Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Knowing the unknown: The hunting loop

Sultan Saud Alanazi [1], *, Adwan Alowine Alanazi [2]

[1]*College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*
[2]*Department of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*

ARTICLE INFO

Article history:
Received 14 July 2021
Received in revised form
28 October 2021
Accepted 29 October 2021

Keywords:
Threat hunting
Threat response
Threat detection
Adversary detection
TTPs
Tactics
Techniques
Procedures
Indicator of compromise
IOCs

ABSTRACT

There are several ways to improve an organization's cybersecurity protection against intruders. One of the ways is to proactively hunt for threats, i.e., threat hunting. Threat Hunting empowers organizations to detect the presence of intruders in their environment. It identifies and searches the tactics, techniques, and procedures (TTP) of the attackers to find them in the environment. To know what to look for in the collected data and environment, it is required to know and understand the attacker's TTPs. An attacker's TTPs information usually comes from signatures, indicators, and behavior observed in threat intelligence sources. Traditionally, threat hunting involves the analysis of collected logs for Indicator of Compromise (IOCs) through different tools. However, network and security infrastructure devices generate large volumes of logs and can be challenging to analyze thus leaving gaps in the detection process. Similarly, it is very difficult to identify the required IOCs and thus sometimes makes it difficult to hunt the threat which is one of the major drawbacks of the traditional threat hunting processes and frameworks. To address this issue, intelligent automated processes using machine learning can improve the threat hunting process, that will plug those gaps before an attacker can exploit them. This paper aims to propose a machine learning-based threat-hunting model that will be able to fill the gaps in the threat detection process and effectively detect the unknown adversaries by training the machine learning algorithms via extensive datasets of TTPs and normal behavior of the system and target environment. The model is comprised of five main stages. These are Hypotheses Development, Equip, Hunt, Respond and Feedback stages. This threat hunting model is a bit ahead of the traditional models and frameworks by employing machine learning algorithms.

1. Introduction

In recent years, cyber-attacks have become more complex and increased in volume and targeting all industries. These attacks have a lasting impact on consumers, organizations, and their infrastructure. Organizations use various network devices and gateways, including switches, demilitarized zones, intrusion detection and prevention systems, SIEMs, and advanced firewalls to keep attackers out of the environment to ensure safety. Attackers can use sophisticated techniques (such as encoding packages and uses of Advanced Persistent Threats (APT)) to understand the internal information infrastructure and its workings. This can cause serious problems for organizations (Brooks, 2021). Some organizations based on customer/financial information deployment systems may disclose information in the form of credentials and personally identifiable information. The following intrusions and breaches indicate that the deployed system cannot handle the latest sophisticated intrusion technologies being used by attackers (Brooks, 2021; TMI, 2020):

- Naikon APT was active in the Asia Pacific region until 2015 but it was recently discovered that this was also active after that via a backdoor called "Aaria Body." This means that APT was active and operative for five more years without being detected.
- A report was released on June 25, 2020, about web skimming through an e-commerce platform. The

* Corresponding Author.
Email Address: s20200343@uoh.edu.sa (S. S. Alanazi)

https://doi.org/10.21833/ijaas.2022.01.002
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-8448-5273
2313-626X/© 2021 The Authors. Published by IASE.

report revealed that hackers embedded JavaScript code in EXIF files using Steganography.

- On July 24-25, 2020, the Garmin smartwatch network was made unavailable due to a ransomware attack on the infrastructure.
- On July 27, 2020, malware that had previously stolen data from over 62,000 devices was found to have been inserted into multiple Network Attached Storage (NAS) devices.
- The Taj Mahal APT was discovered on April 10, 2019, because a diplomatic mission's system was found infected with APT. This was a very standard malware with many other components that could cause serious damage
- In 2017, WannaCry ransomware infected hundreds of thousands of computers around the world, affecting more than 150 countries. The main and largest victim of the affected victim is the United Kingdom's National Health Service (NHS) (NAO, 2018).

Defending networks and information systems are drastically changed in this digital era. Security professionals do red and blue team exercises to test the security of their network infrastructure. Security operations centers are often used as a security barrier for multiple organizations. The SOC team is inherently effective as it has experts in specific areas of incident detection and response. If an organization doesn't have a security team, they usually outsource security to a third-party service provider (TMI, 2020). To ensure the security of the entire infrastructure, security teams must actively work on the network infrastructure to detect and respond to threats, which is ensured by threat hunting.

Threat hunting is a proactive cyber defense activity. It is "the process of proactively and iteratively searching through networks to isolate complex threats that circumvent existing security solutions" (Strom et al., 2017).

This differs from traditional threat management methods like firewalls, intrusion detection systems (IDS), malware sandboxes, honeynets, and SIEM solutions, which examine evidence-based data after a warning and are made aware of potential threats. Threat hunting was able to defend against the range of targeted attacks that were bypassing even the most innovative of security tools. Tools and methodologies can only take you so far unless you recognize their limitations and are constantly looking to improve on their capabilities. Threat hunting is all about identifying areas that your detection capability doesn't cover, then deriving use cases that can plug those gaps. Threat hunting complements and enhances your detection capability by ensuring that gaps are discovered and dealt with before an attacker has the chance to exploit them.

Threat hunting is mostly based on Presumptions of Compromise. Threat hunting focuses on quickly monitoring and analyzing logs using automatic and manual analysis to detect threats and anomalies in the organization's networks and systems. Fig. 1 shows a bid picture of the threat hunting process, where network threat intelligence sources, various logs, alerts from traditional IDS and firewalls, are providing input to the process, and verified intrusions are populated because of the process (Strom et al., 2017; Gunter, 2018; Daszczyszak et al., 2019).

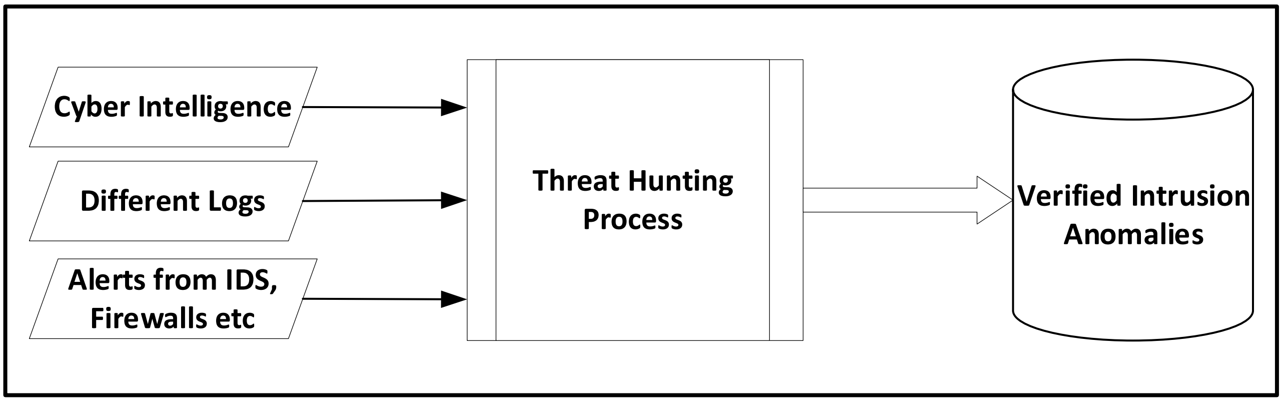


Fig. 1: Threat hunting process (Miazi et al., 2017)

Formal threat hunting techniques are aimed at detecting attacker tactics, techniques, and procedures (TTPs) in environments that are not yet detected by existing detection technologies like IDS, IPS, SIEM, anti-virus solutions. A more reliable way to characterize and search for tools and artifacts is to characterize and find the methods attackers use to reach their goals (Strom et al., 2017; Gunter, 2018). Due to the limitations of technology, these methods do not change frequently and are common among criminals. This study proposes a practical and rigorous machine learning-based threat detection model that uses using five stages: Hypotheses Development, Equip, Hunt, Respond, and Feedback; to identify the presence of an intruder. The system has been trained by providing datasets of different TTPs and the normal behavior of the target systems and network. The more detailed and granular dataset of TTPs, the most effective threats hunting it will be.

The rest of the paper has been divided into the literature review, proposed threat hunting model, discussion, and conclusion.

2. Literature review

Several threat hunting models have been researched and proposed over the years. Some of the most well-known and widely used among them are the diamond model for intrusion analysis, the SANS threat model, FireEye attack lifecycle, MITRE's ATT&CK™ framework, and Lockheed Martin Cyber Kill Chain.

2.1. Diamond model for intrusion analysis

Diamond Model is a novel intrusion model proposed in 2013 and shown in Fig. 2. This model shows that every invasion has an adversary, and he/she uses their abilities to achieve the goals set by him against a target infrastructure. The diamond model is divided into four steps: Adversary, infrastructure, victim, and ability (Fig. 2) (Caltagirone et al., 2013). This model differs from traditional threat hunting models and provides a different insight into threat hunting using threat intelligence and TTP. It can also be used to identify data sources that can be used for forensic investigation of an incident or attack (Caltagirone et al., 2013).

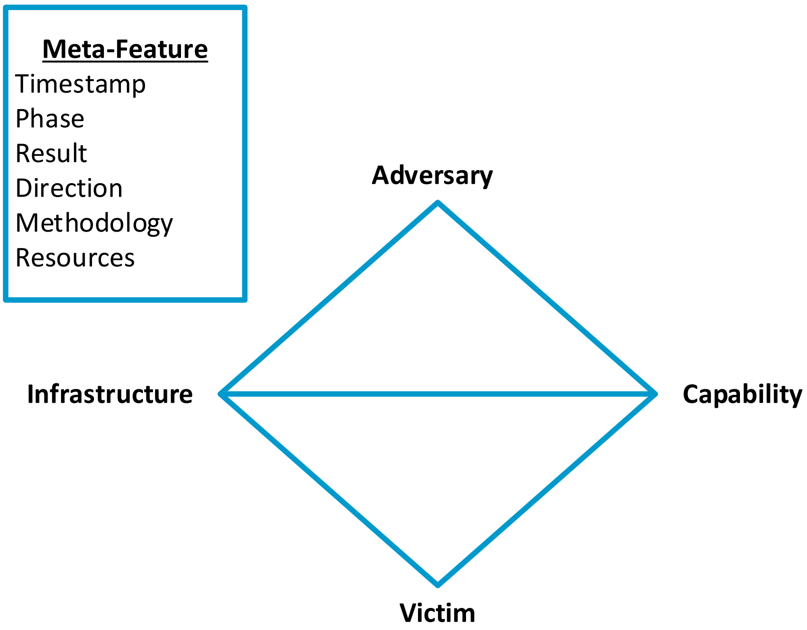


Fig. 2: The diamond model

The adversary and victim vertices in the Diamond are majorly focused on the intention of the attacker's group to launch an attack on one or more target victims. The adversary vertex does not associate the attack with a specific country, group or person, but takes into account the intent and purpose of the attack. In a threat hunting context, threat hunting can be focused on attacks within a specific sector.

The infrastructure vertex in the Diamond defines a set of systems that an attacker uses to launch attacks on specific victims. Indicator-based protection generates indicators from sources such as IP addresses and domain names. Both IP addresses and domain names act as indicators to attack a target infrastructure. For an attacker using a botnet, the attack infrastructure consists of all types of computers in the botnet. However, the top of the infrastructure doesn't have to be solely about indicators, but the threat intelligence also provides an insight into attacker behavior and way of performing the task. For example, an attacker may use encrypted DNS messages for command and control (C2) or covert channels. Infrastructure vertices can include IP addresses assigned to DNS servers and can include some TTP and C&C behaviors of attackers related to the infrastructure (Caltagirone et al., 2013).

The capability vertex is associated with the well-known tools and methods of intrusion used by attackers. This knowledge is usually obtained through threat intelligence. Threat Hunting uses this information to focus data collection on sources that can be helpful in revealing the attacker's tools and techniques (Caltagirone et al., 2013).

2.2. FireEye attack lifecycle

The FireEye attack lifecycle model (also known as "Red Team Operations") focuses on an actual attack scenario on the IT infrastructure environment. The Red Team uses any necessary non-destructive techniques to simulate the attacker's behavior and use of TTPs to achieve a mutually agreed set of objectives. The red team uses the adversary's TTPs, found in real-world incident response activities, to accurately simulate the active and secret attack methods used by real-world attackers. This can help an organization's security teams to assess their ability to identify, detect and respond to active attacks (Mandiant, 2019; FireEye, 2019).

After setting the goal, the red team began its first reconnaissance. Mandiant uses a combination of its own analytics repository and open-source intelligence tools and techniques (OSINT) to explore the target environment.

Mandiant tries to gain initial access to the target environment by exploiting security flaws and carrying out social engineering attacks. Mandiant uses techniques used by actual attackers to gain privileged access to target systems and infrastructure. After gaining access, the red team attempted to elevate permissions by providing command and control infrastructure to ensure and maintain persistence in the environment, just as attackers do (Mandiant, 2019; FireEye, 2019).

After establishing persistence and C&C in the environment, the red team will try to achieve its goals with the necessary non-destructive means. Fig. 3 shows the FireEye attack lifecycle.

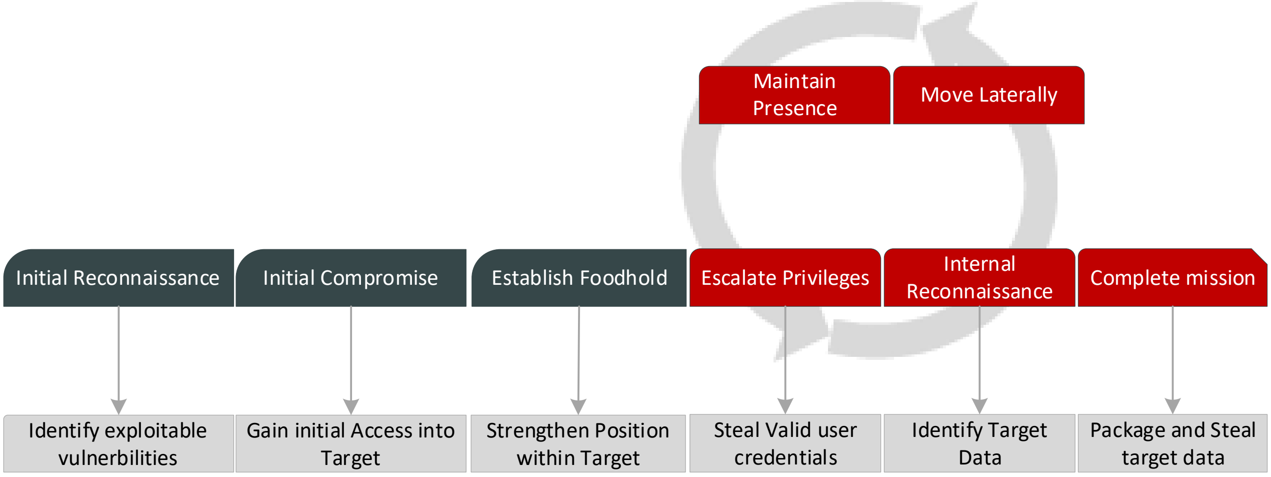


Fig. 3: FireEye attack lifecycle

2.3. Cyber kill chain

Lockheed Martin's Cyber Kill Chain includes a series of steps that can be traced from the early stages of a reconnaissance to the stage of data exfiltration. Kill chains help companies understand and eliminate ransomware, security vulnerabilities, and advanced persistent threats (APTs). The cyber kill chain structure is based on a military model originally designed to identify targets and prepare for an attack, then attack and destroy. Since its inception, the kill chain has been designed to better predict and detect internal threats, social engineering attacks, ransomware, and advanced attacks (Huang et al., 2021; Yadav and Rao, 2015).

The cyber kill chain model consists of 7 stages. The model defines the goals that the adversary must achieve. Blocking adversaries at any stage will break the chain of attacks thus making the systems and infrastructure secure. The attackers must fully pass through all the stages of success to be able to achieve their goals. This gives organizations a chance to stop them at any stage by breaking the chain. Attackers need to complete all the stages for success while the organizations only need to stop them at only one stage for being successful. Each intrusion attempt is an opportunity to learn more about the adversaries and reveal their strengths and weaknesses. The stages are of the Cyber Kill chain are Reconnaissance, i.e., to identify the targets by the attacker; Weaponization, i.e., attacker's preparation for the operation; Delivery, i.e., launching of the operation; Exploitation, i.e., gaining the access to the victim or target system or infrastructure; Installation, i.e., establishing a beachhead at the victim/target system; Command and Control (C2), i.e., deploy payload to remotely control the implants and system; and Actions on Objectives, i.e., achieving the attacker's final goal (Huang et al., 2021; Yadav and Rao, 2015). The stages are shown in Fig. 4.

2.4. MITRE's ATT&CK™ framework

Based on the Cyber kill chain, this framework offers deeper details about the attackers' TTPs. The behavior-based threat model of the MITRE ATT&CK framework is developed, tested, and refined using behavior-based analysis and detection functions by defining suitable security sensors and simulating attackers. This method is based on an understanding of the attacker's tactics, techniques, and procedures (TTP) in cyberspace to detect malicious activity. By interpreting the attacker's behavior at a suitable level of abstraction, organizations can learn about attackers TTPs and can deploy suitable sensors (both host and network-based) to analyze and detect attackers in different locations with high accuracy (Strom et al., 2017; Daszczyszak et al., 2019).

ATT&CK is a model and a framework for describing the behavior of attackers which are present in the organizations' network and system infrastructure. This model can be used to describe the attacker's behavior more accurately after refining and highlighting the general behavioral characteristics of the adversary or a combination of behaviors and goals that the attacker can achieve. The framework is very detailed and consists of seven stages. These are Reconnaissance, weaponization, Deliver, Exploit, Control, Execute and Maintain

(Strom et al., 2017; Daszczyszak, et al., 2019). The model is shown in Fig. 5.

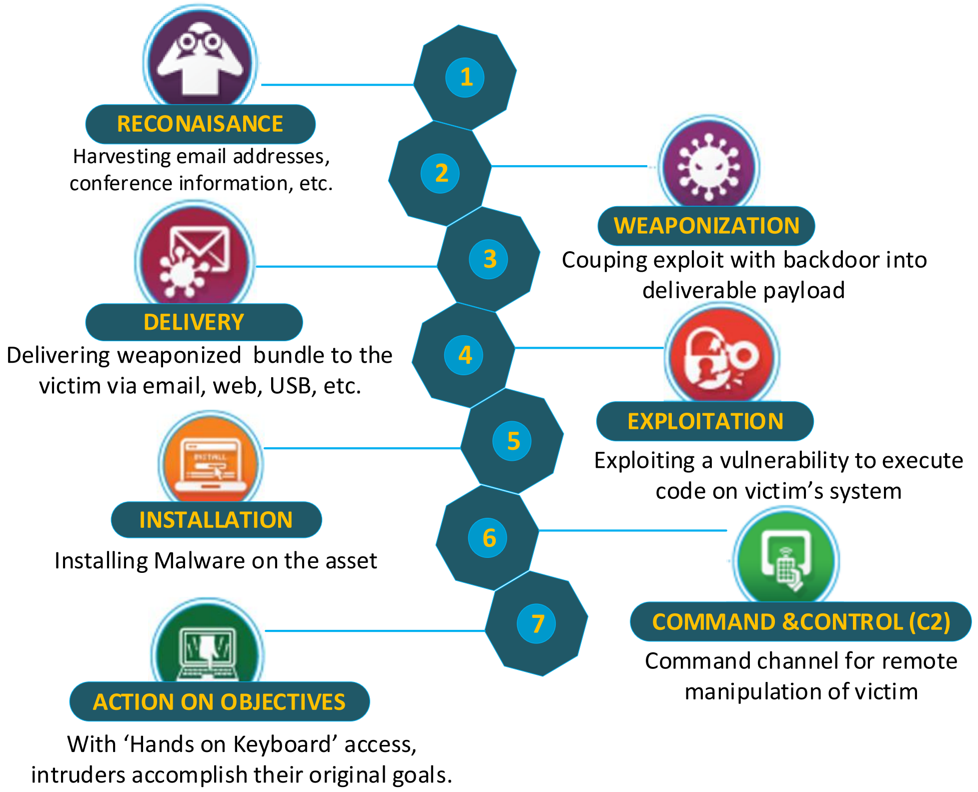

1
2
3
4
5
6
7
RECONAISANCE
Harvesting email addresses, conference information, etc.
WEAPONIZATION
Couping exploit with backdoor into deliverable payload
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
INSTALLATION
Installing Malware on the asset
COMMAND &CONTROL (C2)
Command channel for remote manipulation of victim
ACTION ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals.

Fig. 4: The cyber kill chain (Huang et al., 2021; Yadav and Rao, 2015)

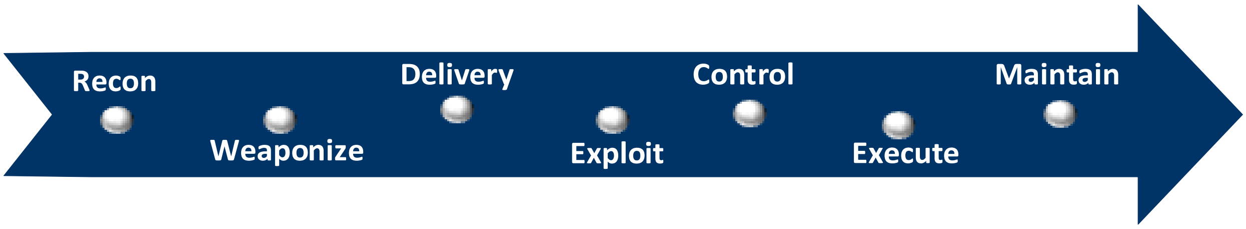


Fig. 5: MITRE's ATT&CK™ framework (Daszczyszak et al., 2019)

Formal threat hunting techniques are aimed at detecting attacker tactics, techniques, and procedures (TTPs).

2.5. SANS threat hunt model

The SANS threat hunt model consists of six successive stages: Purpose, scope, equip, plan review, execute, and feedback (Gunter, 2018) as shown in Fig. 6.

The details of these stages are as follows: 1) Purpose: Focus on the locations of the hunt, what to hunt for, and the outcomes of the hunt. 2) Scope: The scope determines the hunting plan and the information needed to perform the hunt. The scope is divided into two parts. The first part identifies the system to be tested, and the second part proposes a hypothesis. 3) Equip: This step focuses on the tools, techniques, and datasets, that are used for hunting. 4) Plan Review: At this stage, the actual results obtained from the preliminary hunt are compared with the expected ones. If the hunting goal is not achieved, the gaps/weaknesses will be identified and covered for the next hunting process. 5) Execute: This stage hunts for a real threat based on the analyzed data. The results are recorded in a summary report. 6) Feedback: This stage discusses the areas that need improvement across the entire hunting process model (Gunter, 2018).

3. Proposed model: The hunting loop

The difference between the model proposed in this article and the schemes above is that it tries to develop a general threat hunting method to identify hostile behavior that runs counter to normal behavior. It is based on Machine Learning algorithms that will consume necessary logs and datasets of the attackers' TTPs to identify the adversaries in the environment, respond to the adversaries being tracked, and improve the process through continuous feedback. The Proposed model is based on the identified TTPs by the MITRE ATT&CK framework (Fig. 8).

MITRE ATT&CK framework is a growing common reference for attackers to better understand the activity they saw during an intrusion. 11 strategies can be derived from the four cyber-attack lifecycles listed below and shown in Fig. 7.

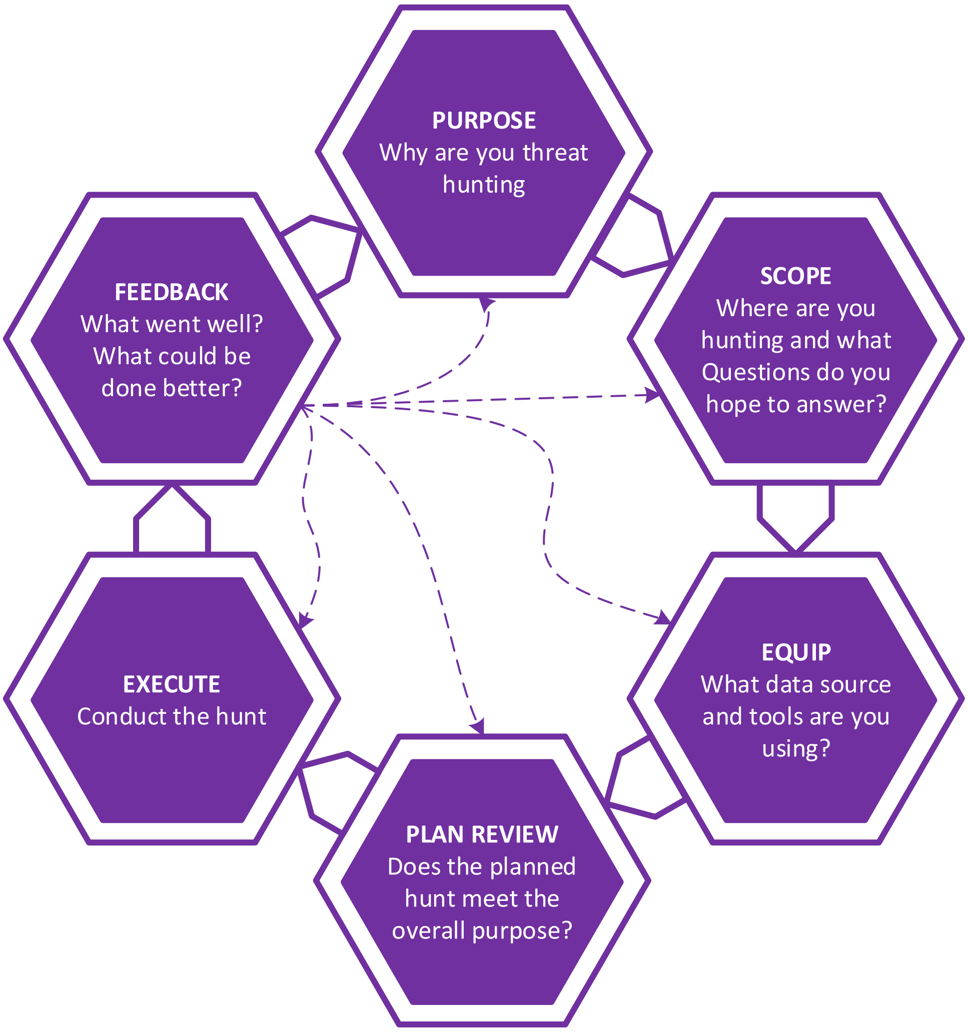
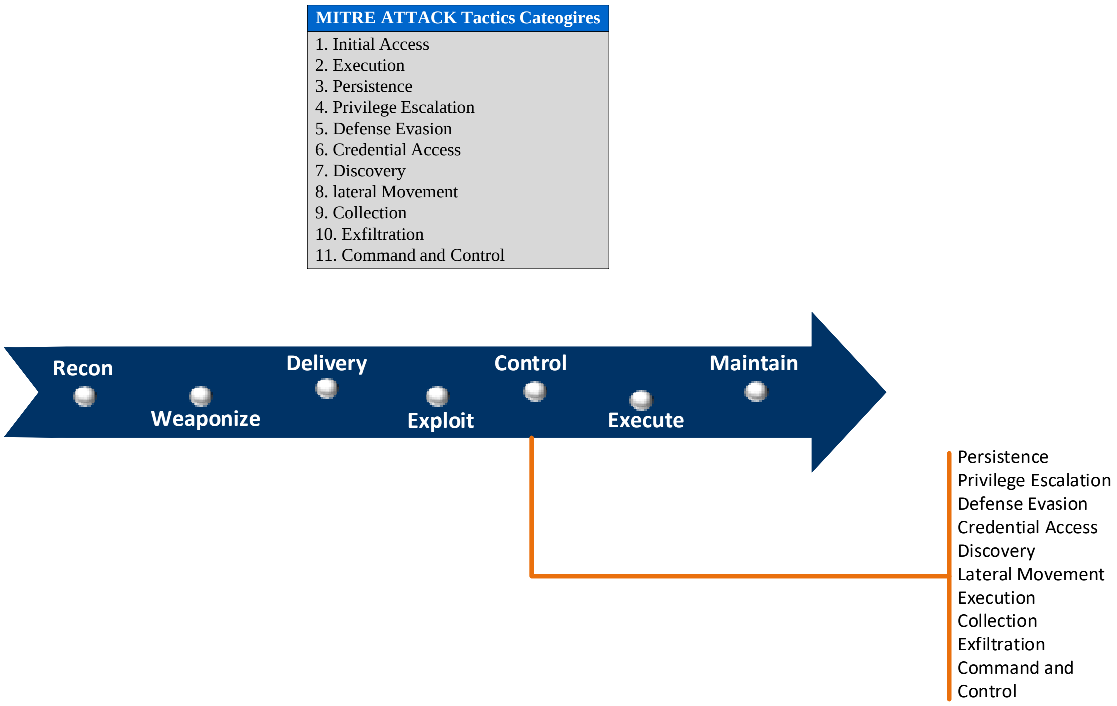

PURPOSE
Why are you threat hunting
SCOPE
Where are you hunting and what Questions do you hope to answer?
EQUIP
What data source and tools are you using?
PLAN REVIEW
Does the planned hunt meet the overall purpose?
EXECUTE
Conduct the hunt
FEEDBACK
What went well? What could be done better?

Fig. 6: SANS threat hunt model

Tactics, techniques, and procedures (TTPs) represent the highest level of abstraction within the MITRE ATT&CK framework. These are the tactical targets that the attacker identifies and sets in the target domain/infrastructure during the action. The ATT&CK tactical classes are listed here (Strom et al., 2017; Daszczyszak et al., 2019):

- Persistence–By accessing, manipulating, or changing the configuration of the system, the adversary becomes persistent in the system. Attackers usually need to maintain access to the system through interruptions, such as system restart, lost credentials, and other errors.
- Privilege Escalation–Through Privilege Escalation, the attacker can obtain a higher privilege level on the system or network because they need higher levels of privileges to perform specific tasks or operations, and they may need to use specific tools or processes in many places during remote operations.
- Defense Evasion–Technique that enemies can use to evade detection and other defensive structures.
- Credential Access–Technology and techniques that lead to access or control of credentials for systems, areas, or services used in the corporate environment.
- Discovery–Methods that an attacker can use to obtain information about a system or infrastructure.
- Lateral Movement–A technique that allows an attacker to access and control a system on a remote network. Typically, the next step in a lateral move is the remote execution and exploitation of the payload by the attacker.
- Execution–The technique of executing malicious code on a local or remote system
- Collection–A method used to identify and collect information (such as user credentials, banking information, intellectual property, sensitive documents, etc.) from the target network before it is exfiltrated to the C&C servers or attacker's destination.
- Exfiltration–Hacking techniques and ways that cause or help an attacker to delete files or information from the target network and then send to attackers' location or C&C servers, i.e., exfiltrated. This category also includes identification and searching of the locations on the networks and systems where attackers can find their required data or information.

- Command and Control–The methods and attributes of how the attacker interacts with the system under the control of the target network. An example of this is using a legal protocol (such as HTTP or DNS) to send C2 information.



MITRE ATTACK Tactics Cateogires

1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Defense Evasion
6. Credential Access
7. Discovery
8. lateral Movement
9. Collection
10. Exfiltration
11. Command and Control

Fig. 7: MITRE ATT&CK tactics categories

Fig. 8 summarizes the tactical classes and related techniques illustrated in the ATT&CK model. The table clearly categorizes each tactic and then their subcategories are mentioned that can be applied to that specific tactic.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account Enumeration	Application Deployment Software	Command Line	Commonly Used Port	Automated or Scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File System Enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data Compressed
AddMonitor		DLL SideLoading	Network Sniffing	Group Permission Enumeration	Logon Scripts	PowerShell	Custom application layer protocol	Data Encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local Network Connection Enumeration	Pass The Hash	Process Hollowing	Custom Encryption cipher	Data Size Limits
Edit Default File Handlers		File System Logical Offsets		Local Networking enumeration	Pass the ticket	Registry	Data Obfuscation	Data Staged
New Service		Process Hollowing		Operating System Enumeration	Peer Connections	Rundll32	Fallback Channels	Exfil Over C2 channel
Path Interception	Bypass UAC			Owner/ User Enumeration	Remote Desktop Protocol	Scheduled Task	Multiband Communication	Exfil over alternate channel to C2 Network
Scheduled Task	DLL Injection			Process Enumeration	Windows Management Enumeration		Multilayer encryption	Exfil over other network medium
Service File Permission Weakness	Exploitation of Vulnerability	Indicator Blocking on Host		Security Software Enumeration	Windows Remote management		Peer Connections	Exfil over physical medium
Shortcut Modification		Indicator removal from tools		Service Enumeration	Remote Services	Service Manipulation	Standard App Layer Protocol	From local system
BIOS		Indicator removal from host		Window Enumeration	Replication trough Removable Media	Third Party Software	Standard Non-App Layer Protocol	From network Resource
Hypervisor Rootkit		Masquerading			Shared Webroot		Standard Encryption Cipher	From Removable Media
Logon Scripts		Rootkit			Taint Shared Content		Uncommonly Used Port	Scheduled transfer
Master Boot Record		Rundll32			Windows Admin Shares			
Mod. Exist'g Service		Scripting						
Registry Run Keys		Software Packing						
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Fig. 8: MITRE ATT&CK adversary techniques/TTPs (Daszczyszak et al., 2019)

It is important for organizations and threat hunters to only consider those activities and TTPs that are organizational-specific. For example, a healthcare provider can list potential attacker actions to access PHI and underlying servers. Organizations should also strive to find TTPs that have not been found before, rather than TTPs that have been found in some way. Leave it to the automatic detection system.

These potential attacker activities and techniques are very difficult to detect through traditional manual methods. But if there is some automated technique that can differentiate and identify these activities based on the normal system/infrastructure operations, then this can be detected.

For this purpose, this paper proposed a Threat hunting model called "The Hunting Loop" based on Machine learning that will automate the process of detecting the attacker's activities. Following is the depiction of the proposed threat hunting model "The Hunting Loop." The model is composed of five primary stages-Hypotheses Development, Equip, Detect, Respond and Feedback-that works in an iterative fashion. The hunting loop is depicted in Fig. 9.

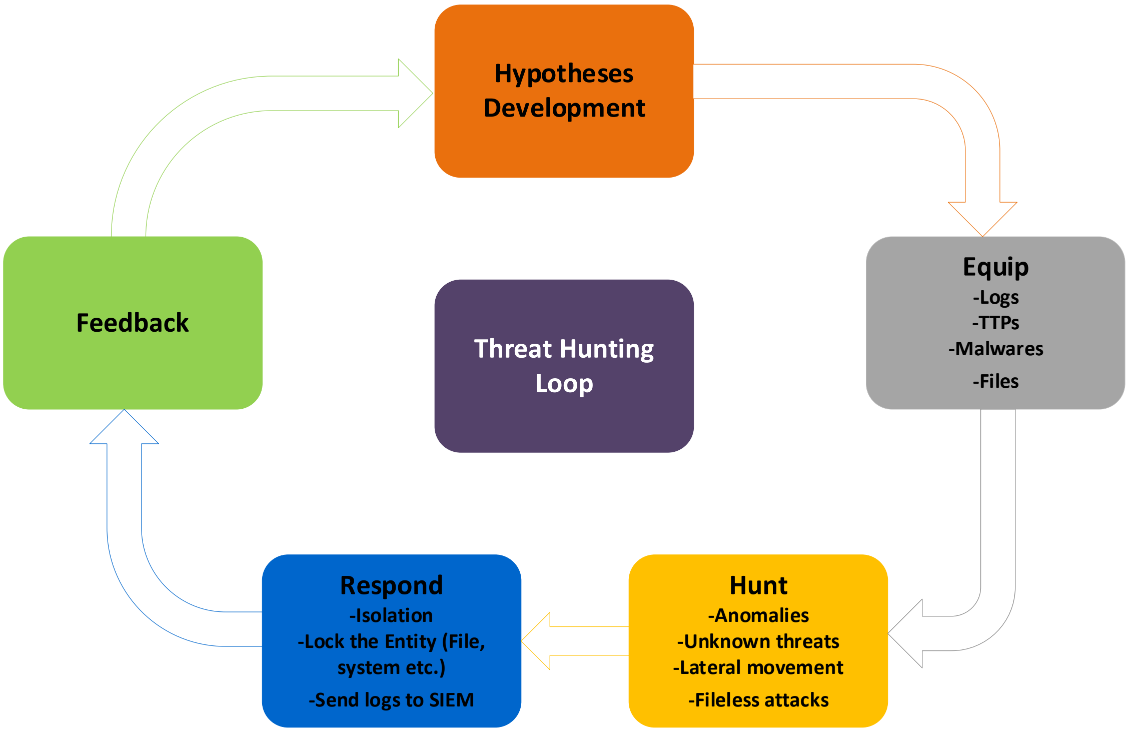


Fig. 9: Threat hunting loop

3.1. Hypotheses development

The first stage is hypothesis development. The threat hunters will develop hypotheses relevant to their threat environment and infrastructure. Hypotheses are used as analytical questions to keep the hunt focused on specific things and guide the search for sophisticated unknown threats. Just as targeting algorithms are used to select targets, hunting TTPs can be used to apply different approaches to develop a hypothesis.

Hypothesis development focuses on the type of hypothesis. According to the SANS Institute, the definition of a hypothesis is based on intelligence, domain knowledge, and situational awareness (Ajmal et al., 2021). Intelligence-based assumptions come from an understanding of the attacker's tactics, techniques, and procedures (TTPs), and behaviors.

The second element of the hypothesis identifies the analytical question to be answered. Threat intelligence plays an important role in assumptions and hypothesis development as it provides a context for threat chasers to generate analytical questions about the TTP of a specific attacker. To track threats with particular attention to certain attackers, it is required to improve the accuracy of the threat intelligence. Threat intelligence informs threat hunters of content that can be detected by a particular attacker's TTP (Ajmal et al., 2021).

The third element of the hypothesis defines the focus of the analytical problem. Each hypothesis covers only a part of the full range of threat hunts. The combined hypothesis should cover the entire system under investigation. Each hypothesis focuses on a specific analytical problem related to the target, regardless of its composition (Ajmal et al., 2021).

A good hypothesis is the one that helps in the identification of threats, gains good information about the environment, and can be proved right or wrong. For example:

- Geography: If a person is logging in from a geographic location very much different from his/her normal pattern of locations. This indicates that the account may be used by an intruder.

- Registry Changes: An unusual change in the registry is a sign of trouble.

Data sources then will be identified based on the formulated hypothesis. For example, for geographical hypothesis proving/disproving, the location dataset both benign and malicious will be fed to the system.

3.1.1. Data source identification

After proposing a hypothesis, identifying the data source is the next logical step in hypothesis testing. Threat hunters use data sources to confirm or refute hypotheses.

By combining the goals and capabilities of the attacker's infrastructure, threat hunters can create data source mappings on the system under investigation to search for threats. Data source identification assesses and considers relevant data sources to determine if a particular source is suitable for confirming or rejecting the current hypothesis. For effective threat scanning, logs are the most important product of the threat hunting process and algorithms. The key to speeding up threat hunting is to keep all logs. No one knows which data will be useful during a threat hunt, so collect all the information. Some of the most important items to record are all traffic logs from all network devices, systems, servers, workstations, email logs, antivirus protocols, DNS protocols, agent protocols, administrative activity logs, and more.

3.2. Equip stage

The Machine Learning algorithm that we are proposing in this paper needs to be developed using Linear Regression and SVM ML algorithms. These are the best for traffic log analysis with the more accurate result than the other algorithms. Implementation of this algorithm is a future work of this study.

The algorithms will be equipped with training data sources of different TTPs. The more details that we can put into the algorithm, the more accurate its results will be. The algorithm will be trained with the normal behavior of the target environment or system or sever or anything else and then also training with TTPs. In this way, it will be better to analyze the malicious behavior like Lateral movement, privilege escalation, credential access, or any other TTPs for which it is trained.

The equip stage focuses on comprehensive data collection, statistical analysis, outlier elimination, data/log analysis, and ML algorithms training process. The equip phase includes data source selection, analytical strategies, methods, and procedures for threat chasers to answer hypotheses raised using data sources and logs. The input will include Traffic logs, Files, Workstations and servers; Network, and security objects/devices. Determination of the appropriate analysis methods plays a major role in the equip stage. Some of the major analysis methods are STRIDE, PASTA, CVSS, and attack trees. Other sources such as malware signatures, adversary TTPs, and infrastructure information are also input to the system and trained with this input. Two substages of the equip stage are the determination of the data source and choosing the method of analysis.

First raw data logs will be fed to the system and the system will perform statistical analysis/visualization and eliminate outliers. The refined data will then be fed to the algorithm for training purposes and in this way, the algorithm will learn about the normal behavior of the system or environment. The process is depicted in the following figure (Fig. 10).

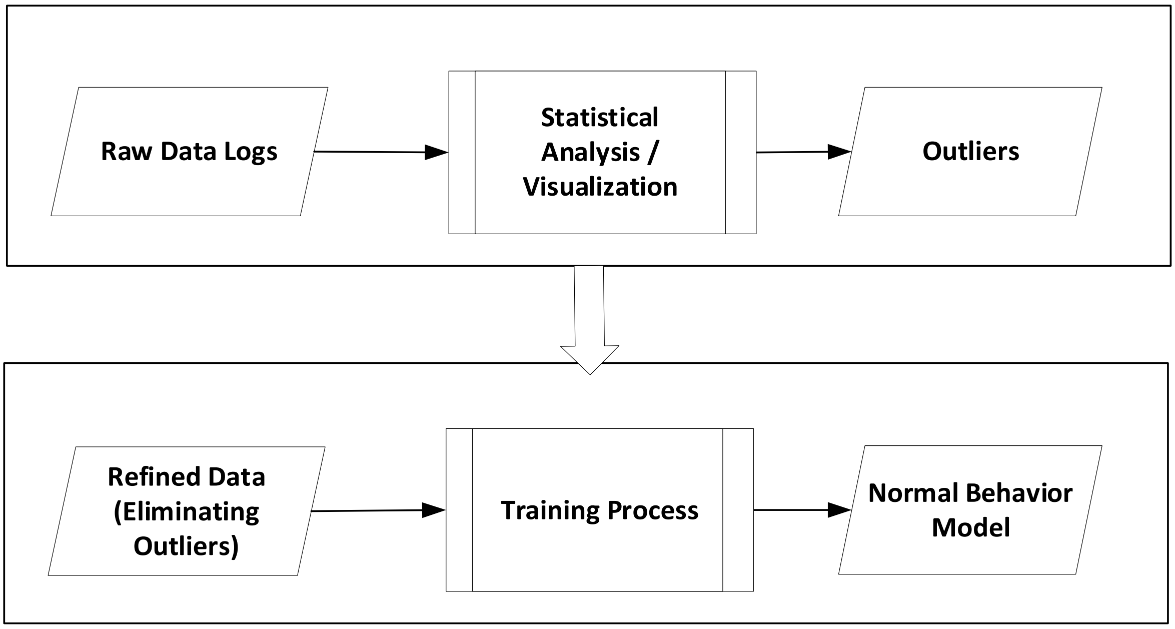

Raw Data Logs
Statistical Analysis / Visualization
Outliers
Refined Data (Eliminating Outliers)
Training Process
Normal Behavior Model

Fig. 10: Equipping the threat hunting algorithm/solution

3.3. Hunt/detect stage

The hunt or detection stage occurs after the equip stage and consists of multiple iterations of data analysis and detection. Threat hunters collect the information presented at the equip stage and use analysis techniques to detect anomalies, thus proving or denying the formulated hypothesis. Analysts also need to turn to other available data sets and use other analysis techniques to achieve hunting goals as needed.

The output of the hunting stage will result in the detection of Anomalies; Unknown threats; Lateral movement; Fileless attacks and any TTP for which the algorithm has been trained for as mentioned in Fig. 9-MITRE ATT&CK adversary techniques/TTPs. The major task will be performed by the Machine learning algorithm in the stage. The process is depicted in Fig. 11.

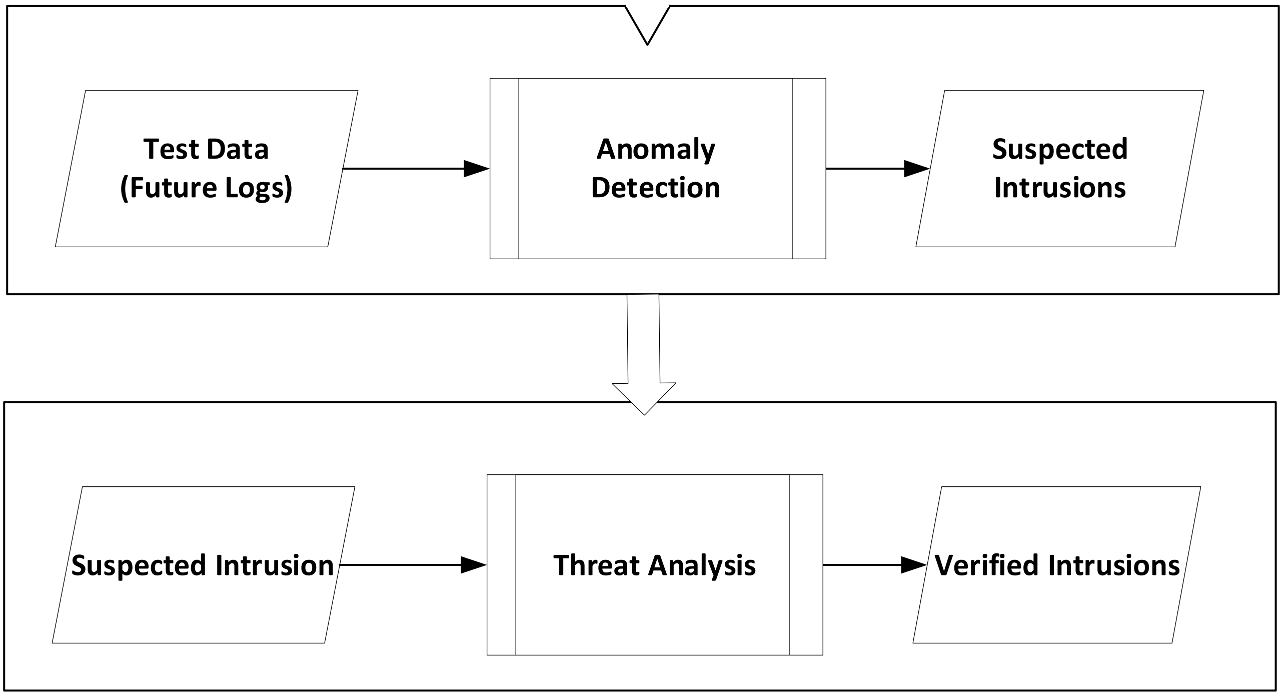


Fig. 11: The hunt/detect process

3.4. Respond stage

The next step is the response stage. In this stage, the verified intrusions are being responded to as per the implemented policy. This step is more like the incident response in the overall incident management plan. After verifying the intrusion, the system will generate an alarm and notify the intrusion to the next level by notifying the administrator. With the notification and alarm generation the system will do one or more of the following operations:

- Isolation of the process or system or server or any infected entity
- Lock the File or Process or system
- Send logs to SIEM or SOAR or EDR which one is implemented for a thorough investigation and get a detailed picture.

3.5. Feedback stage

The next stage is the feedback stage. The feedback stage provides a detailed analysis of all the performed stages and their impacts on the overall threat hunts and their results. At the end of the threat hunt, several questions will be asked about each stage in order to engage and sough the strengths and weaknesses of the process from the threat hunting participants. Answering these questions will help organizations respond more effectively to future threat hunts by establishing the threat hunt on the strengths and weaknesses of previous hunting feedback. Following is feedback for each stage.

3.5.1. Feedback to equip stage

The Feedback to equip stage focused on how much support the logs, datasets, and analytical techniques were to track the threats. If the provided dataset and logs were ineffective or insufficient to hunt for threats, the equip phase feedback will be to update the dataset or logs immediately or be provided with more detailed records and training sets that may indicate the presence of this information.

If the method of analysis chosen for the hunt is insufficient to prove or disprove the hypothesis, feedback to the equip stage may indicate improvements. Some other questions might include: was the outcome successfully achieved? Did the outcome match our required expectations? Were the input sources enough for getting the desired results?

3.5.2. Feedback to hunt stage

The feedback to hunt stage focus on analyzing the data and how to properly the anomalies were detected during the threat hunting process. The feedback stage is to assess the accuracy of the analyst's hunt. Rigor focuses on the ability to apply analytical techniques to relevant data sources to identify observations related to the presence of an attacker.

Feedback might also consider TTP's coverage of the attacker within the environment. By understanding an attacker's TTPs and associated behavior in an environment, threat hunters can create a watchable list of known hosts and networks associated with the attacker's TTP.

3.5.3. Feedback to response stage

Feedback to the response stage focuses on how well the identified threats were dealt with. What was the false positive and false negative rate? Were the isolation of the identified infected systems or files or servers were qualified the expected result?

Based on this feedback, the threat hunting system will be enhanced for the new threat hunts.

4. Discussion

This paper concludes that traditional manual threat hunting is somewhat difficult to perform, mainly due to manual operations and anomaly identification. The threat hunting process, which includes machine learning, can make the whole process semi-automatic and make more informed decisions based on the normal behavior of the system. Formally defined hypotheses and the implementation of the equip phase can effectively detect unidentified attacks and adversaries during the hunting phase and also provide a better way to react to a detected adversary or anomaly by isolating the entity from the environment. If the desired result is not achieved, the system will notify the administrator to provide additional resources for data and logs to train the algorithm. Organizations using this model can quantify unknown adversaries and attacks by analyzing TTPs.

The hunting loop provides the organizations with an opportunity to ensure that the threat hunt maintains the analytical integrity and makes the best use of the provided data sources. Important steps are taken at each stage to complete a comprehensive threat hunt. In addition, the model provides a framework for the various actors involved in the threat hunting process to help them succeed.

5. Conclusion and future work

This paper proposed a threat hunting model called the hunting loop. The resulting model consists of five main stages: Hypotheses development, equip, hunt or detect, respond and feedback stages. Performing threat hunting using this method will make the threat hunting process easy and will provide effective results. The hunting loop provides a comprehensive and targeted method for detecting the TTP of attackers in the target environments. By using this model, the overall hunt results can better track to its goals and objectives and maintain the accuracy and integrity of the analysis.

In the future, this model will be implemented for real-life threat hunting using Linear Regression and SVM Machine Learning algorithms.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Ajmal AB, Shah MA, Maple C, Asghar MN, and Islam SU (2021). Offensive security: Towards proactive threat hunting via adversary emulation. IEEE Access, 9: 126023-126033. https://doi.org/10.1109/ACCESS.2021.3104260

Brooks C (2021). Alarming cybersecurity stats: What you need to know for 2021. Available online at: https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=2733f50858d3

Caltagirone S, Pendergast A, and Betz C (2013). The diamond model of intrusion analysis. Center for Cyber Intelligence Analysis and Threat Research, Hanover, USA.

Daszczyszak R, Ellis DR, Luke S, and Whitley SM (2019). TTP-based hunting. Technical Papers, The MITRE Corporation, McLean, USA.

FireEye (2019). Red team operations (RTO): Test your ability to protect your most critical assets from a real-world targeted attack. Available online at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf

Gunter D (2018). A practical model for conducting cyber threat hunting. SANS White Paper 38710. Available online at: https://www.sans.org/white-papers/38710/

Huang YT, Lin CY, Guo YR, Lo KC, Sun YS, and Chen MC (2021). Open source intelligence for malicious behavior discovery and interpretation. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2021.3119008

Mandiant (2019). Red team cyber security assessment. Available online at: https://www.fireeye.com/mandiant/red-team-assessment.html

Miazi MNS, Pritom MMA, Shehab M, Chu B, and Wei J (2017). The design of cyber threat hunting games: a case study. In the 26th International Conference on Computer Communication and Networks, IEEE, Vancouver, Canada: 1-6. https://doi.org/10.1109/ICCCN.2017.8038527

NAO (2018). Investigation: WannaCry cyber-attack and the NHS. National Audit Office, London, UK.

Strom BE, Battaglia JA, Kemmerer MS, Kupersanin W, Miller DP, Wampler C, and Wolf RD (2017). Finding cyber threats with ATT&CK-based analytics. Technical Report No. MTR170202, The MITRE Corporation, Bedford, USA.

TMI (2020). A constant state of flux: Trend micro 2020 annual cybersecurity report. Trend Micro Inc., Tokyo, Japan.

Yadav T and Rao AM (2015). Technical aspects of cyber kill chain. In: Abawajy J, Mukherjea S, Thampi S, and Ruiz-Martínez A (Eds.), Security in computing and communications: 438–452. Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-319-22915-7_40