Stay ahead of the game: automate your threat hunting workflows

Christopher van der Made
Developer Advocate Security

Today

Who am I?

- Christopher van der Made.
- Developer Advocate Security, joined through graduate Program in 2015.
- Studied Neuro-, Computer- and Information-Science @ University of Amsterdam.
- Love being outdoors, brewing and building stuff!
- Love automation and coding!

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.

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
  - Demo
- 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
  - Demo
- 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

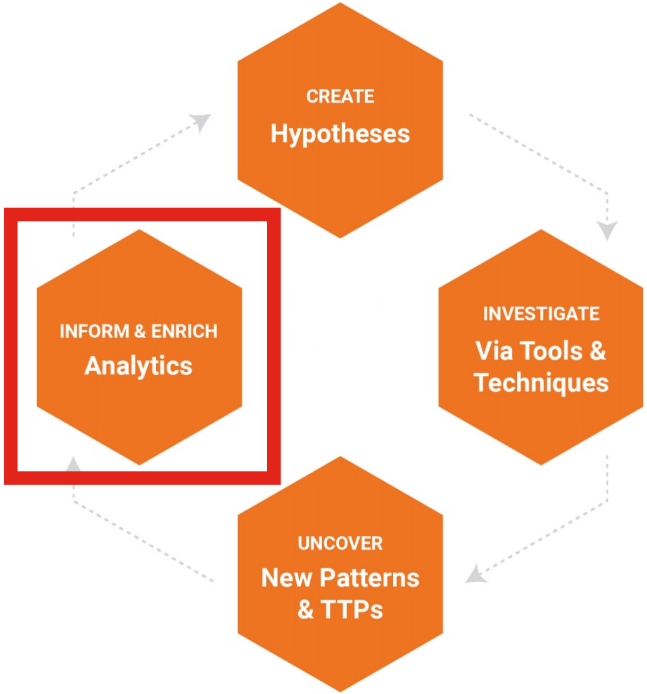
- TTP's: tactics, techniques, procedures
- Methodologies used by advanced attackers
- Systematic approach for discovering unknowns

3 Anomaly-Driven

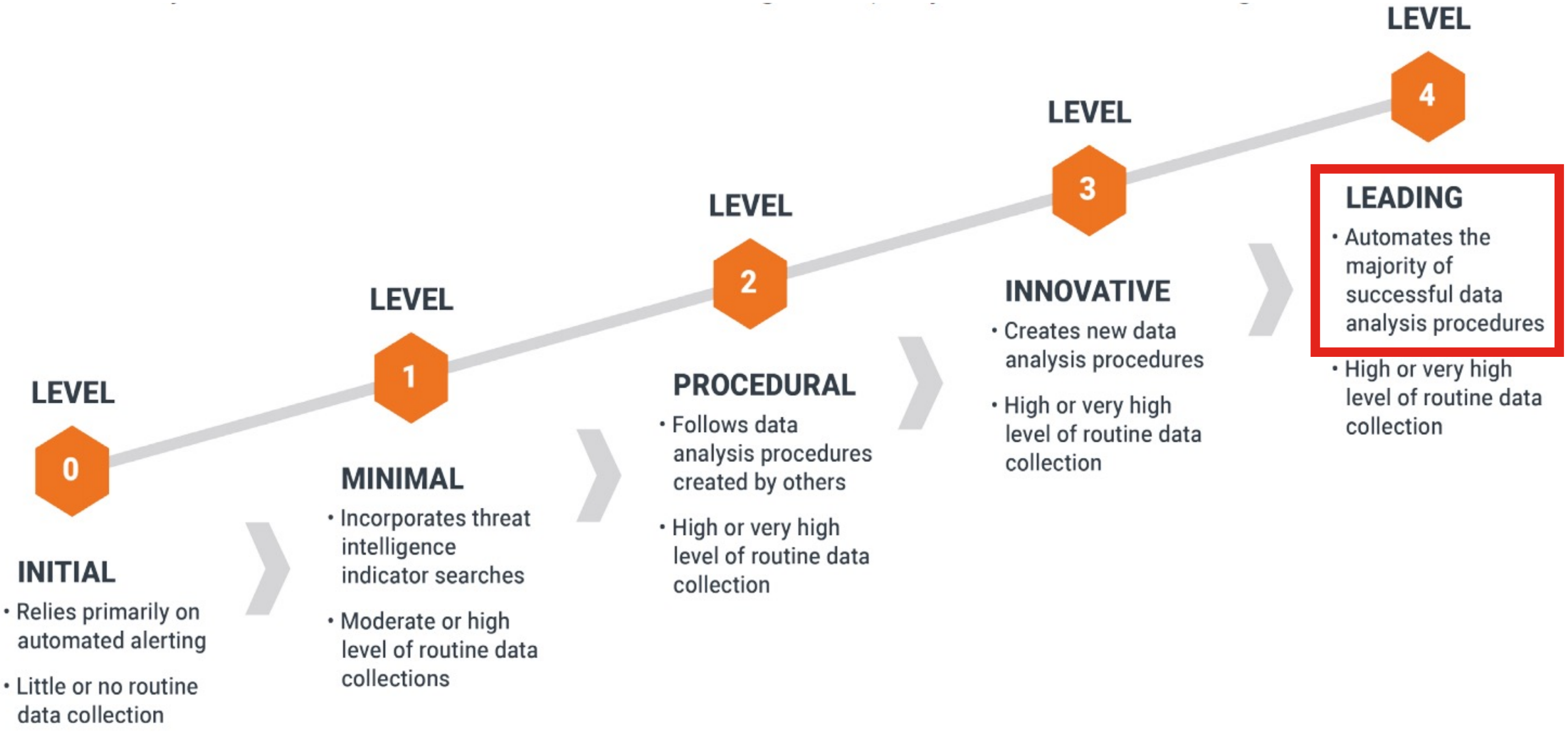
Generic Behaviors

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

The Hunting Loop



Source: “A framework for Cyber Threat hunting” by Sqrrl



LEVEL 0

INITIAL

- Relies primarily on automated alerting
- Little or no routine data collection

LEVEL 1

MINIMAL

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

LEVEL 2

PROCEDURAL

- Follows data analysis procedures created by others
- High or very high level of routine data collection

LEVEL 3

INNOVATIVE

- Creates new data analysis procedures
- High or very high level of routine data collection

LEVEL 4

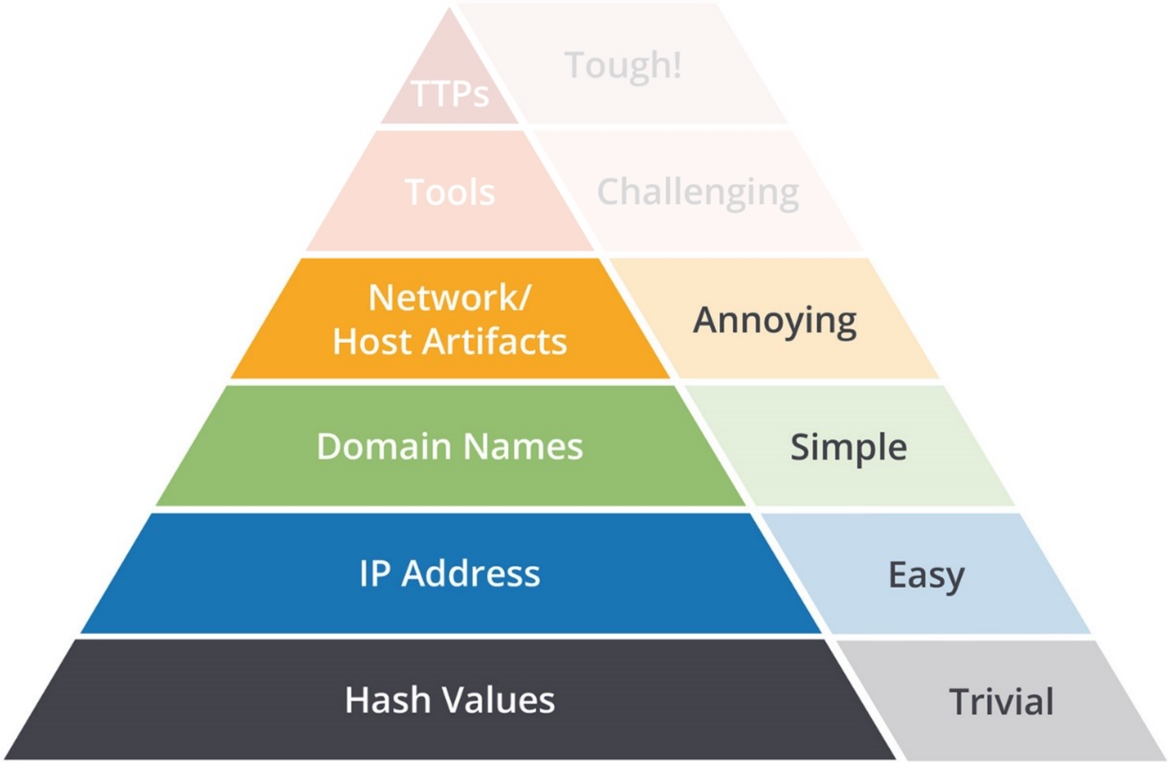
LEADING

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

On-Demand Hunting

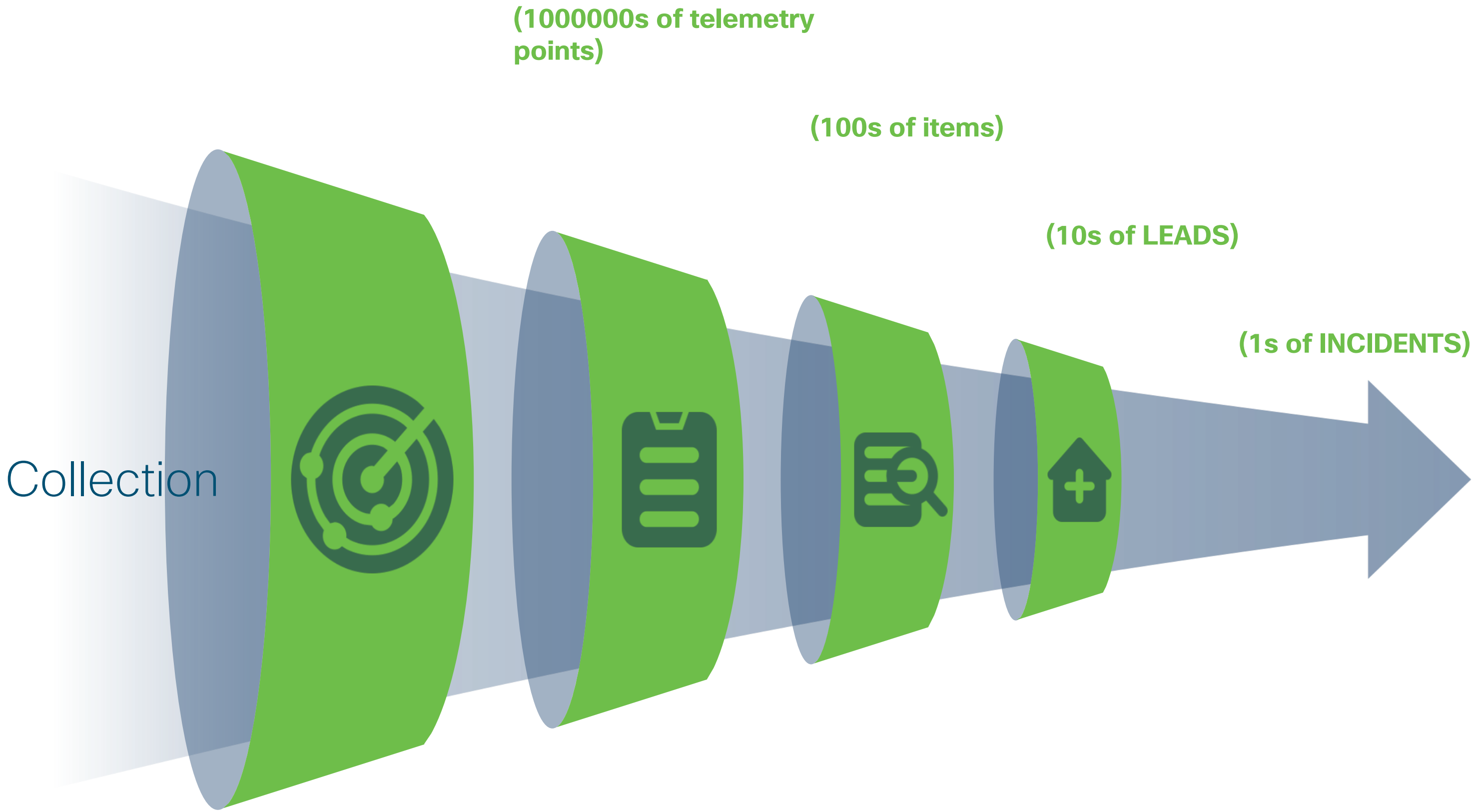
Automated Continuous Hunting

The Pyramid of pain…

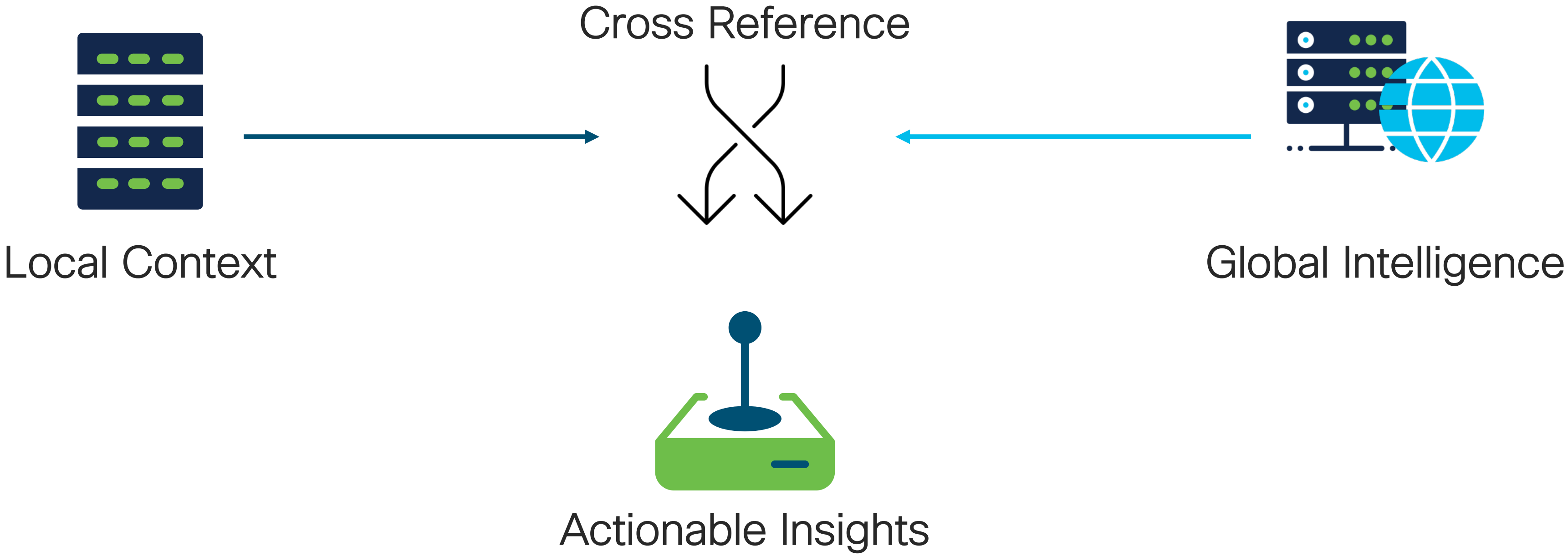


Source: David J. Bianco, personal blog

How to hunt


(1000000s of telemetry points)
(100s of items)
(10s of LEADS)
(1s of INCIDENTS)
Collection

Intelligence-Driven Threat Hunting



Cross Reference

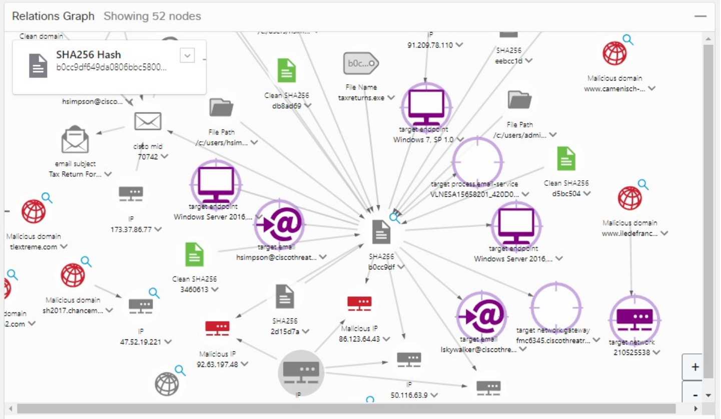
Local Context

Global Intelligence

Actionable Insights

The Hunting tools in this session...

python™



Relations Graph Showing 52 nodes

SHA256 Hash
b0cc9df649da0806bbc5800...

Agenda

- Introduction to Threat Hunting

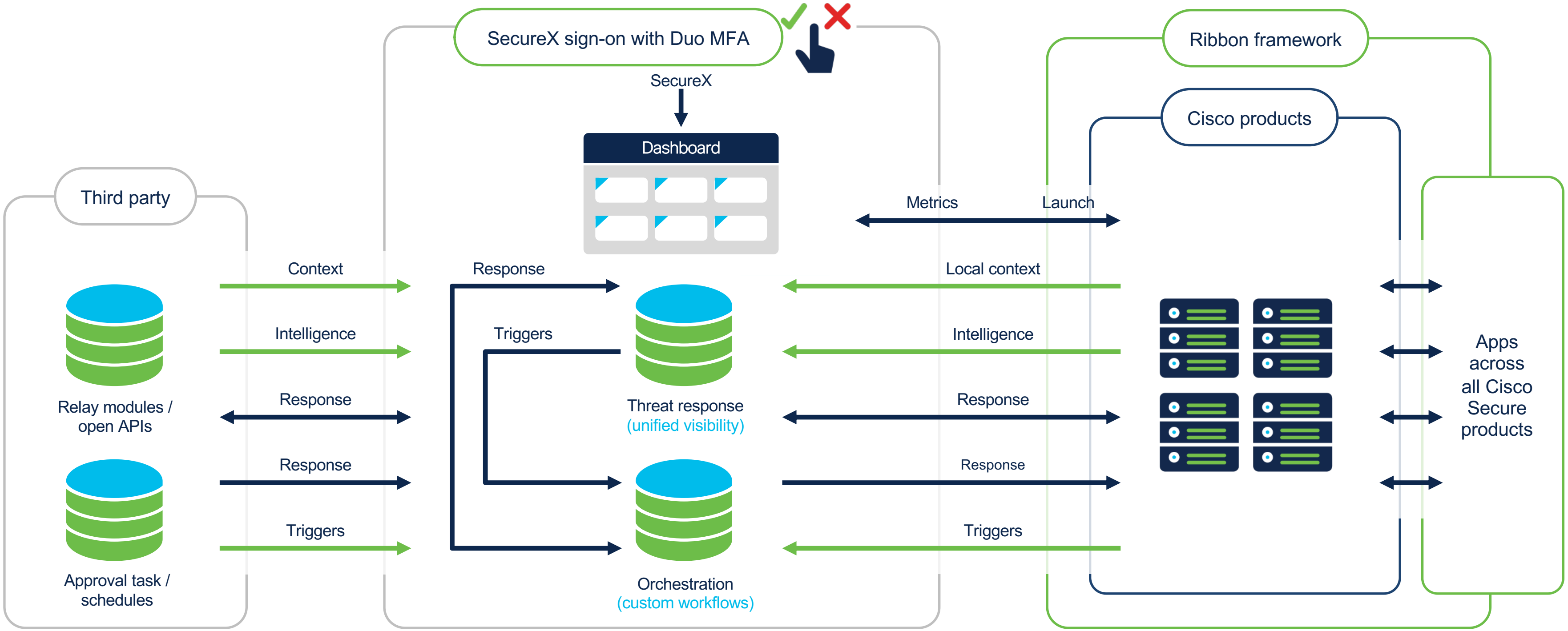
➢ **Introduction to SecureX and Threat Response**

- Use Case 1: Ingest Twitter posts for Threat Intel
  - Overview
  - Demo
- Use Case 2: Ingest (Talos) Blogs for Threat Intel
  - Overview
  - Demo
- Conclusion

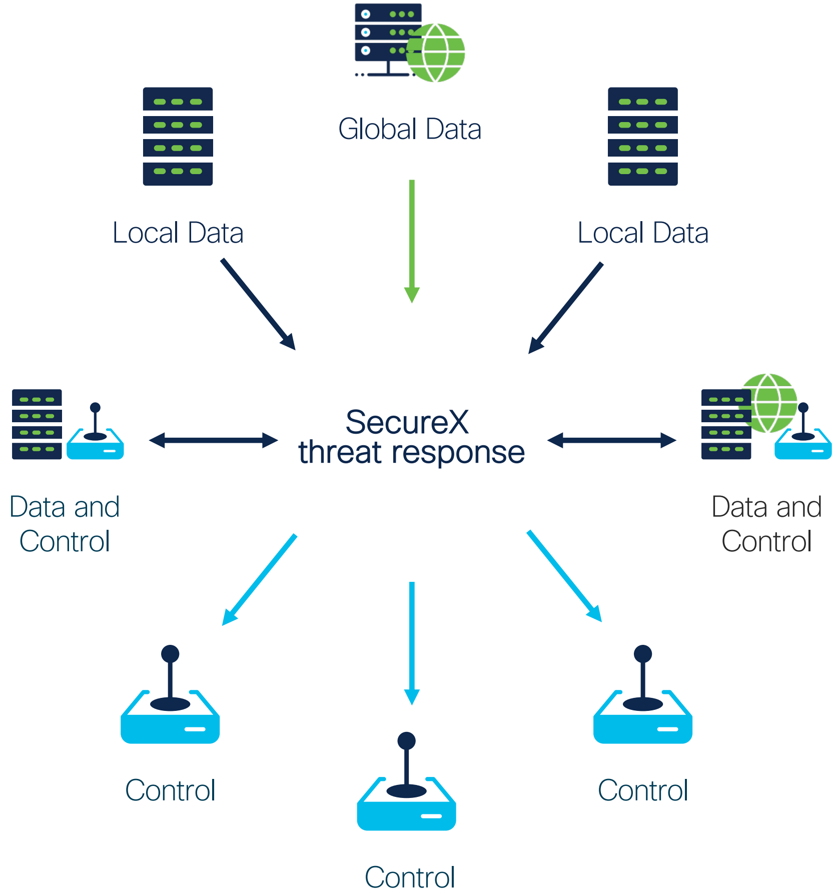
THIS IS NOT A MARKETING PRESENTATION.
CISCO PRODUCTS USED AS EXAMPLE...

Introduction to SecureX and Threat Response

SecureX architecture



API aggregation at work



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.

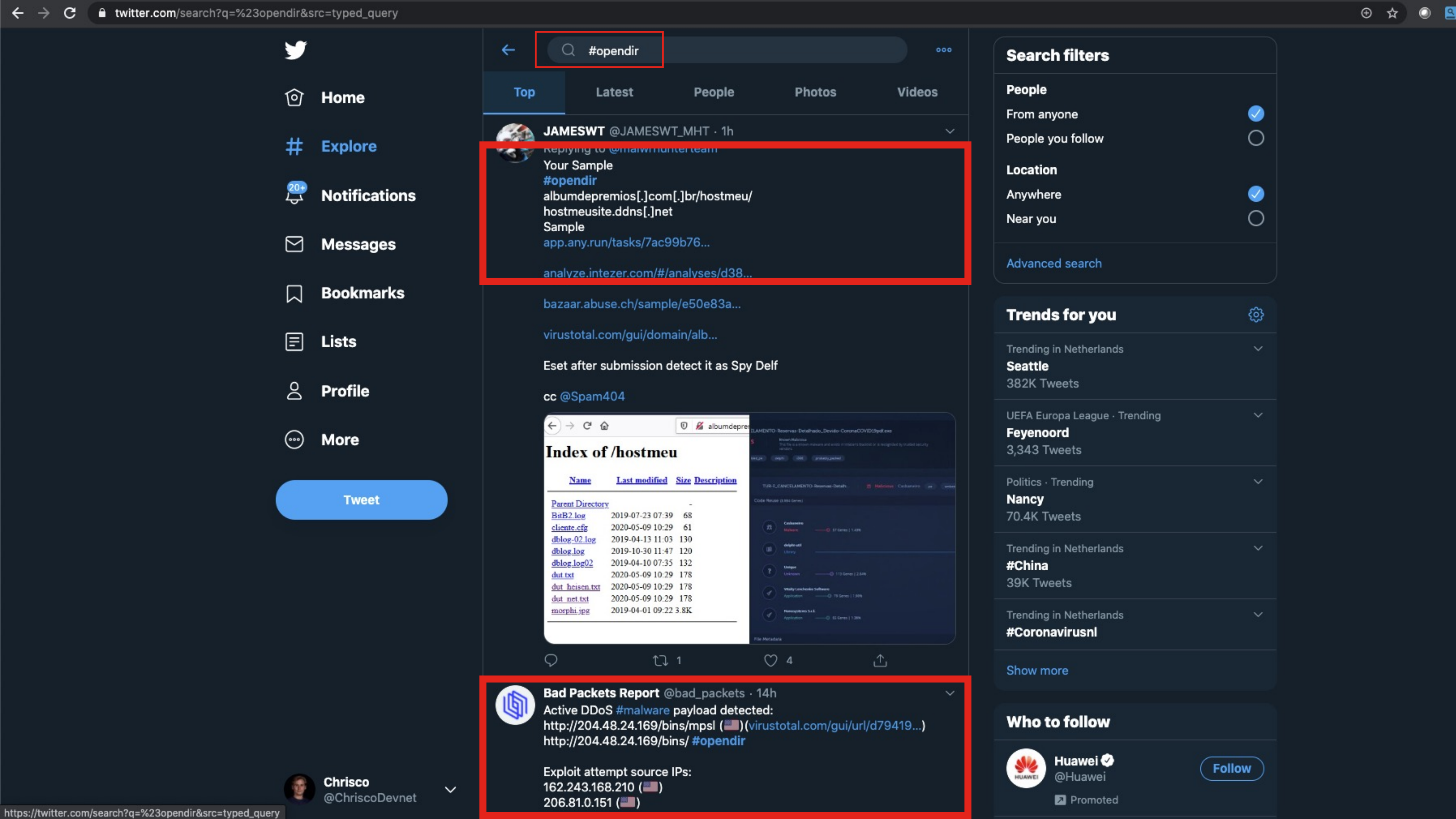
Agenda

- 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
  - Demo
- Conclusion

Use Case 1: Ingest Twitter posts for Threat Intel

#OPENDIR



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

#opendir

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

albumdepre

Index of /hostmeu

```
Name              Last modified     Size Description
Parent Directory                      -
BitB2.log         2019-07-23 07:39   68
cliente.cfg       2020-05-09 10:29   61
dblog-02.log      2019-04-13 11:03  130
dblog.log         2019-10-30 11:47  120
dblog.log02       2019-04-10 07:35  132
dut.txt           2020-05-09 10:29  178
dut_heisen.txt    2020-05-09 10:29  178
dut_net.txt       2020-05-09 10:29  178
morphi.jpg        2019-04-01 09:22 3.8K
```

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

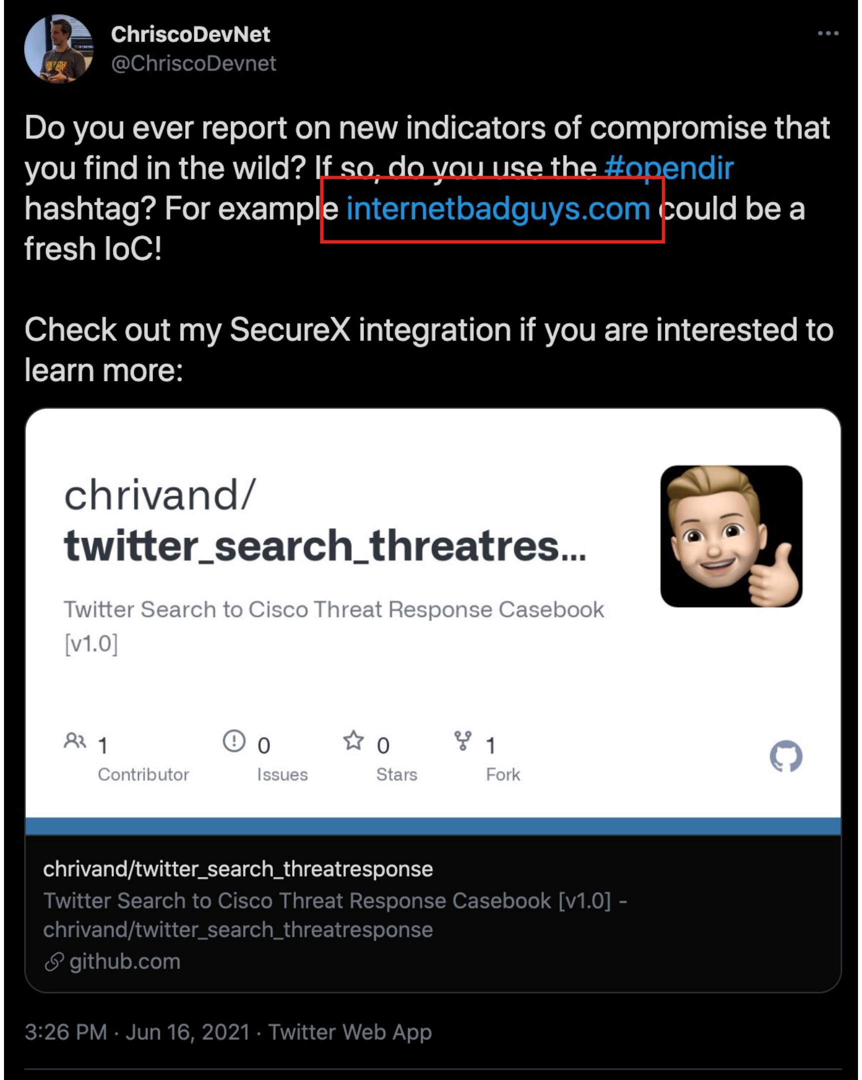
Who to follow

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...

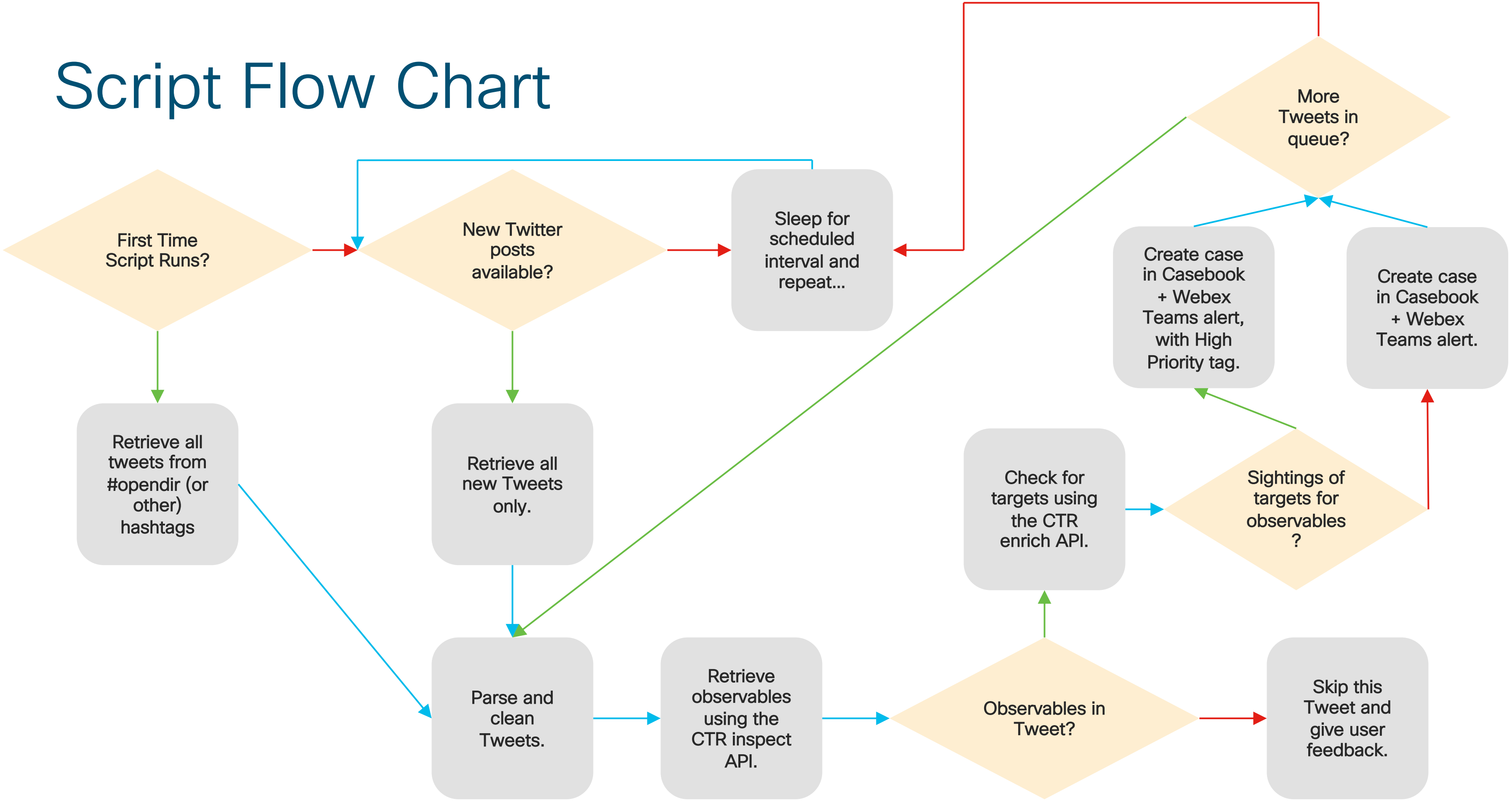
Twitter Search to Cisco Threat Response Casebook [v1.0]

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

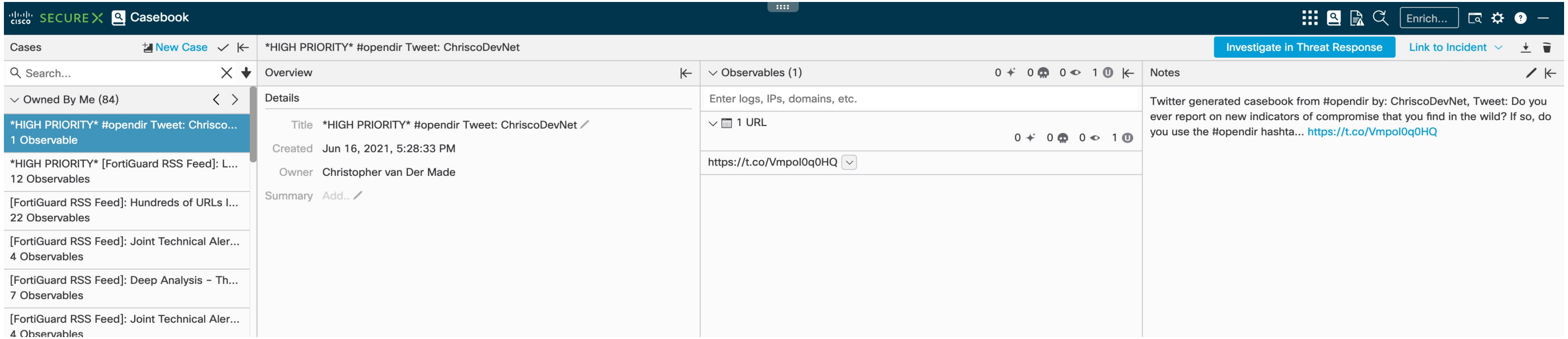
Script Flow Chart



First Time Script Runs?
New Twitter posts available?
Sleep for scheduled interval and repeat…
More Tweets in queue?
Create case in Casebook + Webex Teams alert, with High Priority tag.
Create case in Casebook + Webex Teams alert.
Retrieve all tweets from #opendir (or other) hashtags
Retrieve all new Tweets only.
Check for targets using the CTR enrich API.
Sightings of targets for observables ?
Parse and clean Tweets.
Retrieve observables using the CTR inspect API.
Observables in Tweet?
Skip this Tweet and give user feedback.

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

Result in SecureX Casebook and Webex



HIGH PRIORITY #opendir Tweet: ChriscoDevNet

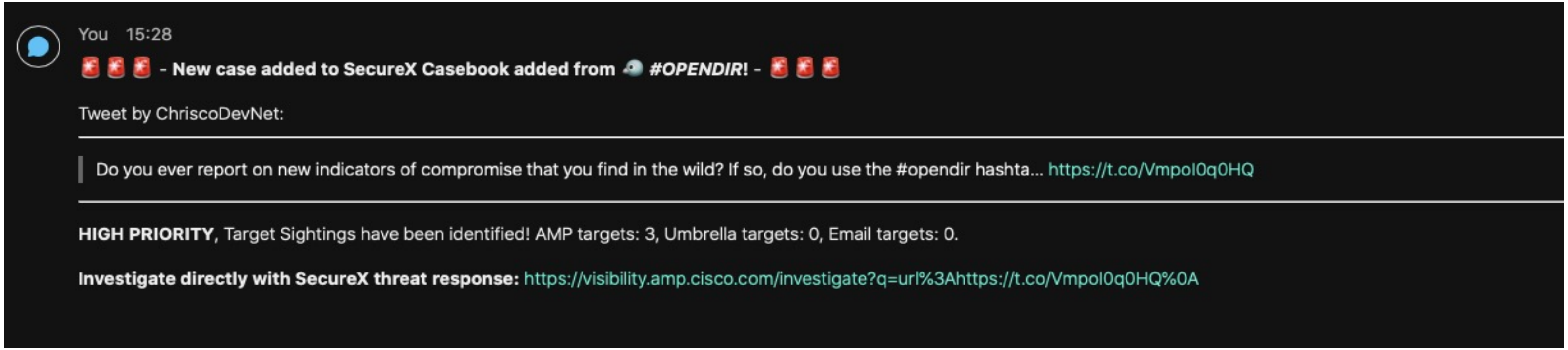
- *HIGH PRIORITY* #opendir Tweet: Chrisco...
1 Observable
- *HIGH PRIORITY* [FortiGuard RSS Feed]: L...
12 Observables
- [FortiGuard RSS Feed]: Hundreds of URLs I...
22 Observables
- [FortiGuard RSS Feed]: Joint Technical Aler...
4 Observables
- [FortiGuard RSS Feed]: Deep Analysis – Th...
7 Observables
- [FortiGuard RSS Feed]: Joint Technical Aler...
4 Observables

Title	*HIGH PRIORITY* #opendir Tweet: ChriscoDevNet
Created	Jun 16, 2021, 5:28:33 PM
Owner	Christopher van Der Made
Summary	Add..

0 0 0 1

https://t.co/Vmpol0q0HQ

Twitter generated casebook from #opendir by: ChriscoDevNet, Tweet: Do you ever report on new indicators of compromise that you find in the wild? If so, do you use the #opendir hashta... https://t.co/Vmpol0q0HQ



You 15:28

🚨 🚨 🚨 - **New case added to SecureX Casebook added from 🔍 *#OPENDIR*! -** 🚨 🚨 🚨

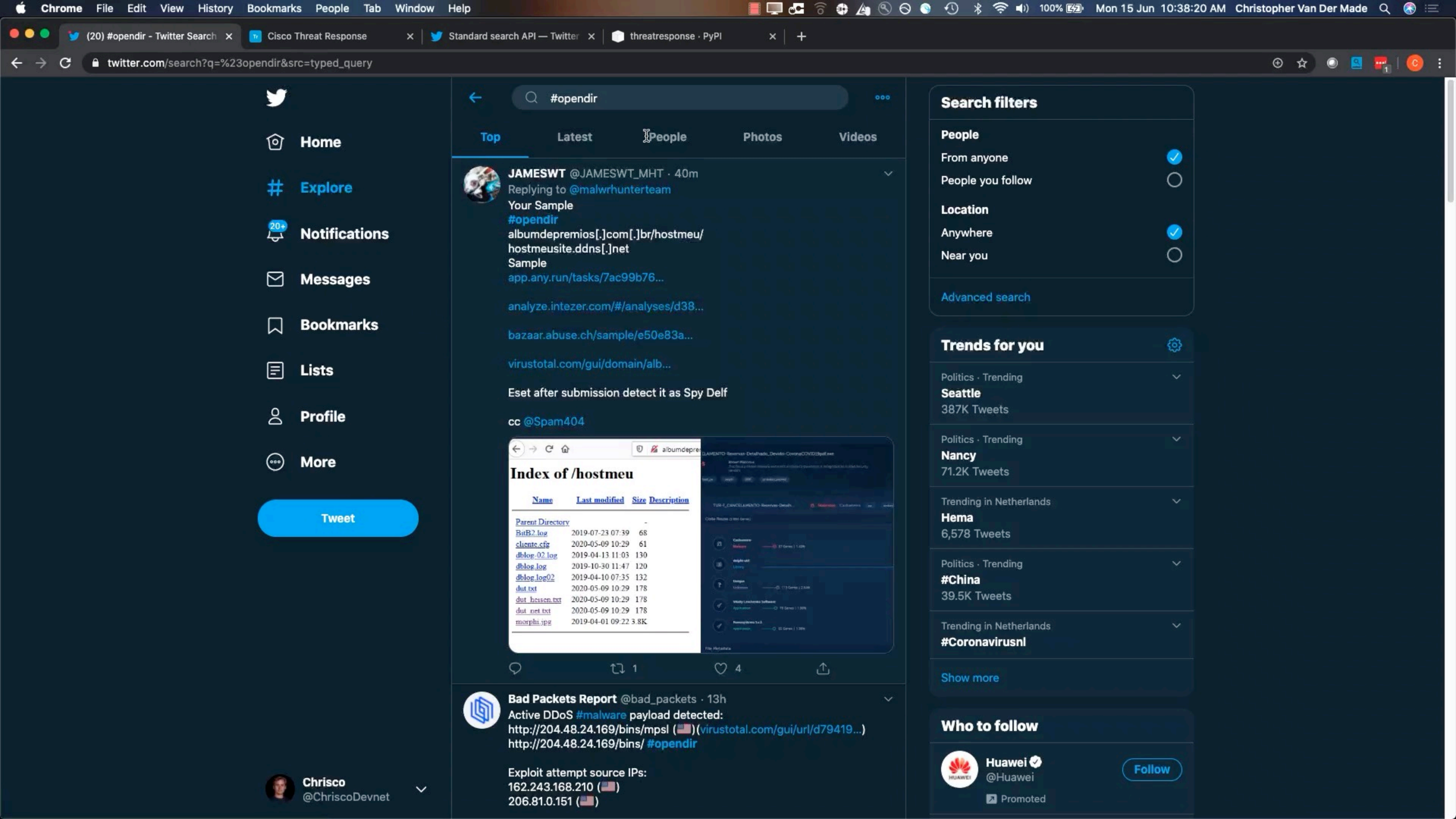
Tweet by ChriscoDevNet:

> Do you ever report on new indicators of compromise that you find in the wild? If so, do you use the #opendir hashta... https://t.co/Vmpol0q0HQ

HIGH PRIORITY, Target Sightings have been identified! AMP targets: 3, Umbrella targets: 0, Email targets: 0.

Investigate directly with SecureX threat response: https://visibility.amp.cisco.com/investigate?q=url%3Ahttps://t.co/Vmpol0q0HQ%0A

Demo please!



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

Index of /hostmeu

Name	Last modified	Size	Description
Parent Directory		-	
BitB2.log	2019-07-23 07:39	68	
cliente.cfg	2020-05-09 10:29	61	
dblog-02.log	2019-04-13 11:03	130	
dblog.log	2019-10-30 11:47	120	
dblog.log02	2019-04-10 07:35	132	
dut.txt	2020-05-09 10:29	178	
dut_heisen.txt	2020-05-09 10:29	178	
dut_net.txt	2020-05-09 10:29	178	
morphi.jpg	2019-04-01 09:22	3.8K	

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

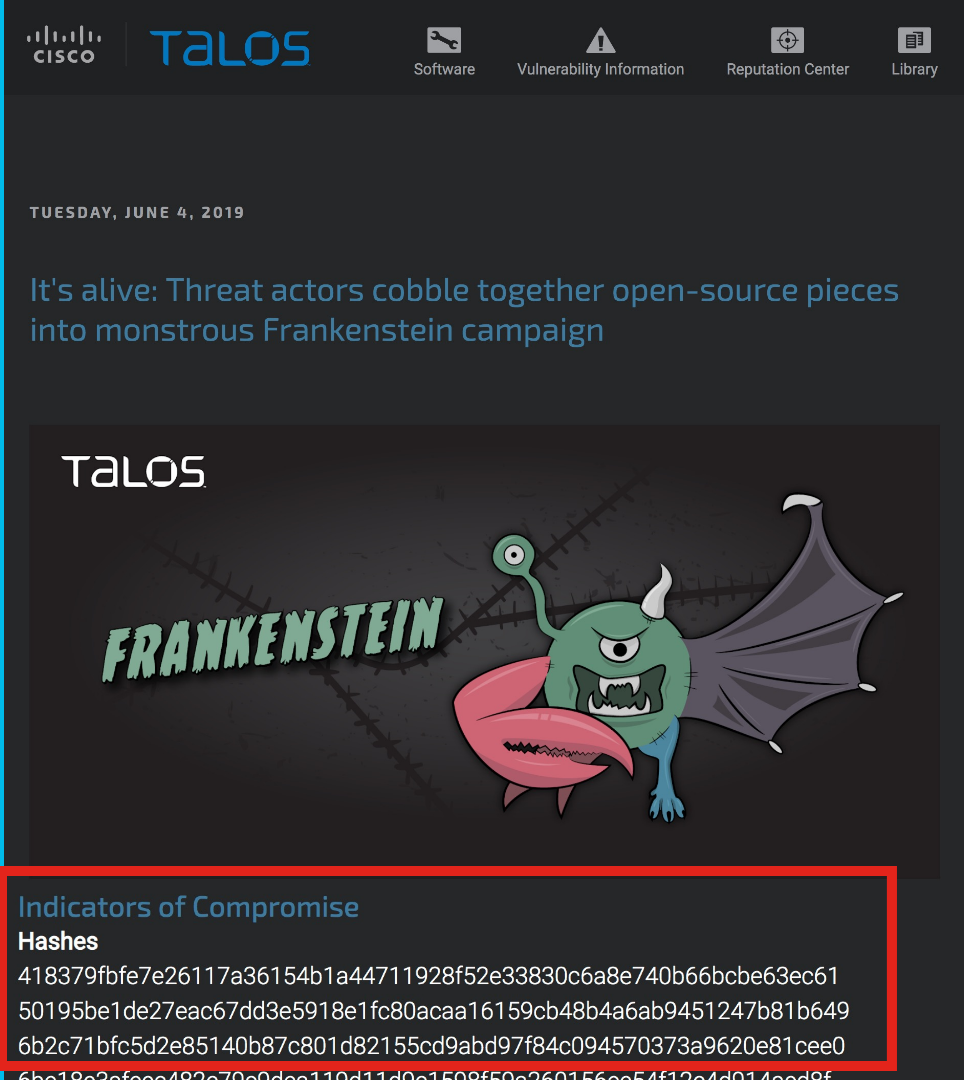
➢ **Use Case 2: Ingest (Talos) Blogs for Threat Intel**
  - **Overview**
  - **Demo**

- 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

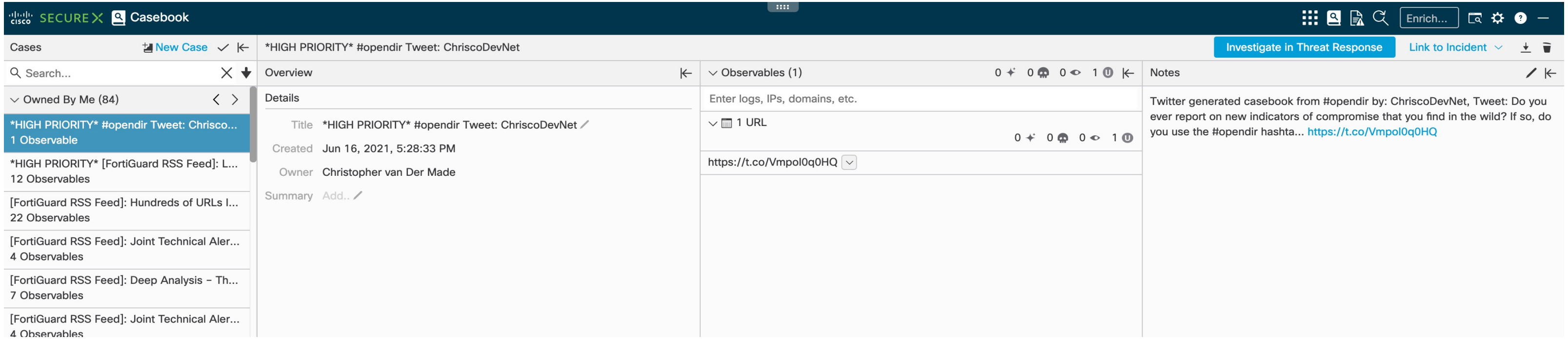
Agenda

- 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
  - Demo

➢ **Conclusion**

Conclusion

Is this easier than manually searching Twitter?



HIGH PRIORITY #opendir Tweet: ChriscoDevNet

Search...

Owned By Me (84)

HIGH PRIORITY #opendir Tweet: Chrisco...
1 Observable

HIGH PRIORITY [FortiGuard RSS Feed]: L...
12 Observables

[FortiGuard RSS Feed]: Hundreds of URLs I...
22 Observables

[FortiGuard RSS Feed]: Joint Technical Aler...
4 Observables

[FortiGuard RSS Feed]: Deep Analysis – Th...
7 Observables

[FortiGuard RSS Feed]: Joint Technical Aler...
4 Observables

Details

Title *HIGH PRIORITY* #opendir Tweet: ChriscoDevNet

Created Jun 16, 2021, 5:28:33 PM

Owner Christopher van Der Made

Summary Add..

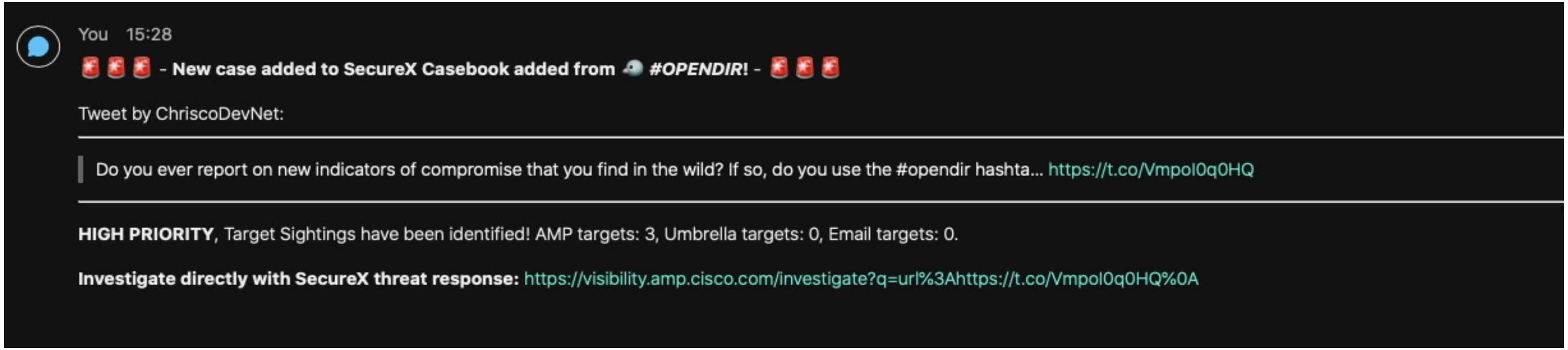
Observables (1)

Enter logs, IPs, domains, etc.

1 URL

https://t.co/Vmpol0q0HQ

Twitter generated casebook from #opendir by: ChriscoDevNet, Tweet: Do you ever report on new indicators of compromise that you find in the wild? If so, do you use the #opendir hashta... https://t.co/Vmpol0q0HQ



You 15:28

🚨 🚨 🚨 - **New case added to SecureX Casebook added from #OPENDIR!** - 🚨 🚨 🚨

Tweet by ChriscoDevNet:

> Do you ever report on new indicators of compromise that you find in the wild? If so, do you use the #opendir hashta... https://t.co/Vmpol0q0HQ

HIGH PRIORITY, Target Sightings have been identified! AMP targets: 3, Umbrella targets: 0, Email targets: 0.

Investigate directly with SecureX threat response: https://visibility.amp.cisco.com/investigate?q=url%3Ahttps://t.co/Vmpol0q0HQ%0A

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
  - Demo
- 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