A Practical Model for Conducting Cyber Threat Hunting

Dan Gunter

A Practical Model for Conducting Cyber Threat Hunting

Dan Gunter (dgunter@dragos.com), Marc Seitz (mseitz@dragos.com)

Abstract

There remains a lack of definition and a formal model from which to base threat hunting operations and quantifying the success of said operations from the beginning of a threat hunt engagement to the end that also allows analysis of analytic rigor and completeness. The formal practice of threat hunting seeks to uncover the presence of attacker tactics, techniques, and procedures (TTP) within an environment not already discovered by existing detection technologies. This research outlines a practical and rigorous model to conduct a threat hunt to discover attacker presence by using six stages: purpose, scope, equip, plan review, execute, and feedback. This research defines threat hunting as the proactive, analyst-driven process to search for attacker TTP within an environment. The model was tested using a series of threat hunts with real-world datasets. Threat hunts conducted with and without the model observed the effectiveness and practicality of this research. Furthermore, this paper contains a walkthrough of the threat hunt model based on the information from the Ukraine 2016 electrical grid attacks in a simulated environment to demonstrate the model's impact on the threat hunt process. The outcome of this research provides an effective and repeatable process for threat hunting as well as quantifying the overall integrity, coverage, and rigor of the hunt.

Introduction

There are many different approaches to increasing an organization's cybersecurity defenses against adversaries. One fundamental solution is known as a threat hunt. Threat hunts provide a proactive opportunity for an organization to uncover attacker presence in an environment. While no formal academic definition exists for threat hunting, this paper defines threat hunting as the proactive, analyst-driven process to search for attacker tactics, techniques, and procedures (TTP) within an environment. Attacker TTP must be researched and understood to know what to search for in collected data. Information about attacker TTP most often derives from signatures, indicators, and behaviors observed from threat intelligence sources [15]. This added context should include targeted facilities, what systems were affected, protocols manipulated, and any other information pertinent to better understanding an attacker's TTP. The attacker targeted nature of the threat hunt requires accurate threat intelligence to achieve success. The formal model for threat hunting presented in this paper ensures the focus of the hunt remains on the attacker outlined purpose of the hunt while also maximizing usage of threat intelligence. The presented formal threat hunt model is also agnostic of the analytic techniques employed throughout the hunt allowing the model flexibility to work with any hunt tools or techniques such as machine learning or stateful analysis [2]. Just as incident response

requires a formal process to handle an investigation rigorously, threat hunting requires a formal process also to protect the integrity and rigor of the analysis [8].

Related Work

Joint Targeting Cycle

The proposed model for threat hunts derives from the United States Department of Defense's Joint Targeting Cycle model. The Department of Defense utilizes the Joint Targeting Cycle to capture commander intent, priority targets, allocate resources, execute operations and gather feedback [5].

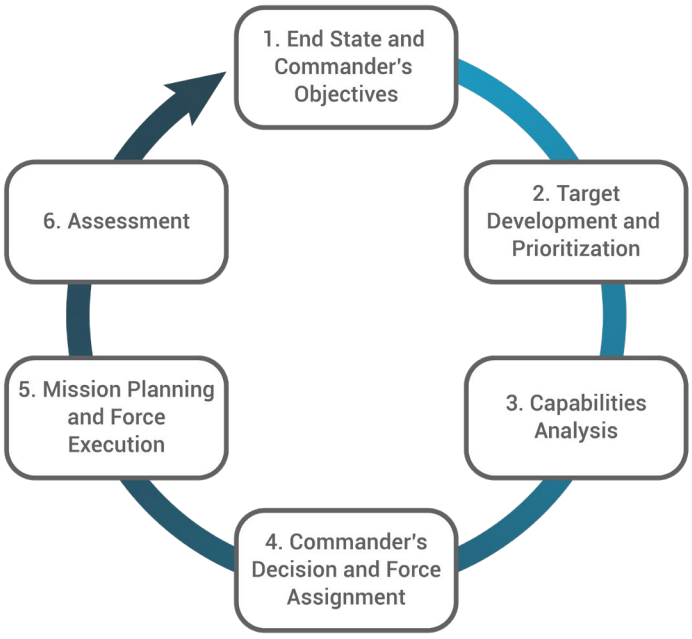

Fig. 1. The US DoD Joint Targeting Cycle serves as the basis by which military operations are planned and also provides a good framework to plan rigorous threat hunts from.

The Joint Targeting Cycle focuses the weight of military operations on the areas and techniques that result in the defined end goal. In addition to the military focus, the Joint Targeting Cycle provided this research a framework for adapting to a threat hunt process. The practical model for threat hunts capitalizes on the strengths of the Joint Targeting Cycle that keep the developed plan relevant to the organization's end goals. The practical threat hunt model additionally takes into account the multiple groups of individuals involved in a successful threat hunt.

The Joint Targeting Cycle focuses the weight of military operations on the areas and techniques that result in the defined end goal. In addition to the military focus, the Joint Targeting Cycle provided this research a framework for adapting to a threat hunt process. The practical model for threat hunts capitalizes on the strengths of the Joint Targeting Cycle that keep the

developed plan relevant to the organization's end goals. The practical threat hunt model additionally takes into account the multiple groups of individuals involved in a successful threat hunt.

Diamond Model for Intrusion Analysis

"The Diamond Model for Intrusion Analysis," a paper describing in-depth attacker intrusions and providing a model for classifying attacker behavior is the foundational paper for identifying attackers, their victims, the infrastructure targets, and capabilities. Ultimately, this provides threat intelligence with a way to take attacker tradecraft and form TTP for threat hunts. In addition to TTP, threat hunts use this model to identify relevant data sources for an investigation [11].

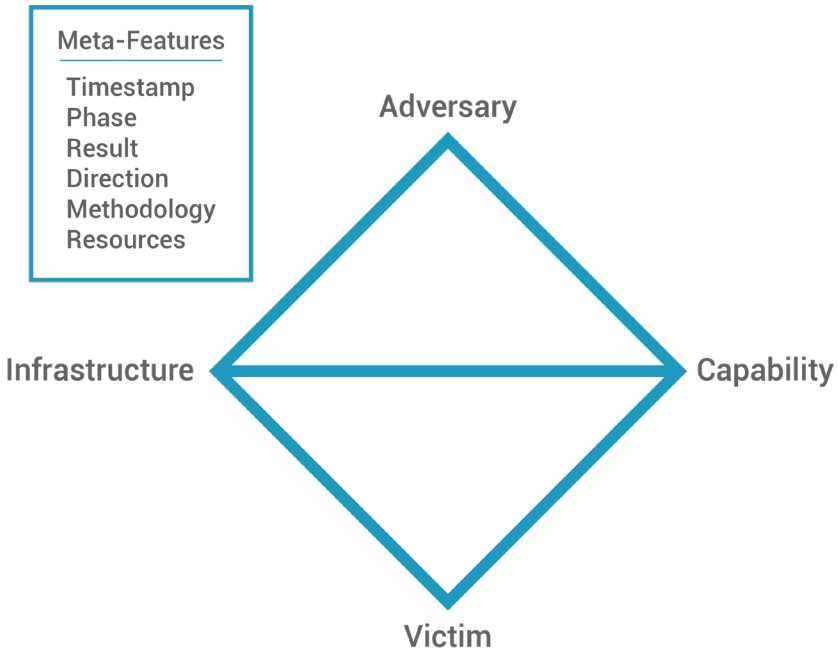

Fig. 2. The diamond model provides a model for threat intelligence central to threat hunting. Each vertex of the diamond model provides a classification point for adversary tactic, techniques and procedures.

The adversary and victim vertices focus on the observed intent of the activity group performing attacks against a single victim or multiple victims. The adversary vertex does not attribute the attack to a particular nation, group, or individual but instead looks at the intent of the attack. In the context of threat hunting, a threat hunt might choose to focus on attacks within a particular sector. A threat hunt focused on the ELECTRUM activity group responsible for the 2016 Ukranian transmission substation attack serves as an example of a threat hunt that might focus on attack TTP from a single victim [3]. A threat hunt focused on COVELLITE, an attack group that targeted North American power generation companies in 2017 might focus on attacker TTP used across multiple victims.

The infrastructure vertex defines the set of systems an attacker uses to launch attacks against a given victim. Indicator-based defense approaches build indicators from sources such as internet

protocol (IP) addresses and domain names. IP addresses and domain names both serve as indicator based descriptors for attack infrastructure. For attackers that exploit and use botnets, the attack infrastructure would consist of all types of machines within the botnet. The infrastructure vertex, however, should not solely consist of indicators. Threat intelligence should also provide insight into attacker behavior. For example, an attacker might use encoded DNS messages for command and control (C2). The infrastructure vertex might consist of the IP addresses associated with the DNS servers but can also contain some of the unique C2 behaviors associated with the attacker's infrastructure TTP.
The capability vertex derives from known attacker intrusion tools and techniques. Acquiring this knowledge often comes from threat intelligence. Threat hunts make use of this intelligence to focus data collection to sources with the potential to uncover attacker tools and techniques.

Kill Chain Analysis

One method to analyze the phases of attack includes analysis of attacker actions over the cyber kill chain. The Cyber Kill Chain™ is a framework that provides one means to model attacker action across the continuum of general attack steps. An alternative to Leido's Cyber Kill Chain™ is MITRE's ATT&CK™ framework [10]. Both models seek to define and categorize the general activities an adversary does during an attack. By categorizing actions, defenders can identify attack behaviors that might fit into a given stage of each model. A paper published by the Chinese CERT defined and studied Advanced Persistent Threat (APT) groups by building a system to both detect and try to predict APT action using the Cyber Kill Chain [10]. The same analysis can be used to evaluate the rigor of a threat hunt by ensuring that the hunt focuses on the full range of attacker action.

Cognitive Biases

Just as cognitive biases impact technical decisions made when developing software, the same cognitive bias-based errors also relate to the practice of threat hunting. Cognitive biases refer to the situation where a person's ordinarily good decision-making ability "consistently and predictably errs" from a rational decision [13]. Examples of cognitive biases range from confirmation bias, where an analyst might seek out on the information to prove a preconceived notion or availability bias which weights recent information more favorably than past information. The formal threat hunt model puts protections in place to attempt to combat common cognitive biases that adversely impact the results of a threat hunt.

Threat Hunt Model

The formal threat hunt model consists of six sequential stages: purpose, scope, equip, plan review, execute, and feedback. The first stage of the threat hunting cycle, known as the purpose stage, outlines the goals and outcomes of the threat hunt. The second stage is scope and includes the development of a detailed plan of where to collect data as well as the development of analytic questions, also known as hypotheses. The first phase of the scope stage identifies the area that a hunt takes place and all associated systems and protocols. The second phase of the scope stage involves developing hypotheses that support the overall

purpose. Hypotheses are matched to data sources to prove or disprove the analytic question at hand. It is important to note that hypotheses development should occur after the definition of the purpose and scope stages. The development order is vital because hypotheses must be created to prove or disprove an analytic question. Without an initially defined purpose or scope driving analytic question generation, assumptions about data sources and hypotheses might lead the hunt away from the intended outcome and introduce unnecessary cognitive biases. The equip stage focuses on identification of the analysis techniques and tools needed to process data and prove or disprove developed hypotheses. A plan review ensures the developed hypotheses and identified resources meet the overall purpose of the hunt. Once the plan is approved, the execute stage is where a threat hunter collects and analyzes data according to the identified hypotheses. Finally, the feedback stage allows retrospection on the execution of each previous stage of the threat hunt model and provides an opportunity to identify improvements for future hunts. The threat hunting cycle is cyclical to ensure that the results and lessons learned from previous hunts influence future hunts.

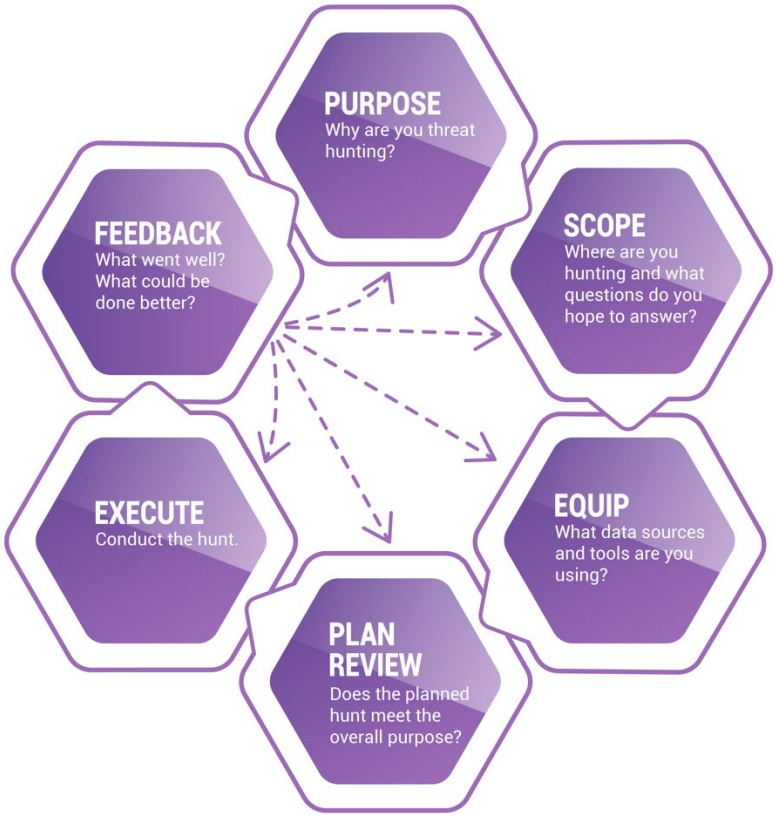

Fig. 3. The practical threat hunt model we propose contains six stages that cover all activities within the entire threat hunt. The dashed line from the feedback stage represent calculation of overall rigor and completeness.

Purpose

Purpose focuses on the organization's goals the threat hunt will accomplish. An organization’s executive leadership or management might guide the purpose of a threat hunt to meet larger, long-term business objectives. The three areas of study defined within the purpose stage include:

- Purpose of the hunt
    - The overall purpose states why the hunt needs to occur
- Where the hunt will occur.
    - Purpose also includes scoping the environment as well as identifying assumptions and limitations of the hunt.
- Desired outcome of the threat hunt
    - The desired outcome should align with business objectives and how the threat hunt supports reduction of risk.

Examples for why a hunt takes place might range from the connection of a new network to an existing trusted network following a corporate merger and acquisition event, new threat intelligence suggesting the presence of an attacker in the environment or the desire to gain higher awareness and confidence of the environment. While purpose does not take over the task of scoping the threat hunt, purpose provides general guidance that might focus a threat hunt on a desired regional or subsystem area of interest to business objectives. Finally, purpose focuses on the end outcome of the hunt. Outcomes may include the discovery of an attacker within the environment or identification of gaps in incident response processes that drive acquisition decisions.

Scope

Scope follows the purpose stage and contains a variety of functions including identification of specific systems and networks to be studied. Also, the scope stage defines hypotheses, or analytic questions, for the systems under study to achieve the defined purpose. The primary objective of the scope stage is to identify what hypotheses or analytic questions achieve the purpose and the relevant systems to study.

Threat hunters should complete the two phases of the scope stage sequentially to preserve the integrity of the hunt. Hypothesis generation can only occur after the definition of a purpose. The purpose drives the identification of what systems are relevant to the purpose. Finally, hypothesis development defines the study areas for the previously defined systems.

Phase 1: System Under Test Selection

In the first phase of scope, the threat hunt defines the systems under test. Identification of systems under test might begin with specific facilities. Furthermore, hunters might define the subnet or subnets that need to be studied within and between identified facilities. The field narrows further by adding the specific systems that matter to the threat hunt. The final step of the system under test selection stage is selecting the network and host data relevant to a successful threat hunt. Throughout the scope stage, threat hunters must ensure the defined scope of analysis supports the overall purpose of the hunt. Common errors made during the system under test selection phase consist of making the scope of the hunt too narrow at the expense of missing attacker presence in the environment.

Phase 2: Hypothesis Development

After the system under test is defined, threat hunters generate hypotheses. Hypotheses serve as analytic questions that maintain the focus of the hunt and define the direction of the threat hunt. Just as attack targets can be chosen using a targeting algorithm, defensive hunting TTP can also leverage targeting approaches and algorithms for hypothesis generation [6].

The first element of a hypothesis focuses on the type of hypothesis. While no formal definition for threat hunting hypothesis exists in peer reviewed academic publications, a paper issued by the SANS Institute defined a hypothesis as being driven by intelligence, domain knowledge, or situational awareness [9]. Intelligence-driven hypotheses derive from understanding both indicators and behaviors of attacker tactics, techniques, and procedures.

The second element of a hypothesis defines the analytic question to answer. Threat intelligence plays a significant role in intelligence-driven hypotheses as threat intelligence provides threat hunters context to create analytic questions targeted at a particular attackers TTP. Threat hunts with a strong focus on a particular attacker require a higher fidelity of threat intelligence. Threat intelligence also informs what observables a threat hunter might find from a given attacker's TTP [9,13].

The third element of a hypothesis defines where an analytic question will focus. Each hypothesis might only cover a subset of the entire scope of the threat hunt. The combined hypotheses should cover the entirety of the system under study. Each hypothesis, regardless of combination, will focus on a specific analytic question about the purpose [9].

Equip

The equip stage centers on the development of a thorough data collection and analysis plan. The equip plan includes both the selection of data sources and analytic tactics, techniques, and procedures the threat hunter will employ to answer the developed hypotheses using the data sources defined during the scope stage. Identification of relevant analytic approaches plays a central role in the equip stage. Collection bias occurs when a threat hunter erroneously favors a given data source by building hypotheses around a data source. The two phases of the equip stage focus on the identification of data sources followed by the selection of analytic approaches.

Phase 1: Data Source Identification

Following hypothesis development, identification of data sources is the logical next step for validation of the hypotheses. Data sources will be used to either prove or disprove the created hypotheses.

The combination of attacker infrastructure targets and capabilities create a mapping of data sources for the threat hunt on the system under study. The data source identification phase evaluates potential data sources and decides if a given source is relevant to confirming or denying the present hypothesis. The output of this process might leverage a Collection Management Framework (CMF). The CMF is a data table marking the location, data type, kill chain step, collection process, and typical storage duration for each data source identified as

relevant to the threat hunt. While a data source may be useful, the CMF validates whether the data source is feasible for collection. A defined threat hunt might want to leverage six months of Windows Event Logs. However, the CMF might indicate only a week's worth of logs is obtainable. If a source offers no evidence for a defined hypothesis, then the source has no bearing on the threat hunt and should not be evaluated.

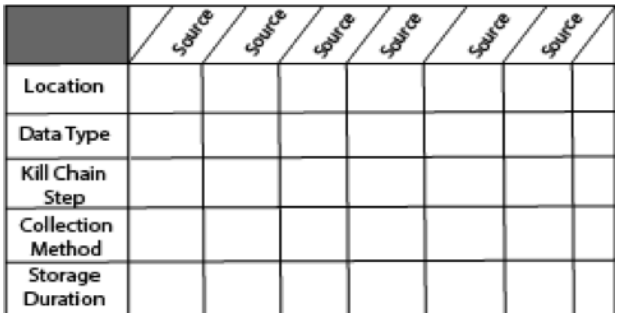

Fig. 4. The collection management framework provides a record of available data sources, how the sources are collected and the duration. An updated CMF assists threat hunters in knowing what data sources are available and where additional collection might be required.

Plan Review

The plan review stage provides a checkpoint to ensure the planned hunt meets defined objectives. A project manager might brief the hunt plan to stakeholders to ensure the planned hunt meets the intended objectives. The plan review stage also includes the allocation of any additional resources required to execute the hunt. If a hunt team does not have all the requisite resources to conduct the hunt, the plan review stage should identify deficiencies and suggest potential solutions to resolve identified issues. Additional resources might include the acquisition of new tools, hiring of external resources, or rescoping of the overall hunt. Finally, the plan review should also consider the time a threat hunt will consume. In addition, the plan review should ensure the time range for the hunt has enough data collection coverage as a final review before the execute stage.

Execute

The execute stage occurs after approval of the hunt plan and consists of multiple iterations of data collection and analysis. Threat hunters gather the information identified in the scope stage and use analysis techniques to prove or disprove the developed hypotheses. Analysts should also pivot into other available datasets and employ additional analysis techniques as needed to meet the purpose of the hunt.

Development of the hunt report commences at the end of the execute stage after all analysis has concluded. The final hunt report should focus on results of hunting efforts and answering the purpose. The resulting threat hunt report should contain any additional data sources, analytic techniques, and other notable events or discoveries during the hunt.

Feedback

The feedback stage provides analysis for all of the previous stages and the effects they had on the hunt. Several questions are asked of each stage upon the conclusion of the threat hunt to

engage those involved in the retrospective. The graphics below describe several questions to ask at each stage. The answers to these questions should drive the organization to handle future threat hunts with higher efficiency based on strengths and shortcomings from previous retrospectives.

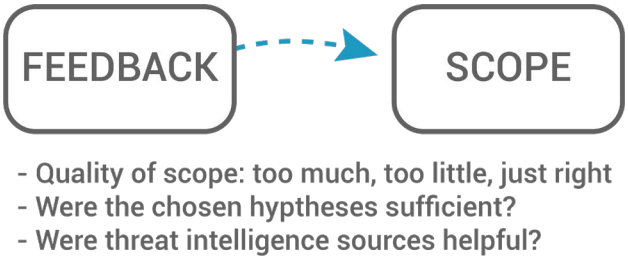

Fig. 5. Feedback to the scope phase focuses on the quality of the scope, the relevance of chosen hypotheses to the scope and the helpfulness of threat intelligence sources.

Feedback to scope focuses on the systems under study selected to hunt on and the hypothesis generation process. If a threat hunt fails to identify a system relevant to the overall purpose of the hunt, feedback to the scope stage should identify the deficiency and provide potential solutions for avoiding the error in the future. If hypotheses are not relevant to the purpose of the hunt, the feedback provided to the scope stage identifies improvements to hypothesis development.

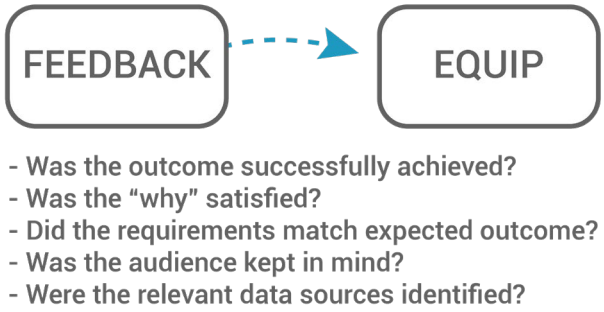

Fig. 6. Feedback to the equipping phase addresses if the outcome of the hunt was successfully achieved, if the “why” of the hunt was satisfied, if requirements matched expected outcome, if the audience was kept in mind and if relevant data sources were identified.

Feedback to equip focuses on how well the datasets and analytic techniques supported the threat hunt. If a Collection Management Framework did not exist or did not contain an updated list of available data sources, feedback to the equip stage might suggest the need for immediate updates to the Collection Management Framework. If a threat hunt overlooked data sources due to cognitive biases or analyst error, feedback to the equip stage might address how future hunts can avoid data source selection errors.

If the chosen analytic techniques for a hunt were not sufficient or comprehensive enough to prove or disprove a given hypothesis, feedback to the equip stage might suggest improvements. The cognitive bias of recency might cause an analyst to weight the effectiveness of one tool based on success during a recent hunt where another analytic technique might yield more accurate or comprehensive results. The feedback to the equip stage suggests corrections to how the equip stage is conducted to avoid undue analytic biases.

Another critical component of feedback to the equip stage is automation. Threat analysts may use manual analysis techniques in a given threat hunt that, where possible, should be automated for efficiency.

Fig. 7. Feedback to plan review focuses on if the plan review stage missed any observable issues and if additional plan validation checks should be implemented during future hunts.

Feedback to the plan review stage identifies how well the plan review kept the hunt focused on the purpose. The plan review stage is where an organization ensures the planned threat hunt meets the overall purpose. If the plan review stage fails to identify a deficiency in the defined scope and approach developed in the equip stage, improvements to the plan review process should provide feedback on how better to focus the hunt. Another feedback for the plan review stage focuses on the efficiency of resource allocation for a hunt.

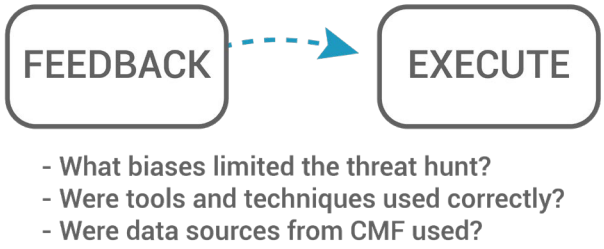

Fig. 8. Feedback to the execute phase addresses where cognitive biases were encountered during the threat hunt as well as the effective use of tools, techniques and data.

Feedback to the execute stage focuses on how well data collection, analysis, and data pivoting occurred during the hunt. The feedback stage should assess the degree of rigor that an analyst uses to conduct the hunt. Rigor focuses on how well analytic techniques were used on relevant data sources to uncover observables related to attacker presence.

Feedback to the execute stage might also consider attacker TTP coverage within the environment. Through the understanding of attacker TTP and related behaviors in the environment, it is possible to build a list of known observables on the host and network related to the attacker TTP.

Impact of Model on Threat Hunts

This research found that hunts that followed the formal threat hunting model maintained a closer focus on the objectives outlined in the purpose stage. A formally defined purpose for the hunt enables the feedback stage to consider the relevance of decisions made in the scope and execute stages. A formally defined purpose also enables the organization to prioritize and adequately resource the threat hunt team for success during the equip and plan review stage. When additional resources are required, the formal purpose provides the project manager

responsible for the hunt with a justification for why additional resources are necessary. In the event additional resources are unavailable, the overall purpose of the hunt might change to accommodate available resources. The formal threat hunting model accounts for the multiple parts of a hunt that might lead to the scope being changed to preserve the expected result of the hunt.

Organizations that use the formal threat hunting model gain the ability to quantify the overall coverage of a hunt. By comparing the observables the hunt analyzed within available data sources associated with known attacker TTP, it is possible to calculate the overall coverage of the hunt. Consider a threat hunt focused on the attacker TTP leveraging PsExec for lateral movement. PsExec is a lightweight remote access tool developed in the early 1990s that enables authorized remote access to Windows machines [7]. The behaviors of PsExec are well known and very observable both in network and host logs. A threat hunt focused on the observables related to PsExec might look at suspicious use of Server Message Block (SMB) shares by unexpected accounts, unexpected network connections between network zones and host process activity associated with how PSExec executes. If a threat hunt for PsExec only focused on a subset of observables related to the use of SMB shares, this threat hunt would attain a meager coverage score. A high coverage score for PsExec would analyze a high percentage of observables from the majority of PsExec's behaviors. The threat hunting model enables precise calculation of the coverage of how well threat hunting techniques matched observables related to attack TTP.

The threat hunting cycle also assists analysis of cognitive bias impact [13]. The creation of the Collection Management Framework provides a catalog for an organization to know what data sources are available when hunting. The Collection Management Framework also assists an organization to recognize when cognitive biases impact analysis. Consider a threat hunt for PsExec where an analyst had recent success looking at SMB logs from Bro Intrusion Detection System (IDS) [1]. If the analyst decides to only look at SMB logs from Bro IDS in the current hunt and dismisses other equally or more valuable data sources, the analyst falls victim to recency bias. This bias will be noted because the analyst did not consider other available data sources. Recency bias refers to when information encountered recently outweighs older data that might be more valuable for analysis. Useful feedback to the execute stage should identify situations where an analyst did not use all available data sources to prove or disprove a hypothesis.

The formal threat hunt model provides the security community the ability to ensure threat hunts maintain the analytic integrity and maximize the use of data sources. Each stage performs a vital step necessary for the overall threat hunt. Additionally, the model outlines a framework for the various stakeholders involved in a hunt to contribute to the successful outcome.

Threat Hunt Model Applied

Purpose

Suppose the chief information security officer of the electric power utility directed the hunt team to conduct a threat hunt on all 500kV transmission substations and the top ten largest distribution substations. The overall outcome is to uncover ELECTRUM presence in high-risk environments and also know where best to invest resources to counter ELECTRUM capabilities. This purpose statement captures the necessary elements of where the hunt will occur, the desired outcome of the hunt, and the purpose of the hunt.

Scope

The purpose stage defined several facilities of interest to the chief information security officer. The scope stage digs deeper to develop a technical plan and identifies subnets, systems, and protocols to study. Hypothesis development also occurs during this stage. Threat intelligence concerning ELECTRUM's tactics, techniques and procedures play a central role when scoping. Extensive analysis of the CRASHOVERRIDE malware and attacker tactics, techniques and procedures exist via open source resources. Scoping information derives from these available open source resources.

Scope: System Under Test Selection

Within the first part of the scope stage, the control system assets and human-machine interfaces will serve as the systems under test, and IEC 60870-5-104 will serve as the central protocol under analysis for the example threat hunt [4]. ELECTRUM's CRASHOVERRIDE attack capability possessed the ability to attack IEC 60870-5-104 devices [3]. Internal knowledge essential to the context of the example hunt is that the transmission and distribution substations use IEC 60870-5-104. Threat intelligence played a significant role in the focus on IEC 60870-5-104 based on open source knowledge of the Ukraine 2016 attack [3].

Scope: Hypothesis Development

An intelligence-driven hypothesis will focus on ELECTRUM's capabilities against the substation with the attacker's custom IEC 60870-5-104 attack tool. The analytic question to be answered will be "if ELECTRUM uses their custom IEC 60870-5-104 attack tool against the substation, a subset of observables consistent with the behavior of the CRASHOVERRIDE malware will be present." This hypothesis is provable using knowledge of the observables related to ELECTRUM's IEC 60870-5-104 attack tool and the forensic artifacts left behind.

Equip

The equip stage will focus on the principal IEC 60870-5-104 data sources needed to prove the previously developed hypothesis. An analyst might need to determine the best method of analysis to analyze the protocol traffic. The analyst might use a commercial tool to analyze the protocol state of IEC 60870-5-104 or an open tool like Wireshark to analyze network traffic [14]. If a threat hunter determines existing internal analysis techniques for IEC 60870-5-104 exist that support the generated hypothesis, the analyst should research potential solutions for the

analysis gap and document the impact on developed hypotheses. A threat hunter might plan to use the Snort (IDS) to look for the presence of CRASHOVERRIDE execution artifacts. Mainly, when CRASHOVERRIDE executes, an IEC 60870-5-104 STARTDT ACT message is generated which triggers Snort's protocol detection rules. The threat hunter also might plan to check Windows Event Logs for events related to the termination of the legitimate communication process and CRASHOVERRIDE's IEC 104 module taking control of the port and sending IEC 60870-5-104 traffic.

Plan Review

The plan review stage provides an opportunity to assess if the developed hunt meets the threat hunt purpose. Additional resources might also be allocated to cover the gaps identified in the equip stage. Outside teams might be hired to support a threat hunt or tools might be acquired to ensure the success of a developed hypothesis. For the example threat hunt, the plan review might bring in an external expert familiar with IEC 60870-5-104 to ensure the threat hunter conducts a comprehensive analysis of the protocol. The developed hypothesis is focused on ELECTRUM and uses knowledge of ELECTRUM tactics, techniques, and procedures.

Execute

Threat hunters collect and analyze data during the execute stage. Within the example hunt, threat hunters first collect Windows Event Logs for all hosts communicating IEC 60870-5-104 as well as a network capture of subnets with IEC 60870-5-104 traffic. The threat hunters then might run the packet capture files through Snort to view the output of Snort's IEC 60870-5-104 module [12]. Threat hunters analyze the host logs for unusual behavior related to the process managing IEC 60870-5-104 protocol traffic. The analyst reviews host and network logs for ELECTRUM TTP during the execute stage. If necessary, threat hunters pivot to new datasets or analytic techniques to prove or disprove the studied hypotheses. At the completion of the execution stage, threat hunters summarize findings and document any conditions that might impact the integrity of the overall hunt. At the conclusion of the execute stage, the threat hunters produce the hunt report.

Feedback

Strength and shortcoming analysis should occur for each stage in the threat hunt model in the feedback stage. A finding for the feedback stage out of the threat hunt might identify the need for an internal development team to develop additional IEC 60870-5-104 analysis tools. If no internal development team exists, a tool might be purchased to fill the gaps. The feedback stage might also identify deficiencies in hypotheses or data sources identified in the scope and equip stages.

Conclusion

This research defined a formal model for the threat hunting process. The resulting model consists of six stages: purpose, scope, equip, plan review, execute, and feedback. The paper outlines the model flow as well as diving into each stage. The deep dive demonstrates the

importance each stage has on the model itself as well as how to accomplish the objectives outlined in each stage. Threat hunts conducted with and without the model provided validation of the practicality and efficiency of use. The formal threat hunting model provides a comprehensive and focused approach for uncovering adversary TTP within an environment. By using the formal threat hunting model, the overall results of the hunt better track the purpose and preserve analytic rigor and integrity.

References

[1] "The Bro Network Security Monitor" Bro IDS. 2014 [Online] Available: https://www.bro.org/

[2] D. Karev, C. McCubbin, and R. Vaulin, "Cyber Threat Hunting Through the Use of an Isolation Forest," in Proceedings of the 18th International Conference on Computer Systems and Technologies - CompSysTech'17, 2017

[3] Dragos. CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Retrieved from https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[4] International Standard 60870-5-104. International Electrotechnical Commission. 2006.

[5] JP 3-60 Joint Targeting. 2013. United States Department of Defense. 2013. Retrieved from http://handle.dtic.mil/100.2/ADA434278

[6] L. Qiong, B. Wang, and H. Wu, "Targeting Algorithm Based on ITSM," in Proceedings of the 2017 International Conference on Software and e-Business - ICSEB 2017, 2017.

[7] "PsExec - Windows Sysinternals," Microsoft. 2016. [Online] Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

[8] R. L. Rollason-Reese, "Incident handling," in Proceedings of the 31st annual ACM SIGUCCS conference on User services - SIGUCCS '03, 2003

[9] R M. Lee, D Bianco. "Generating Hypotheses for Successful Threat Hunting," SANS Institute InfoSec Reading Room. 2016. [Online] Available: https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

[10] S. Wen, N. He, and H. Yan, "Detecting and Predicting APT Based on the Study of Cyber Kill Chain with Hierarchical Knowledge Reasoning," in Proceedings of the 2017 VI International Conference on Network, Communication and Computing - ICNCC 2017, 2017.

[11] S Caltagirone, A Pendergast, and C Betz. "The Diamond Model of Intrusion Analysis," DTIC, July 2013. [Online] Available: http://www.dtic.mil/docs/citations/ADA586960

[12] "Snort - Network Intrusion Detection and Prevention System ," Snort. 2018. [Online] Available: https://www.snort.org/

[13] W. Stacy and J. MacMillan, "Cognitive bias in software engineering," Communications of the ACM, vol. 38, no. 6, pp. 57–63, Jun. 1995.

[14] "About Wireshark," Wireshark. 2018. [Online]. Available: https://www.wireshark.org/#aboutWS

[15] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the IOC Game," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16, 2016.

Last Updated: May 3rd, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**