



Maturing Your Threat Hunting Operations



Topics

- Guiding Principles of Threat Hunting
- Maturity Models
- Reactive vs Proactive Detection
- Building the Foundations
 - Detection
 - Intelligence
- Types of Hunts
- Use as many lego graphics as possible



C:\Whoami

Contoso\Andrew Skatoff

| @DFIR_TNT | <https://www.linkedin.com/in/amskatoff/> |

- Virginia-native... sorta
- Brilliant/Beautiful wife of 24 years
 - Aspiring Trauma-informed Urban Planner.
- 4 kids.
 - 3 love performing arts, one loves biology and crime documentaries. ??
- Notable employers:
 - Dominion, Cap1, and Federal Reserve
 - Currently managing a team of malware analysts and threat hunters (MATH) within an IRT.

To Threat Hunt...

Before we dig into methodologies, here a few things to keep in mind...



Threat Hunting is very young

Threat Hunting as a Cybersecurity Discipline was only recognized by NIST in 2020.



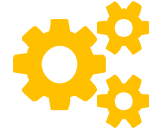
Threat Hunting is also very old

IT pros have been threat-hunting in some way since computers have been around.



Creative and Open Process

There are many ways to approach a hunt and analysts have freedom to pivot or change a hunt during the process.



Threat Driven

Threat Hunting should be driven by Threat Intelligence. This is not a risk assessment, or vulnerability scan. It is more akin to a "Breach Assessment."





Value Proposition

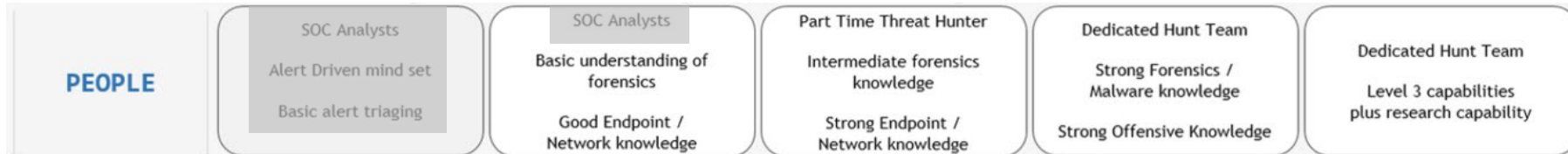
- Increased familiarity with and confidence in the security of customer systems.
- Optimize efficiency of rapid response to high priority threat intelligence.
- Accelerate development of security alert use-cases.

A Threat Hunting Maturity Model



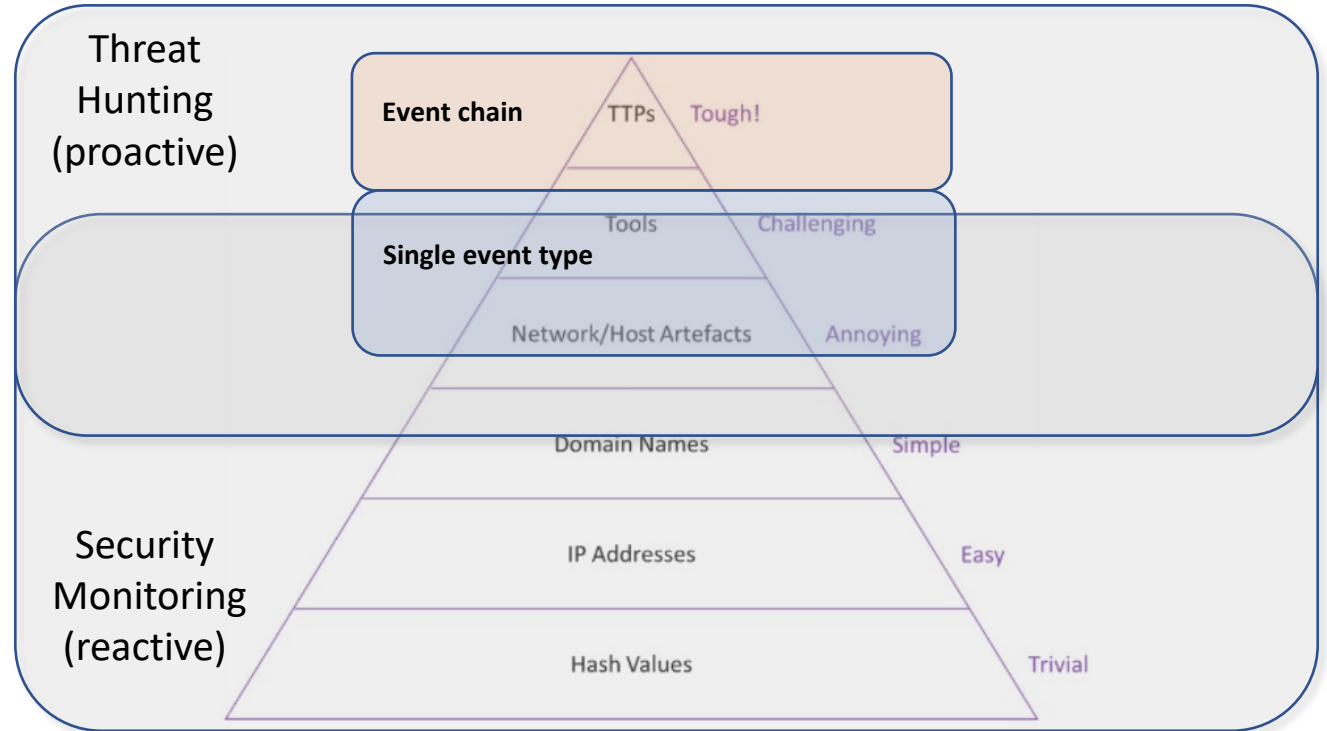
Threat Hunting Capability Maturity Model	Level 1 INITIAL	Level 2 MANAGED	Level 3 DEFINED	Level 4 QUANTITATIVELY MANAGED	Level 5 OPTIMISING
Process 	<ul style="list-style-type: none"> Hypothesis generation is unstructured <i>Hunts occur ad-hoc, if at all</i> <i>Little or no data collected</i> Little understanding of anomalies indicative of malicious activity Abnormalities not routinely searched for 	<ul style="list-style-type: none"> CTI and Domain Expertise used to generate hypotheses and prioritisation by lead Hunts occur occasionally <i>Moderate data collection from key areas</i> <i>Basic threat feeds with IOCs utilised</i> Targeting of IOCs at bottom of POP 	<ul style="list-style-type: none"> Formal hunting process Hunts occur regularly <i>High data collection from key areas</i> <i>CTI and previous experience used to detect malicious activity</i> Targeting of IOCs in middle of POP 	<ul style="list-style-type: none"> Manual risk scoring e.g. Crown Jewels Hunts occur frequently <i>Moderate data collection from most of estate</i> <i>CTI tailored to organisation</i> Targeting of IOCs at top of POP 	<ul style="list-style-type: none"> Automated risk scoring e.g. machine learning Hunts occur continuously <i>High data collection from full estate</i> Hunt analytics and IOCs shared across community Automated TTP and campaign tracking
Tools 	<ul style="list-style-type: none"> <i>Reactive SOC tools</i> Little or no automation Little or no documentation produced 	<ul style="list-style-type: none"> Basic searching via text or SQL-like queries <i>Automatic matching of IOCs</i> Documentation using basic office suites 	<ul style="list-style-type: none"> Statistical analysis techniques Library of hunt procedures automated on regular schedule Central workflow and knowledge repository tools Lab environments used to aid hypothesis generation and testing 	<ul style="list-style-type: none"> Visualisation tools utilised, and analytics tested for effectiveness Library of hunt procedures automated on frequent schedule Dashboards utilised 	<ul style="list-style-type: none"> Machine learning is leveraged, with horizon scanning maintained Library of hunt procedures automated continuously Central workflow and knowledge repository are integrated and shared

Note: Items in *italics* are not strictly part of a Threat Hunting capability, but are essential prerequisites and enablers.

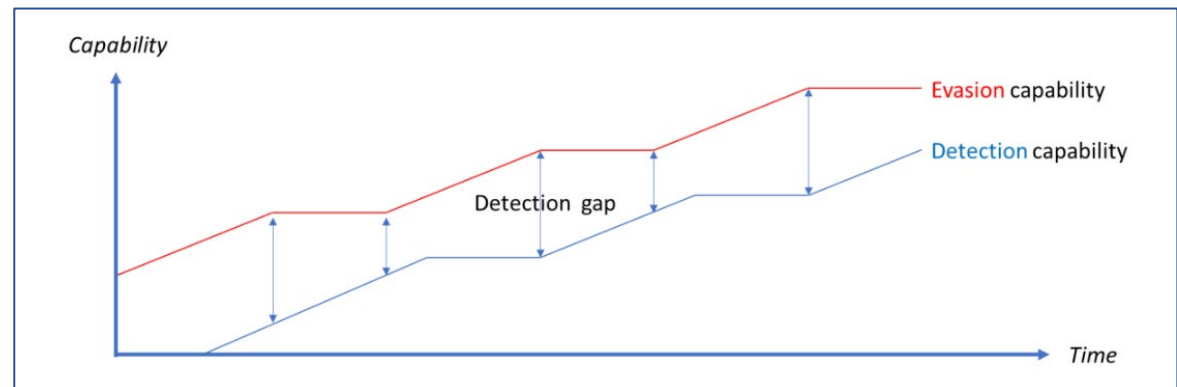


Reactive vs Proactive Detection

- All SOC alerts and incident response investigations can be considered a type of hunt but cannot tolerate high FP rates
- Threat Hunting services can tolerate a higher FP rate than SOC
- Efficiency is found in augmenting current detection content



A good threat hunting program aims to continuously reduce the breach detection gap between actors evading detection and detection upgrades



Cyber Threat Intelligence

Analytic tradecraft to transform disparate, raw information into actionable intelligence to support decision makers. Serves to:

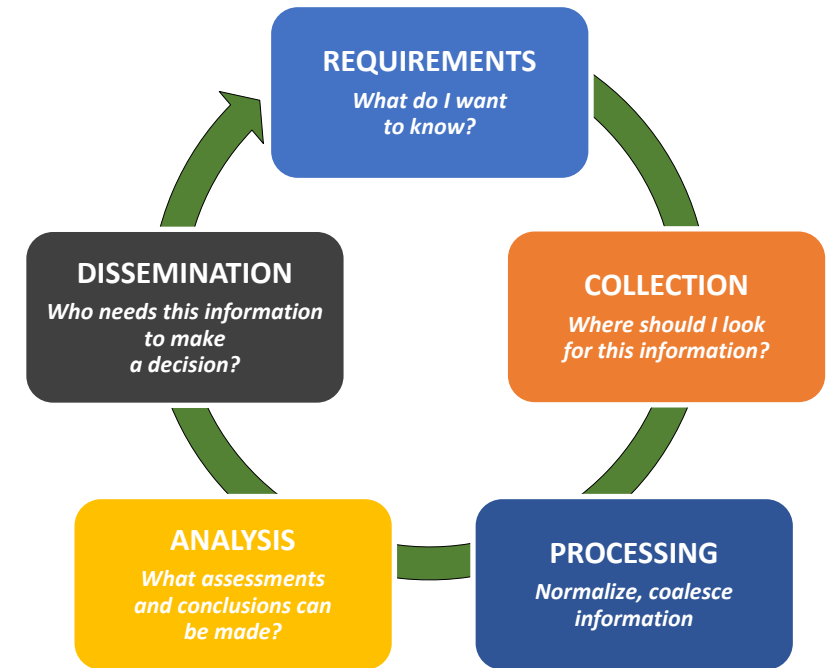
- Provide timely intelligence on relevant threats and vulnerabilities, highlighting threat actor capabilities, intent, targeting opportunities, and potential CVE exposures
- Help stakeholders make informed cyber risk decisions
- Help stakeholders determine possible mitigation activities

Current Intelligence timely and contextualized analysis of cyber threat events that are of immediate interest, could have broad impact on the cyber threat landscape, or could pose a risk to critical business functions,

Strategic Intelligence analysis to forecast future developments, predict adversary behavior, contextualize geopolitical events, and assist customers in making risk decisions, and

Tactical Intelligence extraction of indicators of compromise and TTPs from cyber intelligence on threat actors, campaigns, malware, and vulnerabilities to support stakeholders, drive operations, and help stakeholders build robust detection capabilities

...is provided to designated stakeholders through a variety of products and channels.



Prioritizing Threat Actors – Capability / Motivation

Determining Capability

- The Capability metric consists of determining the TA's technical **skills**, tooling skills, **organization**, and **recent activity**. These criteria, when combined, are given a weighted value of 60 .
- Use weighted scoring to better prioritize criteria used in ranking TAs. The Capability score is then standardized to be on a scale of 0-10.

Determining Motivation

- The goal of the Motivation metric is to explain the TA's underlying **reasons** for its behavior.
- To determine a TA's Motivation score, each actor is given **intent, industry, region, and historical targeting** scores, which are then added together and given a weighted value of 40 .
- The Motivation score is then standardized to be on a scale of 0-10.



Prioritizing Threat Actors

- <https://www.passagetechology.com/what-is-the-analytic-hierarchy-process>



Criteria	Weight	Slippery Pete	Cocaine Bear
Technical Capability (0-5)	35%	3.5	5.0
Tooling (0-3)	20%	1.0	3.0
Organization (0-1)	2.5%	1.0	1.0
Half-Life (0-1)	2.5%	1.0	1.0
Motivation (0-20.2)	40%	7.2	12.2
Cap= 60%, Mot=40%	100%	4.36	7.28
Standardized Score	Weight	Slippery Pete	Cocaine Bear
Technical Capability	35%	7.00	10.00
Tooling	20%	3.33	10.00
Organization	2.5%	10.00	10.00
Half-Life	2.5%	10.00	10.00
Motivation	40%	3.56	6.04
Total	100%	5.04	8.42

Detection Fundamentals: Endpoint

- Command Line Auditing is a MUST!
 - Security log EventCode 4688 – requires GPO settings to capture
 - EDR | Sysmon
- EventLogs (SANS Know Normal, Find Evil)
 - Security.evtx
 - Application.evtx
 - System.evtx
 - WinRM-Operational.evtx
 - PowerShell Admin.evtx
 - PowerShell Operational.evtx
 - Microsoft-WindowsTerminalServicesRDPClient Operational.evtx
 - Task Scheduler Maintenance.evtx
 - TaskScheduler Operational.evtx
 - Microsoft-WindowsSmbClient Security.evtx
 - TerminalServices-LocalSessionManager Operational.evtx
 - Bits-Client Operational.evtx
 - Application-Experience Program-Telemetry.evtx
- Some critical configs for full visibility:
 - <https://www.malwarearchaeology.com/cheat-sheets>
 - [The Windows Sysmon Logging Cheat Sheet](#)
 - [The Windows Advanced Logging Cheat Sheet](#)
- Centralized Logs are a MUST!

Category	Source	Comments
Command Line of Process Execution	Sysmon.evtx	EventCode=1
	Security.evtx	EventCode=4688
EDR	*	*



Risk Event Aggregations

Risk Events Overview

Allows our detection to identify unusual, suspicious, malicious activity at a much more **granular, risk-centric level**.

Mechanics

Emphasize **small, discrete, flexible events** of interest aggregated for analysis & correlation. Allows for detection of individual events and more subtle patterns of activity. Allows team to leverage the power of all our security monitoring in one escalation.

Dynamic Risk Scoring

A system for dynamic risk scoring for critical assets. The risk of the particular activity is appropriately adjusted to account for the **increased criticality** of the asset.

Testing

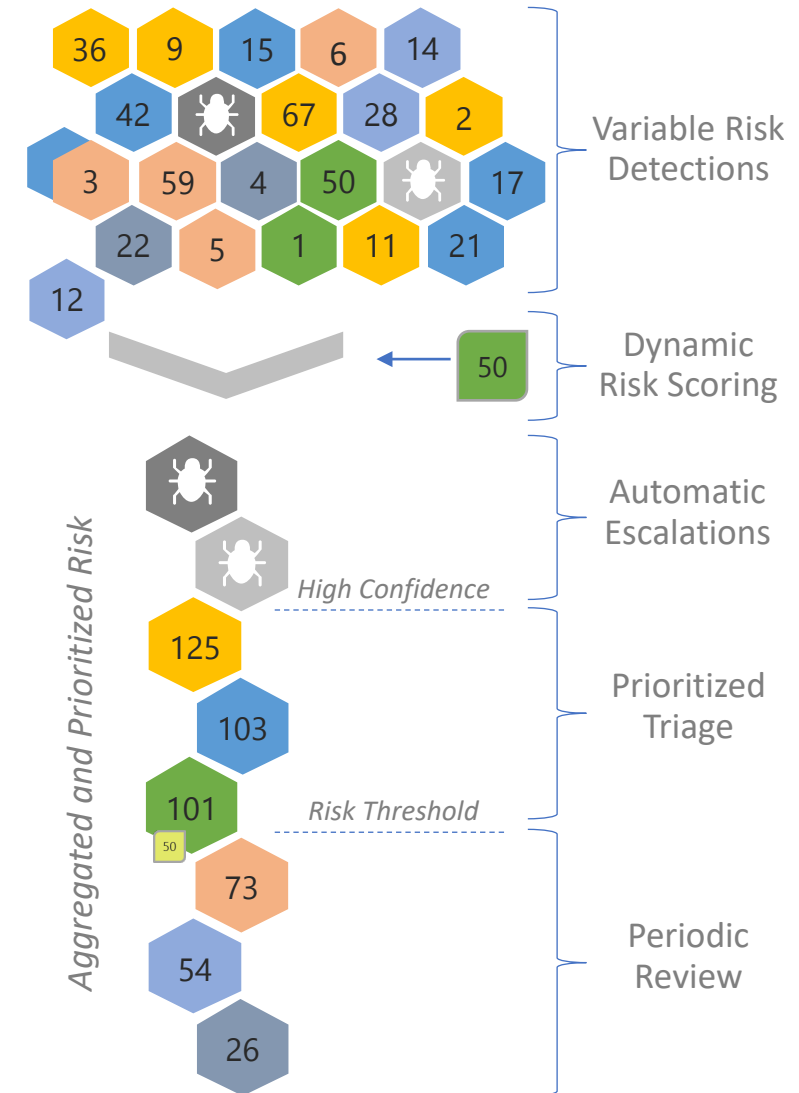
Manual and automated test events that replicate real-world cyber attacks to **ensure effective detection**

Threat Driven

Utilizes the risk scoring methodology to help bring noteworthy activity to an analyst's attention more quickly and with greater clarity. The new platform uses **dynamic risk scoring and aggregation** to correlate events across larger timeframes to allow for streamlined detection.

Streamlined Detection

- The analyst can see **case related data in aggregate** with other notable events and **easily pivot** to investigation dashboards with a click.
- The analyst can aggregate risk by entity over different time frames; three days is currently standard facilitating case analysis.
- Comprehensive documentation is only required on escalation, **reducing analyst fatigue**.



Four Operational Modes

Recurring Hunts

Low fidelity hunts looking for TTPs and IOCs within any for specific actors, campaigns, or tailored to specific High Value assets/users. Examples:

- LOLBins/LOLBAS
- Difficult to collect in real time
 - (e.g. CISA Azure hunts, Zoom abuse)
- Notables under alert threshold

Outputs:

- Findings/Incidents
- - Detection Engineering Recommendations

Customer Engagements

Short term, focused engagements in specific customer technology stack using both TTPs and IOCs from intel reports.

Outputs:

- Tailored Intel Report
- Formal Hunt Report
- Detection Engineering Recommendations

Micro-Hunts

Small, point-in-time hunts in telemetry and tools, based on a specific **TTPs** or events. Prioritized by Threat Intelligence

Outputs:

- Findings/Incidents
- - Detection Engineering Recommendations
- Recurring Hunt

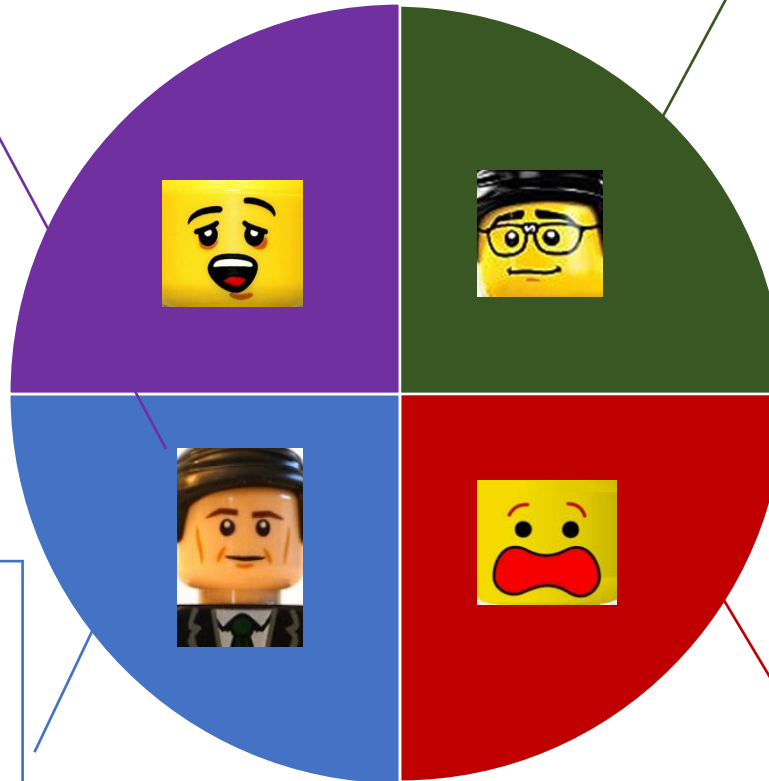
Priority Incident Response Hunts

Hunts begun by priority threats.

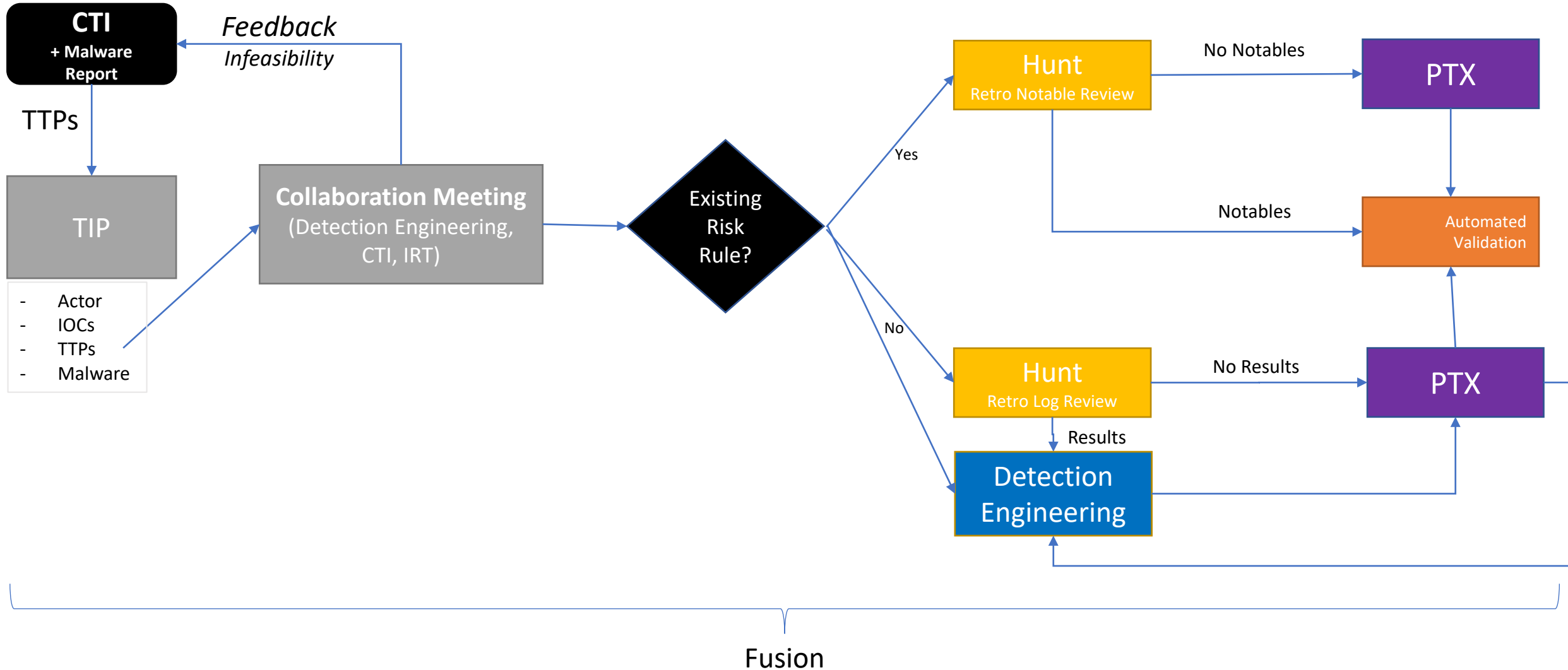
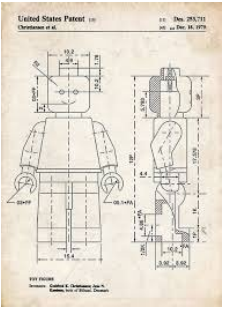
- Incidents or exposed vulnerabilities conducted until mitigations are in place
- Latest OSINT IOC retro hunts (not covered by alerts)

Outputs:

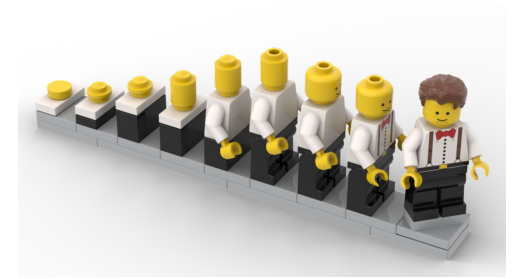
- Incident Case updates
- Heightened Monitoring / - Detection Engineering



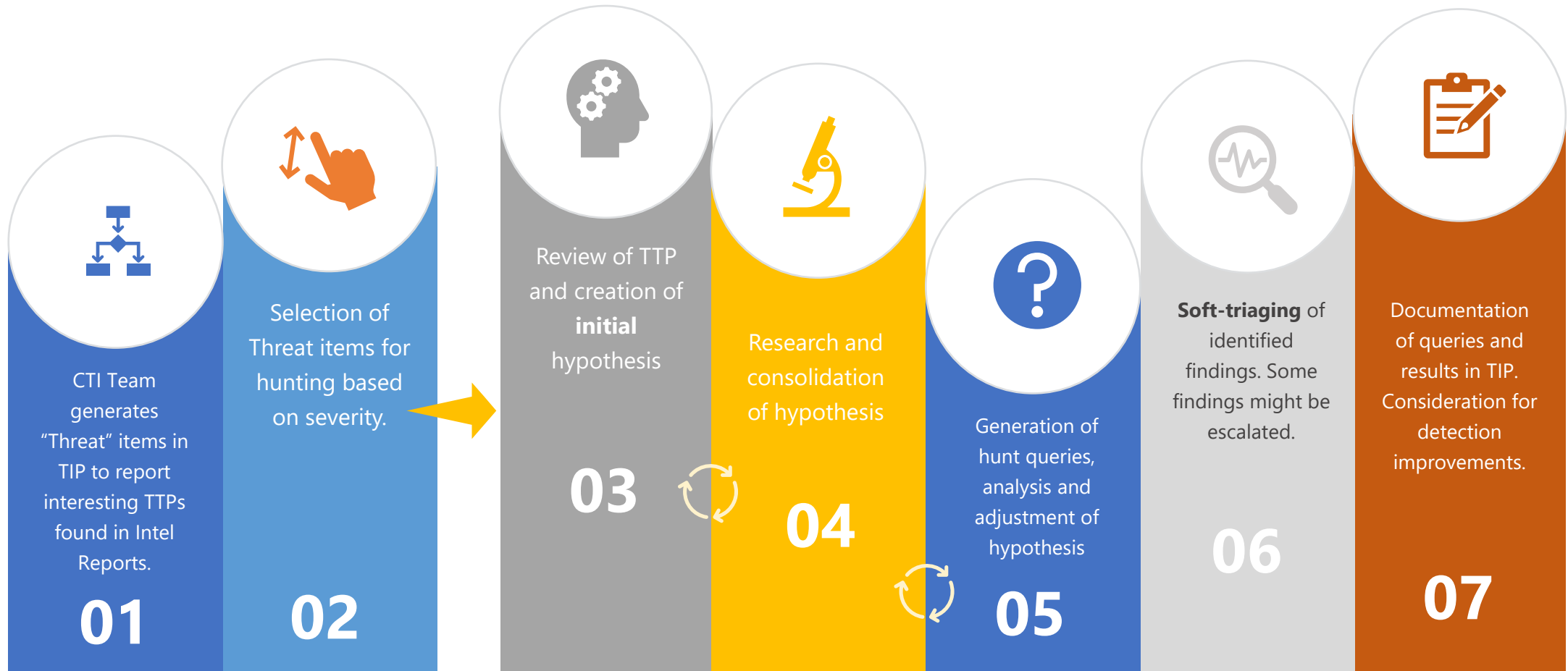
Pipeline for Integrated TTP Processing



MicroHunt - Timeline



Overview of the MicroHunting process





Review of
TTP and
creation of
initial
hypothesis

1

Review of TTP and contextualization within intel report

Falcon OverWatch and Falcon Complete detected an Emotet campaign featuring **slightly altered Tactics, Techniques, and Procedures (TTPs)**. Rather than using regsvr32.exe, XLS documents used in this wave contained macro code to write an embedded batch script to C:\programdata\hfwiue.bat and to execute it. This obfuscated script runs an encoded PScommand. This command downloads a randomly named Emotet DLL from several URLs to C:\ProgramData and runs the DLL using rundll32.exe



2

Outline TTP by 7 propositions

- XLS documents used in this wave contained
- macro code
- to write an embedded batch script to C:\programdata\hfwiue.bat
- and to execute it.
- This obfuscated script runs an encoded PScommand.
- This command downloads a randomly named Emotet DLL from several URLs to C:\ProgramData
- and runs the DLL using rundll32.exe
-

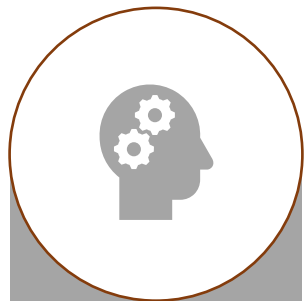


Review of
TTP and
selection of
initial
hypothesis



3 Contextualize original propositions to turn them into potential hunt ideas

- XLS documents used in this wave contained
 - macro code
 - to write an embedded batch script to C:\programdata\hfwiue.bat
 - (*) Excel Process Writing BATCH files
 - and to execute it.
 - (*) Excel Process Executing BATCH files ← ?
 - This obfuscated script runs an encoded PScommand.
 - (*) Excel Process spawning encoded PowerShell
 - This command downloads a randomly named Emotet DLL from several URLs to C:\ProgramData
 - (*) Encoded PowerShell referencing a DLL or a URL
 - and runs the DLL using rundll32.exe
 - (*) PowerShell spawning rundll32 to run a DLL out of ProgramData



Review of
TTP and
selection of
initial
hypothesis

4 Create initial hypothesis

(*) Excel Process Executing BATCH files



*When a malicious Excel document containing macros is opened, and that macro executes a batch file, **if** the parent-child relationship between the original Excel process and the process executing the Batch file is maintained, this activity should be visible in existing telemetry and serve as an indicator of attack.*



Find available evidence to consolidate our hypothesis:

- Use evidence from original report (i.e., detailed process tree
- Test hypothesis in a lab.
- Research the technique (google, twitter, sigma, atomic red t etc.).
- **Leverage available Sandbox reports on samples.**



Review report for IOCs

1

CSA-211073 Mass Phishing Campaigns Leverage Excel 4.0 Macro Documents to De... 3 / 7 | - 200% + | [] []

Indicators of Compromise (IOCs)

Table 1 provides only exemplar macro document IOCs, due to the vast scale of these recent campaigns.

TYPE	VALUE
<i>Emotet dropper documents SH</i>	c359d936b4b3c78a7b9c5366125e7f0870730da24c125335bdf8607b0b0f1499
A256 hashes	11797c2c41ae6f5f3284cc50d6bec9cb9abfec5c9fd11c99a0325a813eaec5ce

Check for sample availability on VT

2

11797c2c41ae6f5f3284cc50d6bec9cb9abfec5c9fd11c99a0325a813eaec5ce Help

32 / 59

32 security vendors and 3 sandboxes flagged this file as malicious

11797c2c41ae6f5f3284cc50d6bec9cb9abfec5c9fd11c99a0325a813eaec5ce 180.00 KB 2021-12-06
informe 01122021.xls Size 1 year ago

xls open-file enum-windows macros runtime-modules detect-debug-environment macro-run-file run-dll calls-wmi direct-cpu-clock-access

Community Score

Research and consolidation of hypothesis



Research and consolidation of hypothesis

3

Review Sandbox reports for process execution evidence

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	TELEMETRY	COMMUNITY	
<input type="checkbox"/>	Display grouped sandbox reports						
<input type="checkbox"/>	BitDam ATP	▲ 1	▲ 0	▲ 0	▲ 0	▲ 0	<input type="checkbox"/> C2AE
<input type="checkbox"/>	VMRay	▲ 0	▲ 0	▲ 0	▲ 5	▲ 12	<input type="checkbox"/> VenusEye Sandbox
<input checked="" type="checkbox"/>	VirusTotal Jujubox	▲ 0	▲ 0	▲ 0	▲ 1	▲ 0	<input type="checkbox"/> Zenbox



Process Tree of sample confirms hypothesis

4

Activity Summary Download Artifacts Full Reports

Processes Tree

- 1556 - EXCEL.EXE
 - ↳ 2552 - c:\programdata\hfwuie.bat
 - ↳ 432 - powershell -enc JABzAHQAcbgBzAD0AlgBoAHQAdABwADoALwAvAGUAdgBIAHIAaQBzAHkAbwB1AGcAbABvAGIAYQBzAC4AZQB2AGUAcgBpAHMALgBj



Generation
of hunt
queries,
analysis and
adjustment
of hypothesis

1 Identify source telemetry (i.e., Sysmon Event Code 1)

2 Start with broad string searches. This allows us to become familiar with the events/fields we are querying

New Search

```
eventtype="*.sysmon" EventCode=1 Excel AND .bat
```

i	Time	Event
>	4/27/23 12:46:32.000 PM	04/27/2023 11:46:32 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName= User=SYSTEM Sid=S-1-5-18 OriginalFileName: Excel.exe CommandLine: "C:\Program Files\Microsoft Office\Office16\EXCEL.EXE" "C:\Data Analytics Unit\Tool.xlsx" "C:\Data Analytics Unit\Tool.xlsx" CurrentDirectory: O:\Data Analytics Unit\ User: LogonGuid: {995e8158-079e-6449-5adc-2d0000000000} LogonId: 0x2DDC5A TerminalSessionId: 1 IntegrityLevel: Medium Hashes: SHA256=6CF57443D25C25832783AEE5607229C500B320C80EE27972F88E7AF7BFC74D24 ParentProcessGuid: {995e8158-a6e2-644a-abb4-00000000f300} ParentProcessId: 12744 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: C:\WINDOWS\system32\cmd.exe /c ""O:\Data Analytics Unit\Tool.bat" "



Use additional telemetry to investigate and contextualize the results found during our hunt. In this case we use a Sysmon Splunk dashboard to review the process execution chain.



Soft-triangling of identified findings. Some findings might be escalated.

Process Drilldown
C:\WINDOWS\system32\cmd.exe /c \[REDACTED].ORG\C1\ [REDACTED]\Template\run.bat
SHA256 of Cmd.Exe : "B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450"

Process Tree:
explorer.exe → EXCEL.EXE → Cmd.Exe (This Process)

Parent/GrandParent Information					Child Process Started by "Cmd.Exe"		
ParentExecutable	ParentMD5	ParentCommand	GrandParentCommand	ProcessId	_time	Executable	CommandLine
Excel.exe	8FB5778DFC640345C855DB33A494337D	"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "H:\Template\Test R.xlsm"	C:\WINDOWS\Explorer.EXE	21544	2022-11-15 10:56:55	-	"C:\Program Files\RR-4.2.0\bin\x64\Rscript" "\\ [REDACTED]\Templates\emBSAutomation\myscript.R" "H:\Template\"

In this case, the result we chose for review didn't match original TTP, yet it is still an interesting lead an analyst might chose to follow. Below are some potential follow-on activities a hunt analyst might perform:

- Further review of process execution chain
- Review activity by each process involved in the chain
- Search activity across time to determine frequency of use or uniqueness.
- Retrieve the files related to the activity from the device for further review.



Documentation of queries and results in TIP.

Consideration for detection improvements.

Attributes

Additional Analysis and Context

None

HuntLogic

Concept: Expanded search for potential BITS downloads from external HTTP sources using concepts by Atomic Red Team.

R2D2: Add Start-BitsTransfer as a keyword for lower scored PS use cases.

(120 days - 9 hits. All false positives found on PowerShell scripts and not related to BITS being leveraged for downloads)

```
eventtype=crowdstrike_json tag=frs (((bitsadmin OR bitsadmin.exe) AND http AND (transfer OR Download OR addfile)) OR (Start-BitsTransfer AND http)) OR ((desktopimgdownldr OR desktopimgdownldr.exe) AND http)
```

```
"| table _time aid event_simpleName _raw  
"| sort _time
```

Playbook Action

Run Name

NIRT Co

Baton Status: Completed

PTX Accept

Add TTP Feedback

Hunt Status: R2D2

Update Hunt Status

- NotStarted
- Accepted
- InProgress
- Complete
- Infeasible
- Rejected
- R3
- R2D2**

05-18-2021

NIRT > Monitoring Content > BATON > Issues

Open 0 Closed 1 All 1

<https://atconnect.com/auth/threat/threat.xhtml?threat=291751>

BITS jobs - CSA-210048 CARBON SPIDER Uses KillACK, P

#434 · created 3 months ago by TC Playbook BATON

ATT&CK - Defense Evasion ATT&CK - Execution ATT&CK - Persistence Hunt Modify_Rule



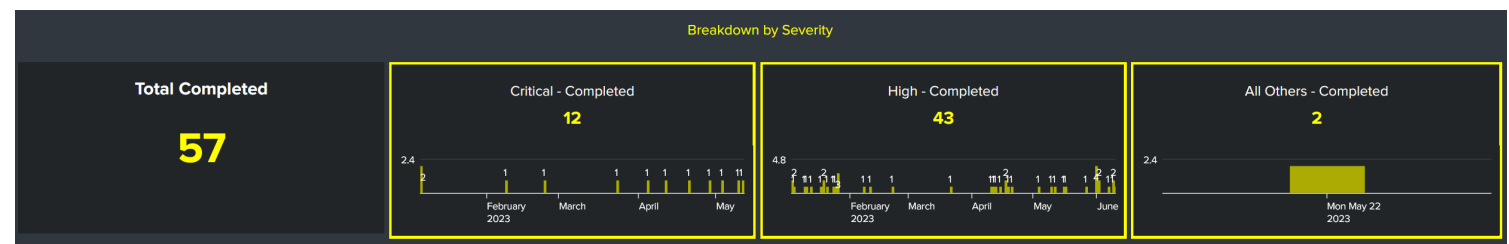
KPIs

How do we know if we are doing a good job?



- Volume Metrics
 - How many hunts completed by severity? Each type.
 - How many detection rules recommended?
 - New and Modified
 - How many escalations?
- Velocity Metrics
 - Time between start and finish

MicroHunts BackLog			
(Click the Totals Under each Severity Levels for Drilldown)			
Total Accepted	Critical - Accepted	High - Accepted	All Others - Accepted
39	2	17	20
Total InProgress	Critical - InProgress	High - InProgress	All Others - InProgress
23	1	20	2
Total NotStarted	Critical - NotStarted	High - NotStarted	All Others - NotStarted
423	0	287	133



Any
Questions?



Sources

- <https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf>
- <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/Cyber%20Threat%20Hunting%20Workshop%20-%20ITU%2019112020.pdf>
- <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf>
- <https://www.passagetechology.com/what-is-the-analytic-hierarchy-process>
- <https://www.malwarearchaeology.com/cheat-sheets>