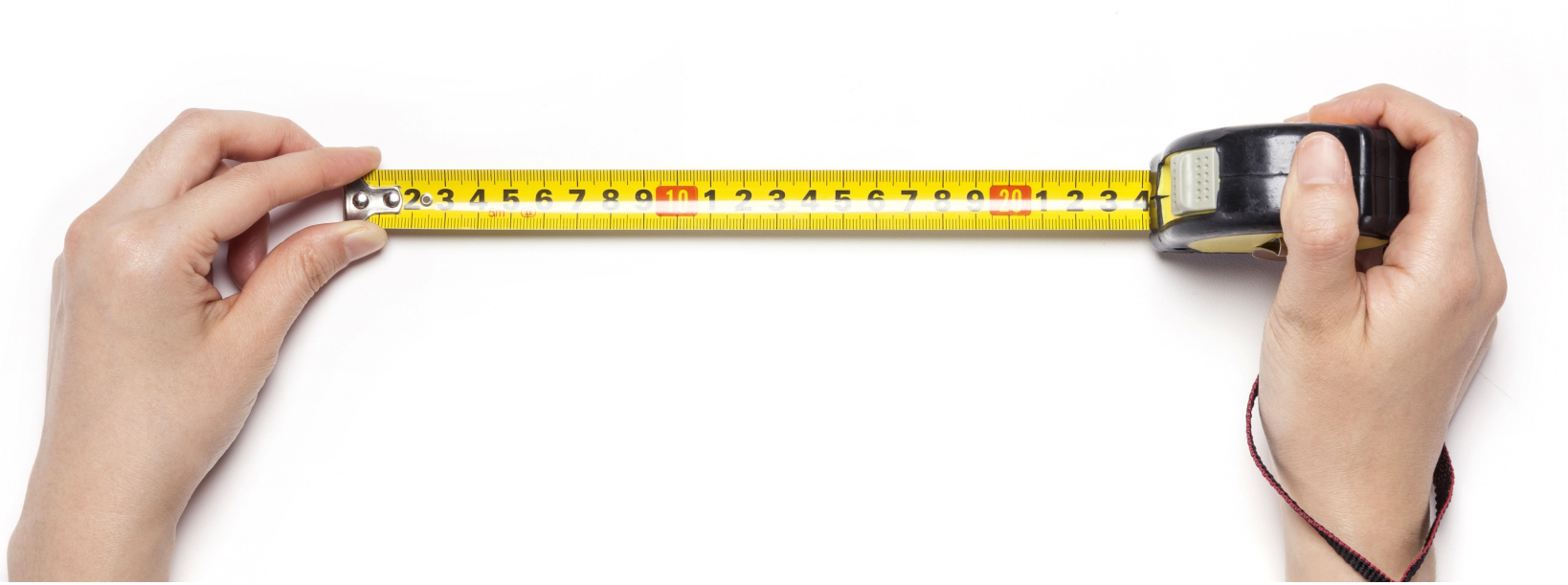


Objectively Measuring Hunt Value

Patrick Perry
Justin Kohler

Agenda

- Us
- The Problem
- The Basics
- The Solution
- The Reports
- And you can too!

Justin Kohler

Sr. Director of Customer Success at ~~ICEBRG~~ Gigamon Insight

I like process and data

USAF vet, MBA + security certs

Patrick Perry

Justin is my boss

Technical Account Manager at ~~ICEBRG~~ Gigamon

Former Special Agent at DHS, GE-CIRT, Systems Engineer at Mandiant

Current computing interest is in analytics

Brad Stevens is the meaning in my life

Disclaimer

This **IS NOT** how-to / why you should conduct Threat Hunting

Process talk on capturing, measuring, and reporting value

Threat Hunting Context

- No defined industry standard
- Retrospective detection
- Human directed
- Begins with a question
- Pivot
- Iterate

Our Favorite Definition

“Threat hunting is the human-driven, proactive and iterative search through networks, endpoints, or datasets in order to detect malicious, suspicious, or risky activities that have evaded detection by existing automated tools.”

-Sqrrl (https://sqrrl.com/media/ebook-web.pdf)

The Problem

(what we saw)

Tons of great content on hunting

- Why threat hunting is important
- How:
  - Hypothesis formation
  - Example hunts
  - Data quality measurements
- Webinars: “Practical threat hunting in <vendor tool>!”

The excitement builds

We have our best people on this

We've got all the tools

We're ready to start our hypothesis

Let's find evil!

This baby can fit so many APTs

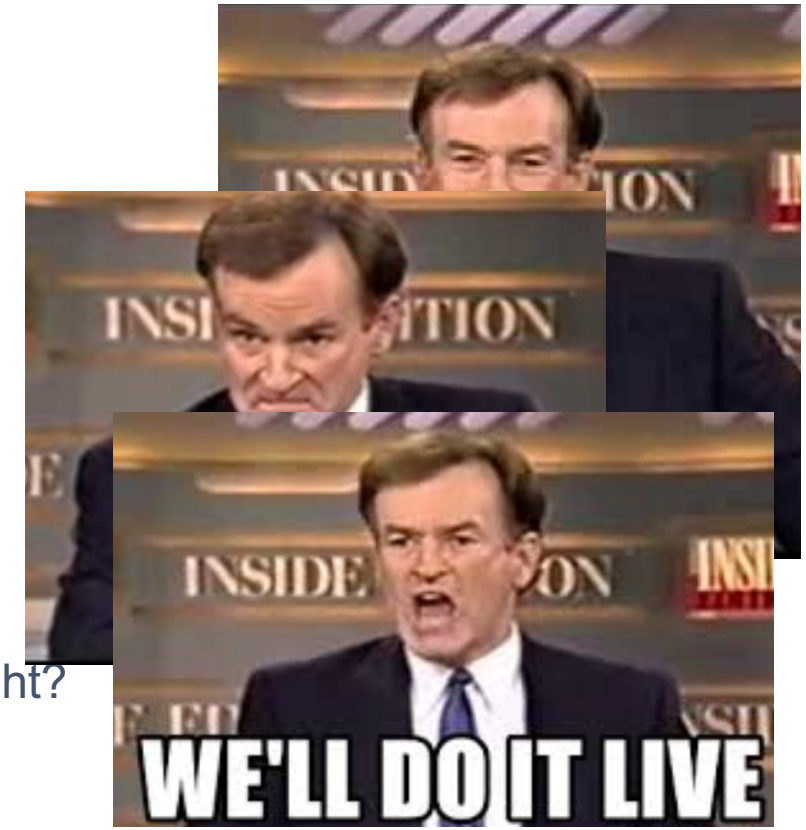
Your Hunt Program

We’re going hunting!

Great….but

- *How are we measuring success?*
- *Does management understand this?*
- *Metrics?*
- *Collecting those in what? Excel?*
- *Long term plan?*

….. Eh, whatever… we’re catching evil right?



Missing logs

“He has local admin!?”

Unpatched systems

Misconfigured systems

“How was that installed?”

Aaaaand, we’re done.
95% of the time….

Shadow IT

“*Is he really using DA creds to login?”*

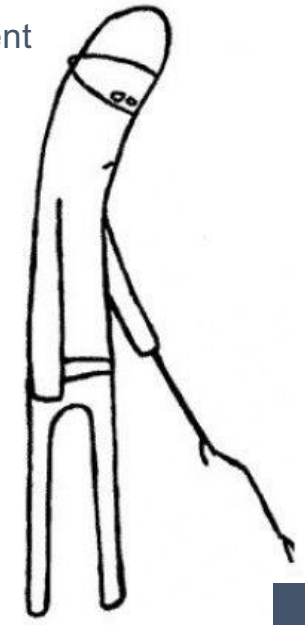
“*What is that partner doing?”*

“We use how many DNS servers?”

Ok... and some evil

Some time later…

Management



Your Hunt Program

“Did you catch them yet?”

“Our lead analyst is doing what again?”

“Since they don’t seem busy, [random task]?”

“Is this really adding value?”

Can you blame them?

….Maybe

This is the target you set

"…detect malicious, suspicious, or risky activities that have evaded detection…"

So let's make our target bigger

The Basics

Let's agree on some terms

Oversimplified view

Define it

Find it

….it

Hunting Hypothesis

The bulk of the work (3+ days)

Starts at MITRE ATT&CK Tactics Techniques and Procedures (TTPs)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public Facing Application	CMSTP	Accessibility Features	Accessibility Features			Application	Application			Communication
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs							
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs							
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming							

Tactics

Technique

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Drive-by Compromise

Technique

ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known

Procedure

Hunting Hypothesis

SpecterOp's five step process:

- Tactic and Technique
- Procedure
- Collection Requirements
- Scope
- Excluded Factors

Hunting Activity

Execute the work (1-2 days)

May inform original hypothesis

Typically ends in one of three ways

- Malicious activity found
- Non-malicious activity found
- Nothing found

Hunting Outcome

< 2 hours to document

Reference the chosen framework

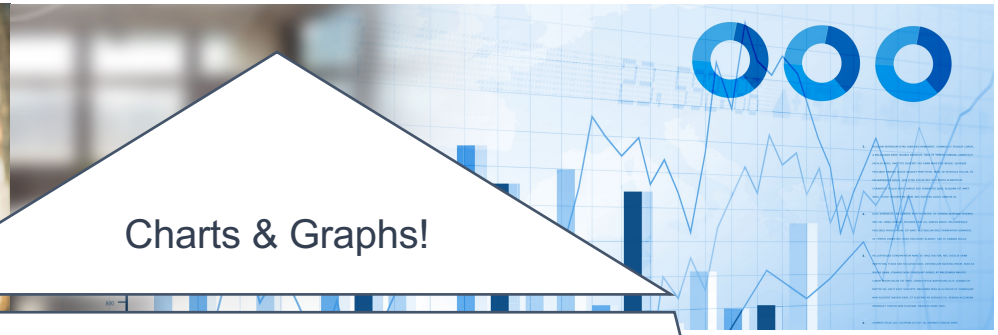
Example outcome types:

- Incident created
- Detection / analytic created
- Vulnerability identified
- Logging gap identified
- Insecure practice identified

The Solution

Or at least our solution

Components

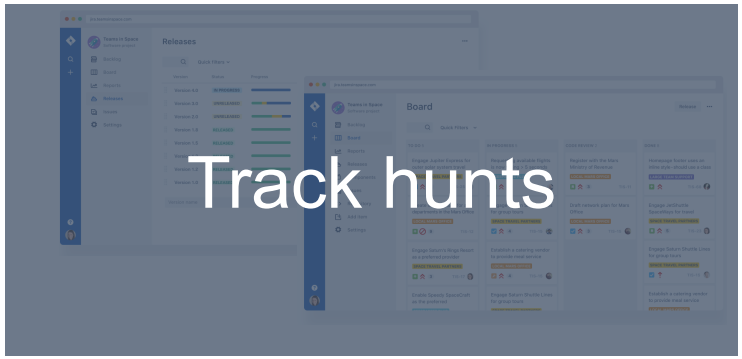


Charts & Graphs!

# logging gaps # Dets created	Business relevant Metrics	# active hunts # of incidents
MITRE ATT&CK™ Adversarial Tactics, Techniques & Common Knowledge	Industry Standard Frameworks	CIS Critical Security Controls
Confluence	Defined Processes	JIRA

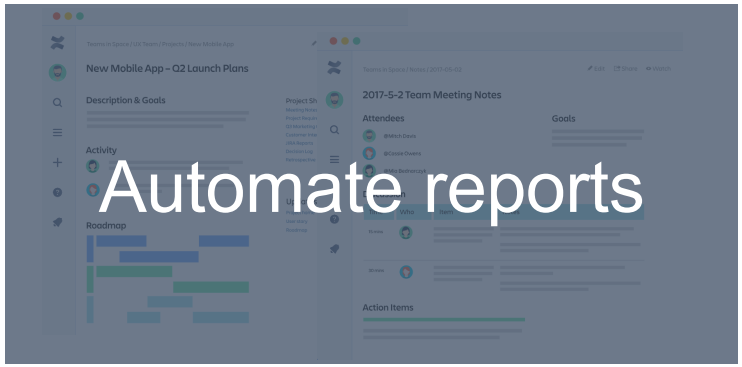
JIRA

Plan / track / report on projects



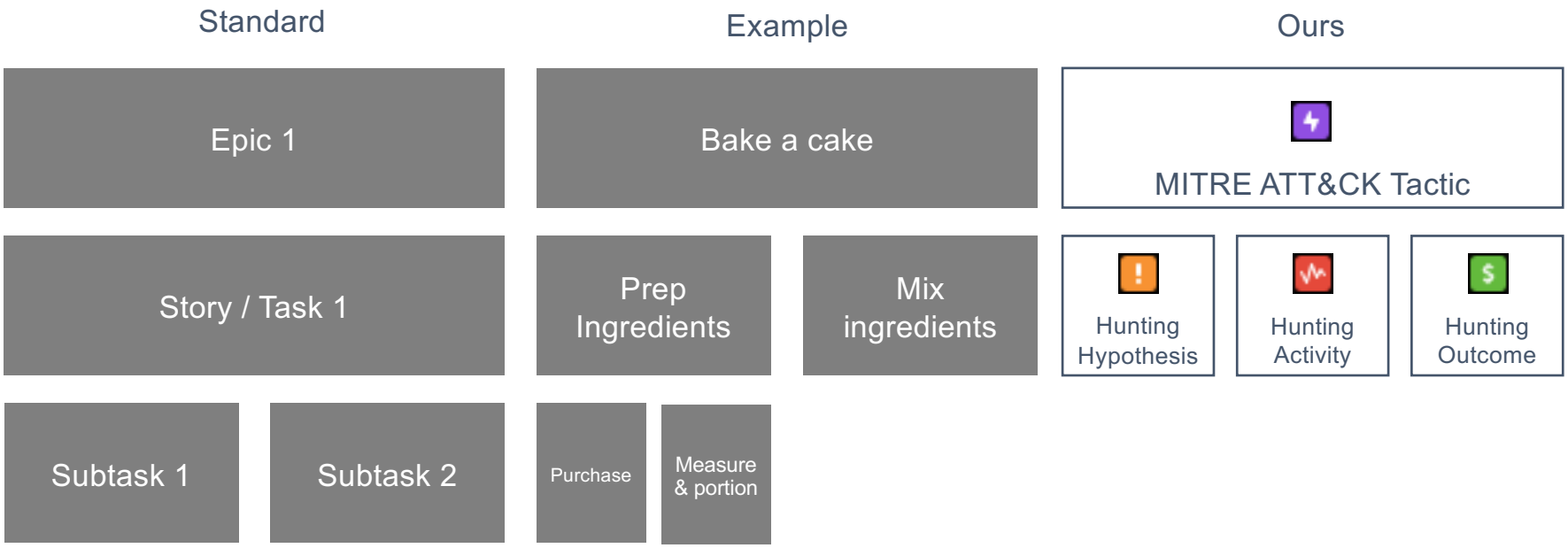
Confluence

Knowledge base

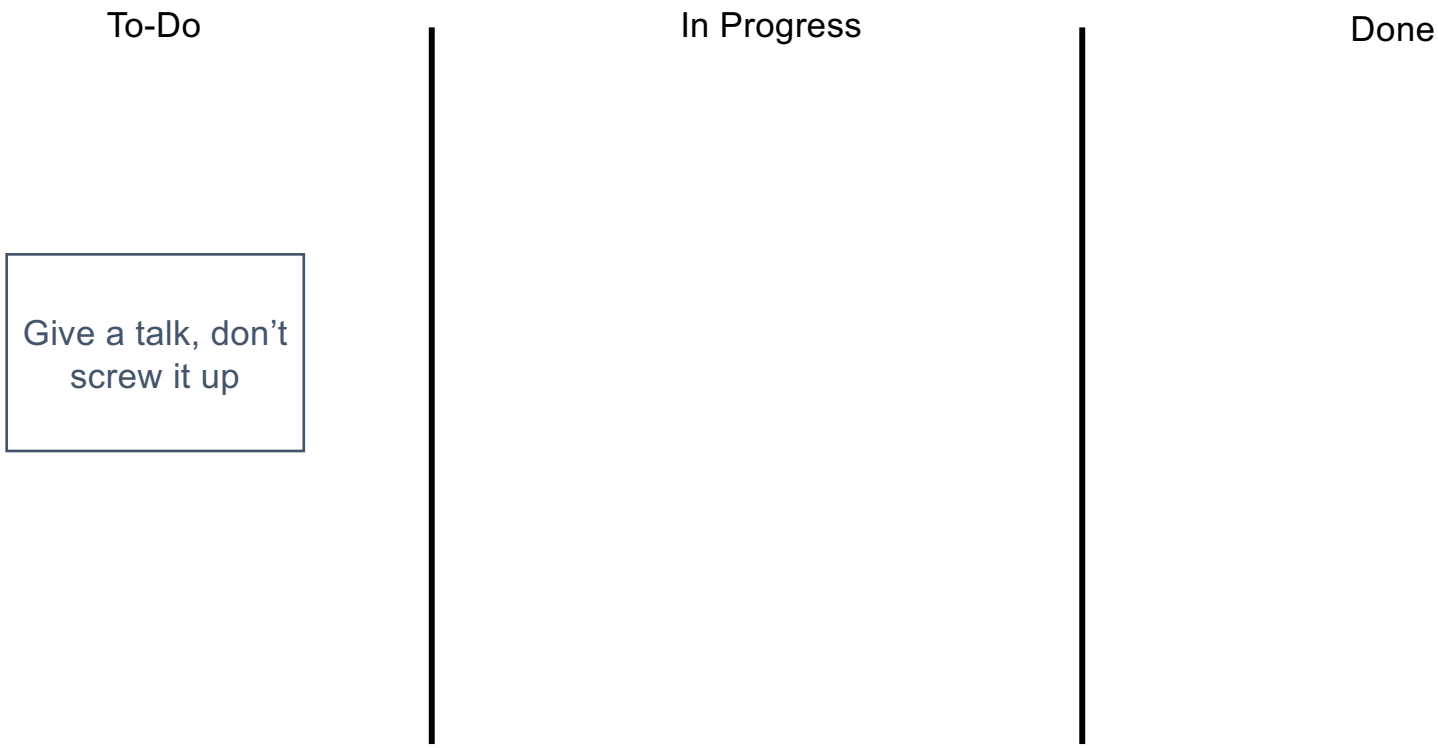


$20 for up to 10 users
Very powerful
Can be supremely frustrating

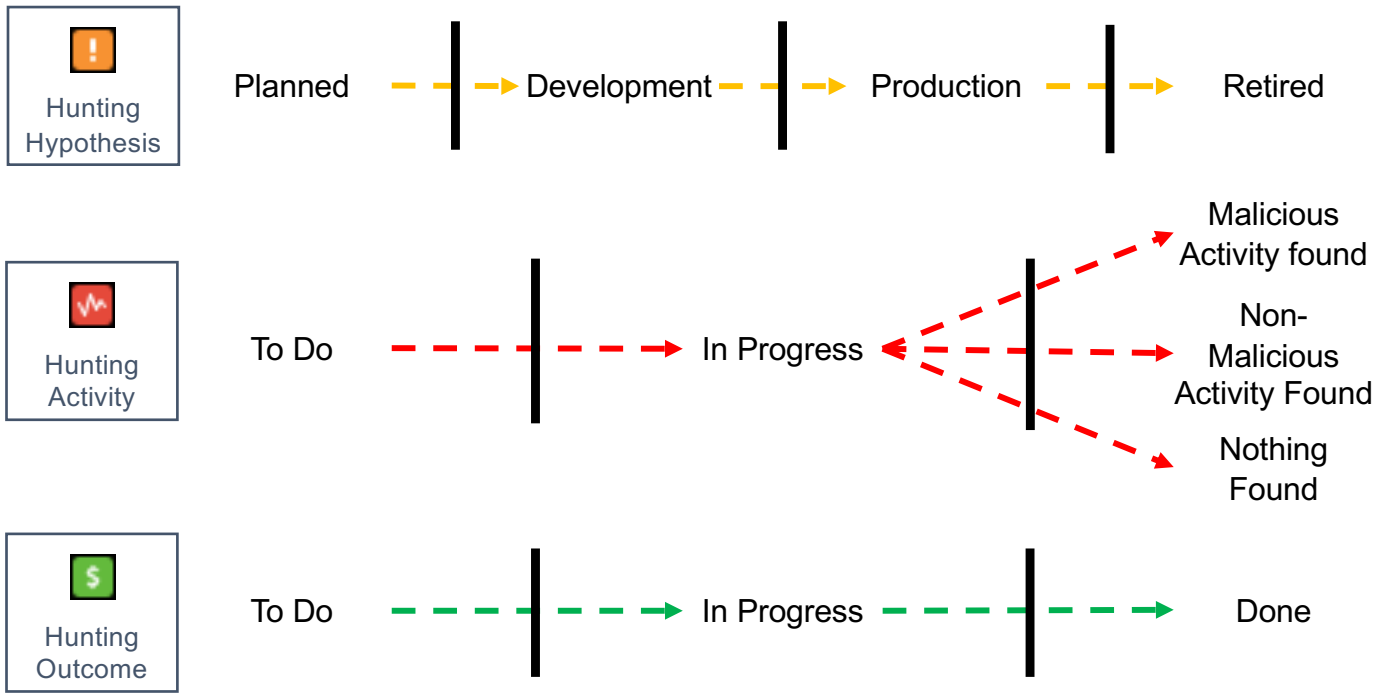
JIRA issue types



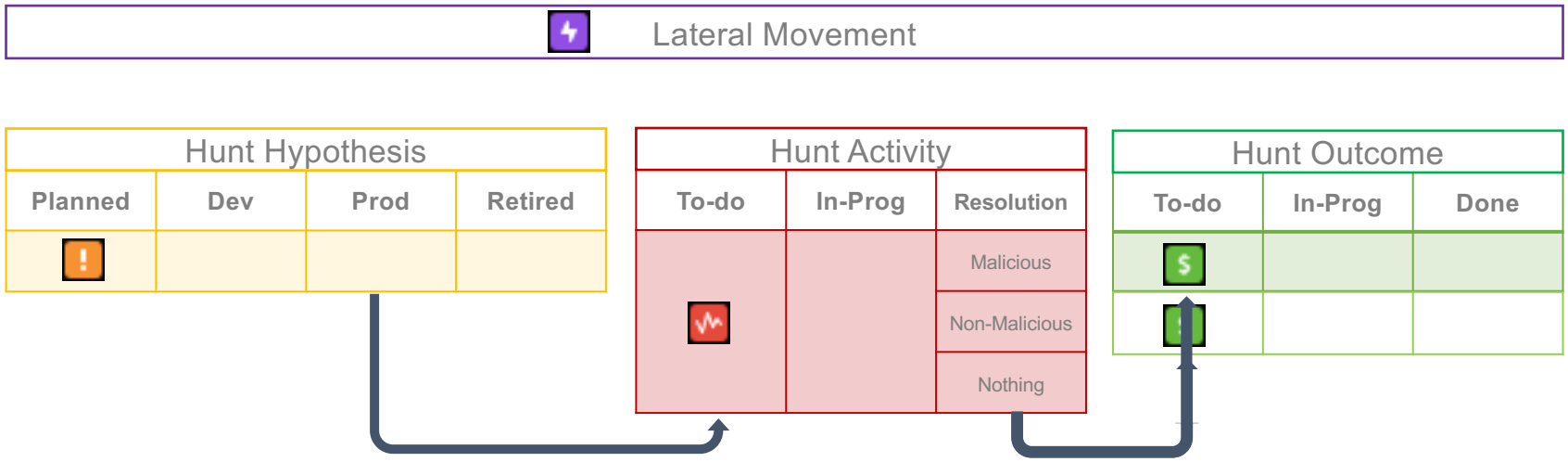
JIRA standard issue states



Our Issue States



All together now



Title/Technique: Remote Desktop Protocol (RDP)
Procedure: Analyze RDP internal access patterns
Utilize: Stacking by Client Name, Stacking by Cookie, Stacking Unique RDP Client Versions
Collection Requirements: windows security log, bro conn log, bro rdp log
Scope: 1 week, corp.fake.com (20 hosts) / corp.fake2.com (35 hosts)
Excluded Factors: RDP access from external sources

(now go do it)
"Justin – 10/20/2018"

Logging gap: No logging of RDP connections in corp.fake2.com

Insecure Practice: Bob using domain admin creds for RDP logins

Hypothesis – Detail view

Title (MITRE Technique)

Status

MITRE Tactic label

Link to Epic (MITRE Tactic)

Hypothesis (MITRE Procedure), collection requirements, scope, etc.

Activity – Detail View

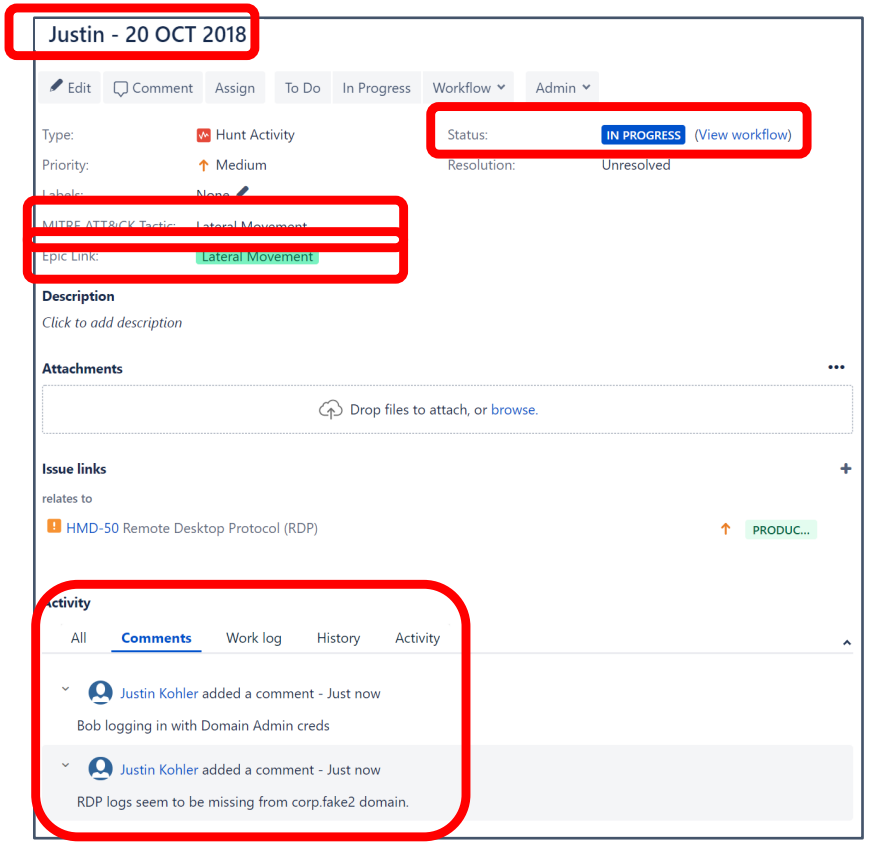
Generic title

Status

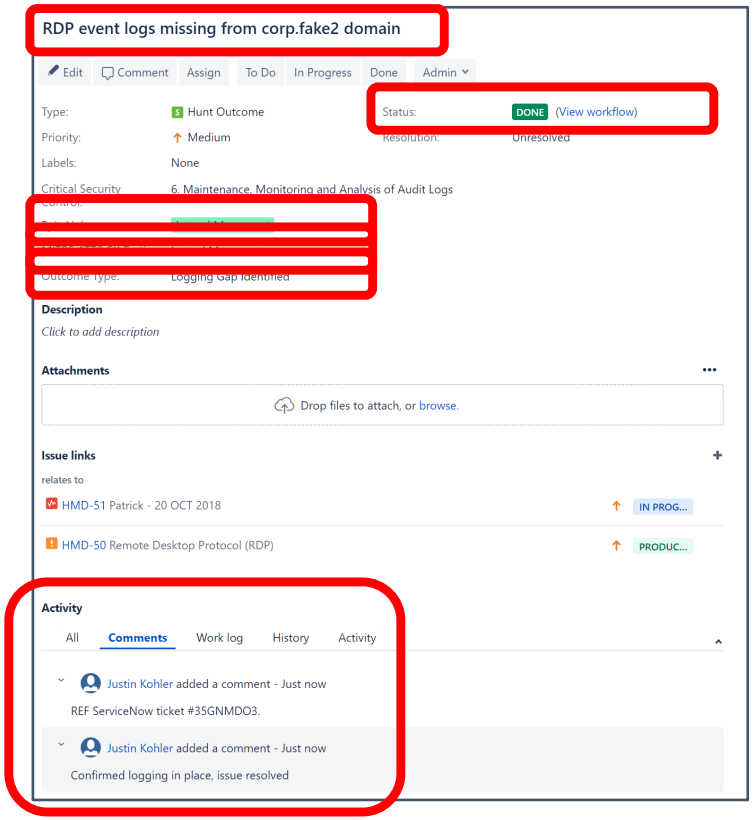
MITRE Tactic label

Link to Epic (MITRE Tactic)

Working notes

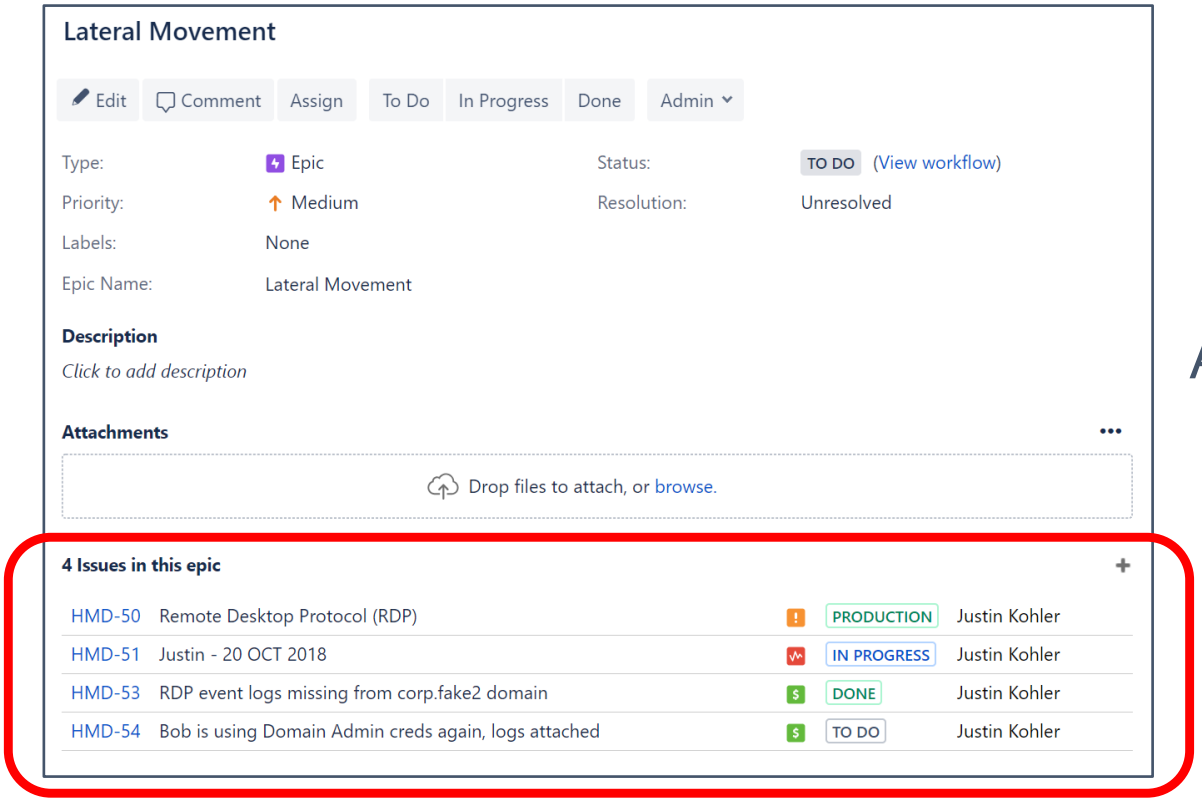


Outcome1 – Detail View



- Descriptive Title
- Status
- Link to Epic (MITRE Tactic)
- MITRE Tactic label
- Outcome Type
- Working notes

Epic (MITRE TACTIC) View



All linked issues

The Reports!

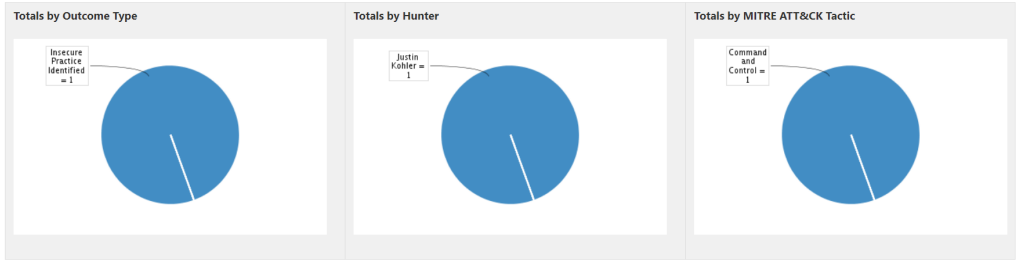
Management kryptonite

Reports

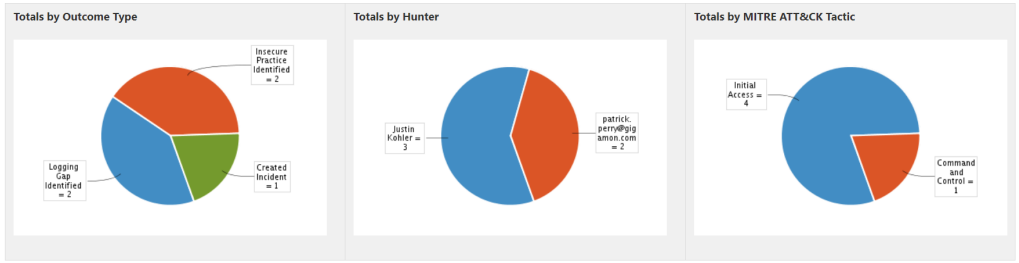
1. Outcomes
2. CIS Top 20
3. MITRE ATT&CK
4. General user statistics

1. Outcomes Report

Hunt Outcomes past 30 days



Hunt Outcomes past year



Outcomes in Progress:

Key	Summary	Created	Updated	Assignee	Status
HMD-49	Altiris sytem has direct C: drive mappings that are abnormal and need to be investigated	Oct 06, 2018 09:18	Oct 06, 2018 10:00	Unassigned	TO DO
HMD-26	Logging gap in DNS records blah	Aug 20, 2018 13:04	Aug 28, 2018 19:44	Justin Kohler	IN PROGRESS
HMD-22	test again	Aug 16, 2018 14:11	Aug 28, 2018 19:44	Unassigned	IN PROGRESS

3 issues Refresh

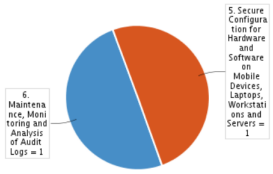
- What are we finding?
- Who is finding it?
- Reporting accuracy?
- Outcomes “actioned”?

2. CIS Top 20 Report

- Large gap anywhere?
- Gaps in the basics?

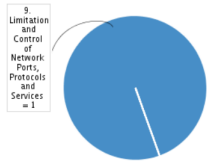
Basic Control Outcomes

1	Inventory and Control of Hardware Assets	2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management	4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	6	Maintenance, Monitoring, and Analysis of Audit Logs



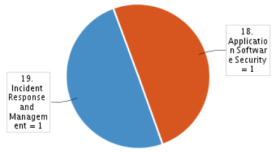
Foundational Control Outcomes

7	Email and Web Browser Protections	8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols and Services	10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	12	Boundary Defense
13	Data Protection	14	Controlled Access based on the Need to Know
15	Wireless Access Control	16	Account Monitoring and Control



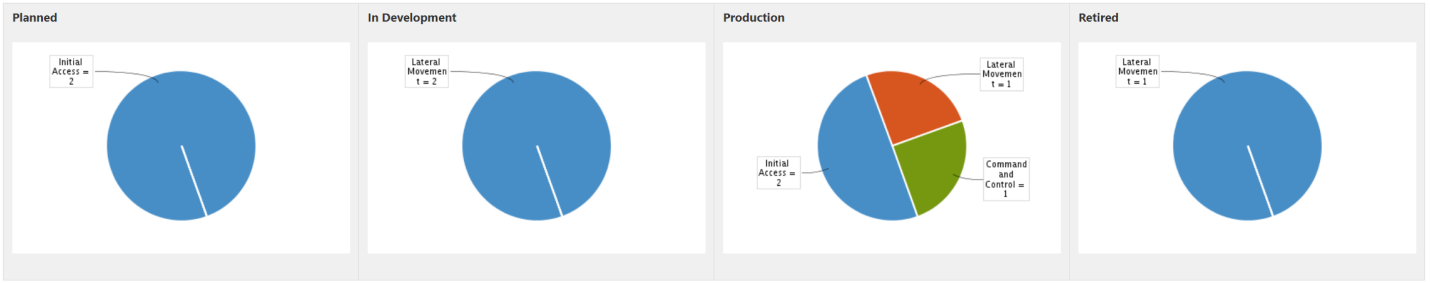
Organizational Control Outcomes

17	Implement a Security Awareness and Training Program	18	Application Software Security
19	Incident Response and Management	20	Penetration Tests and Red Team Exercises



3. ATT&CK Report

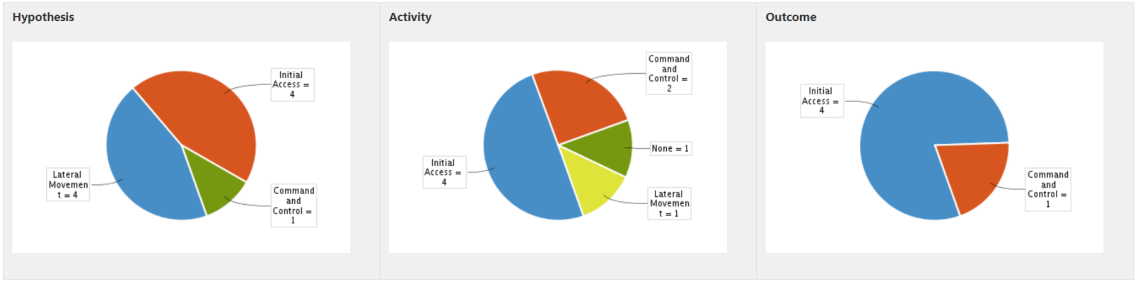
Hunt Hypothesis development by MITRE ATT&CK Tactic



Production-level hunt coverage by MITRE ATT&CK Tactic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
2 issues	0 issues	0 issues	0 issues	0 issues	0 issues	0 issues	0 issues	0 issues	0 issues	0 issues

Hypothesis, Activity, and Outcome distribution by Tactc



- Where is my hunting team focused?
- Where do I need them to focus?

4. General user statistics

Hunting Activities in Progress

Summary	Created	Updated	Assignee	Reporter	Status
Example 5	Sep 04, 2018 16:44	Sep 04, 2018 16:58	Justin Kohler	Justin Kohler	IN PROGRESS

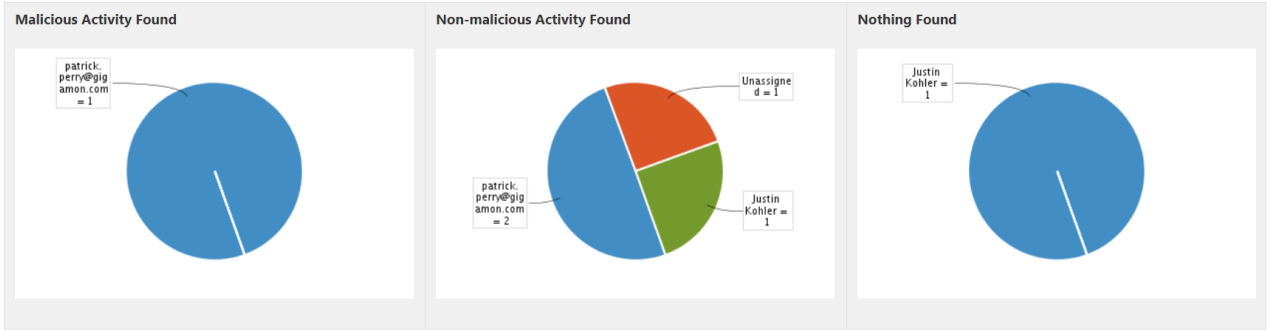
1 issue Refresh

Stalled Hunting Activities (Activities not updated in 5 days)

Summary	Created	Updated	Assignee	Reporter	Status	Resolution
Example 1	Sep 04, 2018 16:44	Sep 04, 2018 16:58	Justin Kohler	Justin Kohler	IN PROGRESS	Unresolved
Example 2	Aug 28, 2018 14:38	Sep 04, 2018 16:58	Unassigned	Justin Kohler	TO DO	Unresolved
Example 3	Aug 28, 2018 14:34	Aug 28, 2018 14:35	Unassigned	Justin Kohler	TO DO	Unresolved
Example 4	Aug 16, 2018 13:19	Aug 16, 2018 14:11	Unassigned	Justin Kohler	TO DO	Unresolved

4 issues Refresh

Hunting Activity Resolutions by Hunter



- What is ongoing right now?
- What is stalled and where can I help?
- Who is the most productive?

Yea…maybe don't do that

General notes

- Plenty of additional reports can be created
- Using native reporting built-in to Confluence for ease of use
  - Confluence / JIRA config will be available soon
- Email us if you want it before we host the config publicly
  - Justin.kohler@Gigamon.com
  - Patrick.perry@Gigamon.com
- Many additional customizations & automations are possible
- Easier to implement without

And you can too!

Maybe you already are?

And you can (are?) too!

“This seems like a lot of work, my team won’t do this”

- Tough, security is hard
- Use this to spread knowledge across your team

“No, you’re just overcomplicating it”

- Ok show us!

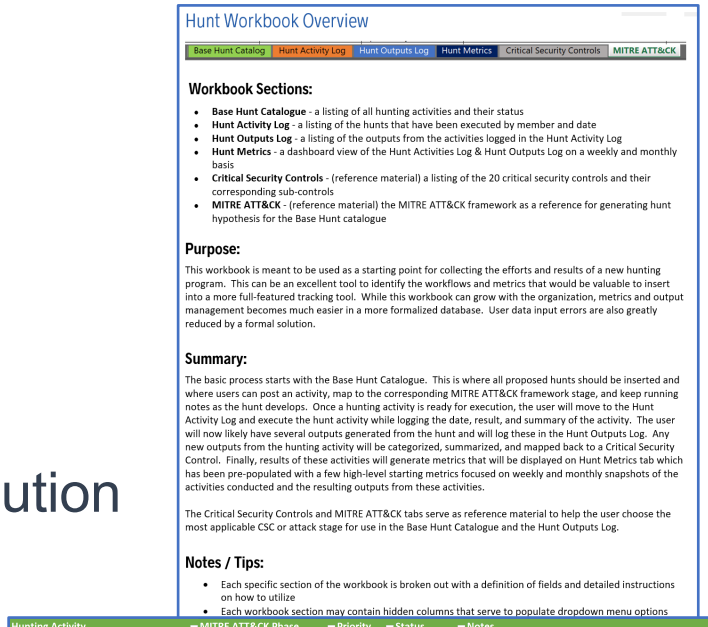
Want to start simpler?

WARNING: Don't actually "use" this

Seriously, this doesn't scale

Easy way to start workflow

Use to plan / scope your long-term solution



Hunt Workbook Overview

Base Hunt Catalog | Hunt Activity Log | Hunt Outputs Log | Hunt Metrics | Critical Security Controls | MITRE ATT&CK

Workbook Sections:

- **Base Hunt Catalogue** - a listing of all hunting activities and their status
- **Hunt Activity Log** - a listing of the hunts that have been executed by member and date
- **Hunt Outputs Log** - a listing of the outputs from the activities logged in the Hunt Activity Log
- **Hunt Metrics** - a dashboard view of the Hunt Activities Log & Hunt Outputs Log on a weekly and monthly basis
- **Critical Security Controls** - (reference material) a listing of the 20 critical security controls and their corresponding sub-controls
- **MITRE ATT&CK** - (reference material) the MITRE ATT&CK framework as a reference for generating hunt hypothesis for the Base Hunt catalogue

Purpose:

This workbook is meant to be used as a starting point for collecting the efforts and results of a new hunting program. This can be an excellent tool to identify the workflows and metrics that would be valuable to insert into a more full-featured tracking tool. While this workbook can grow with the organization, metrics and output management becomes much easier in a more formalized database. User data input errors are also greatly reduced by a formal solution.

Summary:

The basic process starts with the Base Hunt Catalogue. This is where all proposed hunts should be inserted and where users can post an activity, map to the corresponding MITRE ATT&CK framework stage, and keep running notes as the hunt develops. Once a hunting activity is ready for execution, the user will move to the Hunt Activity Log and execute the hunt activity while logging the date, result, and summary of the activity. The user will now likely have several outputs generated from the hunt and will log these in the Hunt Outputs Log. Any new outputs from the hunting activity will be categorized, summarized, and mapped back to a Critical Security Control. Finally, results of these activities will generate metrics that will be displayed on Hunt Metrics tab which has been pre-populated with a few high-level starting metrics focused on weekly and monthly snapshots of the activities conducted and the resulting outputs from these activities.

The Critical Security Controls and MITRE ATT&CK tabs serve as reference material to help the user choose the most applicable CSC or attack stage for use in the Base Hunt Catalogue and the Hunt Outputs Log.

Notes / Tips:

- Each specific section of the workbook is broken out with a definition of fields and detailed instructions on how to utilize
- Each workbook section may contain hidden columns that serve to populate dropdown menu options

Hunting Activity	MITRE ATT&CK Phase	Priority	Status	Notes
Review users with excessive login failures using 1) the same user name 2) different user names	Credential Access			
Review uncommon HTTP user agents using least frequency analysis	Initial Access			
Review non-protocol-compliant traffic, e.g. SSL over unusual port, non-HTTP traffic over 8080, etc.	Command and Control	Low	Planned	

Review outbound traffic that does not originate from proxy	Command and Control	Medium	In Development	ICEBRG draft query:
				src.internal = true AND dst.internal = false // traffic flowing externally
				AND src.ip NOT IN ('192.168.1.50', ' 10.0.2.1') // not originating from the proxy servers
				AND src.ip NOT IN ('10.0.2.0/24') // removing guest wireless networks
				GROUP BY src.ip // group by assets

Review outbound DNS queries to non-standard DNS servers for evidence of C2 (beaconing, tunneling, etc.)	Command and Control			
Stack services and perform analysis based on least frequency	Undefined			

Final thoughts

The specific tool is not important, planning is

Threat hunting is valuable

Don’t let your program get derailed

https://github.com/pjbperry/Presentations

Questions?