2023
Arab Security Conference
& Exhibition

SPEAKERS
2023

CYBER DEFENSE IN AN ERA CYBERWARFARES

Mohammad Khreesha

Senior Cybersecurity Director

Hunting Threats using Open-source Tools & MITRE ATT&CK

7th Round
17th - 18th of September 2023

www.arabsecurityconference.com

Agenda

- Introduction
- Threat Hunting Basics
- Reactive vs Proactive Hunting
- Threat Hunting Components
  - People
  - Processes/Procedures
  - Data Sources
  - Tools
- Threat Hunting Maturity Model
- Threat Hunting Frameworks
  - Pyramid of Pain
  - Cyber Kill Chain
  - MITRE ATT&CK
- Types of Threat Hunting
- Hunting Examples
- Practical Hunting
- Q&A

CYBER DEFENSE IN AN ERA CYBERWARFARES

Introduction

Introduction

Dwell time is the time between an attacker's initial penetration of an organization's environment and the point at which the organization finds out the attacker is there.

GLOBAL MEDIAN DWELL TIME, 2011–2020

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	—	—	—	—	320	107	186	184	141	73
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12

CYBER DEFENSE IN AN ERA CYBERWARFARES

Threat Hunting Basics

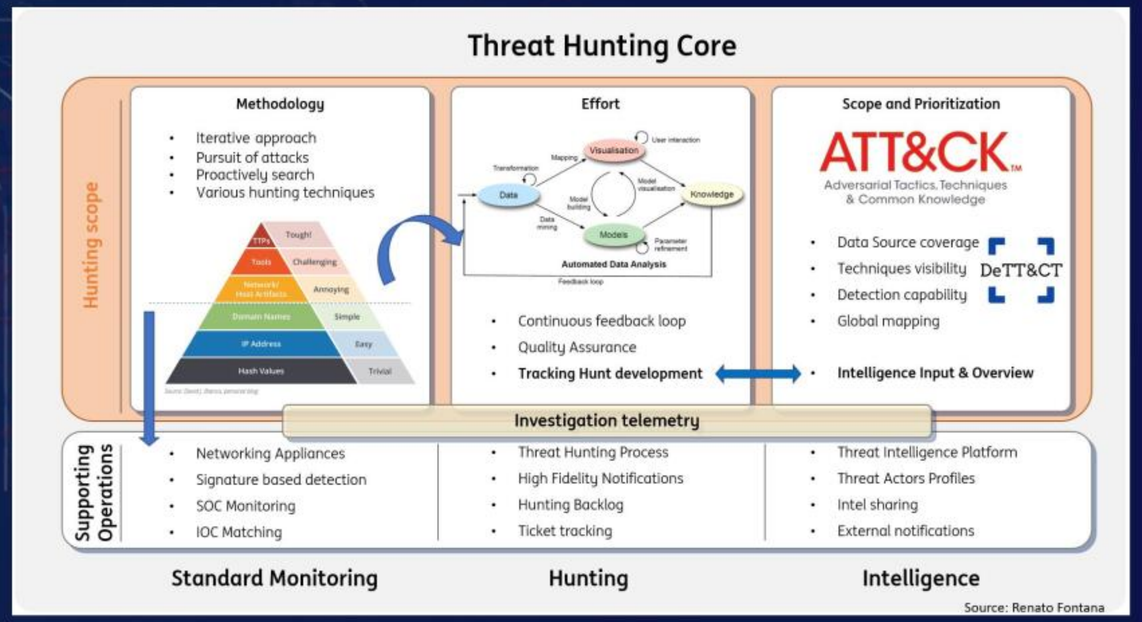
Threat Hunting

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

It is a drastic change from the traditional reactive approach of waiting for an internal system to notify about a breach.

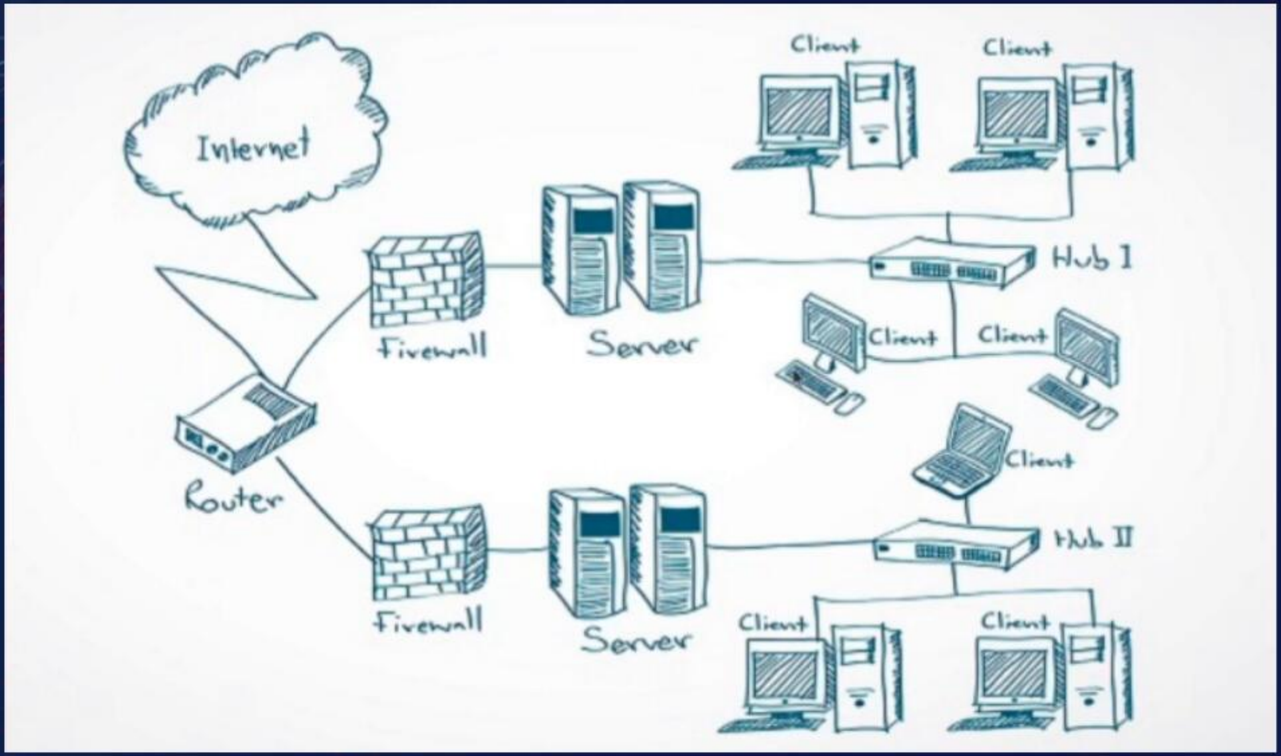
It aims to reduce the dwell time by identifying threats in a very early stage of the infection.

It is not a technology but an approach.

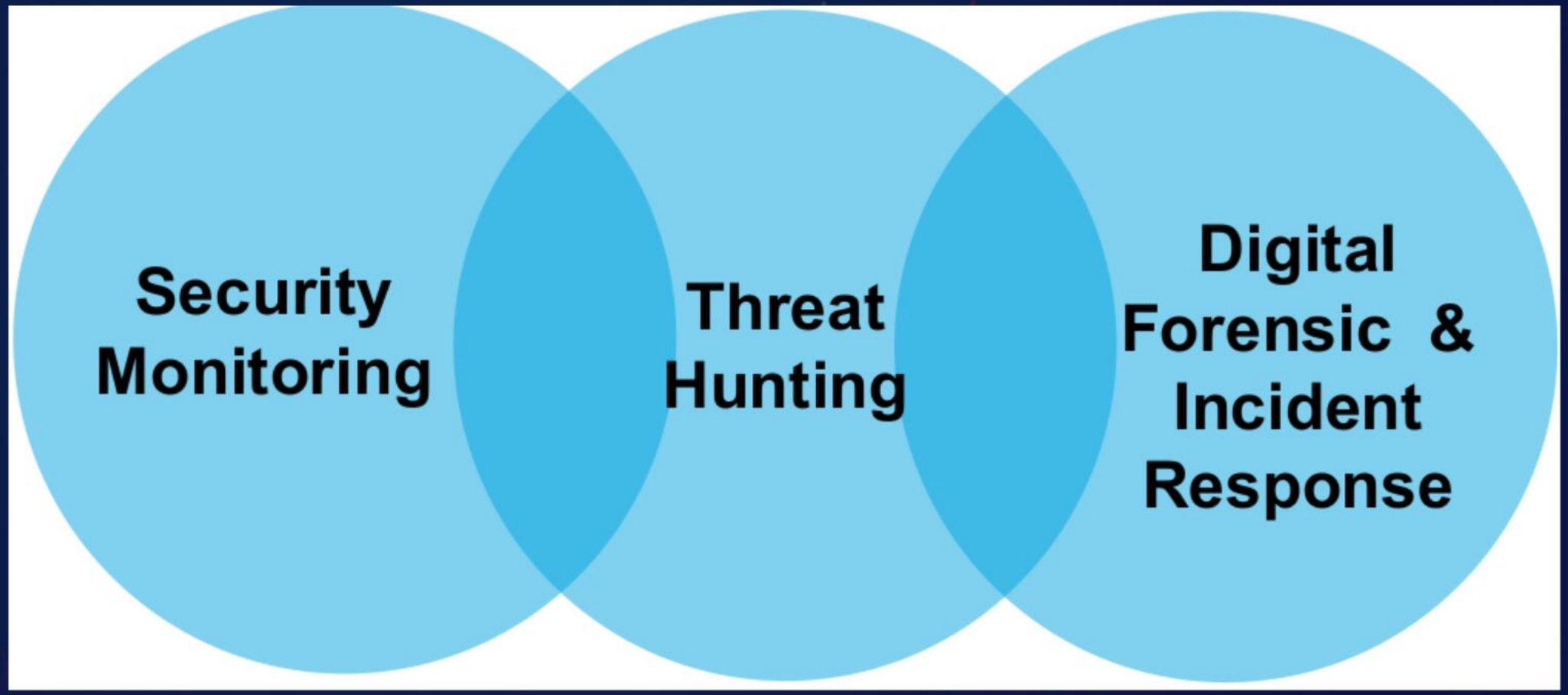


What to Hunt?

Network Data
Host Data
Application Data



Security Monitoring, Threat Hunting, & DFIR



Benefits of Threat Hunting

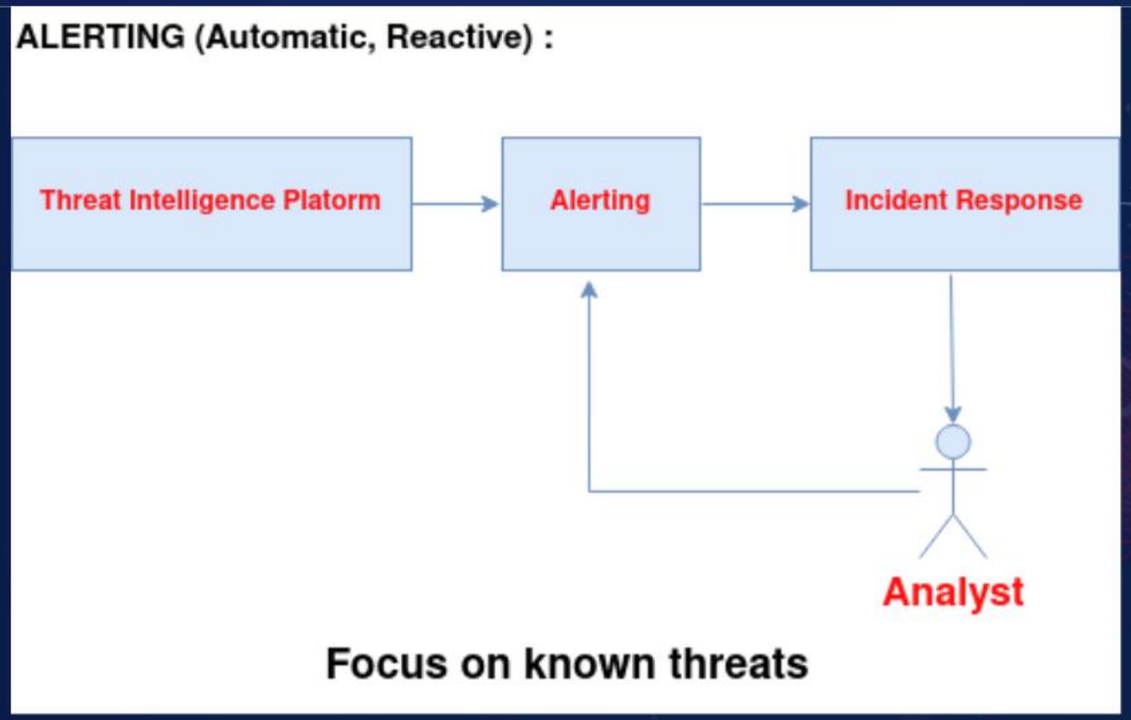
The importance of Threat Hunting

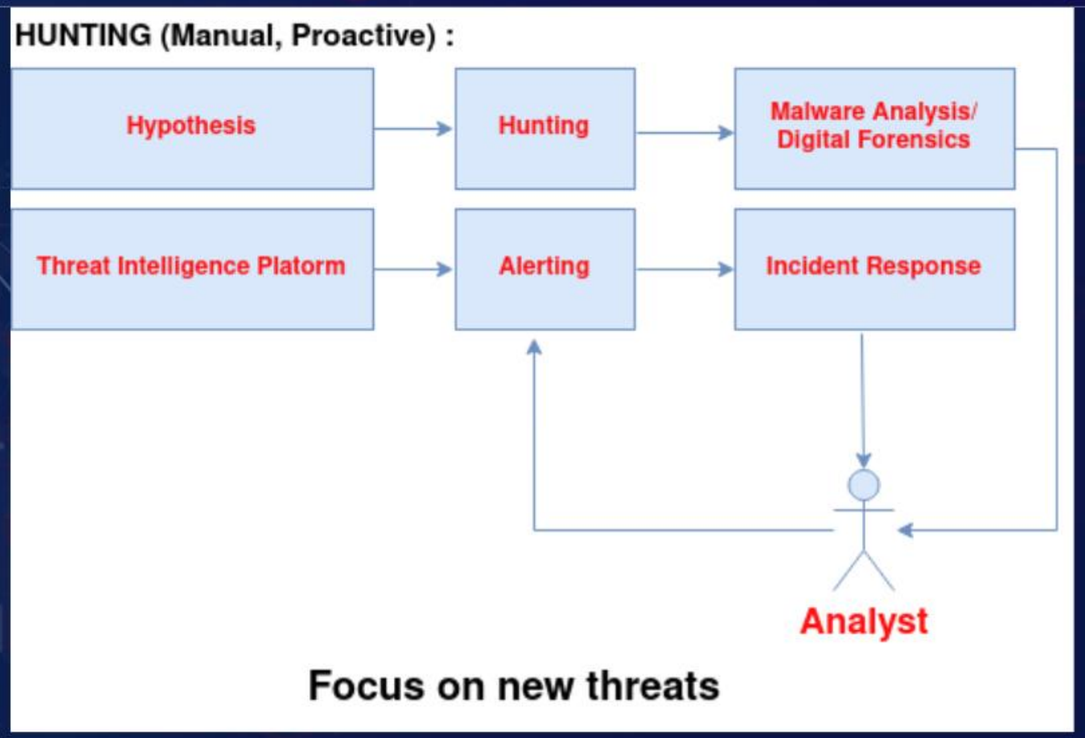
1. Detecting Security Issues Proactively.
2. Improving Security Posture Maturity Level Iteratively.
3. Identify Unknown Data Breaches and Attacks
4. Reduce Threat Invistigation Time
5. Detect Malicious Activities Early

CYBER DEFENSE IN AN ERA CYBERWARFARES

Reactive vs Proactive Hunting

Reactive vs Proactive (Alerting vs Hunting)





Incident starts when notification comes in:

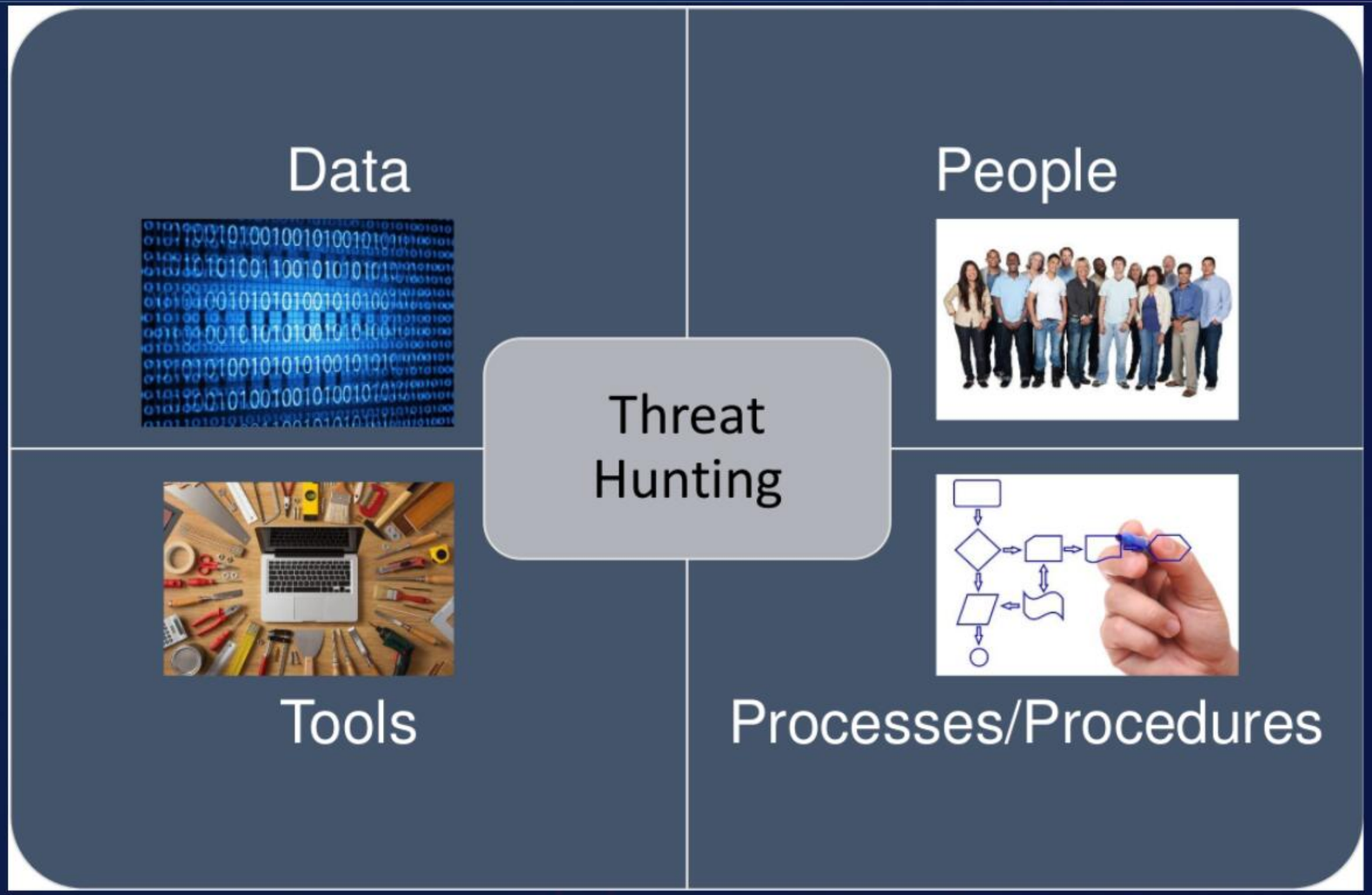
- Security system alert : (NIDS/NIPS/AV/SIEM)
- Call from governmental agency.
- User complaint / report.

Actively looking for incidents without waiting for an alert :

- Iterative search through data
- Using Threat Intelligence
- Using knowledge about attackers' TTPs.

Threat Hunting Components

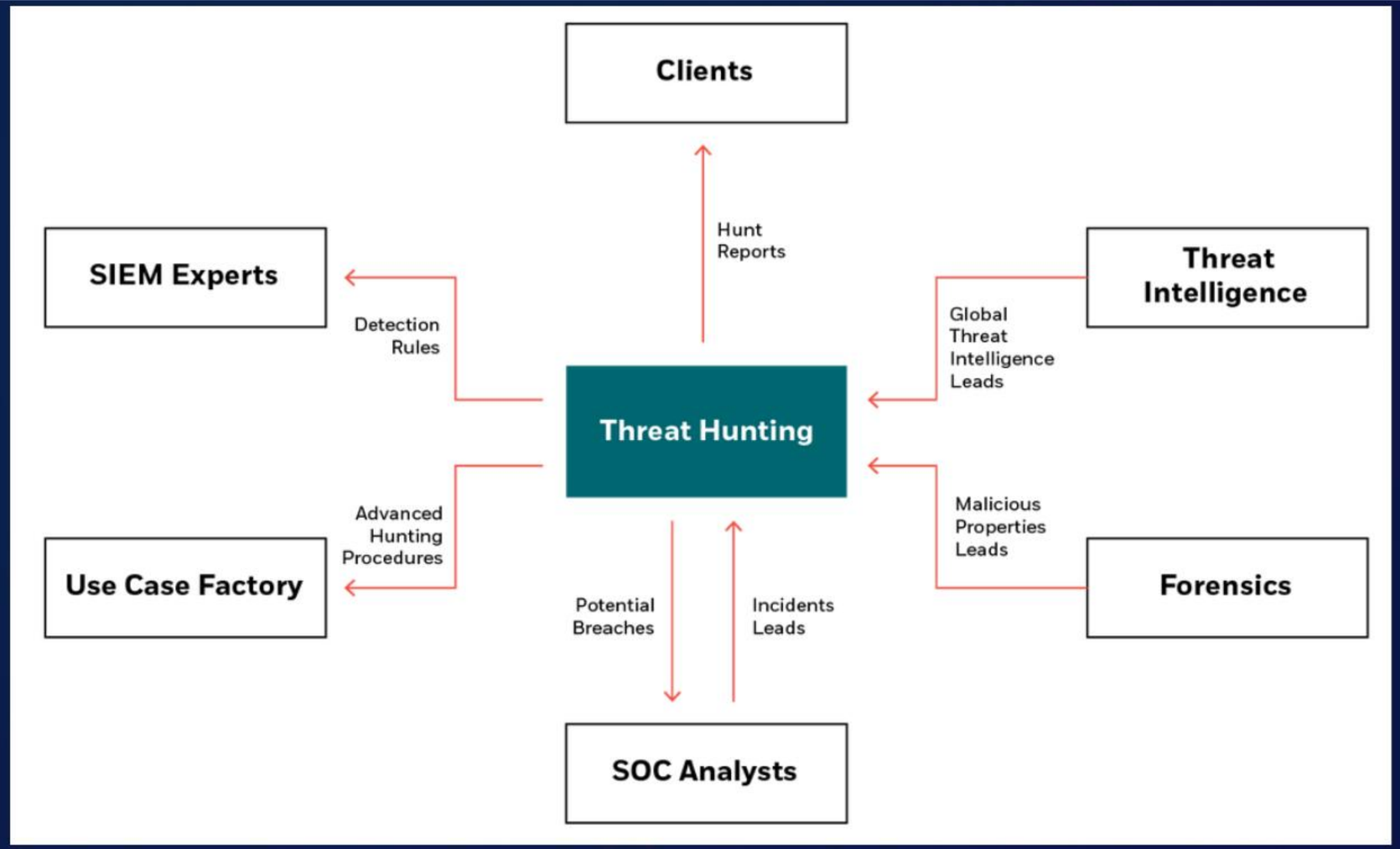
Threat Hunting Components



People - Threat Hunter Skills

Analytical Mindset: ability to generate and investigate hypotheses.
OS Architecture: knowledge of native OS security mechanisms.
Network Architecture: OSI model, TCP/IP, basic protocols.
Attack Lifecycle: attack stages and different events at any given stage.
Attack Methods/TTPs: Attacker mindset, techniques, tools.
Log Analysis: log sources and event types.
Network Forensics: reading and understanding packet capture.
Tools, used for hunting and data analysis: SIEM.

People – Who Should Involved in Threat Hunting?



Process - Threat Hunting Loop

Threat Hunting Loop – Creating Hypothesis

Threat Hunting begins with questions, such as “How would a threat actor infiltrate our infrastructure?”

These questions then need to be broken down into specific and measurable hypotheses that state :

- What is my crown jewel asset?
- What threats might be present in the network?
- How can we identified the threat actors?

Hypotheses cannot be generated by tools. It is defined by threat hunter mindset and knowledge based on the condition in each of their environment.

Example Hypotheses

Threat Actor:
An organisational threat assessment identified Lazarus Group as a high priority threat. Techniques attributed to this threat actor are detailed within MITRE’s ATT&CK Navigator.

We therefore hypothesis that if this threat actor is present in our network, we would be able to detect evidence of multiple techniques being deployed, in a manner consistent with their known attack paths.

Tool:
CTI and our situational awareness suggests that our organisation is currently vulnerable to a variant of the WannaCry ransomware, as SMBv1 is still used.

We therefore hypothesis that if our network is infected with WannaCry, we will see an increase in the rate of file renaming.

Technique:
Lateral Movement, via *Exploitation of Remote Services*, can be performed by exploiting vulnerability MS17-10. Specifically, this can be done via the Metasploit framework with a module that uses a Server Message Block (SMB) request of a specific size to attempt compromise.

We therefore hypothesise that we can see evidence of this technique being used by isolating this SMB request in our network logs.

Threat Hunting Loop – Investigate using Tools

Existing tools owned by organization, such as a SIEM or security analytic platform, EDR, TIP can be used to query the data, from basic searching to more advanced data science techniques, and also visualization can help threat hunters in identifying anomalies and anomalous patterns.

Threat Hunting Loop – Uncover New TTPs

The objective of testing a hypothesis created by the threat hunters in the first process in threat hunting, is to prove whether the hypotheses is prove or not proven.

Even if the hypotheses result is not proven, It does not necessarily mean that no malicious activity is present or the hunters create a wrong hypotheses.

It can be the current visibility in the organization is not enough or the tools that used by threat hunters is not good enough to help them to investigate the case.

In the future maybe this hypotheses can reveal a new TTPs that might be unknown before. The valid hypotheses then become the iterative process as a baseline.

Threat Hunting Loop – Inform and Enrich

Successful hunting process and then should be automated to make the efficient process for the threat hunters to reduce Threat Hunting team's time and to limit them from continuously repeating the same process.

This can be done in many ways, such scheduling a saved search, developing a new analytic within existing tools, or providing feedback to a supervised machine learning algorithm.

Threat Hunting Maturity Model

Relation between HMM and Hypothesis cycle	HM0 – INITIAL	HM1-Minimal	HM2-Procedural	HM3-Innovative	HM4-Leading
Data-Collection	Little or no data collection.	Moderate collection some types of data from a key point of infrastructure.	High collection of a specific types of data throughout IT environment.	High collection of a specific types of data throughout IT environment.	High collection of many types of data throughout IT environment.
Hypothesis-Creation	Respond to automatic alert from SIEM, IDS, Firewall, etc.	Review threat intel to create a new hypothesis.	Review threat intelligence & friendly intelligence to create a new hypothesis.	Review threat intelligence & friendly intelligence and manual cyber risk scoring (i.e. crown jewel analysis) to create a new hypothesis.	Review threat intelligence & friendly intelligence and automated cyber risk scoring to create a new hypothesis.
Tools & Techniques for Hypothesis	Alert Consoles, SIEM searches, no proactive investigation.	Utilized SIEM or log analysis tools to conduct basic search via full text or SQL - like queries.	Use simple tools and histogram to search and analysis data based on existing hunting procedures.	Leverage virtualization and graph search. Build new hunting procedure.	Advance virtualization and graph search. Published and automate new hunting procedure.
Pattern & TTP Detection	None	Integrate threat intel feed into automated alerting for basic match.	Build a library of effective hunting procedures and perform them on a regular schedule.	Build a library of effective hunting procedures and perform them frequently, data science (Machine learning).	Automated effective hunting procedure to continuously improve alerting capabilities & advance data science.

Threat Hunting Capability Maturity Model

Threat Hunting Capability Maturity Model	Level 1 INITIAL	Level 2 MANAGED	Level 3 DEFINED	Level 4 QUANTITATIVELY MANAGED	Level 5 OPTIMISING
People	▪ Existing SOC analysts ▪ Resourcing needs not known ▪ Training needs not known ▪ Performance not managed ▪ Lack of career development plan ▪ Normal systems behaviour not sufficiently understood	▪ Threat Hunting lead ▪ Informal view of resourcing ▪ Informal view of training ▪ Performance is qualitatively managed ▪ Career development informally managed ▪ Normal systems behaviour is moderately understood	▪ Dedicated threat hunters ▪ Formal recruitment plan ▪ Formal training plan ▪ Performance expectations defined with role profiles ▪ Formalised career development plan ▪ Normal systems behaviour is fully understood	▪ SOC analysts rotated for L&D ▪ Succession plans in place ▪ Training completion tracked ▪ Metrics utilised for team performance ▪ Mission critical systems identified	▪ Teams integrated across SOC ▪ Resourcing needs integrated ▪ Training needs integrated ▪ Improvement plans to address underperformance ▪ Situational awareness
Process	▪ Hypothesis generation is unstructured ▪ *Hunts occur ad-hoc, if at all* ▪ *Little or no data collected* ▪ Little understanding of anomalies indicative of malicious activity ▪ Abnormalities not routinely searched for	▪ CTI and Domain Expertise used to generate hypotheses and prioritisation by lead ▪ Hunts occur occasionally ▪ *Moderate data collection from key areas* ▪ *Basic threat feeds with IOCs utilised* ▪ Targeting of IOCs at bottom of POP	▪ Formal hunting process ▪ Hunts occur regularly ▪ *High data collection from key areas* ▪ *CTI and previous experience used to detect malicious activity* ▪ Targeting of IOCs in middle of POP	▪ Manual risk scoring e.g. Crown Jewels ▪ Hunts occur frequently ▪ *Moderate data collection from most of estate* ▪ *CTI tailored to organisation* ▪ Targeting of IOCs at top of POP	▪ Automated risk scoring e.g. machine learning ▪ Hunts occur continuously ▪ *High data collection from full estate* ▪ Hunt analytics and IOCs shared across community ▪ Automated TTP and campaign tracking
Tools	▪ *Reactive SOC tools* ▪ Little or no automation ▪ Little or no documentation produced	▪ Basic searching via text or SQL-like queries ▪ *Automatic matching of IOCs* ▪ Documentation using basic office suites	▪ 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	▪ Visualisation tools utilised, and analytics tested for effectiveness ▪ Library of hunt procedures automated on frequent schedule ▪ Dashboards utilised	▪ 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.

Threat Hunting Frameworks

Threat Hunting needs a framework that can be a baseline or foundation for the threat hunters when starting they hunting process.

The common framework in cyber security used by threat hunting are :

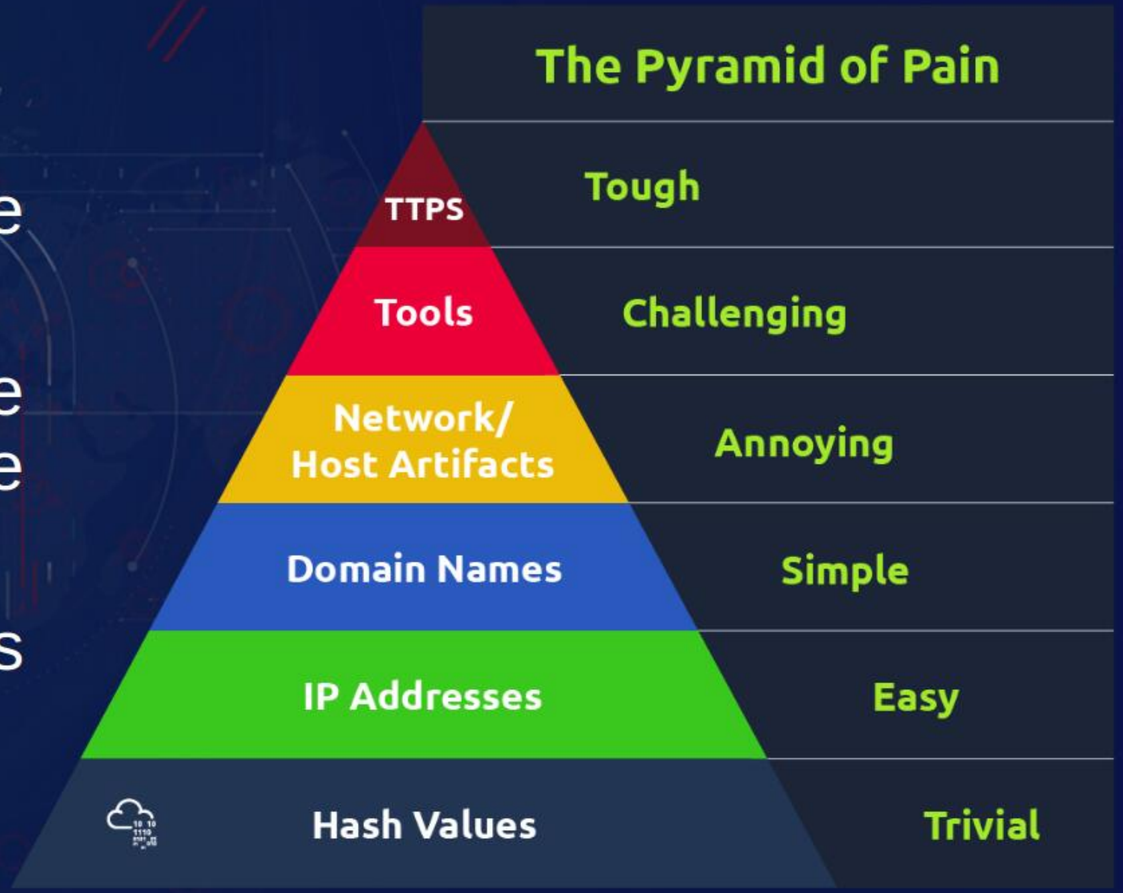
- Pyramid of Pain
- Cyber Kill Chain
- MITRE ATT&CK

Threat Hunting Frameworks - Pyramid of Pains

Pyramid of pain represents the usefulness of your intelligence

The higher of the stacks, the more adversaries have to expend for the resources.

It also indicates to gather the artifacts or threat intelligence from adversaries

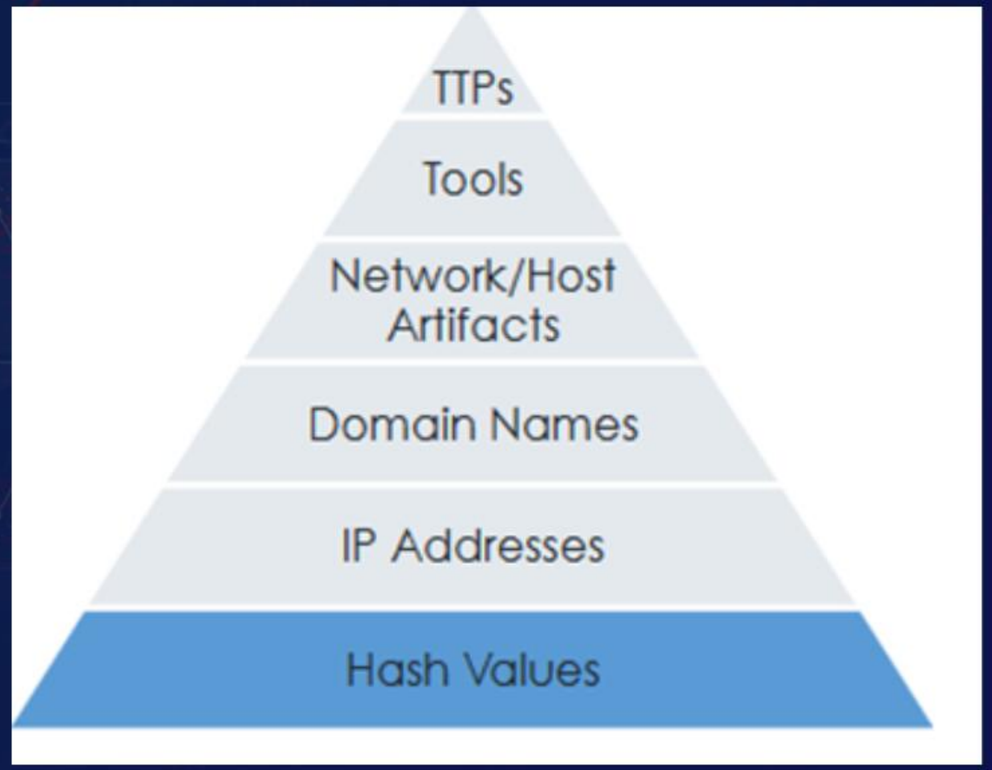


Pyramid of Pains - Hashes

Hash is so far the highest confidence level from artifacts collected or gathered from intel resources.

Hash is very easy to change. . Adversaries only need a little-bit effort to modify and create a new hash for their tradecraft.

It is maybe the reason why hash positioned in the bottom of the pyramid stack.



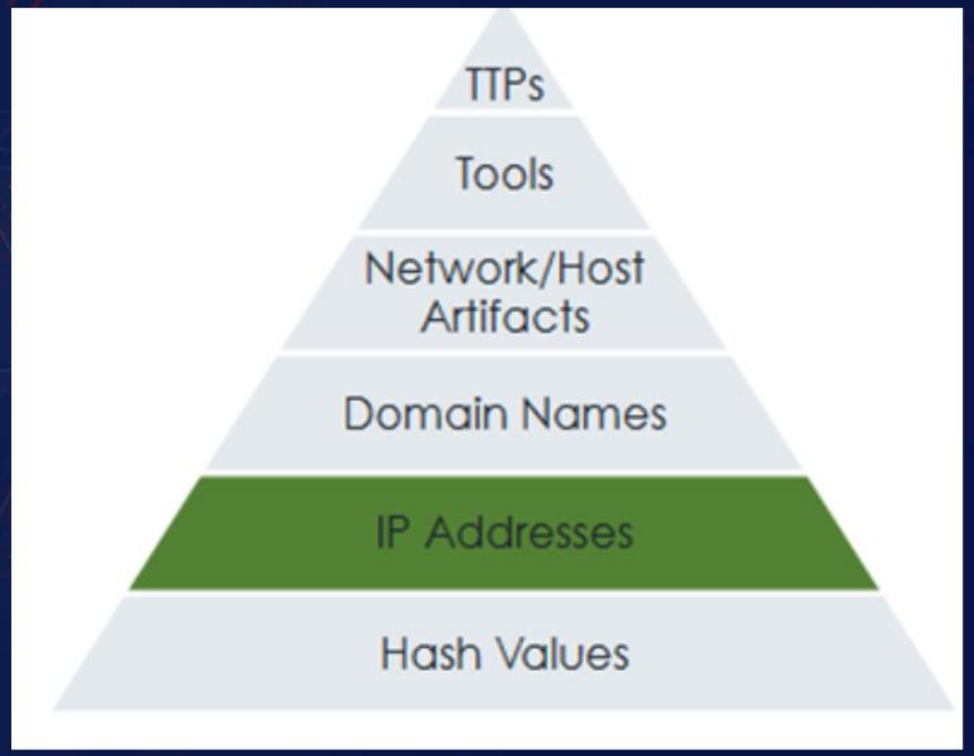
Pyramid of Pains – IP Addresses

Attacker mostly not using their real IP Address.

Adversary used VPN, Proxy, ToR, Compromised Server to hide from their real IP Address.

They can changed the IP address for their infra once it is blocked / blacklisted.

Only need some money and effort to move to the new IP for their infrastructure.

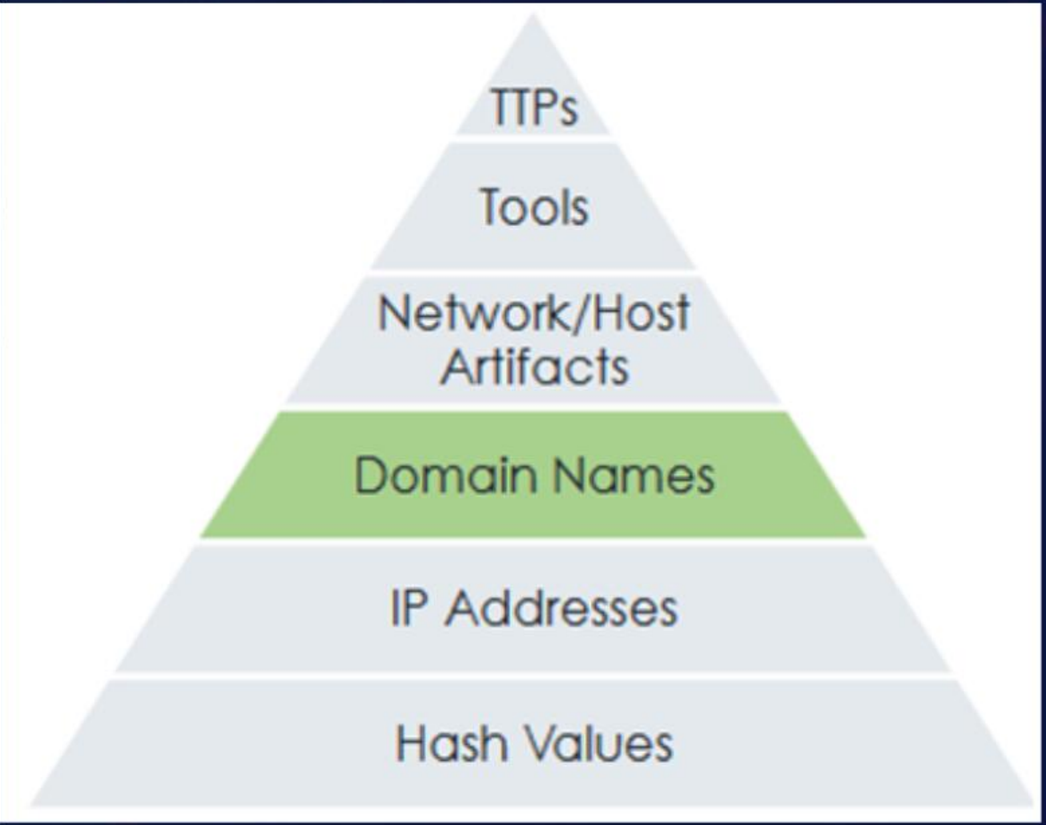


Pyramid of Pains – Domain Names

Almost easy as IP Address to change the domain name. But need more time (Domain propagation in DNS).

Need some registration, and for some reason they mostly hide the whois for domain privacy offered by domain registrars.

Need more money for this services.



Pyramid of Pains – Network/Host Artifacts

Network Artifacts :

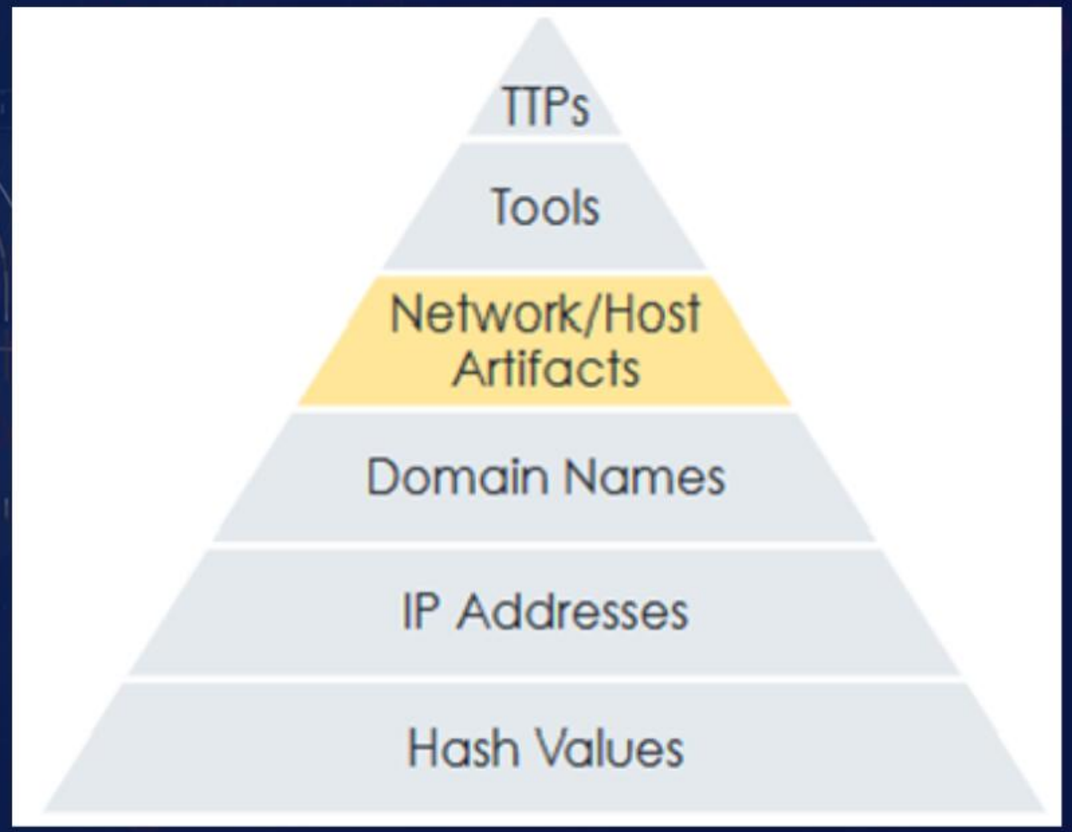
Indicators of activities performed by the adversaries on the network.

Anything communicated over the network by the adversary can be referred to as network artifact, which includes URI patterns, SMTP mailer values, HTTP user agent, and the like.

Host Artifacts :

Indicators of activities performed by the adversaries on the hosts.

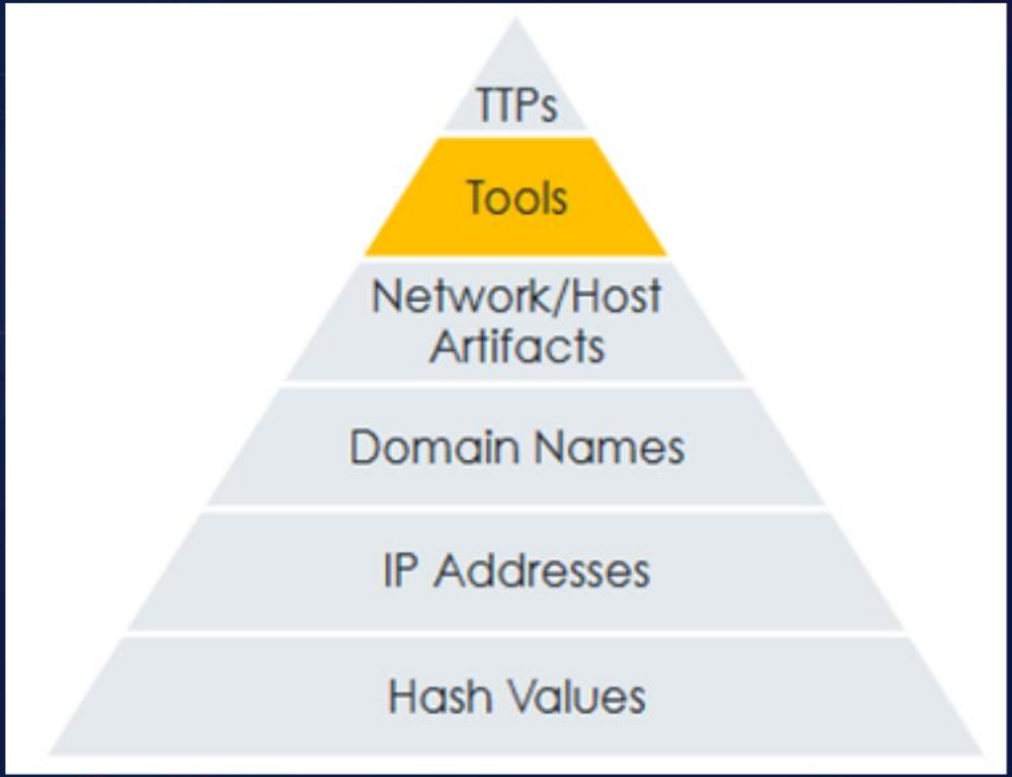
Artifacts like registry keys or values created by malware. Files or directories injected in specific locations, and the like are considered as host artifacts.



Pyramid of Pains – Tools

Software used by the adversary to accomplish their mission.

This can be include software designed to create malicious documents for spearphishing, backdoors used to establish CNC, or password cracking tools or other software that adversaries may want to use for post-exploitation activities.

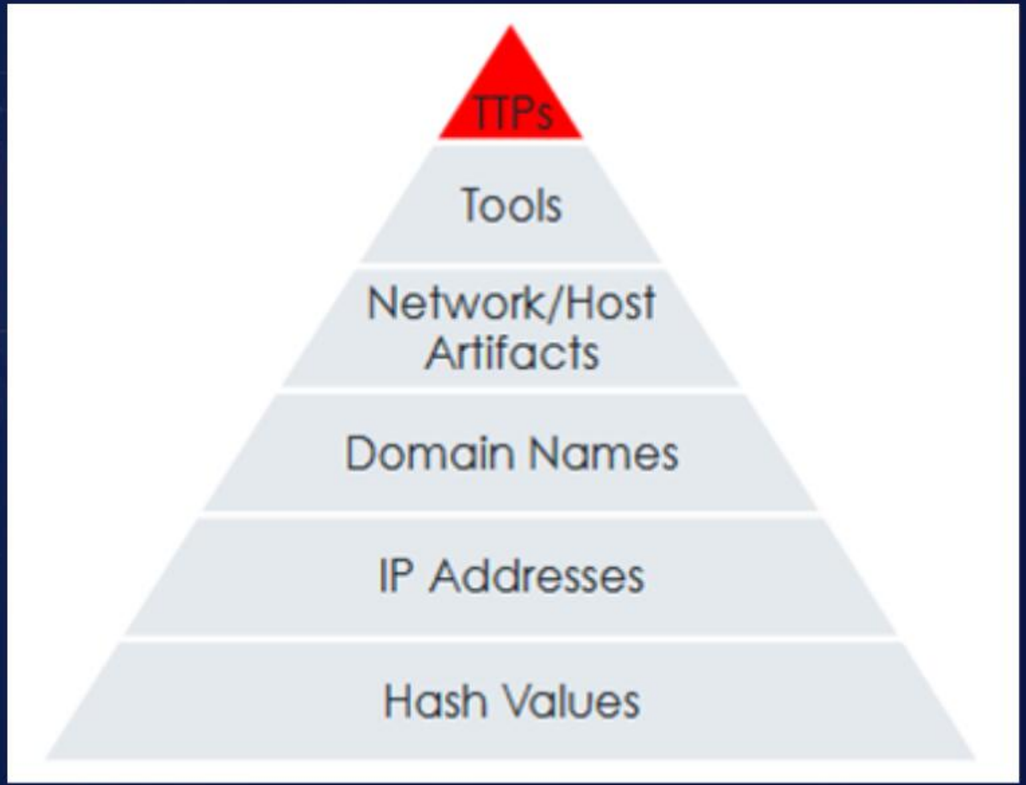


Pyramid of Pains – TTPs

The very Top Level in Pyramid of Pain, indicate the most painful.

Need to combine all the stack below to define the attacker Tactic, Technique and Procedures + Combining with Threat Intelligence to define attacker motivation and attribution.

If Blue Teamers, Defenders, and Threat Hunters can reach at this point for detection and response of the adversaries activities, the adversaries only have 2 options : Give Up on their mission or creating their TTPs from the scratch..



CYBER DEFENSE IN AN ERA CYBERWARFARES

Detection Approaches

Detecting Approaches

Possible attacker actions	IOC-based detection	Tool-based detection	TTP-based detection
Attackers can use Mimikatz or similar tools to dump credentials from memory	Looking for hashes (MD5, SHA1, SHA256) of Mimikatz and other similar tools executable files	Looking for files with predefined names or extensions, that created by Mimikatz and other similar tools. For example, Mimikatz export dumped Kerberos tickets to the files with .kirbi extension and WCE drop DLL with predefined name wceaux.dll	Looking for processes, that access lsass.exe memory or inject code to the lsass.exe memory Look for unsigned DLL libraries that loaded into lsass.exe
Attackers can use PsExec/WinExe or similar tools for remote execution and lateral movement	Looking for hashes (MD5, SHA1, SHA256) of PsExec/WinExe and other similar tools executable files	Looking for installation of services with well-known names (PsExec installs service with name PSEXESVC, WinExe installs service with WINEXESVC)	Looking for remotely installed services that spawn different processes
Malicious software need to communicate with Command and Control center / Attackers use external servers for accepting back connections from compromised hosts	Looking for communications with specific domains or IP-addresses, which are marked as an IOC or bad domains	Looking for User-Agent specific for some hacking utility or penetration testing frameworks Looking for communications with domains generated by a certain algorithm, which is typical for a specific hacking utility or penetration testing frameworks	Looking for connections with periodicity Looking for communications with randomly generated domains Looking for communications with newly registered domains

Cyber Kill Chain

1	Reconnaissance	Collecting information about at target (network enumeration, email addresses, social media, etc.)
2	Weaponization	Adding exploit to malicious code (PDF document, remote template injection, etc.)
3	Delivery	Getting the malicious code to the victim (email, USB, compromised website, etc.)
4	Exploitation	Exploiting a targeted victim with a vulnerability (software, user, etc.)
5	Installation	Installing malicious code onto the system (droppers, backdoors, remote access tools, etc.)
6	Command & Control	Communicating with adversary from exploited system (collect taskings for campaign progression)
7	Actions on Objective	Achieve campaign objects (exfiltration of data, gain further access into the environment, extortion, etc.)

MITRE ATT&CK Framework

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

MITRE ATT&CK™

MITRE ATT&CK Matrix (1)

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (40 techniques)	Credential Access (15 techniques)	Discovery (29 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (5)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (5)		Indirect Command Execution		Peripheral Device Discovery		Screen Capture	Web Service (3)		
				Server Software Component (4)		Masquerading (7)		Permission Groups Discovery (3)		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Process Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (4)		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (1)					
						Process Injection (11)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Signed Binary Proxy Execution (13)		Virtualization/Sandbox Evasion (3)					
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

MITRE ATT&CK Matrix (2)

Tactic : The What”	Technique : The How”
Reconnaissance	Active Scanning
Resource Development	Compromise Account
Initial Access	Drive by Compromise
Execution	Command and Scripting Interpreter

Cyber Kill Chain vs MITRE ATT&CK

The Cyber Kill Chain focuses on the stages of an attack, while the MITRE ATT&CK framework categorizes threats by the techniques and tactics used by attackers.

MITRE ATT&CK framework goes into significantly more depth on how each stage is conducted through ATT&CK techniques and sub-techniques.

MITRE ATT&CK is regularly updated with industry input to keep up with the latest techniques so defenders update their own practices and attack modeling regularly

MITRE ATT&CK Use Cases

ATT&CK can help you create a threat-informed defense.

Do what you can, with what you have, where you are:

- Detection
- Assessment and Engineering
- Threat Intelligence
- Adversary Emulation
- Threat Hunting

Data Sources - Endpoints

Type of Data	Description	Tools
Operating System logs	Useful Data sources. By Default capabilities for each OS.	Built in Function from OS
Process Activity	Process start, DLL libraries loading, Process install driver, Process perform code injection, Process open port for incoming network connections, connections, Process initiate network connection, Process create/change file, Process create/change registry key/value	Sysmon (Windows) Auditd (Linux) Osquery Endpoint Detection Response Operating System Logs
Volatile Artifacts	Temporary artifact collected from endpoint data sources for the purposes of hunting that might not touch the disk on the host Data Collection : Memory, Network Conn, Process Conn,	Winpmem, Comae, (for Collecton) EDR Volatility Google Rapid Response (GRR) Velociraptor
Non-Volatile Artifacts	Artifacts that resides on the endpoint / host disk. Data Collection : Prefetch, Amcache, Shimcache, MFT, Registry, bash_history, Task Scheduler	Brimorlabs KAPE Kansa FastIR Collector

Data Sources - Network

Type of Event	Description	Tools
Netflow	Network traffic flow metadata. NetFlow data is analyzed to create a picture of network traffic flow and volume. used as a network traffic analyzer to determine its point of origin, destination, volume and paths on the network	Silk Nfsen & Nfdump
Packet Capture	Packet Capture is a networking term for intercepting a data packet that is crossing a specific point in a data network. Once a packet is captured in real-time, it is stored for a period of time so that it can be analyzed, and then either be downloaded, archived or discarded.	Moloch, Tcpdump, Wireshark, tshark
Network IDS	A network-based intrusion detection system (NIDS) detects malicious traffic on a network. NIDS usually require promiscuous network access in order to analyze all traffic	Snort, Suricata Bro Commercial NIDS Product
Proxy Log	Proxy server logs contain the requests made by users and applications on your network. This does not only include the most obvious part : web site request by users but also application or service requests made to the internet (for example application updates).	Squid Commercial Proxy Product
DNS Log	One of the constantly re-occurring techniques is DNS-based activities like exfiltration via DNS *(Domain Name System)* or C2 *(Command and Control)* communication via DNS. Still, a lot of companies are lacking in DNS logging, missing DNS-based detection rules, or not aware of their own blindspots. Data collected : DNS Server, DNS Collected from Network, Host Based (Sysmon 10),	Passive DNS Log DNS Server

Types of Threat Hunting

Types of Threat Hunting

IOC Based Threat Hunting

Hypothesis Based Threat Hunting

Baseline Based Threat Hunting

Anomaly Based Threat Hunting

IoC Based Threat Hunting

Hunting based on IOC collected from Threat Intelligence

Checking whether the IOC is present in the environment

Checking on Specific Threat Actor or Specific Threat Intel Report

Hypothesis Based Threat Hunting

Creating a hypotheses for certain TTPs

e.g : Hypotheses for hunting on endpoint, hypotheses for hunting on network,

Leverage Framework such as MITRE ATT&CK Framework for creating hypotheses on TTPs of Threat Actor.

Defining specific asset for hunting (such as Crown Jewel Asset)

Baseline Based Threat Hunting

Detect something haven’t seen before based on baseline data in the environment

Needs larger set of data available about your infra for creating the baseline

Sometimes triggers lot of False Positives

Quite effective to spot changes in your infra

Anomaly Based Threat Hunting

Siting through the log data available for the threat hunters to spot irregularities that might be malicious

Additionally applying patterns on your infra

Quite useful in Fraud detection

Hunting Examples

Hunting Examples

Hunt description	Hunt search query (elasticsearch)
Suspicious processes spawned from MS Office applications	event_id:(1 OR 4688) AND (event_data.ParentOfParent:("*\\excel.exe" "*\\winword.exe" "*\\powepnt.exe" "*\\msaccess.exe" "*\\mspub.exe" "*\\outook.exe") OR event_data.ParentImage:("*\\excel.exe" "*\\winword.exe" "*\\powepnt.exe" "*\\msaccess.exe" "*\\mspub.exe" "*\\outook.exe")) AND event_data.Image:("*\\cmd.exe" "*\\powershell.exe" "*\\wscript.exe" "*\\cscript.exe" "*\\bitsadmin.exe" "*\\certutil.exe" "*\\schtasks.exe" "*\\rundll32.exe" "*\\regsvr32.exe" "*\\wmic.exe" "*\\mshta.exe" "*\\msiexec.exe" "*\\schtasks.exe" "*\\msbuild.exe")
Powershell download cradles	event_data.CommandLine:(*powershell* *pwsh* *SyncAppvPublishingServer*) AND event_data.CommandLine:(*BitsTransfer* *webclient* *DownloadFile* *downloadstring* *wget* *curl* *WebRequest* *WinHttpRequest* iwr irm "*internetExplorer.Application*" "*Msxml2.XMLHTTP*" "*MsXml2.ServerXmlHttp*")
Privilege escalation - Run whoami as System	event_data.Image:"*\\whoami.exe" AND (event_data.LogonId:0x3e7 OR event_data.SubjectLogonId:0x3e7 OR event_data.User:"NT AUTHORITY\\SYSTEM")
Suspicious LSASS SSP was loaded	event_id:4622 AND -event_data.SecurityPackageName:(*pku2u *TSSSP *NTLM *Negotiate *NegoExtender *Schannel *Kerberos *Wdigest "*Microsoft Unified Security Protocol Provider")
Possible logon session hijacking	event_data.Image:"*\\tscon.exe" AND (event_data.LogonId:0x3e7 OR event_data.SubjectLogonId:0x3e7 OR event_data.User:"NT AUTHORITY\\SYSTEM")
Using certutil for downloading	event_data.CommandLine:(*certutil*) AND event_data.CommandLine:(*urlcach* *url* *ping*) AND event_data.CommandLine:(*http* *ftp*)

Threat Hunting Case Study

Threat Hunters defined the Hypotheses and Start Hunting

Hypotheses 1 : User visiting malicious website from Phishing Email

Hypotheses 2 : User downloading malicious file after visiting the Malicious Website (Drive by Download maybe?

Hypotheses 3 : Malware Run on the User System after being downloaded

Hypotheses 4 : Malware doing persistence mechanism on Infected / Exploited Machine

Hypotheses 5 : Malware contacting Command and Control Server

Hypotheses 6 : Threat Actor exfiltrate Sensitive document to Command and Control Server

Hypotheses 7 : Sensitive Data Leaked on the Internet

Case Study – Hypothesis 1

Data Source for Hunting

Passive DNS Log, DNS Server Log, Proxy Log, NGFW Log, Sysmon Log, Email Log, Mail Security Gateway Log

Platform for Hunting

SIEM, Security Analytics Platform

Analysis and Enrichment Data

DNSTwist, Phishing Domain List, Threat Intelligence Feeds, VirusTotal, HybridAnalysis, URL / Domain Sandbox Analysis

Case Study – Hypothesis 2

Data Source for Hunting

Passive DNS Log, DNS Server Log, Proxy Log, NGFW Log, Sysmon Log

Platform for Hunting

SIEM, Security Analytics Platform

Analysis and Enrichment Data

Threat Intelligence Feeds, Alexa top 1M Domain, VirusTotal, HybridAnalysis, URL / Domain Sandbox Analysis, Blacklisted Domain Checker

Case Study – Hypothesis 3

Data Source for Hunting

Prefetch, Shimcache, Amcache, Process Running, Volatile Data (Memory), Sysmon, Auditd,

Platform for Hunting

SIEM, Security Analytics Platform, EDR

Analysis and Enrichment Data

File Hash of Process Executed, Parent-Child Process Analysis(SANS Find Evil Poster as Reference), Folder Location of Executables, Signed of Binary Files, VirusTotal, HybridAnalysis

Case Study – Hypothesis 4

Data Source for Hunting

ASEP (Auto Start Extensibility Points), Registry, Startup Services and Folder, Task Scheduler, Cron Job

Platform for Hunting

SIEM, Security Analytics Platform, EDR

Analysis and Enrichment Data

Signature Check, Autoruns Sysinternals, File Hash Check, Date of Creation

Case Study – Hypothesis 5

Data Source for Hunting

Netflow, Firewall Log, NGFW Log, IDS, Proxy Logs, Full Packet Capture, DNS Log

Platform for Hunting

SIEM, Security Analytics Platform, NDR, XDR,

Analysis and Enrichment Data

Date of Creation Domain, SSL Cert Attribute Checks, JA3 SSL Fingerprint, GeoIP Location Data, Threat Intelligence Feeds

Case Study – Hypothesis 6

Data Source for Hunting

Netflow, Firewall Log, NGFW Log, IDS, Proxy Logs, Full Packet Capture, DNS Log

Platform for Hunting

SIEM, Security Analytics Platform, NDR, XDR,

Analysis and Enrichment Data

Date of Creation Domain, SSL Cert Attribute Checks, JA3 SSL Fingerprint, GeoIP Location Data, Threat Intelligence Feeds

Case Study – Hypothesis 7

Data Source for Hunting

OSINT, Dark Web Search, Underground Forum, Threat Intelligence Feeds

Platform for Hunting

Threat Intelligence Platform

Analysis and Enrichment Data

Pastebin, Github, Honeypot

CYBER DEFENSE IN AN ERA CYBERWARFARES

MITRE ATT&CK Demo

MITRE CAR Examples

Use Case 1 : Process Spawn cmd.exe

MITRE Reference : CAR-2013-02-003

Use Case 2 : RDP Activities

MITRE Reference: CAR-2016-04-005

Use Case 3 : Stopping Windows Defensive Services

MITRE Reference: CAR-2016-04-003

Use Case 4 : Task Scheduler

MITRE Reference: CAR-2020-09-001

Use Case 5 : Credential Dumping via Windows Task Manager

MITRE Reference: CAR-2020-09-001

CYBER DEFENSE IN AN ERA CYBERWARFARES

MITRE ATT&CK Demo

ELK Scenario

ELK Scenario

An attacker was able to trick an employee into downloading a suspicious file and running it. The attacker compromised the system, and along with that, The Security Team did not update most systems. The attacker was able to pivot to another system and compromise the company. As a SOC analyst, you are assigned to investigate the incident using Elastic as a SIEM tool and help the team to kick out the attacker.

ELK Alerts Page

elastic

Search Elastic

Security Overview

Add integrations

Home
Alerts
Cases
Logs
Metrics
APM
Uptime
User Experience

Security
Overview
Alerts
Hosts
Network
Timelines
Cases
Endpoints

Management
Dev Tools
Integrations
Fleet
Osquery
Stack Monitoring
Stack Management

Search

KQL

Jan 8, 2022 @ 19:06:15.76 → Feb 12, 2022 @ 23:11:28.50

Refresh

+ Add filter

Data sources

Recent cases

No cases have been created yet. Put your detective hat on and start a new case!

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Detection alert trend

Stack by signal.rule.name

View alerts

220
200
180
160
140
120
100
80
60
40
20
0

2022-01-09
2022-01-16
2022-01-23
2022-01-30
2022-02-06

Unusual Process Execution - Temp
Component Object Model Hijacking
Whoami Process Activity
Malware Detection Alert

External alert trend

Showing: 19 external alerts

Stack by event.module

View alerts

18
16
14
12
10
8
6
4
2
0

2022-01-09
2022-01-16
2022-01-23
2022-01-30
2022-02-06

endpoint

Continue..

- **Who downloads the malicious file which has a double extension?**
- **What is the hostname he was using?**
- **What is the name of the malicious file?**

- **Search Query :**
  - **file.name : *.*.***

Full screen

Additional

	Reason	host.name	user.name	process.n...	file.name
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	cybery	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2	ahmed	Acount_detail...	Acount_details.pdf.exe
99	malware, intrusion_detection, file event with process msedge.exe, parent p...	DESKTOP-Q1SL9P2	ahmed	msedge.exe	Acount_details.pdf.exe

Continue..

- **What is the attacker's IP address?**

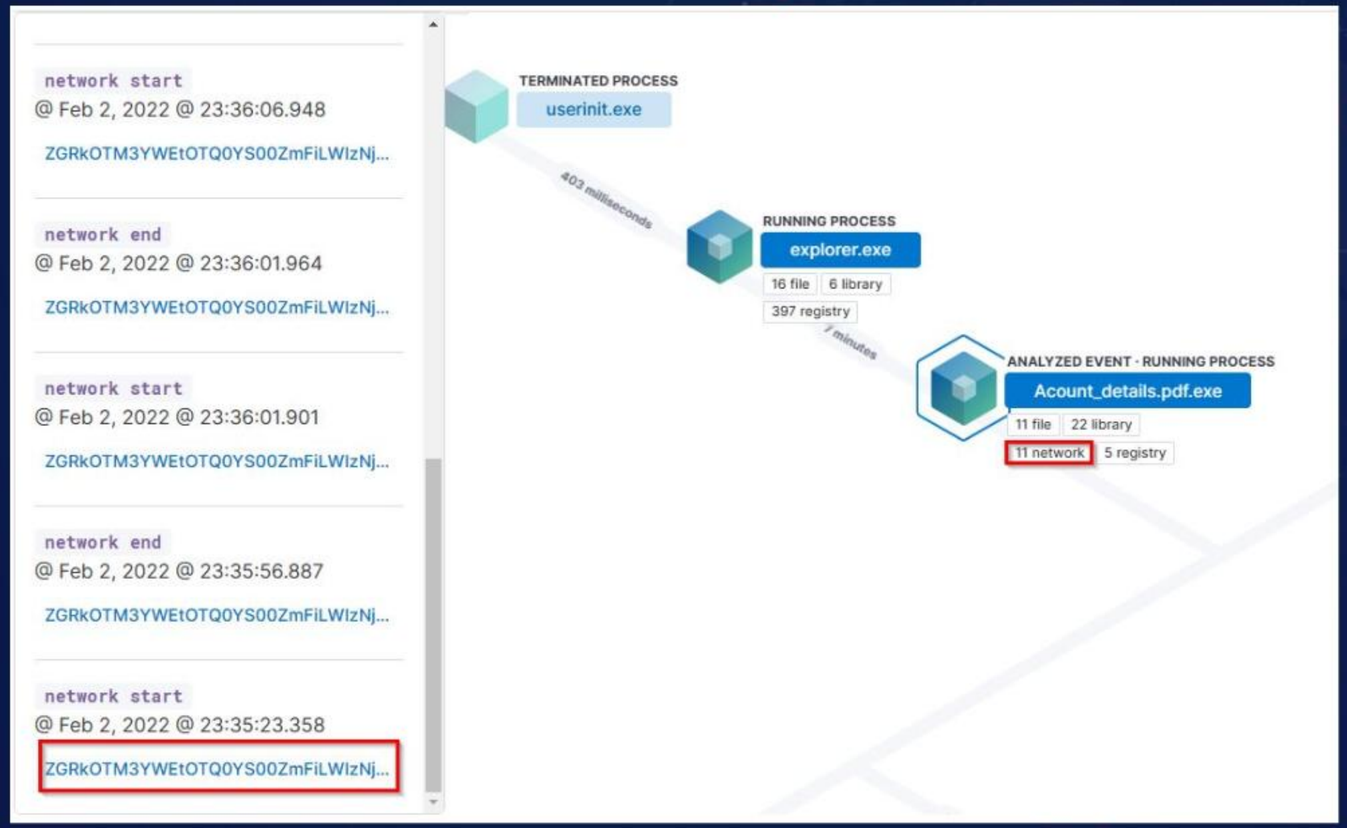
9 alerts | Fields | Columns | 1 field sorted | Full screen

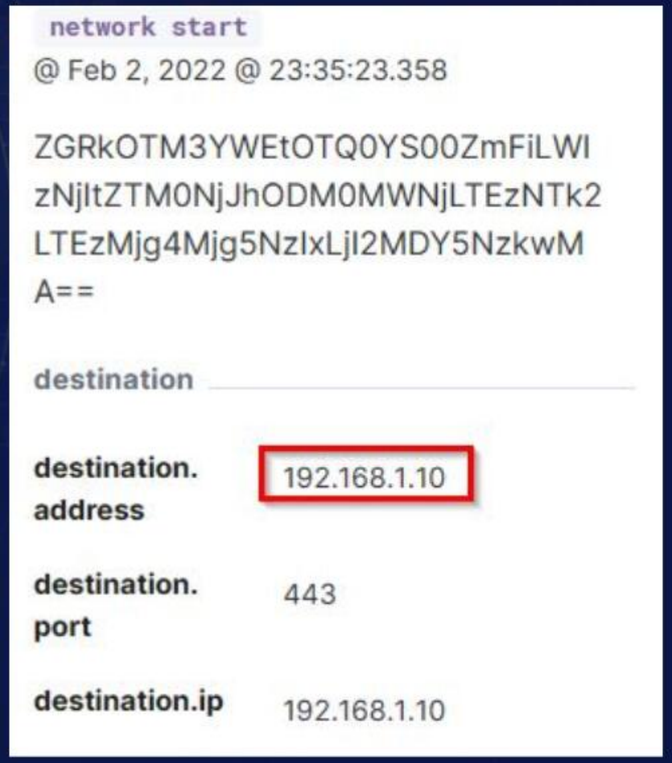
Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name
	Feb 3, 2022 @ 02:08:26.266	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:26.238	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:26.204	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:26.158	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:26.124	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	2022 @ 02:08:26.098	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	2022 @ 02:08:26.068	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:25.924	Malware Detection Alert	critical	99	malware, intrusion_detection, process event with process Acount_details.p...	DESKTOP-Q1SL9P2
	Feb 3, 2022 @ 02:08:25.884	Malware Detection Alert	critical	99	malware, intrusion_detection, file event with process msedge.exe, parent p...	DESKTOP-Q1SL9P2

Analyze event

Continue..

- **What is the attacker's IP address?**





Continue..

- **Another user with high privilege runs the same malicious file. What is the username?**

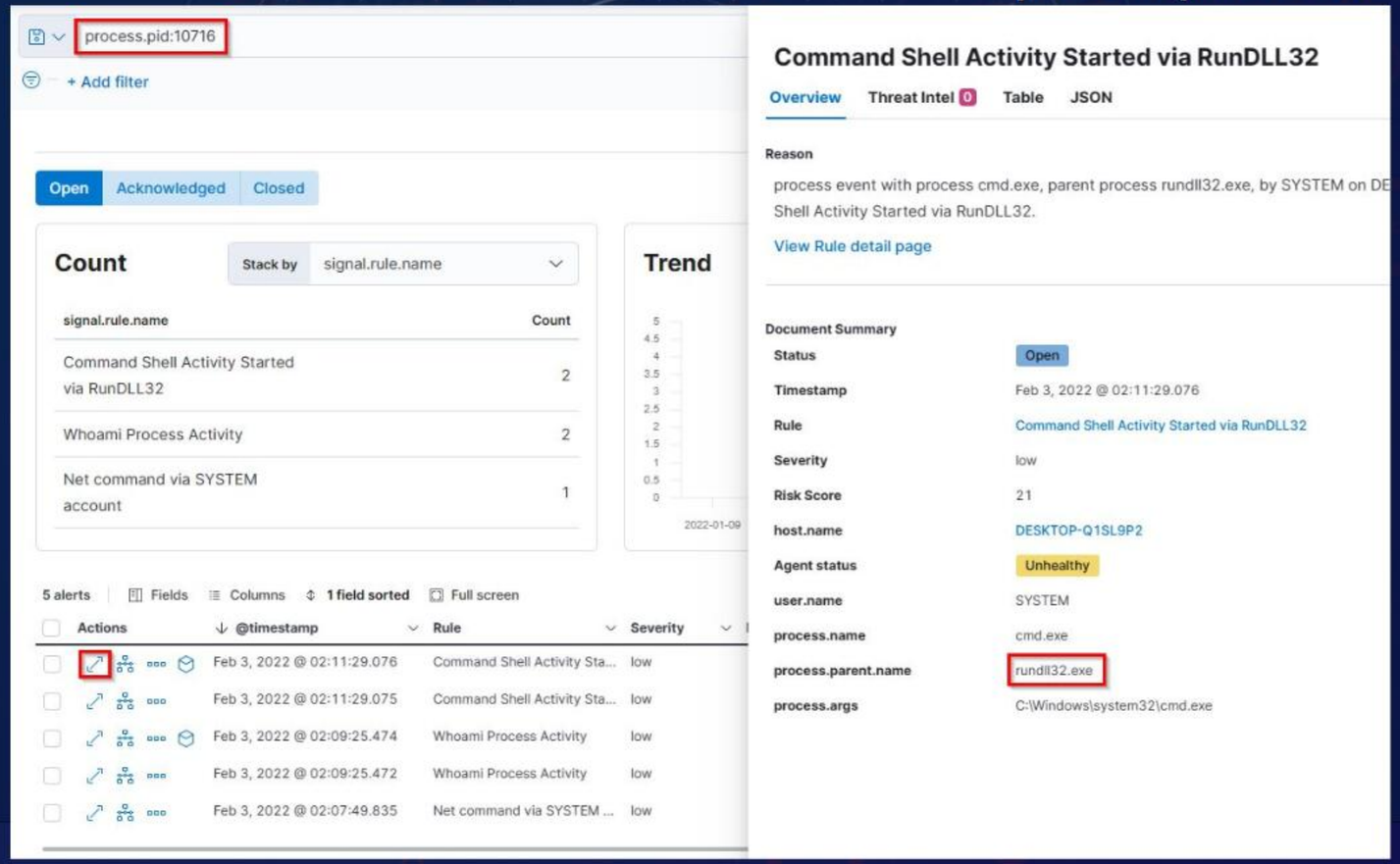
file.name:Account_details.pdf.exe

host.name	user.name	process.name	file.name
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	cybery	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	ahmed	Acount_details.pdf.exe	Acount_details.pdf.exe
DESKTOP-Q1SL9P2	ahmed	msedge.exe	Acount_details.pdf.exe

Continue..

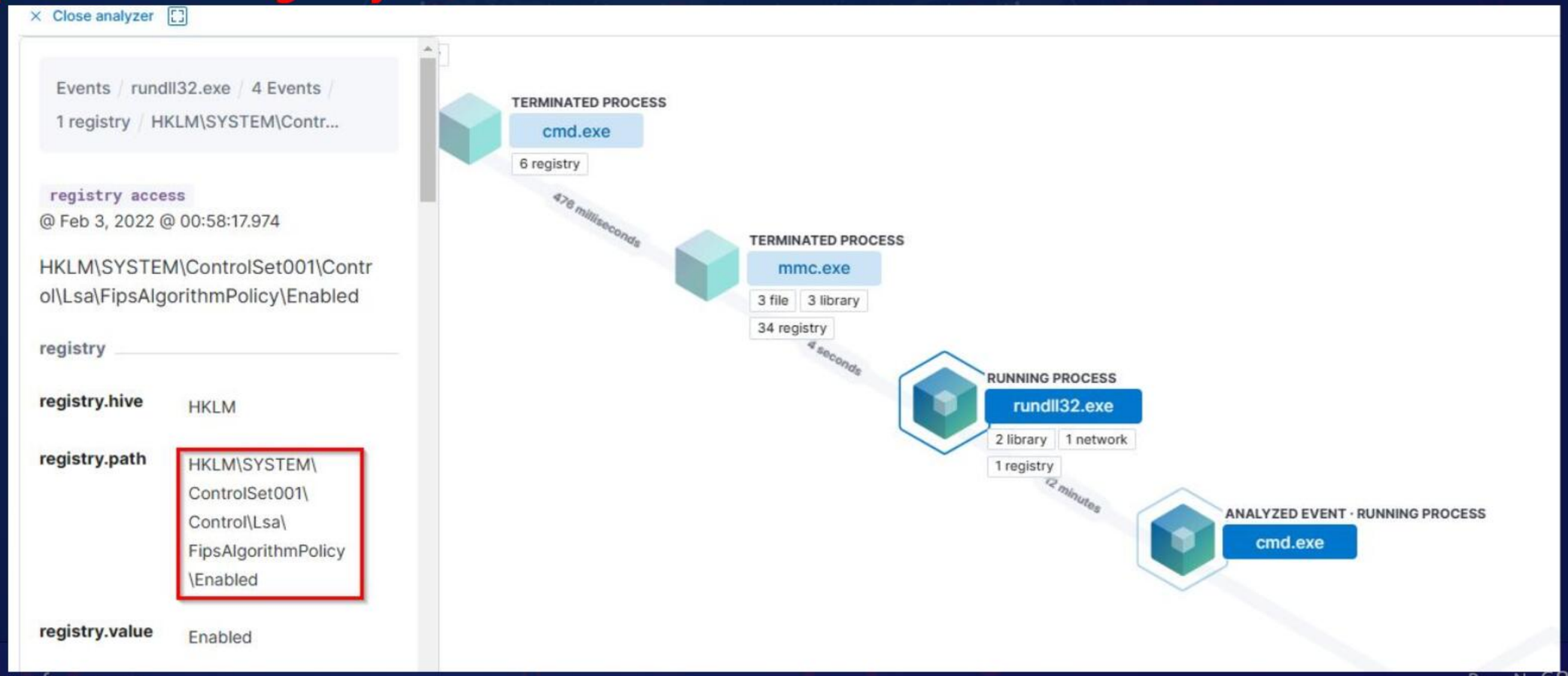
- **What parent process name spawns cmd with NT AUTHORITY privilege and pid 10716?**

process.pid:10716



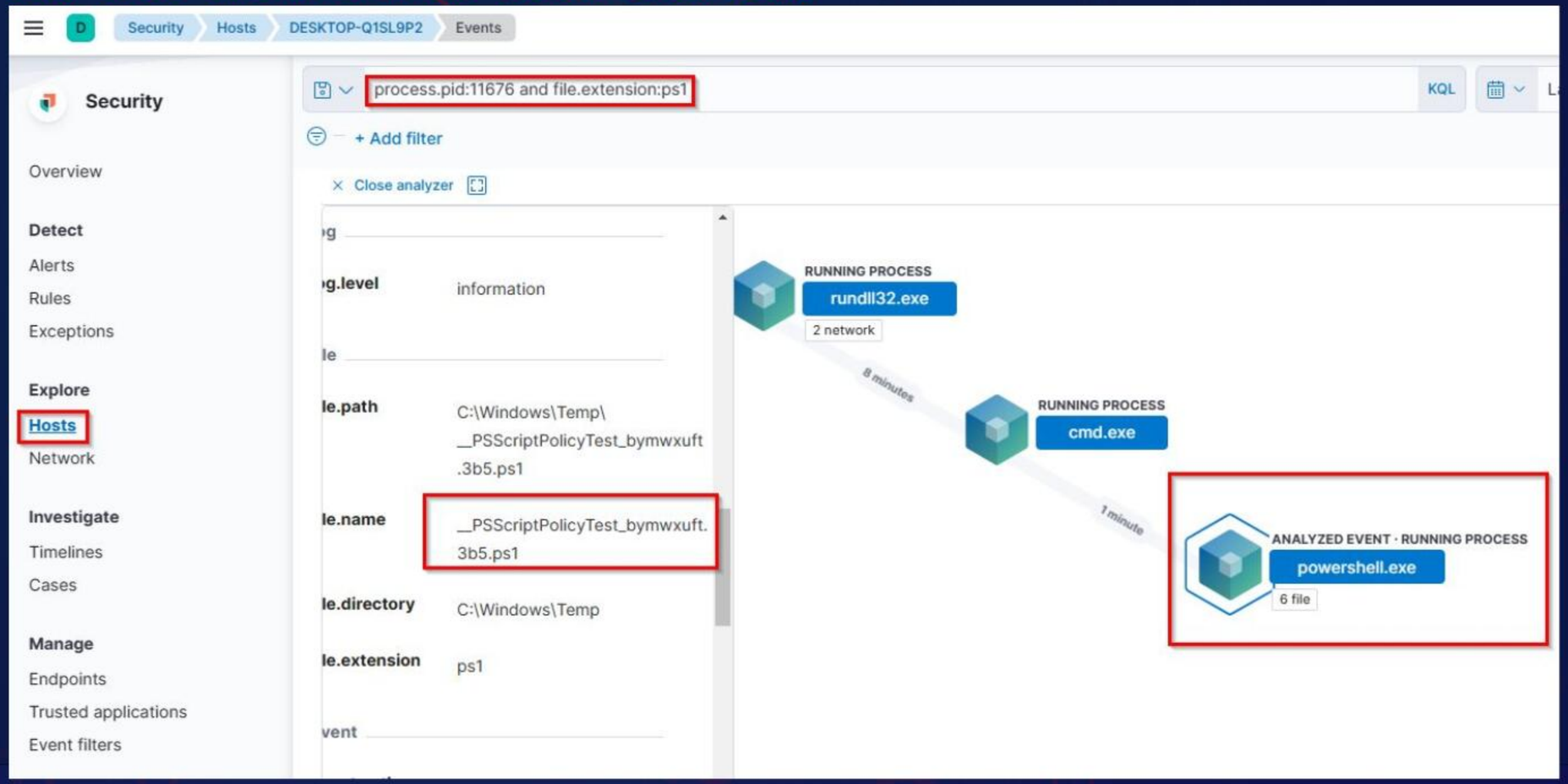
Continue..

- **The previous process was able to access a registry. What is the full path of the registry?**



Continue..

- **PowerShell process with pid 11676 created files with the ps1 extension. What is the first file that has been created?**



CYBER DEFENSE IN AN ERA CYBERWARFARES

Thanks

Mohammad Khreesha

Senior Cybersecurity Director