



# Advancing Threat Hunting

## Cyber Threat Glassing with Augmented Memory

Preparation	3
Formulating a Hypothesis:	3
Data Collection and Consolidation:	4
Investigation / Analysis:	5
Enhance Hunt Operations:	5
Threat Glassing with Polarity	6
The future of Threat Hunting - Glassing Realized	10
References	11



The cyber defense strategies adopted by organizations of all shapes and sizes are constantly in flux; adapting and evolving to meet the growing challenges and demands placed upon them by an ever-growing sum of internal and external business drivers. Chief amongst those drivers are external and internal threat actors who have consistently demonstrated an ability to lurk within organizational networks for unprecedented periods of time prior to their detection and eventual expulsion.

These repeated occurrences of excessive adversarial dwell time have fueled schools of thought that to effectively manage an information security program, leaders must acknowledge that fundamental cyber solutions such as firewalls, endpoint protection solutions, and anti-malware products are defeatable by motivated threat actors.

This acknowledgment has contributed to the adoption of practices affectionately referred to as Cyber Threat Hunting (“Threat Hunting” or “Hunting”) within the cyber security community. We can define threat hunting as a focused and iterative approach to searching out, identifying and understanding adversaries internal to the defender’s networks. (Lee, SANS).

While models for threat hunting have been developed for both commercial and scholarly publication, a model has yet to be published by a standards organization such that a defacto model might be referenced at the time of this document’s release. As such, the following is Polarity’s perspective on the various phases of a hunt.



## PREPARATION:

Successful threat hunting first depends on thoroughly understanding the operating environment (Long, 2016). Similar to traditional hunting, those responsible for cyber hunts will recognize greater successes in their endeavors should they be acclimated to their environment - understand their surroundings. Further, it is not enough to know simply what exists within the environment, but how the orientation of entities within the environment, impact one another. Threat hunters need to be aware of systems available within the target environment, their functions, interconnections, their intended configurations and the value of those systems to a threat actor.

Further, as personnel resources are not unlimited, hunts are typically best targeted against environments where actionable intelligence suggests potential threat action or forcible negative outcomes resulting from a compromise of that environment are so immense, that investment into a hunt within that environment should be made without such intelligence. This can aid in the formulation of hypothesis prior to hunt execution.

### Preparation Challenges:

On a hunt, acclimation is key. Hunt teams often “parachute” into highly prioritized environments. While the organization may collect logs, feed analytical platforms and utilize visualization platforms to support analysis, much of the value of such tools can be nullified if the members of the hunt team have no working understanding of the operating system producing the logs, the business function and features of an application environment subject to the hunt exercise or nature of interconnected systems.



## FORMULATING A HYPOTHESIS

The resources available to any institution are finite. Further, as cyber threat hunting is a relatively new concept within the framework of an information security program, even the largest and most sophisticated of organizations lack the proper staffing to execute hunt operations to the degree that their leaders feel is necessary. As such, environments are targeted in accordance with a risk-based approach and upon consideration of available internal and external intelligence sources.

Value to a threat actor may be one of the most difficult things to anticipate, theorize or develop a hypothesis around. This is because different threat actors recognize different aspects of the network as high-value targets. For example, in a scenario where an organization’s analytical system is being targeted by a threat actor, one such actor may be interested in (1) stealing the data processed by the system, another in (2) disrupting the integrity of the systems output and another in (3) stealing the algorithm(s) running against the data set.

Should hunt team members fail to consider these (and other attributes) the hypothesis formulated by the team may be overly broad, under-resourced and eventually yield little to no value to the organization compared to what could have been realized - had appropriate factors been considered.

### **Hypothesis Challenges:**

Tapping into intelligence sources, ensuring their currency and making the best use of them in the formulation of these hypotheses can be cumbersome. Often times, this will include a review of historical incidents to determine realized or observed adversary activity, a review of historical vulnerability information, identifying the coverage of existing security controls that might mitigate certain threat activity or otherwise create detectability of such activity.



## **DATA COLLECTION AND CONSOLIDATION**

Following the development of a hypothesis, members of the Hunt Team will need to acquire the necessary data in order to prove to disprove the hypothetical scenario subject to analysis. Sources of log data could include, but are not limited to those generated by network appliances, security appliances, native Operating Systems, database applications etc.

Not all logs are created equal. Logs from system to system will vary in availability, reliability, and usability. Unavailability is probably one of the most common obstacles encountered by hunt teams and incident responders alike. While in isolation, log unavailability can be an indicator of malicious activity, it is more commonly a direct result of failures in log management and IT/IS governance - leaving matters of reliability and usability to contend with. Reliability of data sources should be evaluated prior to placing reliance on such log data during a hunt or an investigation. In order to validate the reliability of the log sources, hunt team may need to conduct inquiries into the log sources directly. This could include a review of historical accesses changes to log files/repositories, and timeline analysis of logs for gaps in coverage. Depending on the size and scope of the hunt, validating the reliability of log sources could consume significant resources before the hunt effort is underway, detracting from the mission defined by the hunt team.

Experienced hunters know that their efforts are better served by augmenting their approach with the technology that allows them to be most efficient. In the later phases of a hunt, specifically during investigation/analysis phases, importing logs into a common platform for analysis may be paramount.



## INVESTIGATION / ANALYSIS

The Hunt Team will evaluate collected information within the context of the initial hypothesis to determine if an actual threat has been realized. The analysis process should include the following steps:

- Confirm that a threat has been realized
- To what extent (scope and magnitude)
- Establish a timeline of events
- Determine the overall impact

Often, a mandate to operate in accordance with a risk-based approach as well as within budgetary limits - confines the execution of a hunt within a limited scope. While, not a desired condition, this limited scope could translate the evaluation of information within a narrowed view, or bias, resulting in failure to identify activity as its nature was not a corollary to the scope of the hunt.

To be successful in analysis, hunt team members must collectively position the motivations of all manner of threat actor at the forefront of their mind, and establish a mechanism for understanding the various tools, techniques, and processes leveraged by these actors.

### **Investigation / Analysis Challenges:**

Reviewing at logs in isolation and relying on manual analysis alone can be cumbersome and ineffective. (Lee, Lee 2016) Hours of monotonous lookups, queries, and data entry reduces the quality and speed of human decision making - leading to mistakes of habit. Further, quality pattern recognition degrades to cognitive shortcuts to clear the queue of “false positives”.



## ENHANCE HUNT OPERATIONS

Assuming more hunts are to be performed in the future, hunt team members should strive to enrich their existing data stores and technologies with the information and intelligence that they've gathered in the performance a hunt effort.

Finally, successful hunts form the basis for informing and enriching automated analytics. Don't waste your team's time doing the same hunts over and over. If you find an indicator or pattern that could have the potential to recur in your environment, automate its detection so that your team can continue to focus on the next hunt. Information from hunts can be used to improve existing detection mechanisms, which might include updating SIEM rules or detection signatures. The more you know about your own network, the better you can defend it, so it makes sense to try to record and leverage new findings as you encounter them on your hunts.

## Challenges in Enhancing the Hunt:

One of the biggest challenges to enhancing the hunt while also enhancing operational delivery of results from the hunting exercise is timeliness. Up until now, there has been no effective mechanism allowing for tactical intelligence to be tagged, enriched and disseminated across functional teams in such a way that it is available in a real-time fashion to analysts on their desktops as they are conducting an investigation. Imagine a scenario where multiple analysts working in a collaborative setting have immediate, collective knowledge of all entities being captured and extracted during a hunt. For example, imagine each member of my hunt team having access to intelligence I personally captured moments ago while they scour through hundreds of operating system event logs or network intrusion alerts, etc. Furthermore, once tactical intelligence has been developed, it is often stored in static repositories which must be manually queried by operational analysts working in an operations center setting or similar. This manual retrieval and recall of intelligence has the unfortunate effect of slowing or stalling the process of attack identification even in situations where actionable intelligence already exists.



## THREAT GLASSING WITH POLARITY

Glassing is a lesser known technique employed by more experienced game hunters, that relies on forgotten tradecraft to survey a given landscape, such that the entirety of the landscape can be evaluated for the slightest indicator of the target, without sacrificing range from the narrow view of scope as preferred by most game hunters.

This expanded view, made possible via more traditional tools such as binoculars, tripods and simple awareness of environmental conditions, allows for the expansion of view and

Within the context of a cyber hunt, glassing involves stepping away from targeted point investigative and analysis procedures and evaluating information from a longer and wider view, such that an abundance of contextual information can contribute to the hunt at any time, so long as it is relevant and valuable to the Hunt Team.

Glassing allows for the analyst to make the most use of information at their disposal, without limiting themselves to a limited scope of evaluation or investigative procedures.

In the methodology highlighted in this document, there were several core challenges identified that

- **Preparation**
- **Hypothesis Development**
- **Data Collection/Consolidation**
- **Investigation**
- **Enhancement**

## Preparation

Before launching into a hunt operation, Polarity can enable teams to instantaneously have a working knowledge of all systems within scope for a hunt operation. Such asset information can be accessed from historical hunts, human notations, asset management solutions or Configuration Management Databases.

Further, these team can operate with immediate knowledge of key works, functions, usernames/user associations, service accounts, etc. without having to leave their screen, break from the operation to engage the business or alter critical path to reference internal wikis and data sources.

Almost as soon as the operation is approved, a hunt team can integrate operational intelligence into the platform, and immediate draw upon its value by way of near real-time situational awareness.

Apply Annotations Manual CSV

When we recognize entities with the overlay, we'll display any annotations applied here. You can also leverage channels to keep annotations organized.

CSV File \*

AIX Syntax.csv

Has Header Row  Skip Invalid Annotations  Skip Invalid Entities

Data Preview

Entity	Annotations
bosboot	<b>P</b> PARAMETER: -a <b>P</b> DESCRIPTION: Create a boot image on the default boot device
bosboot	<b>P</b> PARAMETER: -ad /dev/mt<x> <b>P</b> DESCRIPTION: Create a boot image at location and send to tape
cfgmgr	<b>P</b> DESCRIPTION: Configures devices by running the programs in /etc/methods directory.
chcons	<b>P</b> DESCRIPTION: Redirects the system console to device or file, effective next startup

The threat hunter has imported all AIX syntax into Polarity, Whenever the syntax is observed by this threat hunter, or members of the hunt team in the future, the syntax descriptor will be overlaid on their screen in real time.

## Hypothesis Development

A strong hypothesis cannot be developed without making an attempt to include known or anticipated independent and dependent variables. In the context of a cyber hunt, Polarity helps to recover from inefficiencies associated with historical information gathering processes such as accessing ticketing systems, case/incident management platforms, obtaining historical vulnerability data, observing network diagrams, etc.

Further, Polarity helps to avoid breakdowns and intelligence failures prone to manual processes.

Once any member of the hunt team observes in-scope systems on their screen, environmental variables will become clear, collaboration will be enabled via the platform, and strong hypothesis will follow.

The screenshot shows a Wireshark interface capturing traffic from Wi-Fi. The main pane displays a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A packet at time 17.138604 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The Polarity interface is overlaid on the right side, displaying a filter for entities. The filter shows two entities: 54.88.108.21, identified as #Target\_Hunt\_Environment with tags P VPC, P Hosted Application, and P Crown Jewel App; and 192.168.0.12, identified as #Target\_Hunt\_Environment with a tag P Database Server. The Polarity logo is visible at the bottom of the screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.803999	192.168.0.12	54.88.108.21	TLSv1.2	517	Application Data
5	0.804031	192.168.0.12	54.88.108.21	TCP	517	[TCP Retransmission] 6106→443 [PSH, A
6	0.805463	192.168.0.12	54.88.108.21	TLSv1.2	517	Application Data
7	0.805494	192.168.0.12	54.88.108.21	TCP	517	[TCP Retransmission] 6272→443 [PSH, A
8	0.825391	54.88.108.21	192.168.0.12	TCP	124	443→6106 [ACK] Seq=1 Ack=464 Win=1528
9	0.840389	54.88.108.21	192.168.0.12	TCP	1514	[TCP segment of a reassembled PDU]
10	0.840390	54.88.108.21	192.168.0.12	TLSv1.2	624	Applicati
11	0.840391	54.88.108.21	192.168.0.12	TLSv1.2	1382	Applicati
12	0.840502	192.168.0.12	54.88.108.21	TCP	54	6106→443
13	0.840518	192.168.0.12	54.88.108.21	TCP	54	[TCP Dup
14	0.881226	192.168.0.12	54.88.108.21	TCP	54	6272→443
15	0.881255	192.168.0.12	54.88.108.21	TCP	54	[TCP Dup
16	1.138570	192.168.0.12	54.88.108.21	TLSv1.2	591	Applicati
17	1.138604	192.168.0.12	54.88.108.21	TCP	591	[TCP Retr
18	1.206413	54.88.108.21	192.168.0.12	TCP	124	443→6106
19	1.206504	192.168.0.12	54.88.108.21	TLSv1.2	680	Applicati
20	1.206528	192.168.0.12	54.88.108.21	TCP	680	[TCP Retr
21	1.227318	54.88.108.21	192.168.0.12	TCP	124	443→6106

In this screen capture Wireshark information is overlaid from internal annotations or asset repositories, allowing the threat hunter to identify possible High Value Targets (HVT) within the environment.

Not all datasets are considered equal, true to the principles of glassing, the focus may be placed on more likely areas that a target may occupy, but the whole of the landscape is evaluated for outliers. In some scenarios, analysts may opt to exclude data sets from more targeted analysis or inclusion in any analytical functions applied to the data in the context of a wider body of information.

This may be done as a result of consent, or as a byproduct of the bias of a single analyst.

For whatever the reason, Polarity can help give analysts assurance that data points on screen displayed during manual review or analysed in isolation, can be compared to broader datasets on the fly during analysis.

The screenshot shows the Polarity network analysis interface. At the top, it says "Capturing from Wi-Fi". Below the menu bar, there's a display filter bar. The main area is a table of network traffic:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.803999	192.168.0.12	54.88.108.21	TLSv1.2	517	Application Data
5	0.804031	192.168.0.12	54.88.108.21	TCP	517	[TCP Retransmission] 6106->443 [PSH, A
6	0.805463	192.168.0.12	54.88.108.21	TLSv1.2	517	Application Data
7	0.805494	192.168.0.12	54.88.108.21	TCP	517	[TCP Retransmission] 6272->443 [PSH, A
8	0.825391	54.88.108.21	192.168.0.12	TCP	124	443->6106 [ACK] Seq=1 Ack=464 Win=1528
9	0.840389	54.88.108.21	192.168.0.12	TCP	1514	[TCP segment of a reassembled PDU]
10	0.840390	54.88.108.21	192.168.0.12	TLSv1.2	624	Applicati
11	0.840391	54.88.108.21	192.168.0.12	TLSv1.2	1382	Applicati
12	0.840502	192.168.0.12	54.88.108.21	TCP	54	6106->443
13	0.840518	192.168.0.12	54.88.108.21	TCP	54	[TCP Dup
14	0.881226	192.168.0.12	54.88.108.21	TCP	54	6272->443
15	0.881255	192.168.0.12	54.88.108.21	TCP	54	[TCP Dup
16	1.138570	192.168.0.12	54.88.108.21	TLSv1.2	591	Applicati
17	1.138604	192.168.0.12	54.88.108.21	TCP	591	[TCP Retr
18	1.206413	54.88.108.21	192.168.0.12	TCP	124	443->6106
19	1.206504	192.168.0.12	54.88.108.21	TLSv1.2	680	Applicati
20	1.206528	192.168.0.12	54.88.108.21	TCP	680	[TCP Retr
21	1.227318	54.88.108.21	192.168.0.12	TCP	124	443->6106

Below the table, the Polarity logo is visible. On the right side, a detailed view of a packet is shown, including a "SETTINGS" and "FILTER" section. The detailed view shows the following information:

- 54.88.108.21
- #Target\_Hunt\_Environment
- P IP Forwarding Enabled
- P An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
- ARIN Amazon.com, Inc.
- MM Ashburn, VA (United States)
- MM [AS14618] ASAmazon.com, Inc.

### Investigation:

Polarity automatically searches for and delivers relevant context to analysts as they are working. Analysts are less likely to miss critical intelligence because Polarity removes the burden of finding relevant context information. Since Polarity operates at the screen level, Polarity is able to enable collaboration across multiple applications, toolsets, and workflows. Analysts no longer have to choose between working fast and working thoroughly.

192.168.84.1  
Splunk Number of Results 1  
Splunk View in Splunk  
Total number of results: 1

Polarity combats analyst fatigue by automating the most repetitive and time-consuming components of an analyst's daily workflow. Reduced lookups and automatically delivered context data speeds up the decision-making process letting analysts do analysis.

### Enhancement:

Polarity allows for the efforts applied on a single hunt, to be applied to future hunt operations. The experience and tradecraft collected by a team of skilled professionals can be leveraged to augment a modified team in the future, or a completely different team operating in another hemisphere.

FD904ADDBDFE548C22FFA5223ED9EEE7  
RES Hunt RES Crown Jewels RES Potential Exfil  
RES Severity High  
Resilient  
Displaying 2 related incidents  
Incident Notes  
"Investigated IP Forwarding abuses to determine if host was levered as an alternative means of exfil. No evidence discovered."  
Displaying 1 of 1 most recent notes Post  
Joseph Miller Added a note on 03/07/2019 12:45:16  
Vulnerability scan discovered IP Forwarding Vulnerability - to be investigated by Sr. Hunt Team member  
Incident Notes  
View in Resilient  
Phishing email sent to sales staff.  
Name of incident: Brutus  
Severity: High  
Created Date: 07/10/2018  
Date Discovered: 07/10/2018  
Date Due: 07/12/2018  
Matched Field Name: Resolution Summary  
Phase Name: Detect?Analyze

## THE FUTURE OF THREAT HUNTING - GLASSING REALIZED

Imagine hunt teams capable of a superhuman memory, able to apply historical information seamlessly to an operation, share and collaborate across teams effortlessly and instantly arming front line network defenders with high value indicators or guidance on how to properly triage and/or escalate certain types/classes of alerts without the necessity to perform any manual lookups for entities being viewed within any application window on their desktop.

In this screenshot example, investigation notes posted to the Resilient platform ensures investigative teams have historical information easily at hand and enables them to update investigations without ever leaving the platform or tools they are working in.



## REFERENCES

Lee, Rob and Lee, Robert. M. (2017, April). The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey [https://www.malwarebytes.com/pdf/white-papers/SANS\\_Report-The\\_Hunter\\_Strikes\\_Back\\_2017.pdf](https://www.malwarebytes.com/pdf/white-papers/SANS_Report-The_Hunter_Strikes_Back_2017.pdf)

Long II, Michael. C. (2016, July). Scalable Methods for Conducting Cyber Threat Hunt Operations <https://www.giac.org/paper/gsec/38852/scalable-methods-conducting-cyber-threat-hunt-operations/152744>