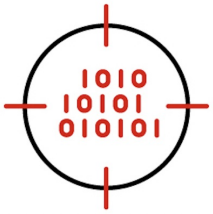
Mandiant

INTRODUCTION TO AN INTELLIGENCE-LED THREAT HUNTING FRAMEWORK



This article focuses on the cyber defense function: **Threat Hunting** – the use of intelligence to pro-actively seek critical threats within your organization's operating environment.

Read Time: 6-8 Min

Threat Hunting is an important complement to your organization's other monitoring and detection capabilities. This article outlines how to structure the Threat Hunt Mission using our A4 Framework.

Objectives and Key Actions for Application

Mandiant uses a specific definition for Threat Hunting:

> **THE METHODICAL, USE CASE DRIVEN, PROACTIVE IDENTIFICATION OF CYBER THREATS WITHIN A COMPUTING ENVIRONMENT OR INFRASTRUCTURE.**

Cyber threat intelligence is required to help identify those threats we should be looking for, based on the likelihood and impact of those threats. In other words, organizations should be actively looking for those threats they expect to target them.

Threat Hunting complements security detection. Organizations often focus on reactive defense - identifying the presence of attacks through alert generation of their malicious activities by deployed security monitoring solutions. Threat Hunting is pro-active – actively searching through your environment to detect and isolate signs of malicious activity that have evaded existing security controls or detection solutions. These two processes complement one another.

Intelligence analysts are often taught an idiom that guides their thinking around threats: the absence of proof is not proof of absence. Put plainly, intelligence analysts shouldn't presume they have seen or are aware of all the threats challenging them. Threat hunting is required to dig into your environment and root out those adversaries sophisticated enough to penetrate your line of defenses and hide their activities. Or, to detect new variants of malware whose capabilities slipped past current detection methods and signatures.

> **The absence of proof is not proof of absence.**

Often the first question Mandiant gets asked regarding threat hunting is: What (or Who) should I be looking for? The answer may be different depending on your type of business, industry, geography, size, internet presence, etc., but in the first instance organizations should be using intelligence to define potential hunt targets.

One useful place to start is to consult your organization's Cyber Threat Profile (CTP). (See **Creating a Cyber Threat Profile (https://docs.mandiant.com/home/creating-a-cyber-threat-profile)**.)

Overall, the three levels of intelligence can provide different information and context to help frame Threat Hunting objectives:

- Strategic intelligence can define the types of threats most relevant to your organization, based on recent and historical reporting of the capabilities and motivations of threat groups active within your industry, geography, etc.
- Operational intelligence can specify the Tactics, Techniques, and Procedures (TTP) adversaries will use should they seek to challenge your organization's defenses.
- Tactical intelligence enables analysts to pivot with purpose through vast amounts of data to confirm (or refute) the presence of previously undetected threat activities by using data recently associated with adversaries and/or their capabilities.

Mandiant's A4 Threat Hunting Framework

To assist in building Threat Hunting capabilities, Mandiant developed a framework to guide intelligence practitioners in scoping, searching, analyzing, and actioning the results of Threat Hunting. We call this process the A4 Framework:

- **ASSESS** sees analysts develop a Threat Hunt query that scopes parameters of the specific hunt.
- **ACQUIRE** encourages analysts to identify their access requirements for the environment to be searched, and then initiate the search.
- **ANALYZE** evaluates the results of the Acquire phase to identify the attack vector, potential impact, and control effectiveness.
- **ACTION** drives the response through identification of security gaps, remediation efforts, and future recommendations.

ASSESS: Threat Hunt Scoping

Scoping the Hunt Mission outlines the parameters under which analysts can conduct a defined search for specific conditions that may indicate adversary activity. Generally, hunt missions are successful when they obtain artifacts within the environment that, upon analysis, indicate an adversary's presence or impact. Given the size of many organizations' operating environment and the innumerable threats using a variety of intrusive methods, scoping the hunt mission is vital to ensure analysts don't waste time second-guessing every piece of data examined.

While the primary strategic goal of a Hunt Mission may be to identify the presence of adversaries to bolster defenses, the tactical objectives of each individual search need to be clearly defined to provide analysts terms of reference under which

they are searching. These searches, or Threat Hunt Queries, will include repeatable elements such as timeframe, type of data to be searched for, adversary TTPs on how they'd use that data, and resources required, including those systems that require access. Each Threat Hunt Query should be constructed in a similar manner using a repeatable template. This allows for future iterations of the same search.

- What are we looking for?
- What do we expect to find/ not find?
- Where will we look?
- Why are we looking for it?
- What does its presence/ absence tell us?
- Who would be interested in our results?

ACQUIRE: Search the Environment

Once the Threat Hunt is scoped, the search can commence! In theory, at least. Often, prior to the first time a query is run, analysts will need to obtain access to relevant source data and systems and, importantly, understand their limitations. Knowing how and what various systems capture and store, including the way they process, sort, and organize data, is vital to accurately analyze the results returned from the query. Transferring (or processing) data may alter or lose some attributes that could have an impact on subsequent analysis.

Fidelity

The loss of factual purity when data is transferred or processed from machine-readable formats to human-readable formats is called Fidelity.

Just as transferring audio recordings may lose clarity and crispness, processing data between platforms, repositories or capture methods may alter the data in subtle ways.

Analysts need to understand these limitations, not to create solutions, but to ensure their analysis accounts for these limitations.

Analysts will also need to have a good understanding of the tools required to execute the search.

Once the search has been executed, an initial analysis or triage is required. Mandiant's A4 Framework is a guide on the Threat Hunt Mission process. However, not all stages may be necessary – consider if the Acquire stage determined an active, present threat. This would likely require escalation to security teams responsible for managing these types of threats—Incident Responders. Hunt Mission analysts should remain focused on their mission. Note: This scenario would count as a great success for the Hunt Mission team! They found an active, unknown threat behind the wall of defenses.

ANALYZE: Validate Results and Draw Conclusions

The analysis phase of Mandiant's A4 Framework focuses on validation, corroboration, and extrapolation of results from the Acquire phase. Analysts will need to evaluate the accurate and strength of the results from the search to determine how closely they adhere to the adversary's known Techniques, Tactics, and Procedures (TTPs). Results should be compared to the original parameters established within the Assess phase. It's not uncommon to have to tweak or refine some search parameters and then run the search again. Like search engine queries, further refinement may be needed upon evaluation of initial results. We don't often find exact matches upon first try.

This evaluation process should seek to prioritize the data returned. Without cyber threat intelligence, evaluation becomes difficult. The results of the Hunt Mission Query should be sorted and linked to matches from cyber threat intelligence. This adds valuable context which allows the results to be prioritized appropriately.

If high enough priority, analysts should pivot to related or new data that expands on this initial context. The parameters of

the Hunt Mission Query should be kept close at hand—these are the justification for the analytical activity and serve as a comparison point to assess the nature of the threat under analysis. Remembering that high fidelity/high priority results are an indication of known threats entering your organization's environment without detection, analysts should focus on determining the attack vectors, TTPs, and the potential impact of the previously undetected attack. This process should also include an evaluation of the security control effectiveness, to determine how the adversary remained undetected.

ACTION: Determine Impact and Drive Action

All intelligence analysis needs recommendations and action. These recommendations and actions should always be tied to the impact the adversary's methods have had, or are likely to have, on your organization's operating environment. At a minimum, this impact will focus on two main areas:

- The damage, exposure, or weakening of data, systems, and controls within your environment (i.e., the **What**)
- The gaps, security flaws, or lack of detection that enabled access, enumeration, movement, and influence over your operating environment (i.e., the **How** and **When**)

The conclusion of the Threat Hunt Mission needs to be a threat summary and concise report that details both the nature of the threat and breakdown of the security controls. These assessments need to be delivered in a professional manner, absent of blame, and focused upon strengthening identified gaps and weaknesses.

Analysts writing Hunt Mission reports should make their recommendations and findings clear. After all, threat adversaries may seek to replicate the same successful process—stakeholders need to be clear regarding their role within preventing a repeat incident.