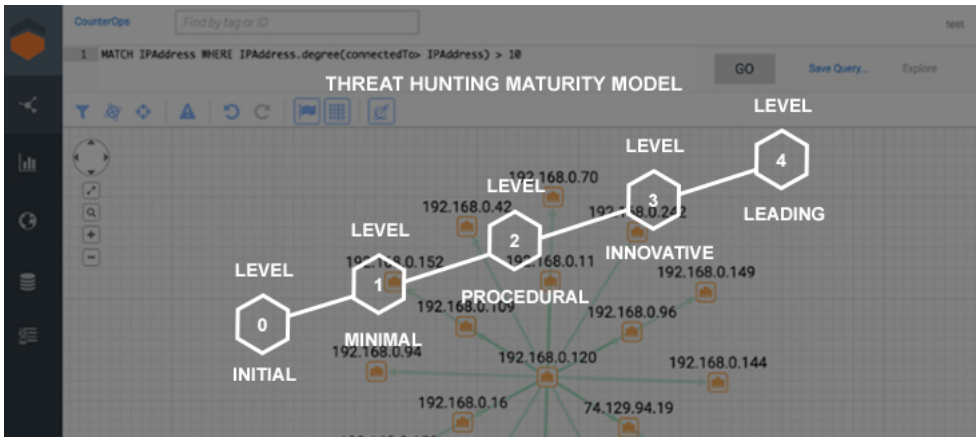
The Threat Hunting Reference Model Part 1: Measuring Hunting Maturity



October 16, 2015 by
Sqrrl Team

The Threat Hunting Reference Model Part 1: Measuring Hunting Maturity

Many organizations are quickly discovering that cyber threat hunting is the next step in the evolution of the modern SOC, but remain unsure of how to start hunting or how far along they are in developing their own hunt capabilities. This blog series will seek to formalize a reference model for how to effectively conduct threat hunting within an organization. We begin with a simple question: How can you quantify where your organization stands on the road to effective hunting? With a general model that can map maturity across any organization.

Cyber threat hunting is a proactive security approach for organizations to detect advanced threats in their networks. Until recently, most security teams have relied on traditional rule- and signature-based solutions that produce floods of alerts and notifications, and typically only analyze data sets after an indicator of a breach had been discovered as a part of forensic investigations.

What is Hunting?

Before we can talk about hunting maturity, though, we need to discuss what exactly we mean when we say “hunting”. We define hunting as the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade automated, rule- and signature-based security systems. There are many different techniques hunters might use to find the bad guys, and no single one of them is always “right”; the best one often depends on the type of activity you are trying to find.

Hunting is often machine-assisted but is always driven by an analyst; it can never be fully automated. Automated alerting is important, but cannot be the only thing your detection program relies on. In fact, one of the chief goals of hunting should be to improve your automated detection capabilities by prototyping new ways to detect malicious activity and turning those prototypes into production detection capabilities.

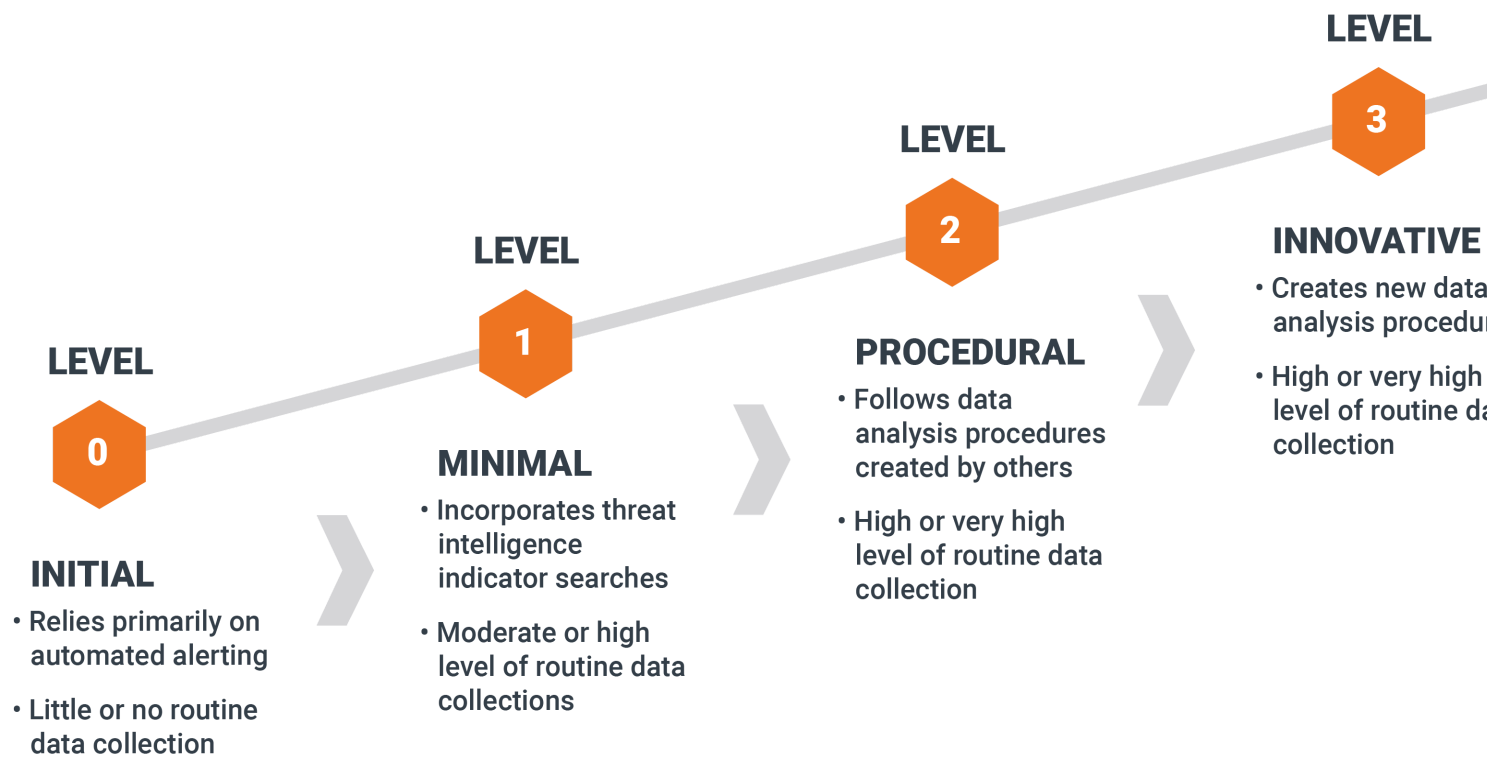
The Hunting Maturity Model

With that definition of hunting in mind, let’s consider what makes a good hunting program. There are three factors to consider when judging an organization’s hunting ability: the quality and quantity of the data they collect for hunting, the tools they provide to access and analyze the data, and the skills of the analysts who actually use the data and the tools to find security incidents.

For a more in-depth definition of hunting, check out our Hunting eBook.

Of these factors, an analysts’ skills are clearly important, since they are what allows them to turn data into detections, even though skills can be enhanced by specific tools. The quality and quantity of the data that an organization routinely collects from its IT environment is also a strong factor in determining the HMM level. The more data from around the enterprise (and the more different types of data) you provide to an expert hunter, the more results they will find. The toolsets you use will shape the style

of your hunts and what kinds of hunting techniques you will be able to leverage.



The Hunting Maturity Model (HMM)

The Hunting Maturity Model, developed by Sqrrl's security technologist and hunter David Bianco, describes five levels of organizational hunting capability, ranging from HM0 (the least capable) to HM4 (the most). Let's examine each level in detail.

HM0 – Initial

At HM0, an organization relies primarily on automated alerting tools such as IDS, SIEM or antivirus to detect malicious activity across the enterprise. They may incorporate feeds of signature updates or threat intelligence indicators, and they may even create their own signatures or indicators, but these are fed directly into the monitoring systems. The human effort at HM0 is directed primarily toward alert resolution.

HM0 organizations also do not collect much information from their IT systems so their ability to proactively find threats is severely limited. Organizations at HM0 are not considered to be capable of hunting.

HM1 – Minimal

An organization at HM1 still relies primarily on automated alerting to drive their incident response process, but they are actually doing at least some routine collection of IT data. These organizations often aspire to intel-driven detection (that is, they base their detection decisions in large part upon their available threat intelligence). They often track the latest threat reports from a combination of open and closed sources.

HM1 organizations routinely collect at least a few types of data from around their enterprise into a central location such as a SIEM or log management product. Some may actually collect a lot of information. Thus, when new threats come to their attention, analysts are able to extract the key indicators from these reports and search historical data to find out if they have been seen in at least the recent past.

Because of this search capability, HM1 is the first level in which any type of hunting occurs, even though it is minimal.

HM2 – Procedural

If you search the Internet for hunting procedures, you will find several great ones. These procedures most often combine an expected type of input data with a specific analysis technique to discover a single type of malicious activity (e.g., detecting malware by gathering data about which programs are set to automatically start on hosts). Organizations at HM2 are able to learn and apply procedures developed by others on a somewhat regular basis, and may make minor changes, but are not yet capable of creating wholly new procedures themselves.

Because most of the commonly available procedures rely in some way on least-frequency analysis (as of this writing, anyway), HM2 organizations usually collect a large (sometimes very large) amount of data from across the enterprise.

HM2 is the most common level of capability among organizations that have active hunting programs.

HM3 – Innovative

HM3 organizations have at least a few hunters who understand a variety of different types of data analysis techniques and are able to apply them to identify malicious activity. Instead of relying on procedures developed by others (as is the case with HM2), these organizations are usually the ones who are creating and publishing the procedures. Analytic skills may be as simple as basic statistics or involve more advanced topics such as linked data analysis, data visualization or machine learning. The key at this stage is for Analysts to apply these techniques to create repeatable procedures, which are documented and performed on a frequent basis.

Data collection at HM3 at least as common as it is at HM2, if not more advanced.

HM3 organizations can be quite effective at finding and combating threat actor activity. However, as the number of hunting processes they develop increases over time, they may face scalability problems trying to perform them all on a reasonable schedule unless they increase the number of available analysts to match.

HM4 – Leading

An HM4 organization is essentially the same as one at HM3, with one important difference: automation. At HM4, any successful hunting process will be operationalized and turned into automated detection. This frees the analysts from the burden of running the same processes over and over, and allows them instead to concentrate on improving existing processes or creating new ones.

HM4 organizations are extremely effective at resisting adversary actions. The high level of automation allows them to focus their efforts on creating a stream of new hunting processes, which results in constant improvement to the detection program as a whole.

Automation and the HMM

It may seem confusing at first that the descriptions for both HM0 and HM4 have a lot to say about automation. Indeed, an HM4 organization always has automation in the front of their minds as they create new hunting techniques. The difference, though, is that HM0 organizations rely entirely on their automated detection, whether it's provided by a vendor or created in house. They may spend time improving their detection by creating new signatures or looking for new threat intel feeds to consume, but they are not fundamentally changing the way they find adversaries in their network. Even if they employ the most sophisticated security analytics tools available, if they are sitting back and waiting for alerts, they are not hunting.

HM4 organizations, on the other hand, are actively trying new methods to find the threat actors in their systems. They try new ideas all the time, knowing that some won't pan out but others will. They are inventive, curious and agile, qualities you can't get from a purely automated detection product. Although a good hunting platform can certainly give your team a boost, you can't buy your way to HM4.

Using the HMM

CISOs that hear that their organization needs to "get a hunt team" may legitimately be convinced that an active detection strategy is the right move, and yet still be confused about how to describe what a hunt team's capability should actually be. A maturity model will ideally help anyone thinking of getting into hunting get a good idea of what an appropriate initial capability would be.

More importantly for those organizations who already hunt, the HMM can be used both to measure their current maturity and provide a roadmap for improvement. Hunt teams can match their current capabilities to those described in the model, then look ahead one step to see ideas for how they can develop their skills and/or data collection abilities in order to achieve the next level of maturity. In order to get anywhere, you must first know where you are and where you want to be.

In part 2 of our blog series , we will dive into how to formalize the iterative hunting process once you reach HM2 or higher.