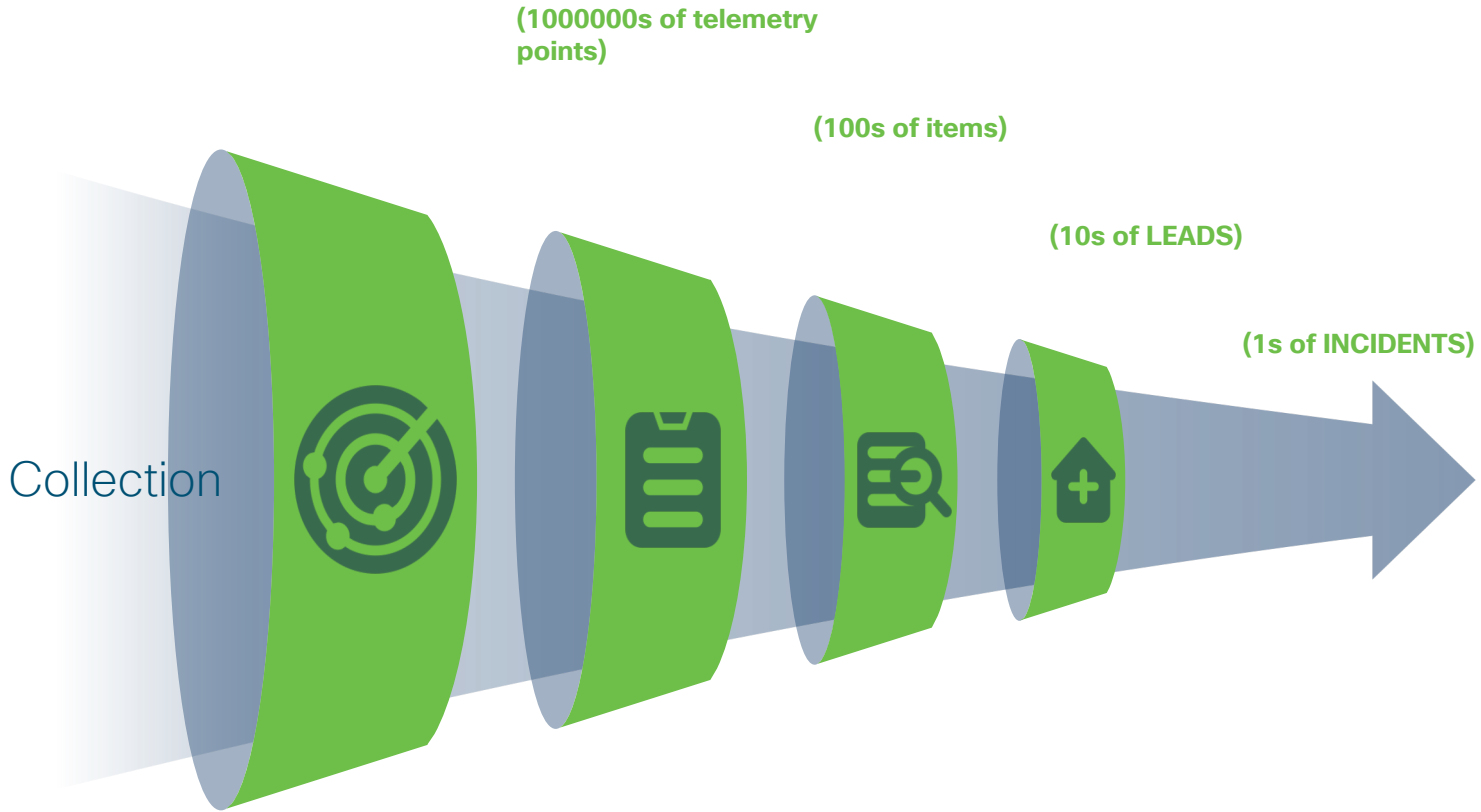
Automated Continuous Hunting

The Pyramid of pain...

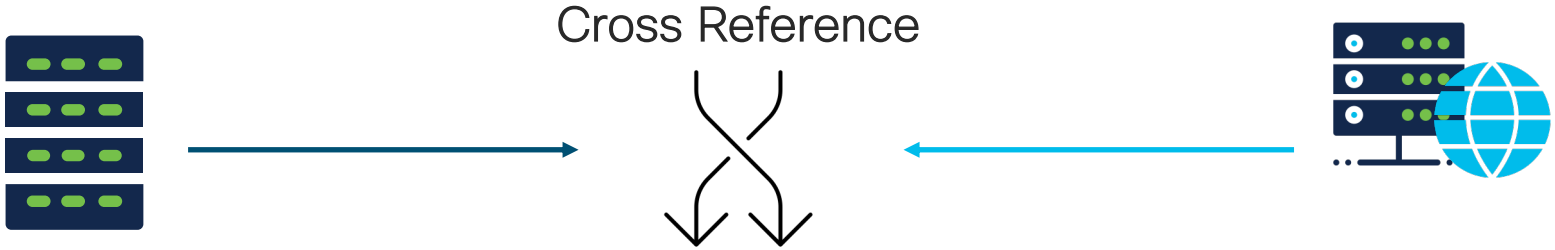


Source: David J. Bianco, personal blog

How to make your hunting efficient



Intelligence-Driven Threat Hunting



Local Context

- Endpoint logs
- Kubernetes audit logs
- Flow data
- Vulnerability scans
- Sandbox results
- DNS logs
- Etc.

Global Intelligence

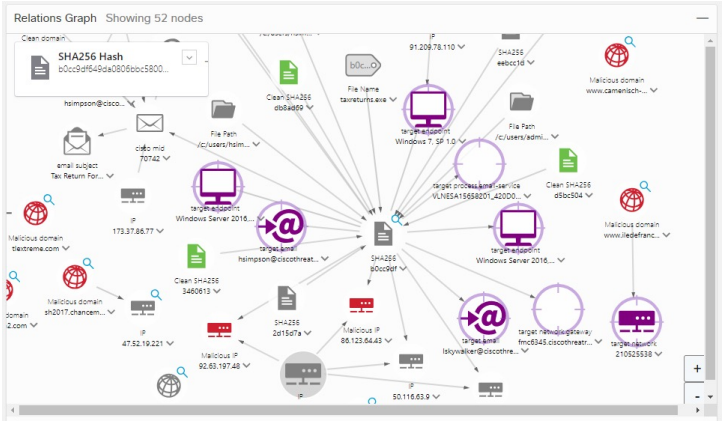
- Threat intelligence reports
- Threat intelligence feeds
- Malware analysis
- Blogs
- Twitter
- Etc.

Actionable Insights

- Block X
- Isolate Y
- Etc.

The Hunting tools in this session...

python™



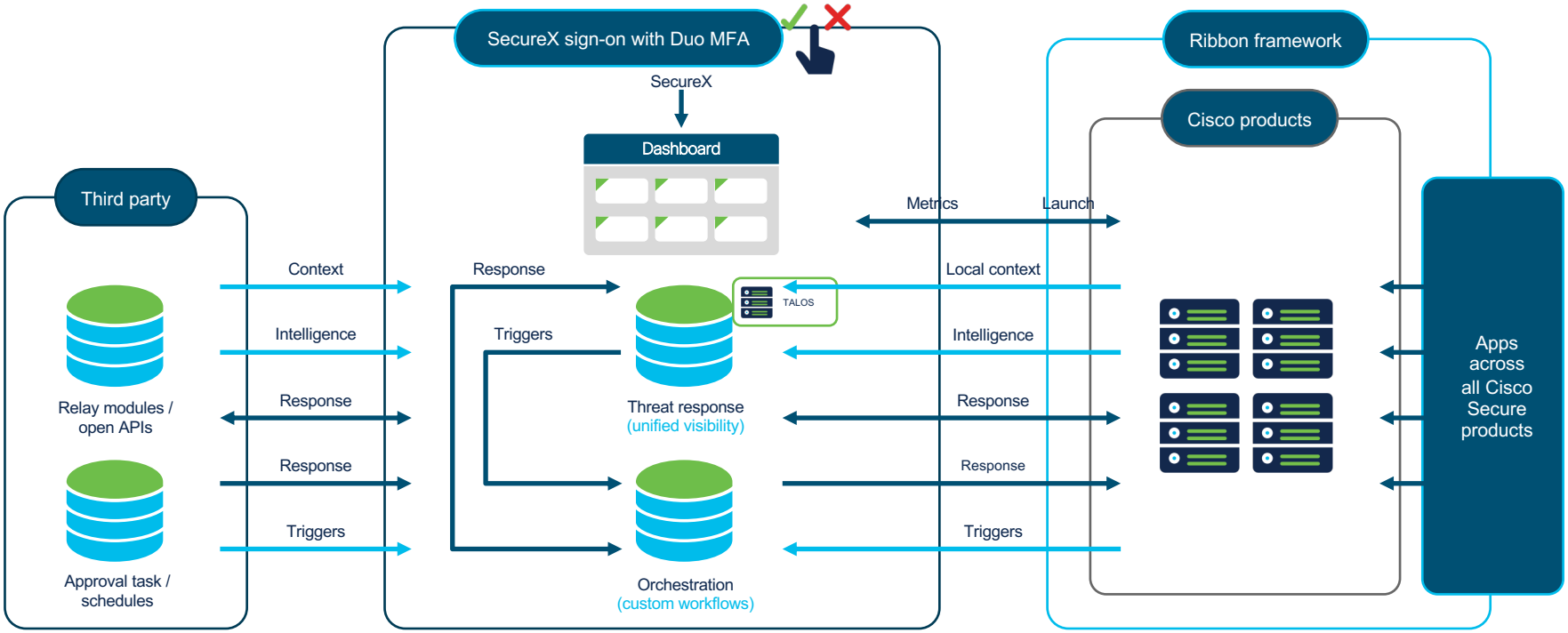
Agenda

- Introduction to Threat Hunting
- ➢ **Introduction to SecureX and Threat Response**
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

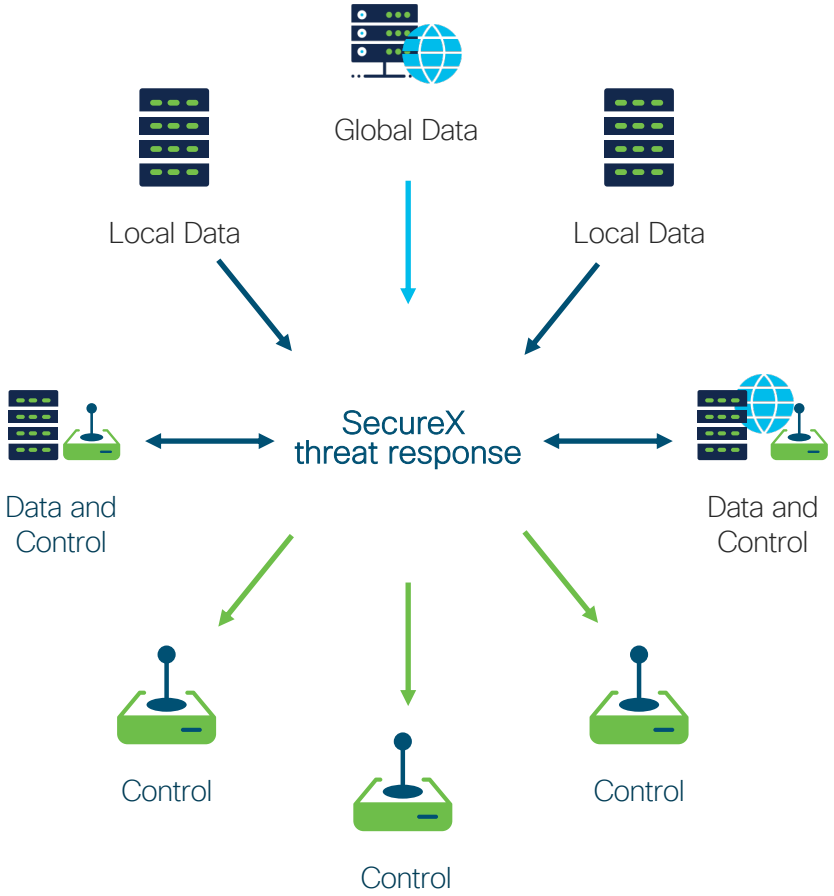
THIS IS NOT A MARKETING PRESENTATION.
CISCO PRODUCTS USED AS EXAMPLE...

Introduction to SecureX and Threat Response

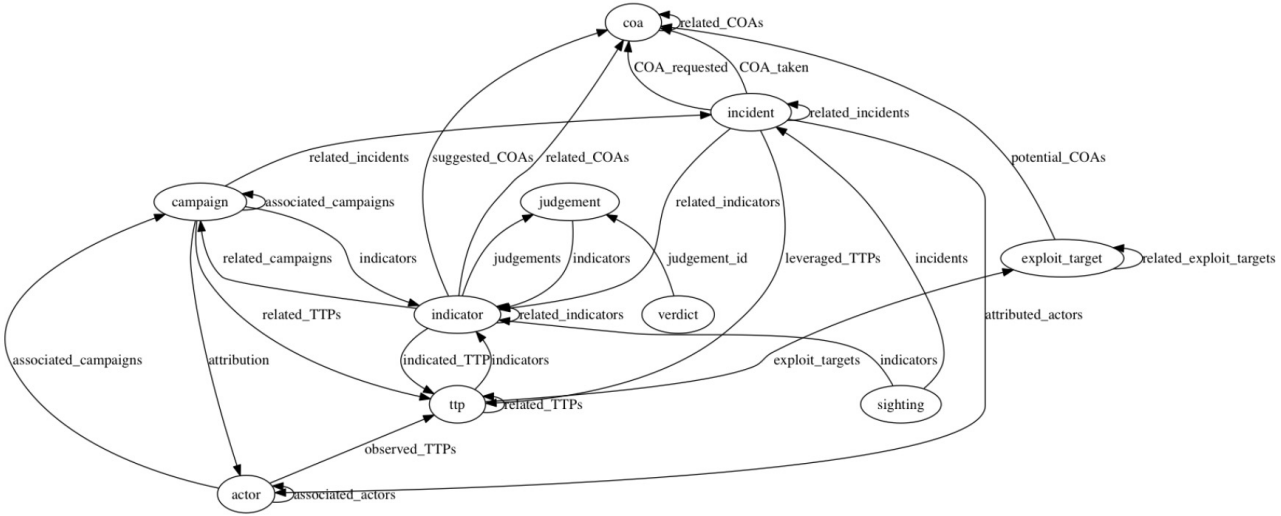
SecureX architecture



API aggregation at work

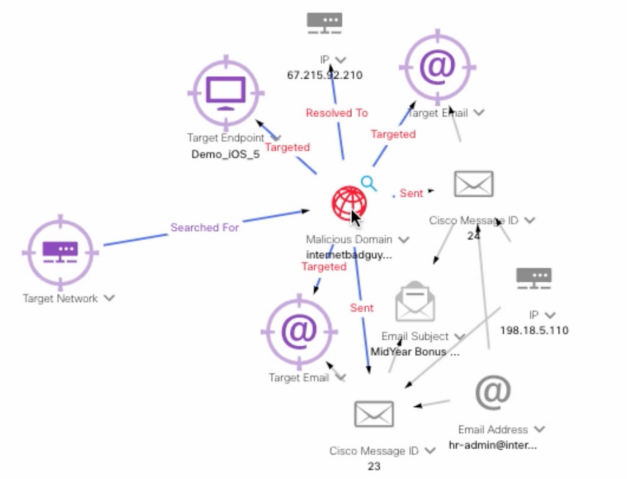


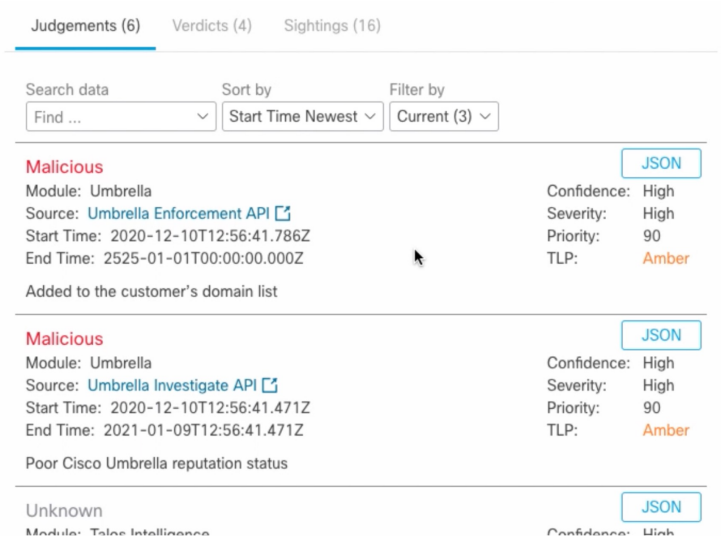
The CTIM (Cisco Threat Intel Model)



- Observable
- Judgement
- Verdict
- Sighting
- Indicator
- Casebook
- Incident

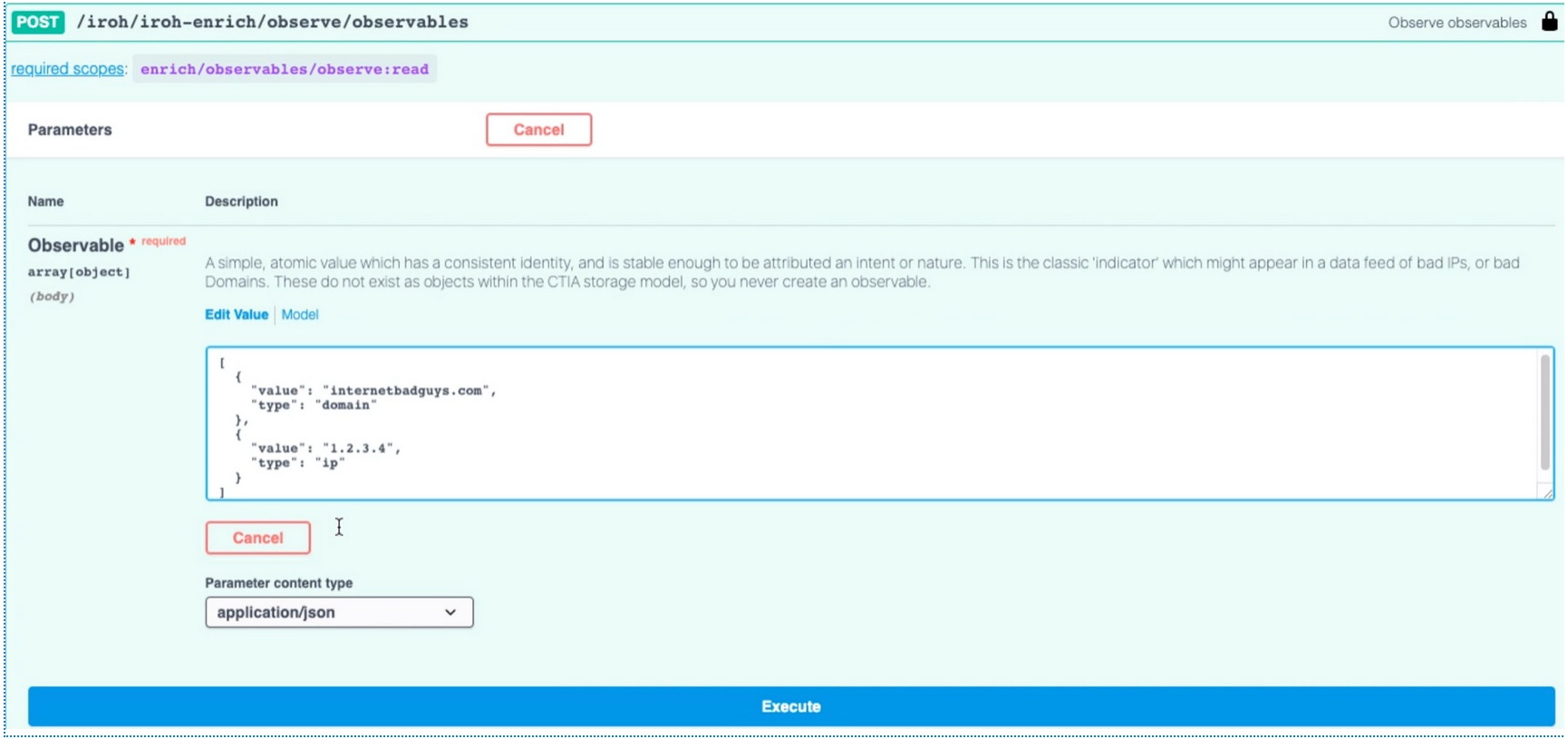
Recognize CTIM in SecureX Threat Response





- Observable
- Judgement
- Verdict
- Sighting
- Indicator
- Casebook
- Incident

Interact with CTIM Enrichment API with Swagger



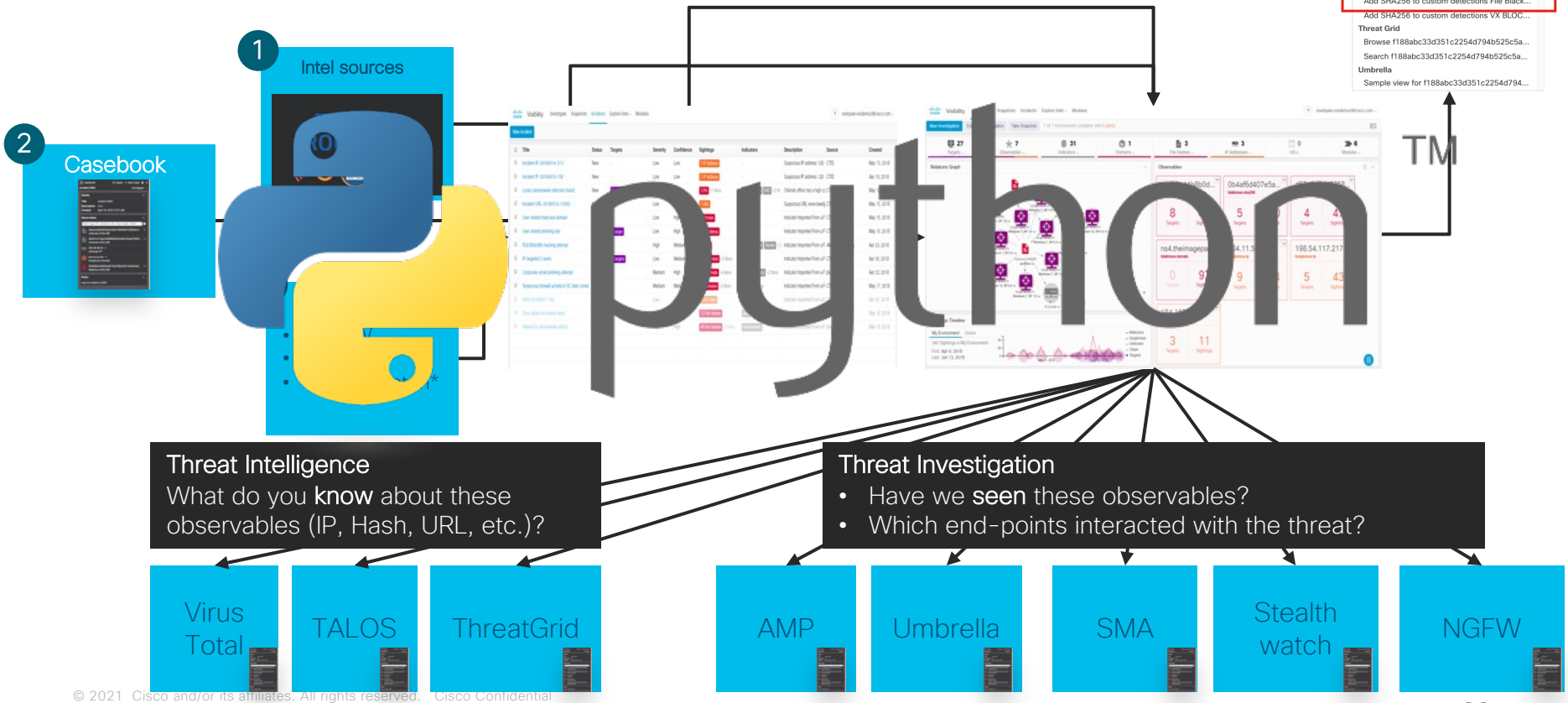
Interact with CTIM Enrichment API with Python

- Enrichment APIs
- Response actions
- Create Casebook
- Create Incident*

* optional exercise, adding your own python

```
119     '''
120     Enrich and Deliberate  (means get more info from) the observables from previous step
121     '''
122     url = 'https://visibility.amp.cisco.com/iroh/iroh-enrich/deliberate/observables'
123     data = json.dumps(OBSERVABLES)
124     response = post(url, headers=headers, data=data)
125     print("Response returned by API is")
126     print(json.dumps(response,indent=4,sort_keys=True))
127
128     input("\nPress Enter to continue with next step - to get even more info from observables\n")
129
130     '''
131     Get Even more info from Observables
132     '''
133     url = 'https://visibility.amp.cisco.com/iroh/iroh-enrich/observe/observables'
134     response = post(url, headers=headers, data=data)
135     print("Response returned by API is")
136     print(json.dumps(response,indent=4,sort_keys=True))
137
138     input("\nPress Enter to continue with next step - to get the response actions of the observables\n")
139
140     '''
141     Get the Response Actions for the Observables
142     '''
143     url = 'https://visibility.amp.cisco.com/iroh/iroh-response/respond/observables'
144     response = post(url, headers=headers, data=data)
145     print("Response returned by API is")
146     print(json.dumps(response,indent=4,sort_keys=True))
147
148     input("\nPress Enter to continue with next step - to create a casebook with the observables\n")
149     '''
150     Create a casebook with the observables
151     '''
152     d = date.today()
```

Cisco Threat Response: Workflow



The 3 custom methods of integrating and automating with SecureX:

1. SecureX APIs

Work with CTIM to create incidents, casebooks, judgments, sightings etc. Anything that can be done in GUI can be done via API.

2. SecureX orchestration

Low-to-no-code orchestrator to automate (scheduled/triggered) security workflows. Perfect middleware and easy to get started.

3. SecureX relay modules

Most advanced and "native" way of integrating with SecureX. Offers possibility to integrate as module in SecureX. Uses the SecureX APIs under the hood.

Cisco SecureX alternatives:

- Sophos Intercept X: Next-Gen Endpoint.
- LogRhythm NextGen SIEM Platform.
- CrowdStrike Falcon: Endpoint Protection.
- Trend Micro Apex One.
- InsightIDR.
- SentinelOne Endpoint Protection Platform.
- Bitdefender GravityZone.
- Cortex XDR.
- The Hive Project.

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- **Use Case 1: Ingest Twitter posts for Threat Intel**
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

Use Case 1: Ingest Twitter posts for Threat Intel

#OPENDIR

twitter.com/search?q=%23opendir&src=typed_query

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet

Chrisco
@ChriscoDevnet

#opendir

Top | Latest | People | Photos | Videos

JAMESWT @JAMESWT_MHT · 1h

Replying to @malwrhunterteam

Your Sample
#opendir
albumdepremios[.]com[.]br/hostmeu/
hostmeusite.ddns[.]net
Sample
app.any.run/tasks/7ac99b76...

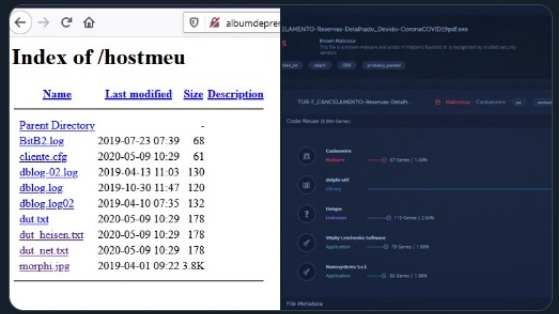
analyze.intezer.com/#/analyses/d38...

bazaar.abuse.ch/sample/e50e83a...

virustotal.com/gui/domain/alb...

Eset after submission detect it as Spy Delf

cc @Spam404



1 4

Bad Packets Report @bad_packets · 14h

Active DDoS #malware payload detected:
http://204.48.24.169/bins/mpsl (🇺🇸)(virustotal.com/gui/url/d79419...)
http://204.48.24.169/bins/ #opendir

Exploit attempt source IPs:
162.243.168.210 (🇺🇸)
206.81.0.151 (🇺🇸)

Search filters

People
From anyone
People you follow

Location
Anywhere
Near you

Advanced search

Trends for you

Trending in Netherlands
Seattle
382K Tweets

UEFA Europa League · Trending
Feyenoord
3,343 Tweets

Politics · Trending
Nancy
70.4K Tweets

Trending in Netherlands
#China
39K Tweets

Trending in Netherlands
#Coronavirusnl

Show more

Who to follow

Huawei @Huawei
Follow
Promoted

https://twitter.com/search?q=%23opendir&src=typed_query

Do you have enough time to keep up to date with your own social media?

https://github.com/chrivand/twitter_search_threatresponse

ChriscoDevNet
@ChriscoDevnet

Do you ever report on new indicators of compromise that you find in the wild? If so, do you use the #opendir hashtag? For example internetbadguys.com could be a fresh IoC!

Check out my SecureX integration if you are interested to learn more:

chrivand/
twitter_search_threatres...

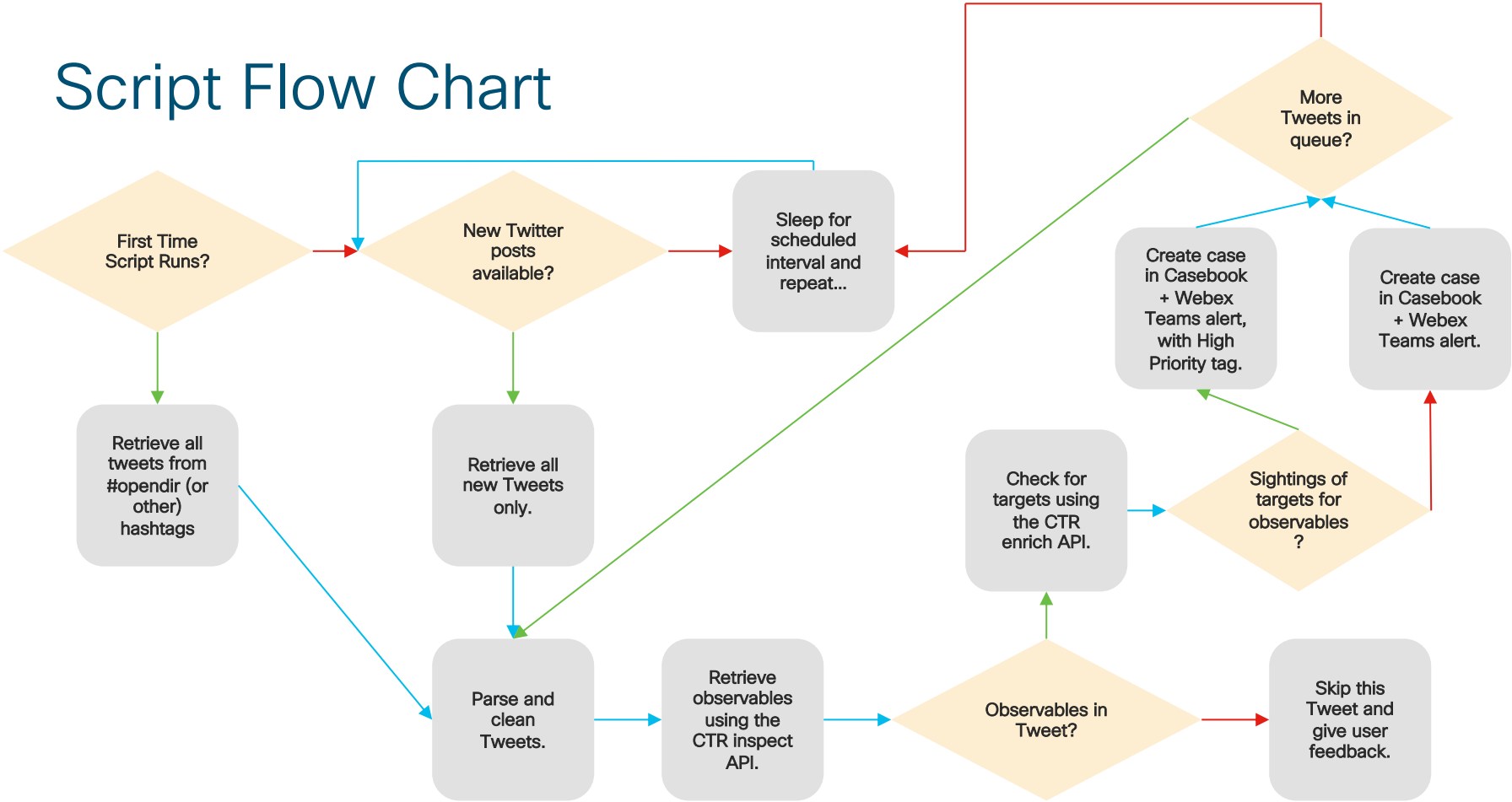
Twitter Search to Cisco Threat Response Casebook [v1.0]

1 Contributor | 0 Issues | 0 Stars | 1 Fork

chrivand/twitter_search_threatresponse
Twitter Search to Cisco Threat Response Casebook [v1.0] - chrivand/twitter_search_threatresponse
github.com

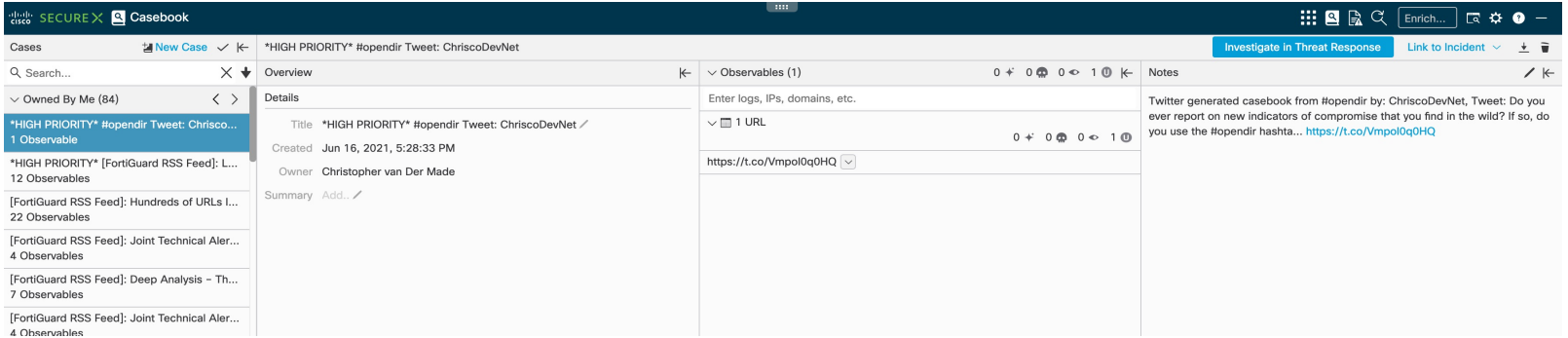
3:26 PM · Jun 16, 2021 · Twitter Web App

Script Flow Chart



Script source: https://github.com/chrivand/twitter_search_threatresponse

Result in SecureX Casebook and Webex



Demo please!

#opendir

Top | Latest | People | Photos | Videos

JAMESWT @JAMESWT_MHT · 40m
Replying to @malwrhunterteam
Your Sample
#opendir
albumdepremios[.]com[.]br/hostmeu/
hostmeusite.ddns[.]net
Sample
app.any.run/tasks/7ac99b76...

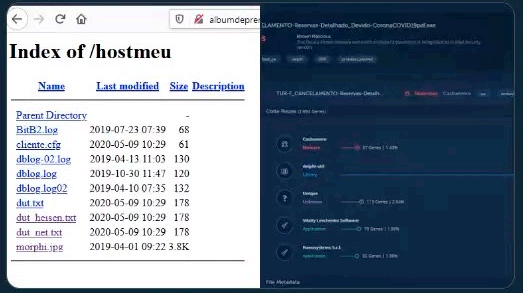
analyze.intezer.com/#/analyses/d38...

bazaar.abuse.ch/sample/e50e83a...

virustotal.com/gui/domain/alb...

Eset after submission detect it as Spy Delf

cc @Spam404



1 4

Bad Packets Report @bad_packets · 13h
Active DDoS #malware payload detected:
http://204.48.24.169/bins/mpsl (🇺🇸)(virustotal.com/gui/url/d79419...)
http://204.48.24.169/bins/ #opendir

Exploit attempt source IPs:
162.243.168.210 (🇺🇸)
206.81.0.151 (🇺🇸)

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- **Use Case 2: Ingest (Talos) Blogs for Threat Intel**
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

Use Case 2: Ingest (Talos) Blogs for Threat Intel

Cisco Talos: Blog

- Talos posts about a couple of blog posts per week.
- Often they contain insights into new Threats / Campaigns.
- These blog posts contain many interesting observables…
- There are many more blogs that have interesting observables…

TUESDAY, JUNE 4, 2019

It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign

Indicators of Compromise

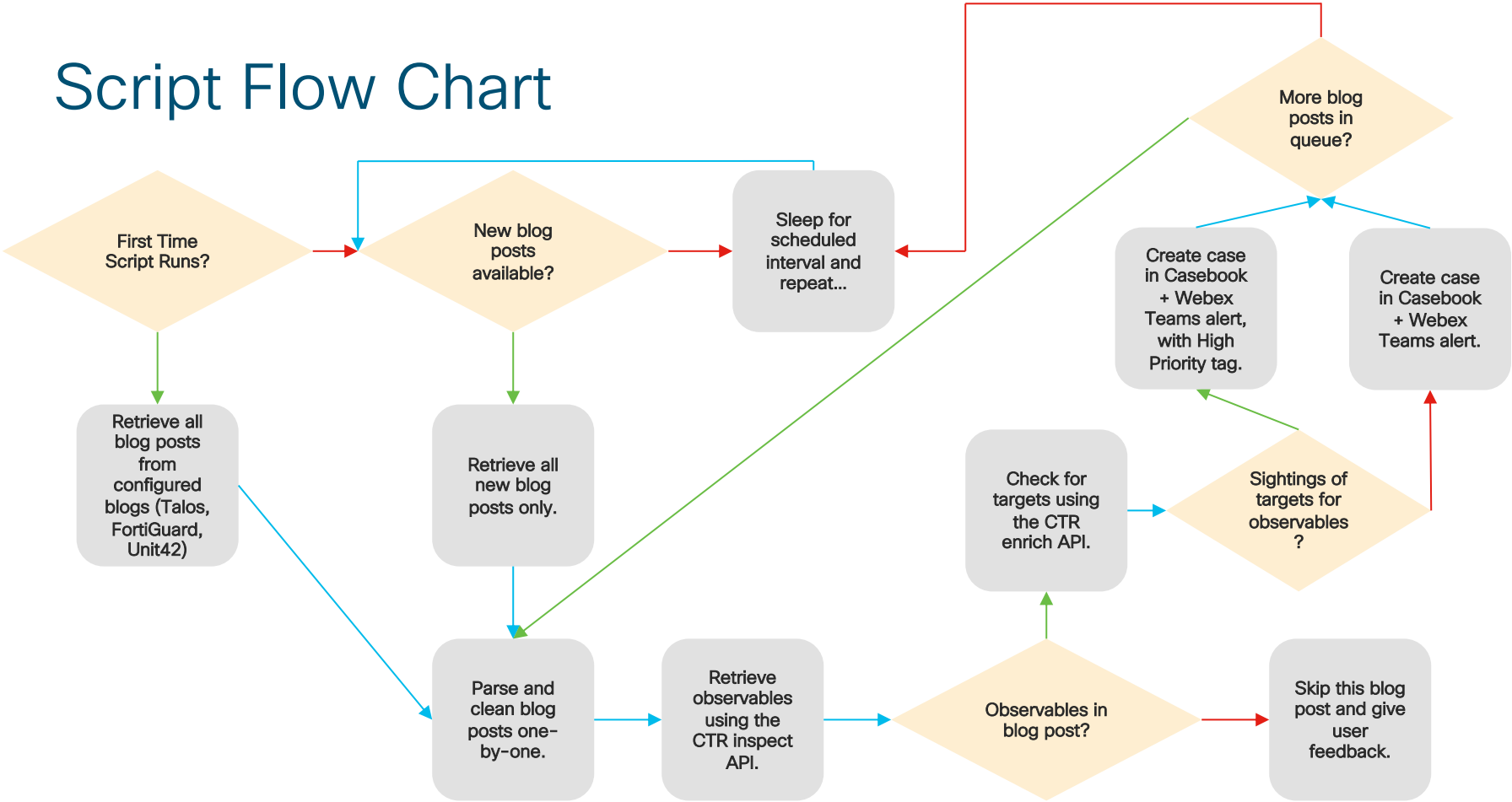
Hashes

418379fbfe7e26117a36154b1a44711928f52e33830c6a8e740b66bcbe63ec61
50195be1de27eac67dd3e5918e1fc80acaa16159cb48b4a6ab9451247b81b649
6b2c71bfc5d2e85140b87c801d82155cd9abd97f84c094570373a9620e81cee0

How does an analyst keep track of all these blog posts from Talos (and many other research teams)?

https://github.com/chrivand/talos_blog_to_casebook

Script Flow Chart



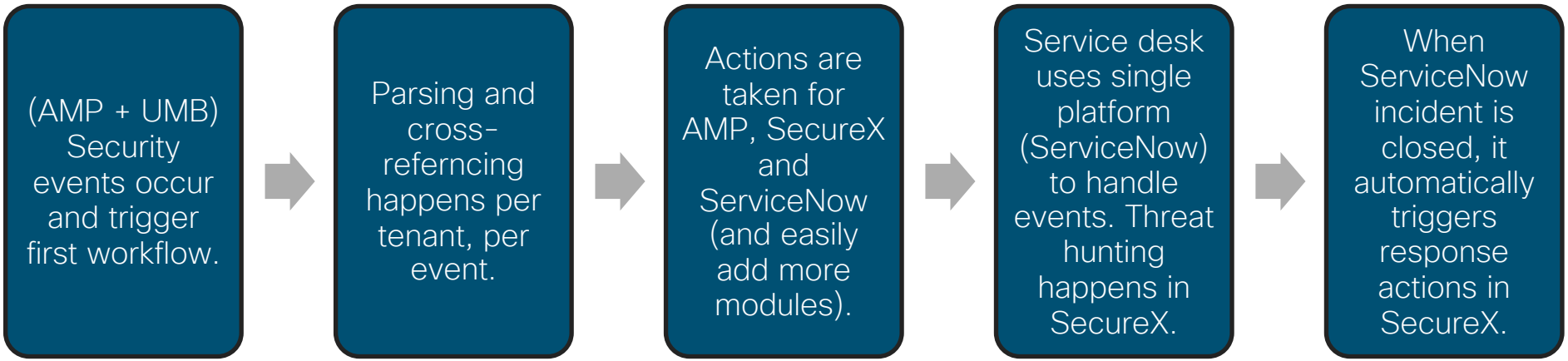
Script source: https://github.com/chrivand/talos_blog_to_casebook

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- ➢ **Use Case 3: MSSP Security Event Handling**
  - Overview
- Conclusion

Use Case 3: MSSP Security Event Handling

Let's check out a specific example…



https://github.com/chrivand/amp-mssp-events-to-snow
https://github.com/chrivand/amp-umb-mssp-sxo
More coming….

README.md

SecureX orchestration workflow: AMP4E (Cisco Secure Endpoint) MSSP customer events to SecureX incident and ServiceNow incident

> **NOTE:** This is sample code and needs to be tested properly before using in production!

This is a set of sample workflows to work with the MSSP environment of Cisco Secure Endpoint (formerly known as Advanced Malware Protection for Endpoints (AMP4E)). It can obtain events from the various customers and create Securex and ServiceNow incidents based on these security events. When the incident in ServiceNow is closed, this will automatically close the SecureX incident too. Please watch a demo in this Youtube video.

Index

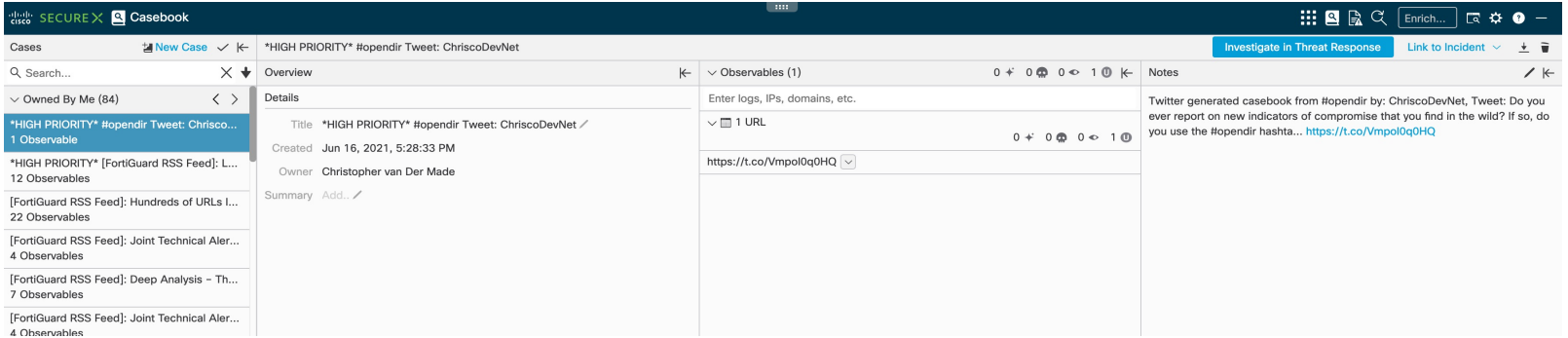
Features and flow

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- ➢ **Conclusion**

Conclusion

Is this easier than manually searching Twitter?



Conclusion

- Threat Hunting is all about gathering data from Local/Internal Monitoring and Global Intelligence.
- Threat Hunting is a continuous process and a loop.
- There are many tools, like SecureX, that can help with this.
- The SecureX API can automate parts of this process!

Agenda

- Introduction to Threat Hunting
- Introduction to SecureX and Threat Response
- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
- Use Case 3: MSSP Security Event Handling
  - Overview
- Conclusion

There is simply too much information and threat intelligence out there for SOC analysts to (consciously) consume. We need to automate as much as possible and provide bitesize cases to them.

Thank you!

@ChriscoDevNet
chrivand@cisco.com
github.com/chrivand