# Structure

Like all aspects of security, having a solid foundation to build on is essential, but where do you go from there? What are the key parts that make up a hunt program? What are the right data sources? Who should be your hunters?

Answering these questions and deciding when and how to hunt can be overwhelming enough to stop some teams before they ever get the chance to do their first data carve. This section will guide you on the path to building your first hunt team by helping you determine who the right people are to be your hunters and what their roles will be within the team.

## Roles and Responsibilities

A common misconception when deciding to create a threat hunting team is that the hunters need to be experts in as many aspects of security as possible. As the security industry grows and becomes more specialized, finding analysts that are well versed in every operating system, network technology and protocol, and the security challenges or flaws with those technologies can be incredibly difficult. And while it’s great to have hunters who’ve been part of the security industry for many years this isn’t always possible, or even necessary.

That being said, if you can find a generalist who’s got a vast amount of security knowledge across a multitude of disciplines then you’ve found yourself a perfect Principal Threat Hunter. But if you’ve got someone who’s really only strong on, for example, network technology, that’s fine, you just have a hunter you need to point in a particular direction until they gain the knowledge to allow them to expand their hunts into different areas.

Deciding what role a hunter falls into can be a challenge, but here are a few guidelines to help you determine where your hunters might fall.

## Principal Threat Hunter

This individual should have extensive experience with all aspects of information security and how they tie together. They should be able to conduct advanced analysis while using best practices that they have either helped develop or understand at a level that allows them to transfer that knowledge to lower level hunters. They should be able to develop dashboards and reports to communicate findings within the team and with senior leadership. Principal Threat Hunters should be involved in selecting the technologies that enable the most effective hunts for their organization. Using findings from hunt activities they should be able to provide feedback and recommendations on how to improve the organization’s security program.

## Senior Threat Hunter

This individual has a strong grasp of security technologies and architecture. They should be able to conduct analysis of host activity and network traffic across a wide variety of platforms and technologies. A Sr. Threat Hunter should understand a wide range of threat intelligence and adversary tactics, techniques, and procedures (TTPs). Using intelligence found through hunt campaigns this individual should be able to assist in, or lead, the development of appropriate countermeasures. They should participate in the creation and documentation of threat hunting hypothesis and track the effectiveness of the associated hunts.

## Threat Hunter

A new threat hunter should have experience with network and/or host based intrusion analysis. They should have a good understanding of how Windows, Linux, and Mac operating systems function. They should have some experience assessing threat intelligence to identify intelligence that is relevant to the organization and be familiar with adversary techniques and attack lifecycles. The ability to communicate clearly and document findings for later research, use, or escalation is also key to this role.

## Mindset

There are things that make a good threat hunter that are less technically quantifiable and yet have an impact on the success of the hunter both in terms of what the organization gains as well as how much the individual enjoys the role.

The following are several traits you might take into account when considering individuals for a threat hunting role:

* Offensive security experience. The ability to think like an attacker will allow easier hypothesis creation as the hunter can see themselves in that role and identify areas that they would consider an area of organizational weakness worth targeting.
* Investigational mindset. Identify who within your team likes to chase down a problem until they find a solution. Not only trying to understand if something is there, but why and how it exists in the first place. The natural root cause analysis seekers. The puzzle solvers.
* Attention to detail. Find those who notice small errors or patterns in everyday things. If an individual is quick to point out a typo in a PowerPoint presentation that no one else noticed, or a pattern in the way someone speaks, the behavior of coworkers, or how information is displayed, this is a good hunter. They recognize patterns, how something should look, and when something deviates from the norm.

Hunters really need to understand how the area they’re hunting in should work. Understanding what something looks like when it’s functioning normally allows you to determine when there’s a potential issue. When a hunter sees a protocol not working the way it’s outlined in the RFC, or a process spawned by an application it shouldn’t normally have a relationship with, that’s when they’re going to find something interesting. Remember, threat hunting is an exercise in outlier detection and it’s only possible to find an outlier when you know what the baseline is.

## Staffing

When building a threat hunting team determining the right people to participate in your hunts can seem like a difficult task. Balancing experience and specialization while ensuring resources for other aspects of your security program. But it’s not just about who the right people are, it’s about how many people should be hunting as well.

Deciding the number of staff to dedicate to a particular offering can be challenging. Each organization has a different sized SOC, is staffed at different levels, and with different roles and responsibilities. Some organizations have no dedicated threat hunters at all, while others have full teams of hunters at their disposal. We’ll approach staffing with those differences in mind.

## Small Organizations

Convincing management that utilizing resources that are already spread thin in order to begin a threat hunting program isn’t easy to do, but just like the size of your team, start small. Don’t think about hunting as something that requires dedicated team members, think about it in hours. Start by carving out a small number of hours for each analyst each week to spend hunting. As each analyst participates in a hunt ensure that they’re documenting the hypothesis that they are working on, what things caught their attention, what they learned by exploring that hypothesis, and of course what findings, if any, there were while working on it.

Going back to management and saying “We’ve spent 16 hours hunting this week but haven’t found anything” isn’t going to get you more time to hunt. However, going back and saying “We tested four different hypothesis that led us to create two new alerts and one resolve one misconfiguration” will.

* Start small. 4-6 hours per analyst per week.
* Document your findings to show value.
* Grow the number of hours as proof of value is shown.

## Large Organizations

Just because an organization is of a significant size doesn’t mean that it’s spoiled for resources. What it does mean is that it can sometimes be easier to move some of those resources around, test new ideas, or launch new projects. Ideally, an organization of any significant size should have 10-20% of its SOC staff dedicated to threat hunting. This number may sound significant, but as you conduct hunts and see the immense value that comes from them this number will absolutely make sense. The option of having dedicated hunters means that you can ensure the time spent by these individuals is focused on putting threat intelligence into action and that they aren’t being distracted by the alerts and tasks assigned to a typical SOC or CIRT analyst.

* Dedicate between 10-20% of SOC or CIRT staff as threat hunters.
* Create clear lines of communication between hunters, the threat intelligence team, SOC/CIRT analysts, and incident responders.
* Document and escalate findings to management in order to show value of this specialized team and make the case for additional full time equivalents (FTEs) to expand the hunt team.

It is the experience of the authors of this framework that threat hunting is responsible for the detection of the types of data that leads to more declared incidents than by working alerts or incidents out of a queue. By its very nature threat hunting is focused on the discovery of activity that isn’t being detected by security appliances, applications, or standard remediations. This leads to hunters encountering attacks or methods of persistence that require varied skill sets and the time to understand how best to handle the threat and create new mitigations to meet them. A dedicated and focused hunt team working side by side with analysts and incident responders is the most effective way to do this.

## Communication

An important aspect of any successful threat hunting team is the ability to communicate freely and effectively. Hunt teams should be able to engage different parts of the organization without barriers and as equals.

## Interdepartmental

Threat hunters should seek out a relationship with all technical aspects of the organization. For example, having a positive relationship with the IT department can lead to a better understanding of why particular applications are included on the golden image of hosts within the environment, or why a particular protocol was chosen as the method of transit for information throughout the organization. This insight allows threat hunters to understand the inner workings of the devices, applications, and data they’re tasked with investigating on a level that will give them an advantage over any would be attackers.

The first thing an attacker will do upon breaching any level of defenses in an organization is to start learning as much about what they’ve gained access to as possible. They’ll try to understand where they are and what’s connected to them so that they can maintain persistence for as long as possible. If the attackers are taking the time to learn as much as they can about our environments, shouldn’t we?

## SOC/CIRT

A critical component of threat hunting is threat intelligence. Threat hunters require the latest, high quality, threat intelligence to know where to spend their time hunting. The type of intelligence that goes beyond indicators of compromise (IOCs) and embraces tactics, techniques, and procedures (TTPs). Working with your team to determine which threat actor groups are the most likely to target your type of organization and what attacks and tools are most likely to come your way can help you focus your hypothesis on areas that will have the most impact to driving down risk to the organization. Hunters should also be feeding intelligence back into the team as it’s discovered. Threat hunters can be an incredible resource for intelligence that is highly relevant to the organization because it was found within the organization.

When a hunter inevitably finds evidence of an attempted, or successful breach they will have to be familiar with the incident responders, and the most current incident response plan so threat they can seamlessly shift gears from hunting, to responding.

## Threat Hunting Team

An absolute necessity of any threat hunting team is the ability to communicate with one another effectively. To share what hypotheses they’re working on, how far down the rabbit hole they’ve gone, what they’ve collected, and how they could hand it off if necessary to do so.

Hunt teams should utilize a shared documentation system, something that allows them to see real time notes and data on not only hunts that are ongoing, but all hunts that have taken place in the past. This allows the team to build a threat hunting knowledgebase; a reference when they detect an anomaly to see if it’s been detected before and how a previous hunter handled that situation. Data silos and tribal knowledge are not useful for the knowledge of the team, or for the ensuring that the organizational resources that were spent to facilitate the hunts were used most effectively.

While teams will consist of hunters with varying skillsets and levels of experience it’s important that any hunter, whether brand new to threat hunting or a seasoned expert, has the ability to review hunt data and call attention to anything they see as a potential concern. All anomalies are interesting and require investigation, regardless of who detected them or whether they ultimately lead to an attacker. Many years ago the airline industry made it an industry practice that any individual involved with an aircraft could raise a concern and all parties must investigate, I repeat, must investigate. From the co-pilot, to the ground crew, to the flight attendant. All parties on or around an aircraft are equal. It’s one of the reasons that the airline industry has such an impeccable safety record. Safety comes first, not rank, expertise, or perceived hierarchy. This same mentality should be used within any threat hunting team when it comes to organizational security. If any member of the team has a concern it’s taken seriously and a proper investigation is completed and documented.

Leadership

Communicating the effectiveness of a threat hunting team to leadership is a challenge all its own. When the SOC sends a report to leadership they can say “We received X number of alerts this week which led to Y incidents or escalations.” As anyone who has spent time as a SOC analyst can tell you, the alerts just keep coming. Quantifying threat hunting can be much more difficult. Leadership is going to want to know what you’re doing with the time spent hunting and how it’s leading to a more secure organization. We can do this with our own metrics. We’ll get into this in greater detail in the Metrics section of the OTHF but understanding that tracking the number of hypotheses you’ve created, what was learned from investigating them, and what additional alerts, automations, and reports were created because of them. We’ll want to track how many vulnerabilities were discovered, misconfigurations identified, and gaps closed to reduce the organizational attack surface. All of these things are what leadership cares about, and we need to be sure they know what their threat hunters are doing and how their improving the overall organizational posture, and driving down risk.

## Skills Matrix

Threat hunting requires varied skills, and understanding where those skills lie within your hunt team, as well as the broader SOC/CIRT is invaluable. One of the best ways of doing this is with a skills matrix. A skills matrix is like a map of the different competencies that exist within a team. It allows you to not only understand where your team is the strongest, but also identifies areas that require development and any gaps in coverage. This is useful for training and development opportunities, but also a great resource when considering hiring additional members of the team.

Access to the skills matrix should be for management or senior leadership only. Often times when this type of resource is expected to be public, individuals will overstate their skills in areas that they believe will reflect poorly on them within the team. This is not a tool for shaming, it’s a tool for tying the most effective resources to the hypothesis that suits them best or pairing an expert with a novice so that they can help the novice level up their abilities.

The following is an example of a skills matrix that might be used to assess a potential threat hunter. It is important to note that each organization is different, this is not meant to needs of every organization or team, but as a stepping stone in the right direction.

Example

Rating on a scale of 1-5

5 - Expert. - Highly experienced. Needs no help from others. A subject matter expert (SME).

4 - Proficient - Experienced. Can work alone with little help. Working toward expert.

3 - Mid-level - Some experience. Can perform on their own with occasional help needed.

2 - Basic - Limited knowledge. Requires significant help from others.

1 - Low - Little to no experience.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat Hunter Skills Matrix | Hunter 01 | Hunter 02 | Hunter 03 |  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| General |  |  |  |
| Report Writing | 4 |  |  |
| Dashboard Creation | 4 |  |  |
| Presentation Skills | 5 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Network |  |  |  |
| Network Foundations | 5 |  |  |
| Network Architecture | 5 |  |  |
| Network Segmentation | 5 |  |  |
| Traffic Flow | 5 |  |  |
| Subnetting & RFC 1918 | 5 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Infrastructure |  |  |  |
| Routers | 5 |  |  |
| Switches | 5 |  |  |
| Firewalls | 5 |  |  |
| Proxies | 4 |  |  |
| IDS/IPS | 4 |  |  |
| VPN | 4 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Network Protocols |  |  |  |
| TCP/IP Foundations | 5 |  |  |
| HTTP | 5 |  |  |
| SSL/TLS | 5 |  |  |
| RDP | 5 |  |  |
| FTP | 5 |  |  |
| SSH | 5 |  |  |
| ICMP | 5 |  |  |
| DNS | 5 |  |  |
| DNS Tunneling | 5 |  |  |
| Packet Capture Analysis | 5 |  |  |
| Wireshark | 5 |  |  |
| Encrypted Traffic Analysis | 3 |  |  |
| JA3 | 3 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Logs |  |  |  |
| Syslog | 5 |  |  |
| Audit Logs | 4 |  |  |
| EMET Logs | 4 |  |  |
| OS Event Logs | 5 |  |  |
| Powershell | 3 |  |  |
| Shimcache & Amcache | 4 |  |  |
| Web Server | 3 |  |  |
| Proxy | 3 |  |  |
| Antivirus | 5 |  |  |
| Bash History | 4 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Operating Systems |  |  |  |
| Windows | 5 |  |  |
| Linux | 4 |  |  |
| MacOS | 4 |  |  |
| Unix | 4 |  |  |
| Android | 3 |  |  |
| iOS | 4 |  |  |
| AIX | 2 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Endpoint |  |  |  |
| Process Relationships | 5 |  |  |
| Scheduled Tasks | 5 |  |  |
| Services | 5 |  |  |
| Permissions | 5 |  |  |
| Windows Registry | 5 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Cloud |  |  |  |
| Amazon AWS | 4 |  |  |
| Microsoft Azure | 3 |  |  |
| Google Cloud Platform | 4 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| General Security |  |  |  |
| Access Control |  |  |  |
| Multi-Factor Authentication |  |  |  |
| Virtual Machines |  |  |  |
| Container Security |  |  |  |
| Social Engineering |  |  |  |
| Phishing |  |  |  |
| Physical Security |  |  |  |
| Internet of Things (IoT) |  |  |  |
| Industrial Control Systems (ICS) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Offensive Security |  |  |  |
| General Offensive Skills |  |  |  |
| Vulnerability Assessment |  |  |  |
| Penetration Testing |  |  |  |
| Red Teaming |  |  |  |
| Kali Linux |  |  |  |
| Webshells |  |  |  |
| Credential Dumpers |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Defensive Security |  |  |  |
| Incident Response |  |  |  |
| Data Forensics |  |  |  |
| Memory Forensics |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Intelligence |  |  |  |
| MITRE ATT&CK |  |  |  |
| STIX Rules |  |  |  |
| General Threat Intelligence Platforms |  |  |  |
| Mandiant Advantage Threat Intelligence |  |  |  |
| ThreatConnect |  |  |  |
| IBM X-Force Threat Intelligence |  |  |  |
| Recorded Future Intelligence Platform |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Malware |  |  |  |
| Malware Analysis |  |  |  |
| YARA Rules |  |  |  |
| Malware Sandboxing |  |  |  |
| Malware Reversing |  |  |  |
| Domain Generation Algorithms |  |  |  |
| Command & Control Infrastructures (C2) |  |  |  |
| Ransomware Families |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Information & Event Management (SIEM) |  |  |  |
| General SIEM Experience |  |  |  |
| Splunk |  |  |  |
| QRadar |  |  |  |
| NetWitness |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Orchestration Automation & Response (SOAR) |  |  |  |
| General SOAR |  |  |  |
| Playbook Creation |  |  |  |
| Splunk Phantom |  |  |  |
| Palo Alto Cortex |  |  |  |
| Rapid7 InsightConnect |  |  |  |
| IBM Resilient |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| User & Entity Behavioral Analytics (UEBA) |  |  |  |
| General UEBA Experience |  |  |  |