Developing a Threat Hunting Program

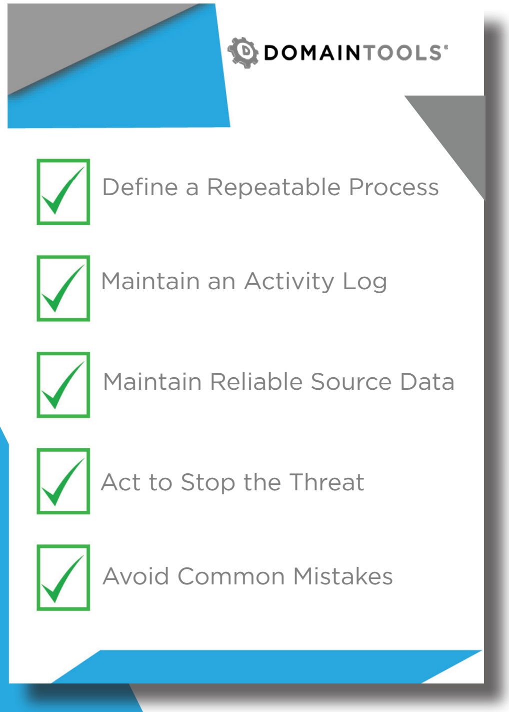
Checklist: A 5-Step Guide

Overview

Threat hunting is one of several approaches to proactively reducing risk. Internal threat hunting attempts to create early identification of activities and artifacts inside the perimeter defenses to reduce dwell time and the associated impact of allowing threats to operate within the environment.

Less practiced but equally problematic is external threat hunting. External threat hunting attempts to identify artifacts outside the perimeter that indicate another entity is targeting an organization and could affect the organization's customer loyalty, brand equity, or compliance. Diligence in external threat hunting allows the defending organization to identify an attack or a campaign early in its lifecycle, thus stopping it in the preparation phase or early in the deployment phase, both of which reduce impact.

Because organizations are now being affected by threat actors both within and without the perimeter, understanding how to conduct internal and external threat hunting activities in a programmatic manner is a growing imperative. This checklist will help organizations new to threat hunting create the foundations for conducting threat hunts.



DOMAINTOOLS

- ☑ Define a Repeatable Process
- ☑ Maintain an Activity Log
- ☑ Maintain Reliable Source Data
- ☑ Act to Stop the Threat
- ☑ Avoid Common Mistakes

Step 1: Define a Repeatable Process

The threat hunting path changes based on choices and decisions made by the hunter. Documentation of threat hunting should include the general process and workflow requirements to aid the inexperienced, while also allowing flexibility for more experienced hunters to deviate based on the choices they must make as the clues are exposed. Details may include information to aid in investigating highly customized systems or applications, but teams should not be expected to have every detail documented.

This structure aids in training the inexperienced but also supports repeatability, which accelerates single investigations and makes the activities more scalable through increased efficiencies. It is important to remember that the process of investigation is a combination of art and science and will evolve over time.

Step 2: Maintain an Activity Log

Activity logs record the actions taken and artifacts gathered by the threat hunter during the investigation, including any ideas and conclusions that result. These journals indicate the dates and times activities were performed and the results of those activities. Documenting failures is as important as documenting successes because the failures create experience for lessons learned and avoid duplication of dead ends should a case be handed off.

Hunting is frequently a side or secondary activity for a security person, meaning personnel are often interrupted during the course of a day. Any investigation may also span multiple shifts or days. Multiple threat hunters could end up working the same case via a shift handoff or because they intersect from different starting points. All of these situations make thorough documentation imperative to reduce rework and accelerate efficiency.

When working externally, quality documentation of malicious domains, suspicious DNS, and other indicators will be crucial to getting external service providers to act on your behalf. Remember, by acting on your request, they will impact one or more of their customers, which may result in revenue loss.

In a general post-incident review, the documentation is a necessary part of the feedback loop to improve the process and assist in training for future investigations. The details of the activity log are considered evidence, so in the event of a legal proceeding or criminal investigation, the activity log is a foundational element of those legal processes.

Step 3: Maintain Reliable Source Data

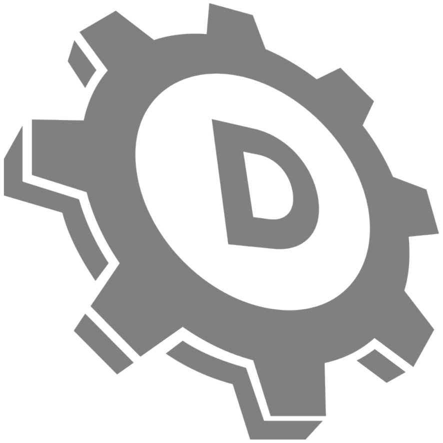
While metadata is all the rage and is very useful for investigations, it is most often not sufficient to gain a conviction or sufficient attribution to motivate a registrar or other third party to act. With this in mind, hunters must take steps to maintain the source data containing the clues they find. Original data must be maintained and its integrity must be held in some form to be usable as a foundation by third parties for cease and desist requests, criminal or civil cases, or other activities.

Any third party can request source data to back up a claim involved in a shutdown or cease-and-desist request. When these requests arise, businesses must have the original data supporting the claims. If you can't provide it or its integrity can be called into question, they will not take action. Some third parties, especially in the case of legal proceedings, may also engage their own forensic investigator to confirm/refute the integrity of the hunter or the findings. This means that investigators will need the same data the hunter had to determine whether other conclusions could be drawn.

In the case that a particular hunt links activity over a longer period of time, if the source data is not maintained, the activities will not be attributable to the threat actor if the source information has been removed during the course of operations and maintenance.

When external data is required, such as domain registration, reputation, and DNS, having a partner with a rich historical repository that is well-maintained and curated is an invaluable asset. Such a partnership allows hunters and their organizations to focus on their work without worrying about whether the data they used or will need will exist when they need it.

Step 4: Acting to Stop the Threat

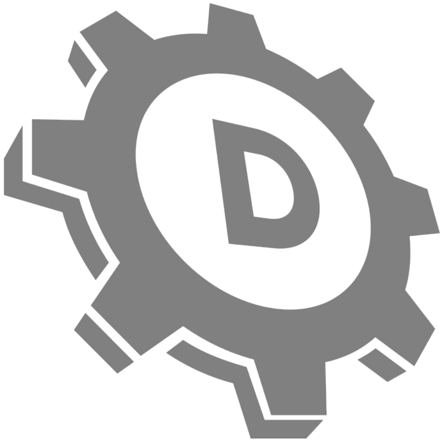


Once the investigation comes to a point where action can be taken, the hunter must have the case documentation in order to motivate a call to action based on their request. If any of the foundational steps previously discussed have been circumvented or missed, the associated request(s) for actions by third parties, such as law enforcement, hosting providers, domain registrars, and any other entities, has a significant chance of being rejected.

Both internal and external relationships are imperative. Motivating internal personnel and third parties to act is as much about the relationships as the evidence. Anyone can indicate that they will take action, but their relationship with and the reputation of the requestor will be large factors in determining the priority they put on acting, especially in the case where there are no laws or treaties supporting the request.

Having a trusted partner for response support will make the largest difference when dealing with third parties. Building relationships and reputations takes many interactions, which individual companies have far less opportunities to achieve. A partner focused on response support has a much greater opportunity to have the repetitive interactions that build that reputation and the necessary relationships to drive timely action.

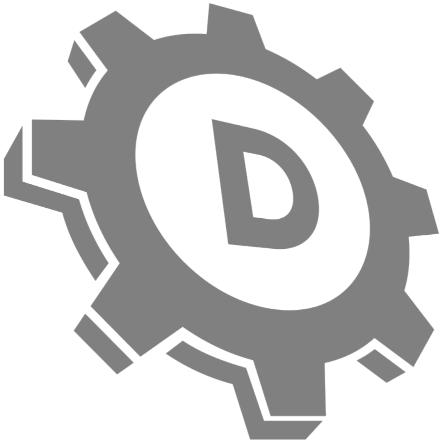
Step 5: Avoid Common Pitfalls and Mistakes



Few (if any) hunts go perfectly from the first clue to the final conclusion. Though problems and roadblocks will decrease as the hunter gains experience and the related intuition, every hunt can be sidetracked and every hunter can get frustrated or discouraged. Below are a few points that can minimize these occurrences.

- It's good to think outside the box (attackers do)
- Dead ends are okay, as long as you learn from them
- As you develop your instincts, trust them
- Not all data is "real" data—attackers can place fake clues
- The absence of data can be data
- Domains that have been used for nefarious purposes during their lifecycle tend to stay bad
- Guilt by domain (or IP) association is real
- Not all registrars are trustworthy
- An adversary may have gotten there first
- Don't let investigations or responses inadvertently interfere with operations
- Even registrars and providers can be duped
- You don't have to act alone—having professional relationships with other hunters and related groups is invaluable

Bonus: Understanding the Scope of the Hunt



In every hunt, there are pieces of information that become the foundation of the investigation. The type of information that is most valuable will depend on the investigation, but listed here are the most common datasets that will provide value on a regular basis.

Internal

- System Configs
- Logs
- Processes
- Network Connections/Packets
- Users/Identity
- Files
- IP Addresses

External

- Domains
- Registrars
- DNS Registrations
- Whois
- Hosting Providers
- Passive DNS
- IP v4 Address (to some degree)
- Web Search (to some degree)

Conclusion

Threat hunting is becoming a more valuable skill for organizations of every size. Finding personnel with significant experience and time to perform the duties in this area is difficult. Using this guide will aid organizations in creating and enlarging that talent pool and improve their programmatic approach to threat hunting.

At the same time, having a trusted partner for data collection and curation should be a serious consideration to accelerate and enhance investigations for faster conclusions and better outcomes.

For more in-depth examples on how to build your own threat hunting program, join Managing Director of Research at EMA, David Monahan, and DomainTools Security Sales Engineer, Taylor Wilkes-Pierce, in their **pre-recorded webinar**. They explore the building blocks necessary to create a threat hunting program from scratch, including practical steps your organization can put into place right away.

Check out the webinar **here**.

About DomainTools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity **https://www.domaintools.com** or follow us on Twitter @domaintools.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** or **blogs.enterprisemanagement.com**. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3825.042219