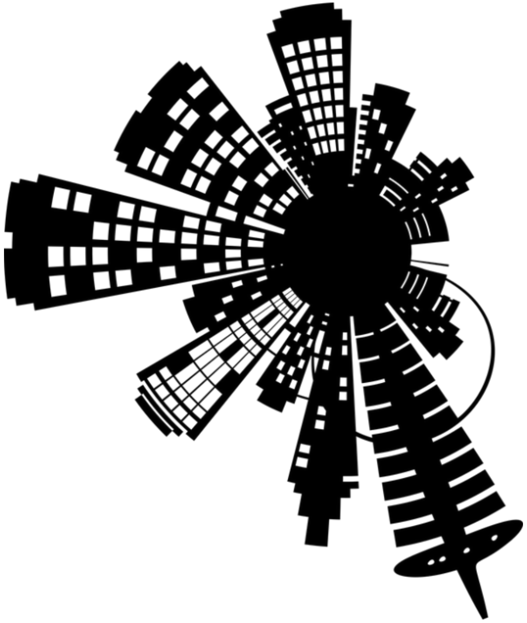
SACON International 2020

India | Bangalore | February 21 - 22 | Taj Yeshwantpur



PRACTICAL THREAT HUNTING: DEVELOPING AND RUNNING A SUCCESSFUL THREAT HUNTING PROGRAM

#SACON #THREATHUNTING

WASIM HALANI
Network Intelligence (NII)
HEAD R&D
@washalsec

ARPAN RAVAL
Optiv Inc
Senior Threat Analyst
@arpanrvl

NETWORK INTELLIGENCE
Global Cyber Security Provider

OPTIV

SACON

PRACTICAL THREAT HUNTING:
Developing and Running a Successful Threat Hunting Program

By Wasim Halani and Arpan Raval

WHOAMI

NETWORK
INTELLIGENCE
Global cybersecurity provider

- Wasim Halani
- Head R&D @Network Intelligence (NII)
- ~12 years in InfoSec
- Speaker at SACON, OWASP, BSides, Malcon, SecurityBytes
- Twitter @washalsec
- https://in.linkedin.com/in/wasimhalani

WHOAMI

- Arpan Raval
- Senior Threat Analyst @Optiv Inc
- DFIR and Threat Hunting
- Twitter @arpanrvl
- https://www.linkedin.com/in/arpanraval

DEFINE THREAT HUNTING

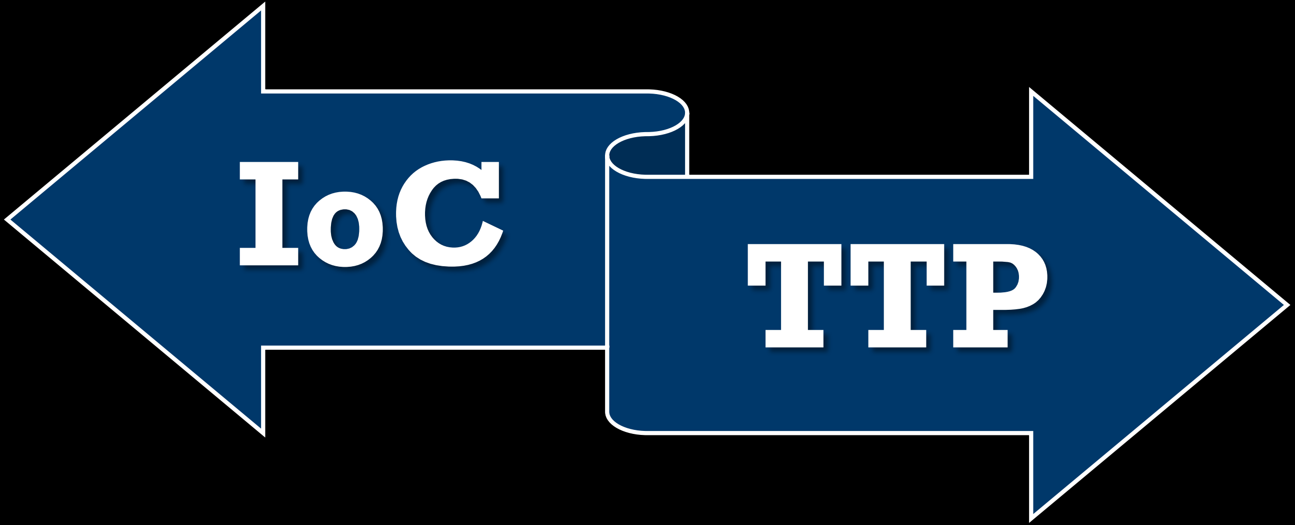
WHY & WHAT?

PROBLEM OF "DWELL TIME"

- In 2011 Global Median dwell time mentioned was **416 days!**
- For 2018, Fire Eye M Trends reports average dwell time mentioned is **101 days!**
- For 2019, Fire Eye M Trends Reports average dwell time mentioned is **78 days!**

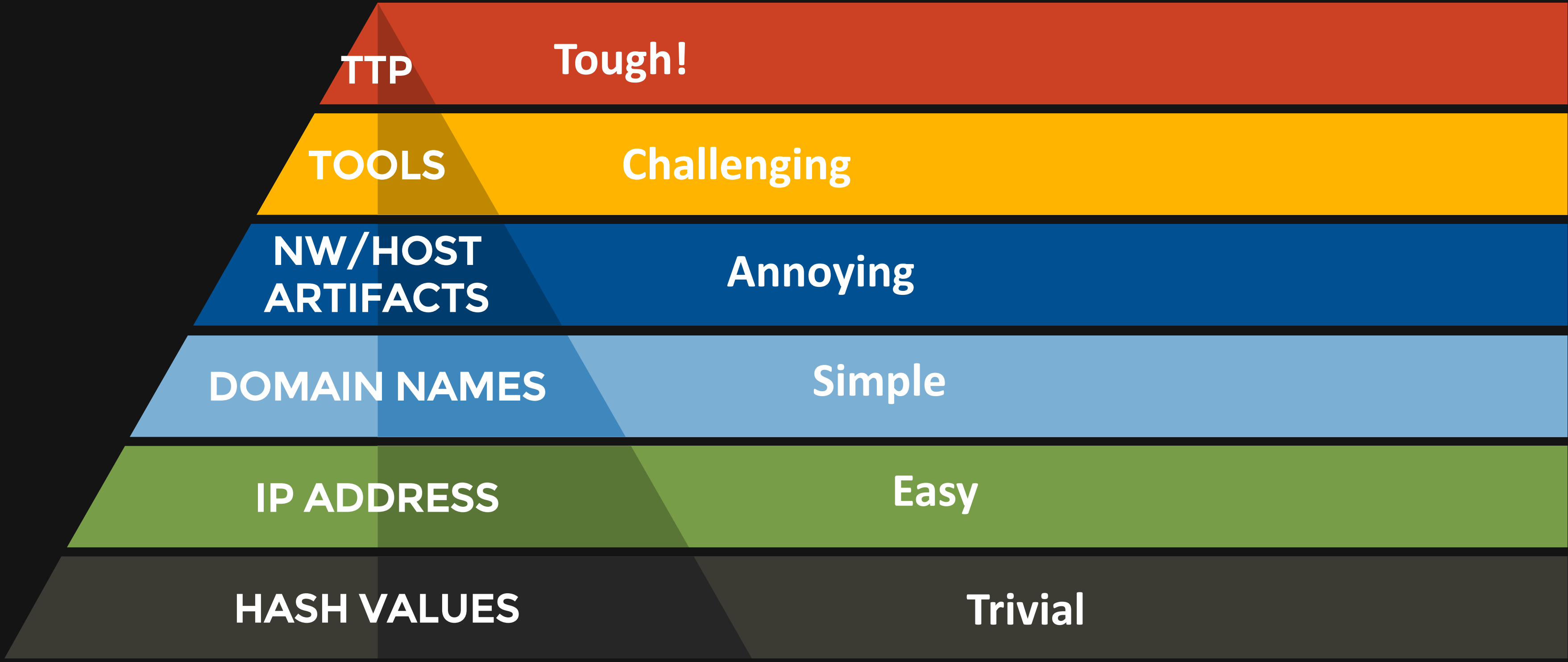
https://www.fireeye.com/blog/executive-perspective/2019/03/mtrends-2019-celebrating-ten-years-of-incident-response-reporting.html

IoC vs TTP



PYRAMID OF PAIN

Introduced by David JBianco



TTP — Tough!

TOOLS — Challenging

NW/HOST ARTIFACTS — Annoying

DOMAIN NAMES — Simple

IP ADDRESS — Easy

HASH VALUES — Trivial

What is Threat Hunting?

"Threat Hunting is a human driven proactive approach to discover malicious activities that have evaded existing security control."

What is Threat Hunting?

Detecting the Undetected

PURPOSE OF THREAT HUNTING

- Reduce the Dwell Time
- Identify Gaps in Visibility
- Identify Gaps in Detection
- Design New Detection Mechanism and Analytics techniques
- Uncover New Threat and TTPs (Producing Threat Intelligence).

What is NOT Threat Hunting?

- Triaging Alerts
- IoC sweeps from Intel Feeds to Incoming telemetry
- Process with guaranteed result.
- A replacement for penetration testing or red teaming.

What is NOT Threat Hunting?

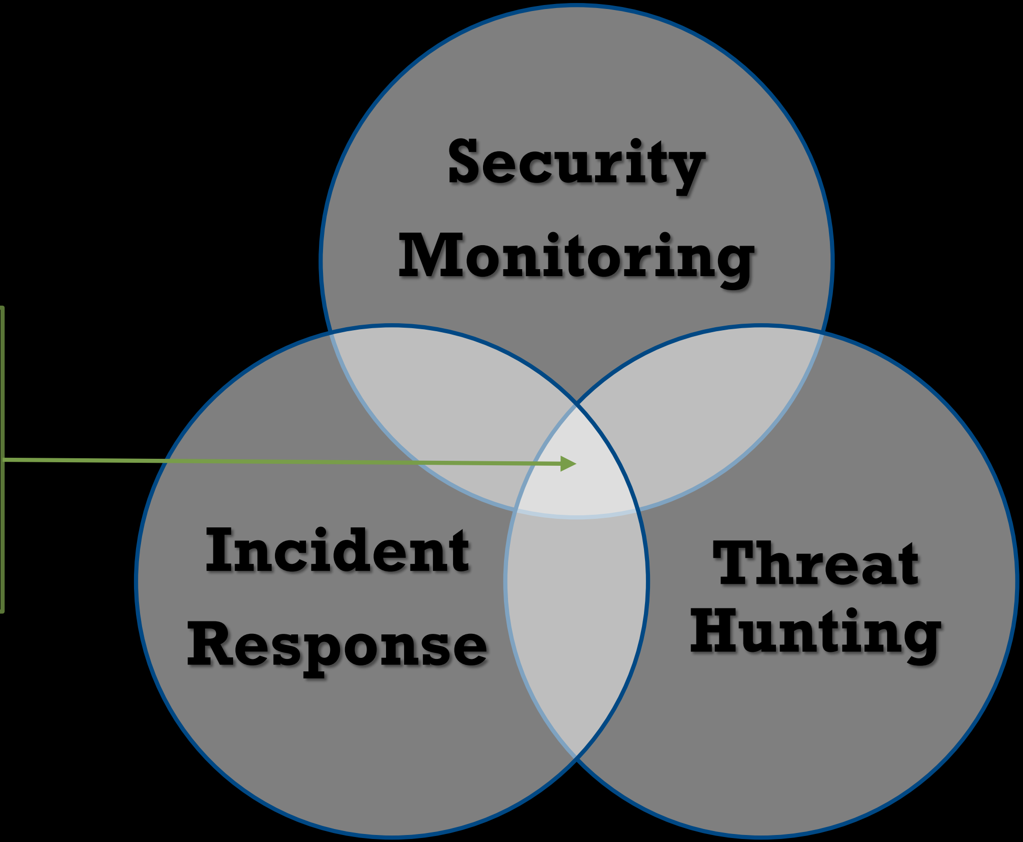
"Autonomous discovery of malicious activity by tools."

Characteristics of Threat Hunting

- Human Driven
- Human Centric
- Proactive
- Assume Breach
- Detect Unknown
- Iterative
- Data dependent
- Hypothesis Driven

Threat Hunting in Security Operations

Search Queries,
CTI Guided
Detections
Retrohunts
Incident Detection
Event Analysis
Detector Creation



MITRE ATT&CK FRAMEWORK

MITRE ATT&CK

MATRICES	Techniques/Numbers
PRE-ATT&CK	174
Enterprise Windows macOS Linux Cloud AWS GCP Azure Office 365 Azure AD SaaS	266
Mobile Android iOS	79
ICS	81
APT Groups	94
Software	414

MITRE | ATT&CK™

- Attack Library
- Knowledge base of adversary's TTPs collected based on real world observations and attacks
- Describes and Categorize adversarial behavioral in different phases of attack cycle.

MITRE Explained: Tactic

- Answers Why? for adversary’s actions.
- Adversary’s objective behind an action
- Represented by Columns in MITRE ATT&CK Matrix

Matrix	Tactic
Enterprise	12
Mobile	13
ICS	11

Example
An adversary want to achieve credential access.

Enterprise	Mobile	ICS
Initial Access	Initial Access	Collection
Execution	Persistence	Command and Control
Persistence	Privilege Escalation	Discovery
Privilege Escalation	Defense Evasion	Evasion
Defense Evasion	Credential Access	Execution
Credential Access	Discovery	Impact
Discovery	Lateral Movement	Impair Process Control
Lateral Movement	Impact	Inhibit Response Function
Collection	Collection	Initial Access
Command and Control	Exfiltration	Lateral Movement
Exfiltration	Command and Control	Persistence
Impact	Network Effects	
	Remote Service Effects	

MITRE Explained: Tactic

ATT&CK TACTIC	EXPLAINATION	OBJECTIVE
Initial Access	Get into your environment	Gain access
Credential Access	Steal logins and passwords	Gain access
Privilege Escalation	Gain higher level permissions	Gain (more) access
Persistence	Maintain foothold	Keep access
Defense Evasion	Avoid detection	Keep access
Discovery	Figure out your environment	Explore
Lateral Movement	Move through your environment	Explore
Execution	Run malicious code	Follow through
Collection	Gather data	Follow through
Exfiltration	Steal data	Follow through
Command and Control	Contact controlled systems	Contact controlled systems
Impact	Break things	Follow through

Source: Helping Your Non-Security Executives Understand ATT&CK in 10 Minutes or Less (Elly Searle, CrowdStrike)

MITRE Explained: Technique

- Answers how? for adversary’s objective achievement.
- Adversary used a technique to achieve an objective
- Represented by individual cell in MITRE ATT&CK Matrix

Example
Example: an adversary may dump credentials to achieve credential access.

Matrix	Technique
PRE-ATT&CK	174
Enterprise	266
Mobile	79
ICS	81

MITRE Explained: Technique-Metainfo

- **Tactic:**

  Related MITRE Tactic

- **Platform:**

  Required platform for a technique to work in.

- **Permissions Required:**

  Lowest permission for an adversary to implement the technique

- **Effective Permissions:**

  Permission an adversary achieves after successful implementation of the technique

- **Data Sources:**

  Recommended data to be collection for detection of the technique

MITRE Explained: Enumeration

Tactic		Example Technique
Obtaining Persistence	via	Windows Service Creation
Privilege Escalation	via	Legitimate Credentials Reuse
Defense Evasion	via	Office-Based Malware
Credential Access	via	Memory Credential Dumping
Discovery	via	Built-In Windows Tools
Lateral Movement	via	Share Service Accounts
Execution	via	PowerShell Execution
Collection	via	Network Share Identification
Exfiltration	via	Plaintext Exfiltration
Impact	via	Data Encryption

MITRE Explained: Procedure

- Answers what? for adversary's technique usage.
- Actual implementation of each technique.
- Individual technique has a page for description, examples, sources, references.

Example

A procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim.

MITRE ATTACK MAPPING

HANDS ON 1

PRIORITIZED MITRE ATT&CK SUBSETS

Let’s create our own prioritized MITRE ATT&CK Subset based adversarial TTPs based derived from any of these:

- ❖ Threat Intelligence
- ❖ Whitepapers
- ❖ Data Sources
- ❖ Ad-Hoc Requests

Note: Matrix in upcoming slides is example matrix with dummy data for example which is not necessarily is true or to promote any tool/technology.

MITRE DETECTION MAPPING

<table>
<tr><th>Initial Access</th><th>Persistence</th><th>Privilege Escalation</th><th>Defense Evasion</th><th>Credential Access</th><th>Discovery</th><th>Lateral Movement</th><th>Execution</th><th>Collection</th><th>Exfiltration</th><th>Command and Control</th></tr>
<tr><td>External Remote Services</td><td colspan="3">DLL Search order Hijacking
WDATP</td><td>Brute Force
Elastic</td><td>Account Discovery
Elastic</td><td colspan="2">🟥 **Windows Remote Management**
TBD</td><td>Automated Collection
UEBA</td><td>Automated Exfiltration
ZScaler</td><td>Commonly Used Port
ZScaler</td></tr>
<tr><td colspan="4">Valid Accounts
UEBA</td><td rowspan="2">🟧 **Credential Dumping**
WDATP</td><td rowspan="2">Application Window Discovery
ZScaler</td><td colspan="2">COM and DCOM
Elastic</td><td>Clipboard Data
WDATP</td><td>Data Compressed
ZScaler</td><td rowspan="2">Communication Through Removable Media
Symantec DLP</td></tr>
<tr><td>Spearphishing Attachment
TBD</td><td colspan="2">Accessibility Features
TBD</td><td>Indicator Removal on Host
WDATP</td><td rowspan="2">Application Deployment Software
Elastic</td><td>🟧 **Command Line**
WDATP</td><td>Data Staged
UEBA</td><td>Data Encrypted
Symantec DLP</td></tr>
<tr><td>Spearphishing Link
TBD</td><td colspan="2">AppInit DLLS
WDATP</td><td>Masquerading
WDATP</td><td rowspan="2">Credential Manipulation
UEBA</td><td rowspan="2">File and Directory Discovery
UEBA</td><td>Execution through API
TBD</td><td>Data from Local System
UEBA</td><td>Data Transfer Size Limits
TBD</td><td rowspan="2">Custom Command and Control Protocol
Symantec DLP</td></tr>
<tr><td></td><td colspan="2">AppCert DLLs
WDATP</td><td>Decode File or Info
TBD</td><td rowspan="2">Pass the Ticket
WDATP</td><td>Graphic User Interface
TBD</td><td rowspan="2">Data from Network Shared Drive
ZScaler</td><td rowspan="2">Exfiltration Over Alternative Protocol
ZScaler</td></tr>
<tr><td></td><td colspan="2">🟥 **Application Shimming**
TBD</td><td>DLL Side-Loading
WDATP</td><td>🟩 **Credentials in Files**
UEBA
WDATP</td><td rowspan="2">Process Discovery
Elastic</td><td>InstallUtil
WDATP</td><td rowspan="2">Custom Cryptographic Protocol
ZScaler</td></tr>
<tr><td></td><td colspan="2">New Service
TBD</td><td>Disabling Security Tools
Elastic</td><td>Input Capture
WDATP</td><td>Remote Desktop Protocol
Elastic</td><td>PowerShell
WDATP</td><td></td><td></td></tr>
</table>

Key

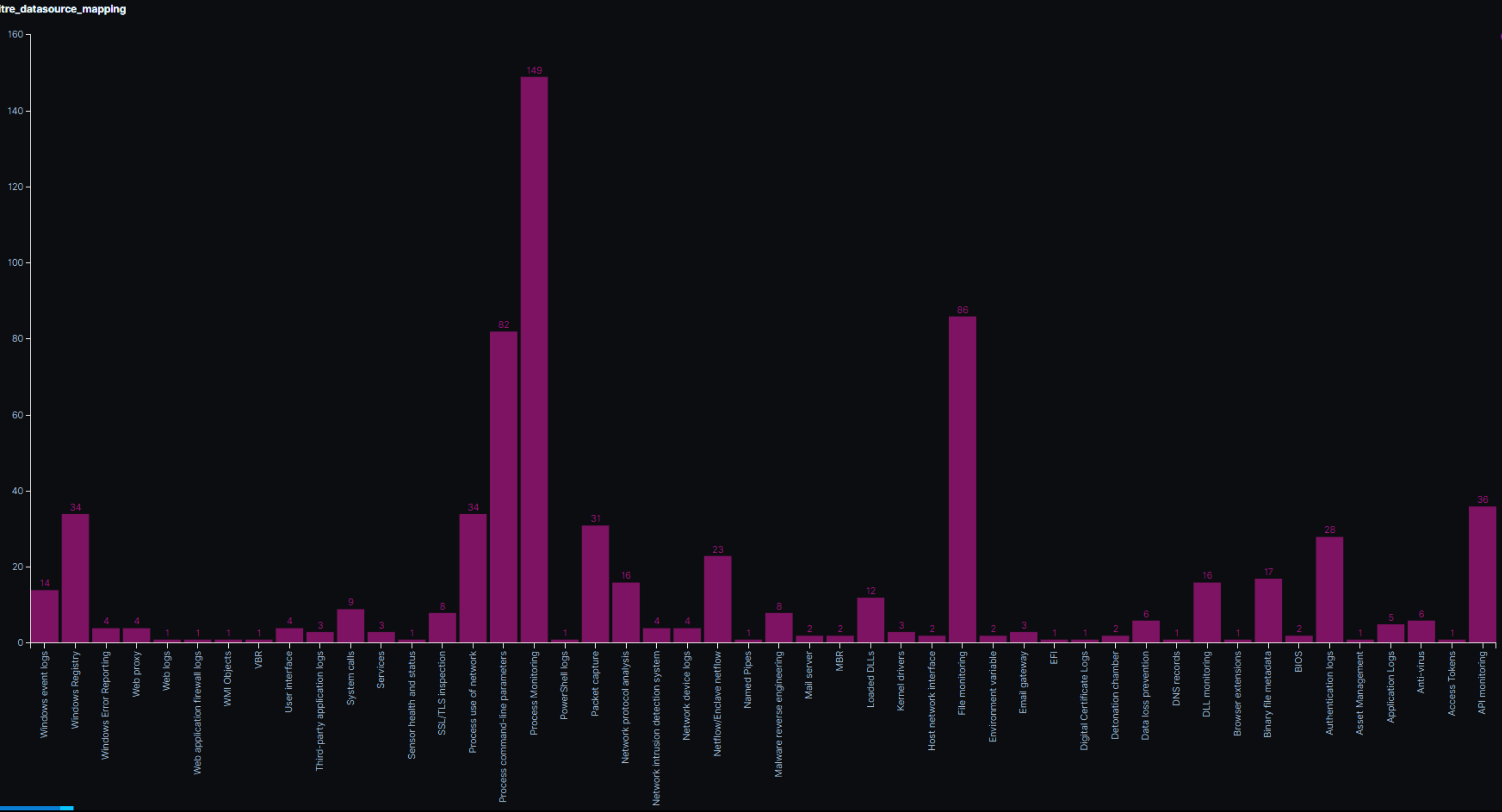
🟥	🟧	🟩
No detection	Detected, No validation	Detected

DATA SOURCE MAPPING

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
External Remote Services	DLL Search order Hijacking			Brute Force	Account Discovery	**Windows Remote Management**		Automated Collection	Automated Exfiltration	Commonly Used Port
Valid Accounts				**Credential Dumping**	Application Window Discovery	COM and DCOM		Clipboard Data	Data Compressed	Communication Through Removable Media
Spearphishing	Accessibility Features		Indicator Removal on Host			Application Deployment Software	**Command Line**	Data Staged	Data Encrypted	
Spearphishing Link	AppInit DLLS		Masquerading	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
	AppCert DLLs		Decode File or Info			Pass the Ticket	Graphic User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
	Application Shimming		DLL Side-Loading	**Credentials in Files**	Process Discovery		InstallUtil			Custom Cryptographic Protocol
	New Service		Disabling Security Tools	Input Capture		Remote Desktop Protocol	PowerShell			

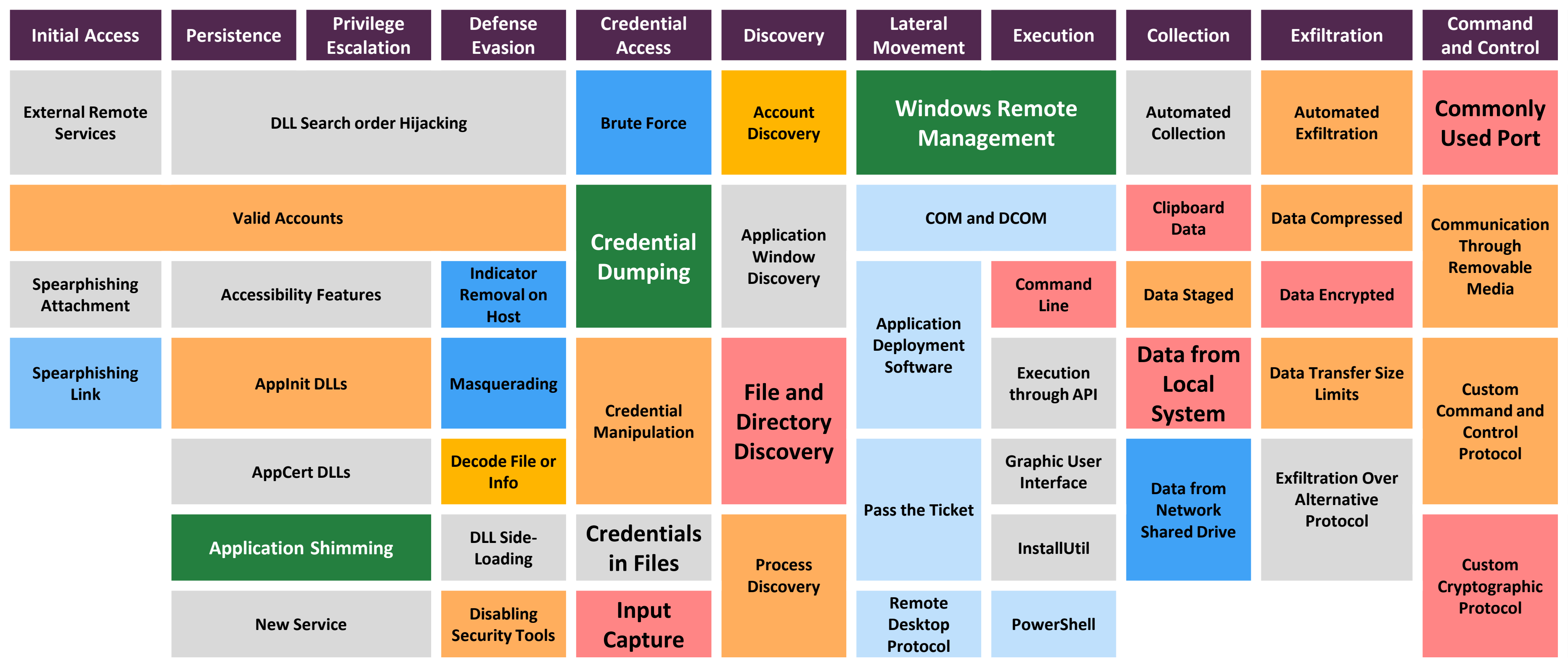
Key

Data does not exist	**Data exists, not monitored**	**Data exists analyzed and monitored**



tre_datasource_mapping

DETECTION MATURITY HEATMAP



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
External Remote Services	DLL Search order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Valid Accounts				Credential Dumping	Application Window Discovery	COM and DCOM		Clipboard Data	Data Compressed	Communication Through Removable Media
Spearphishing Attachment	Accessibility Features		Indicator Removal on Host			Application Deployment Software	Command Line	Data Staged	Data Encrypted	
Spearphishing Link	AppInit DLLs		Masquerading	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
	AppCert DLLs		Decode File or Info			Pass the Ticket	Graphic User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
	Application Shimming		DLL Side-Loading	Credentials in Files	Process Discovery		InstallUtil			Custom Cryptographic Protocol
	New Service		Disabling Security Tools	Input Capture		Remote Desktop Protocol	PowerShell			

Maturity Key: Limited | Initial | Stable | Current | Innovative

THREAT HUNTING METHODOLOGY

TYPES, PROCESS AND CYCLE

Threat Hunting Approaches

- Long Term
- Ad-hoc
- Short Term

Threat Hunting Types

- Structured Hunting
- Unstructured Hunting
- Intel Guided Hunting

- Host Based
- Network Based
- Business Use Case Based

Hunting Type: Intel Guided Hunting

- Guided by Threat Intelligence Inputs
  - Threat Intel Reports
  - Threat White Papers
  - MITRE APT Groups

Hunting Type: Structured Hunting

- Hypothesis Based
- Well Scoped
- TTP driven or Entity Driven
- Other Synonyms in industry:
  - ATT&CK Drive

HANDS ON LAB 2

STRUCTURED HYPOTHESIS – BITS, ACCESSIBILITY FEATURES

BITS Jobs

Defense Evasion, Persistence

MITRE ID	T1197
MITRE Tactic	Defense Evasion, Persistence
MITRE Technique	BITS Jobs
Platform	Windows
Required Privilege	User, Administrator, SYSTEM
Data Sources	API monitoring, Packet capture, Windows event logs

BITS Jobs

Defense Evasion, Persistence

Description	Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications.

Implementation	`Bitsadmin.exe`
	`Powershell.exe Start-BitsTransfer`

BITS Jobs

Defense Evasion, Persistence

Source	Event ID	Event Field	Details
Windows Security Event Logs	4688	New Process Name	*\\bitsadmin.exe
Windows Security Event Logs	4688	Process Command Line	*create*
Proxy-Logs	userAgent		Microsoft BITS/*

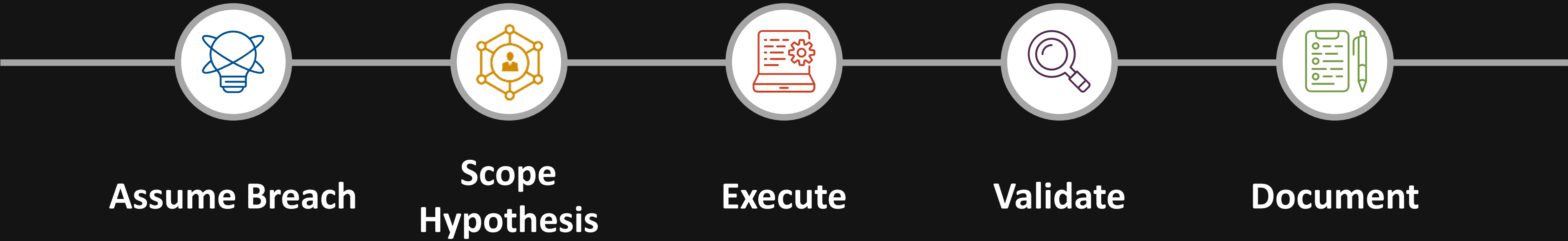
Hunting Type: Unstructured Hunting

- Data Driven
- Anomaly/Outlier based
- Other synonym in industry:
    - Data Driven Hunting
    - Free Style Hunting

HANDS ON LAB 3

PROCESS ANOMALY

HYPOTHESIS GENRATION PROCESS



Assume Breach

Scope Hypothesis

Execute

Validate

Document

Accessibility Features

Persistence, Privilege Escalation

MITRE ID	T1015
MITRE Tactic	Persistence Privilege Escalation
MITRE Technique	Accessibility Features
Platform	Windows
Required Privilege	Administrator
Data Sources	Windows Registry, File monitoring, Process monitoring

Accessibility Features

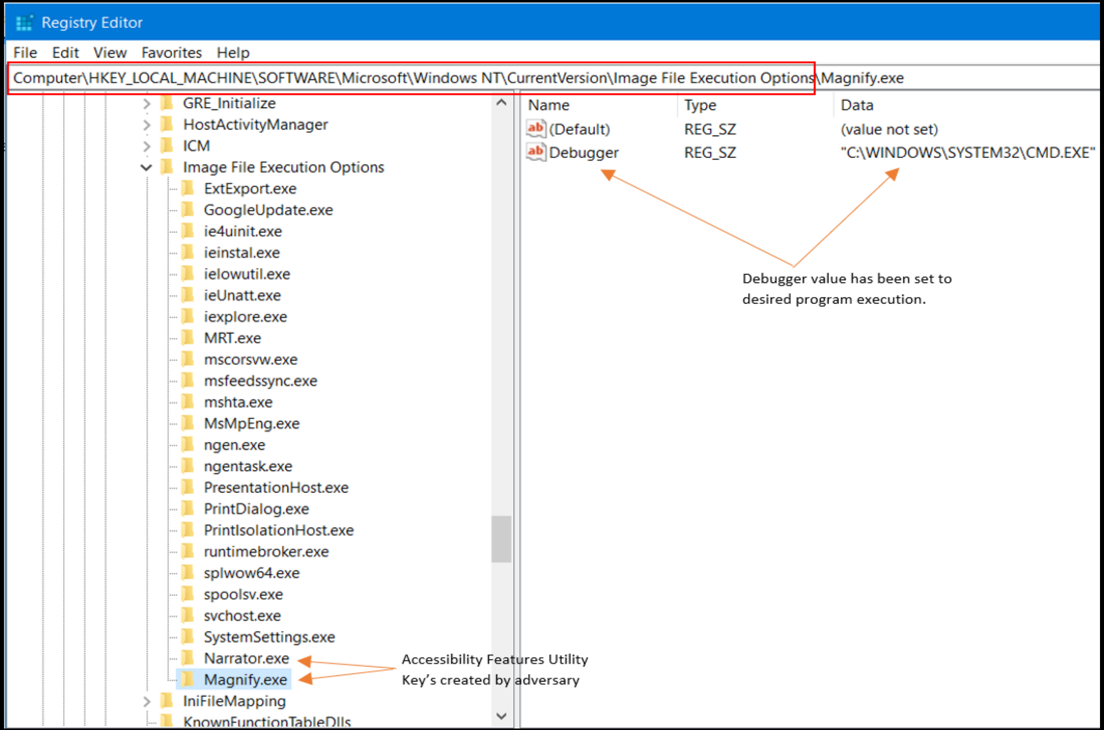
Persistence, Privilege Escalation

Description	Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.
Implementation	Binary Replacement OR Registry Value Change
Limitations	Depending on Windows versions The replaced binary needs to be digitally signed for x64 systems, The binary must reside in %systemdir% It must be protected by Windows File or Resource Protection (WFP/WRP)

Accessibility Features

Persistence, Privilege Escalation

Attack Emulation: Set the Debugger value for the desired accessibility feature application



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Magnify.exe

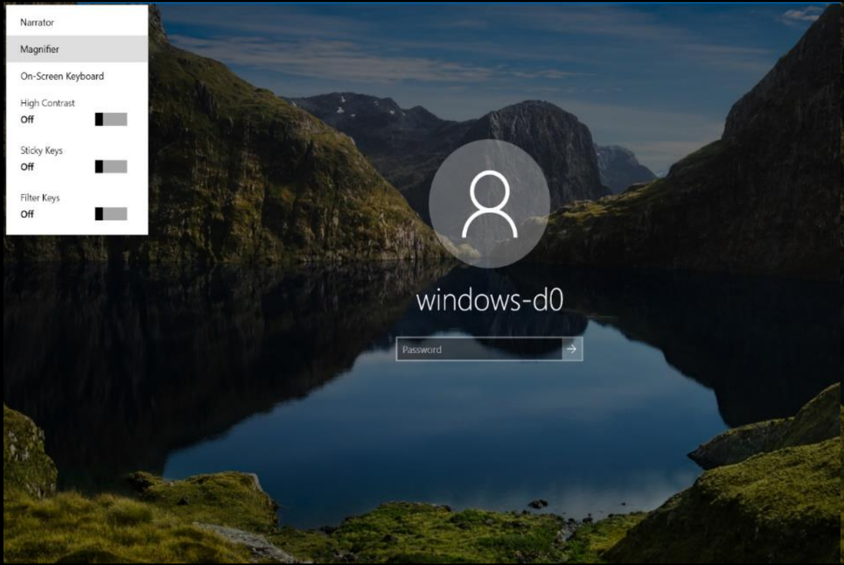
Name	Type	Data
(Default)	REG_SZ	(value not set)
Debugger	REG_SZ	"C:\WINDOWS\SYSTEM32\CMD.EXE"

Debugger value has been set to desired program execution.

Accessibility Features Utility Key's created by adversary

Accessibility Features

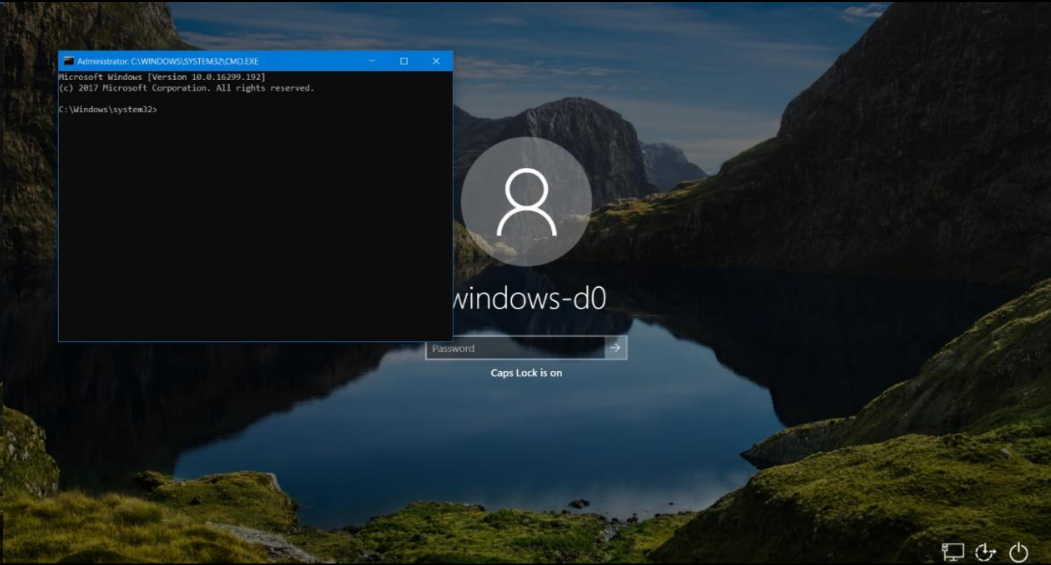
Persistence, Privilege Escalation



High Contrast
Off

Sticky Keys
Off

Filter Keys
Off

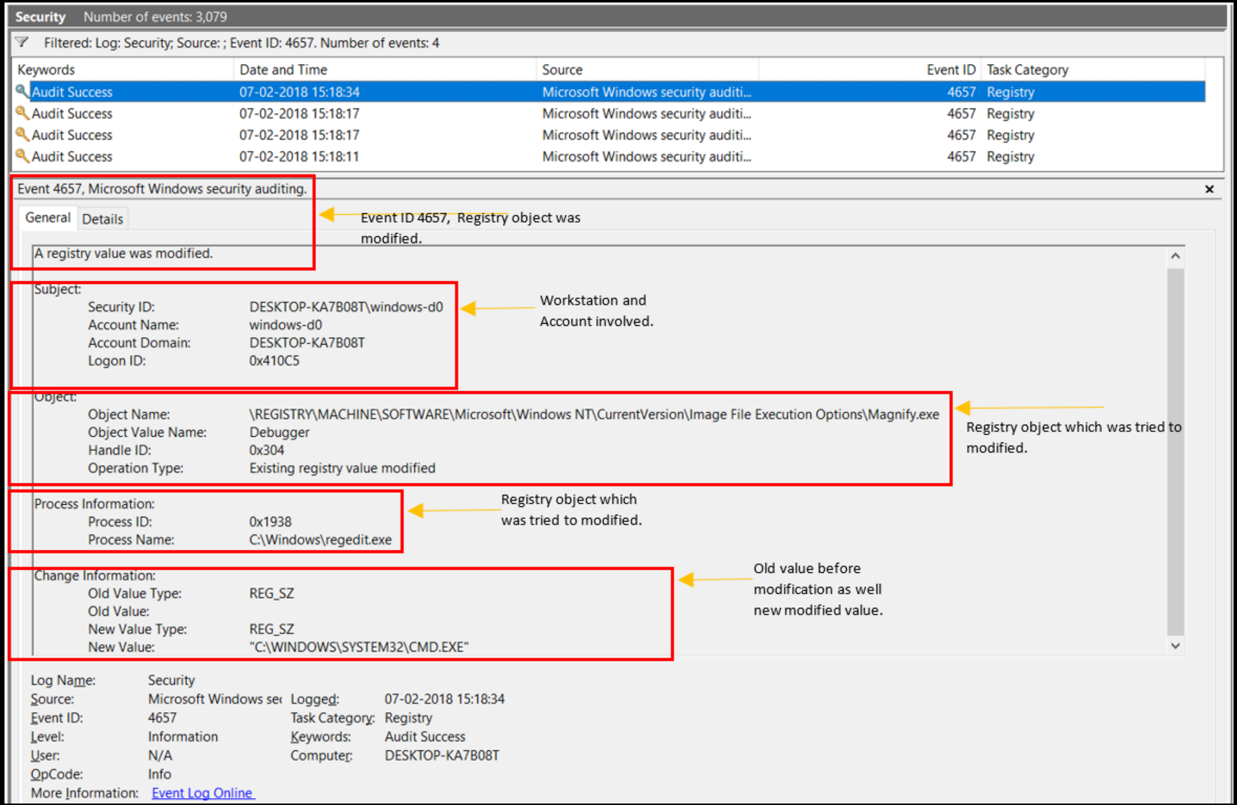


```
Microsoft Windows [Version 10.0.16299.192]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Accessibility Features

Persistence, Privilege Escalation



Security Number of events: 3,079

Filtered: Log: Security; Source: ; Event ID: 4657. Number of events: 4

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	07-02-2018 15:18:34	Microsoft Windows security auditi...	4657	Registry
Audit Success	07-02-2018 15:18:17	Microsoft Windows security auditi...	4657	Registry
Audit Success	07-02-2018 15:18:17	Microsoft Windows security auditi...	4657	Registry
Audit Success	07-02-2018 15:18:11	Microsoft Windows security auditi...	4657	Registry

Event 4657, Microsoft Windows security auditing.

A registry value was modified.

Subject:
- Security ID: DESKTOP-KA7B08T\windows-d0
- Account Name: windows-d0
- Account Domain: DESKTOP-KA7B08T
- Logon ID: 0x410C5

Object:
- Object Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Magnify.exe
- Object Value Name: Debugger
- Handle ID: 0x304
- Operation Type: Existing registry value modified

Process Information:
- Process ID: 0x1938
- Process Name: C:\Windows\regedit.exe

Change Information:
- Old Value Type: REG_SZ
- Old Value:
- New Value Type: REG_SZ
- New Value: "C:\WINDOWS\SYSTEM32\CMD.EXE"

Log Name:	Security		
Source:	Microsoft Windows sec	Logged:	07-02-2018 15:18:34
Event ID:	4657	Task Category:	Registry
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-KA7B08T
OpCode:	Info		
More Information:	Event Log Online		

Event ID 4657, Registry object was modified.

Workstation and Account involved.

Registry object which was tried to modified.

Registry object which was tried to modified.

Old value before modification as well new modified value.

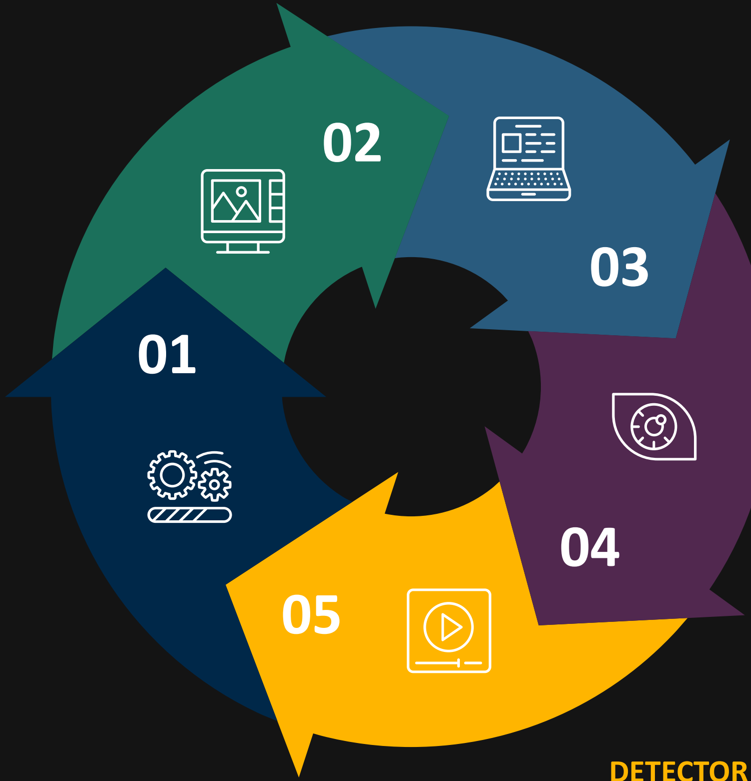
Accessibility Features

Persistence, Privilege Escalation

Source	Event ID	Event Field	Details
Sysmon	12, 13	TargetObject	*\\SOFTWARE\\Microsoft\\Windows\ NT\\CurrentVersion\\Image\ File\ Execution\ Options\\<AFU>\\Debugger AFU=sethc.exe, utilman.exe, osk.exe, Magnify.exe, Narrator.exe, DisplaySwitch.exe, AtBroker.exe
Windows Security Event Logs	4657	Object Name	sethc.exe, utilman.exe, osk.exe, Magnify.exe, Narrator.exe, DisplaySwitch.exe, AtBroker.exe
Windows Security Event Logs	4657	Object Value Name	Debugger

THE THREAT HUNTING CYCLE

HUNT ONCE



OUTLIER/ANOMALY IDENTIFICATION

HUNT EXECUTION

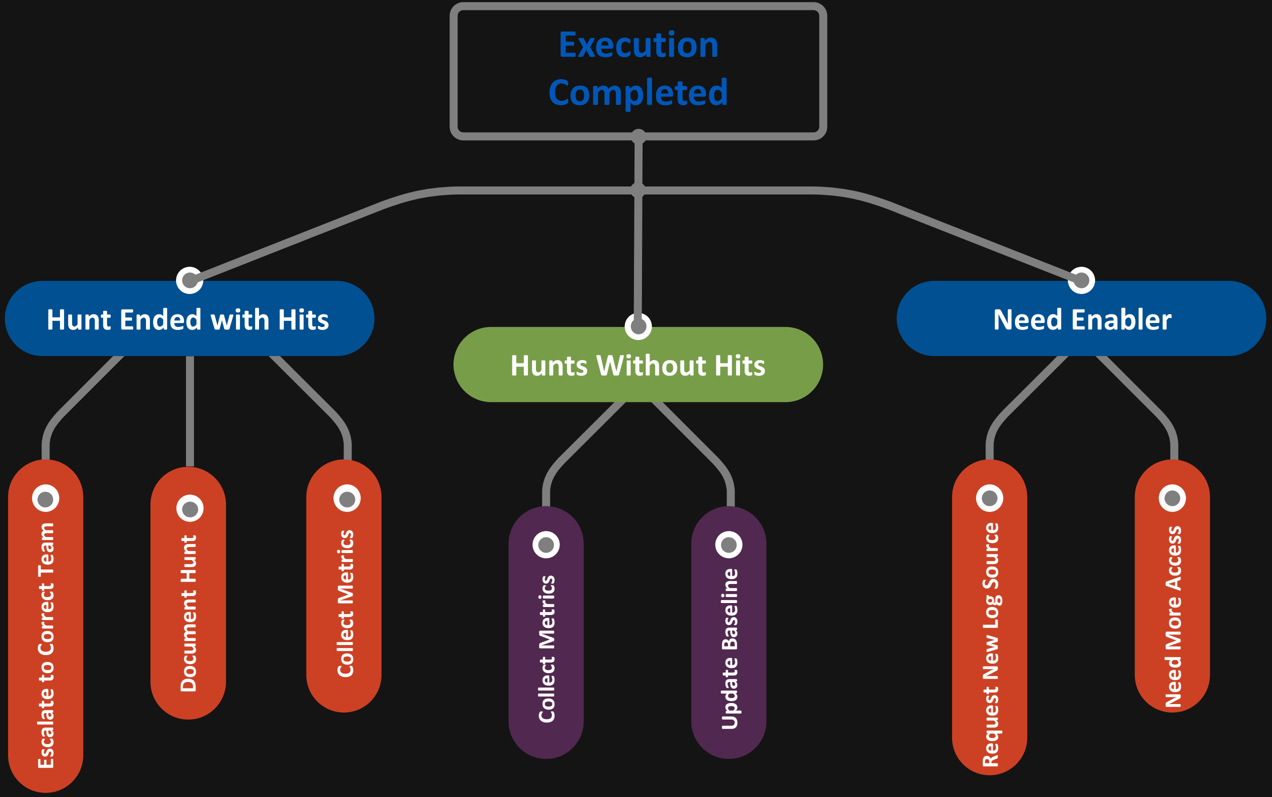
INCIDENT VALIDATION

HYPOTHESIS CREATION

DETECTOR CREATION

POST HUNT ACTIVITIES

POST HUNT ACTIVITY



Execution Completed

Hunt Ended with Hits

Escalate to Correct Team

Document Hunt

Collect Metrics

Hunts Without Hits

Collect Metrics

Update Baseline

Need Enabler

Request New Log Source

Need More Access

PROGRAM METRICS

- Hunt Hypothesis
- Total time spent hunting (hours)
- Total dwell time (hours)
- incidents found
- use cases updated
- vulnerabilities found

Check out Magma Framework for awesome Metrics and Charts in resources link

References and Awesome Resources

- http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- https://github.com/hunters-forge
- https://github.com/ThreatHuntingProject/ThreatHunting/tree/master/hunts
- https://www.threathunting.net/
- https://github.com/clong/DetectionLab
- https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma/
- https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf
- https://mitre-attack.github.io/attack-navigator/enterprise/
- https://github.com/Cyb3rWard0g/HELK

THANK YOU