The Threat Hunting Reference Model Part 3: The Hunt Matrix
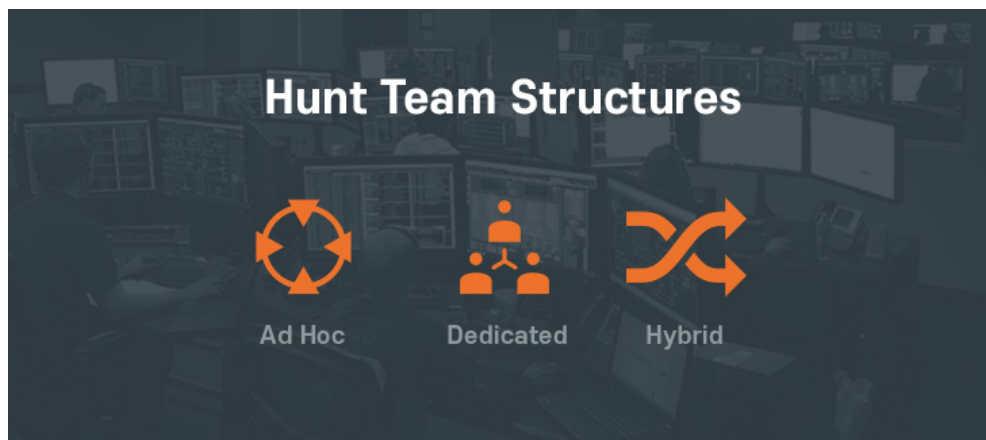

November 19, 2015 by
[Sqrrl Team](#)

The Threat Hunting Reference Model Part 3: The Hunt Matrix

In the first two parts of this blog series, we covered two important parts of a reference model for hunting: [the hunting maturity model](#) and [the hunting loop](#). In this final part of our series, we'll look at how these fit together. In this final part of the series, we develop a matrix for combining the capabilities of each level of the maturity model mapped to different steps of the hunting loop.

We already know that hunting is comprised of four steps and that hunting is most effective when these four steps are carried out iteratively, constantly building on each other. Organizations at different levels of the hunting maturity model will execute steps of the hunting loop in various ways. The matrix combines the four steps of the Hunting Loop and the five steps of the maturity model.

HUNTING MATURITY LEVEL

HUNTING LOOP STEPS	HM0 Initial	HM1 Minimal	HM2 Procedural	HM3 Innovative	HM4 Leading
DATA COLLECTION	Little or no data collection	Moderate collection of some types of data from a few key points in the IT environment	High collection of certain types of data throughout the IT environment	High collection of certain types of data throughout the IT environment	**High collection of many types of data throughout the IT environment**
HYPOTHESIS CREATION	Respond to existing automated alerts from SIEM, IDS, Firewall, etc.	Review threat intelligence to develop new hypotheses	Review threat intelligence and "friendly intelligence" to develop new hypotheses	Review threat intelligence, "friendly intelligence", and manual cyber risk scoring (i.e. "crown jewel analysis") to develop new hypotheses	**Review threat intelligence, "friendly intelligence", and automated cyber risk scoring to develop new hypotheses**
TOOLS & TECHNIQUES FOR HYPOTHESIS TESTING	Alert consoles, SIEM searches; No proactive investigation	Utilize SIEM or log analysis tools to conduct basic search via full-text or SQL-like queries	Utilize simple tools and histograms to search and analyze data based on existing hunting procedures	Leverage visualizations and graph searches. Develop new hunting procedures	**Advanced visualizations and graph searches. Publish, and automate new hunting procedures**
PATTERN & TTP DETECTION	None; Only SIEM/IDS alerts	Identifying IOCs at bottom of PoP like domains, URLs, and hashes	Identification of IOCs at bottom and middle of PoP and mapping trends of those IOCs over time	Able to detect adversary TTPs and other IoCs at the top of the PoP	**Automatic complex TTP discovery and campaign tracking; Active sharing of IoCs with information sharing organization**
ANALYTICS AUTOMATION	None	Integrates threat intel feeds into automated alerting for basic matching	Build a library of effective hunting procedures and performs them on a regular schedule	Build a library of effective hunting procedures and performs them frequently; basic data science (standard deviation, outlier detection)	**Automate effective hunting procedures to continuously improve alerting capabilities; advanced data science (machine learning)**

The matrix includes data collection as an important part of the hunting process. After all, you can't hunt if you can't see anything. Data collection from HM0 to HM4 matures in a linear way, from collecting little to no data to collecting many different types of data from throughout your IT environment.

Scaling up hunting maturity through the hunting loop depends on certain key focus points for each step.

- Maturing **hypothesis creation** is dependent on increasing and leveraging the intel that you have at your disposal to craft dynamic new questions.

- Maturing the **tools and techniques** used to follow up on hypotheses is dependent on the kinds of hunt procedures you can utilize and how powerful the analysis and visualization capabilities of your tools are.

- Maturing your **pattern and TTP detection** is dependent on expanding the kinds of [IoCs you can collect from the Pyramid of Pain](#). This also includes mapping the behavior trends of adversaries over time to better understand your threat landscape.

- Finally, maturing **analytics and automation** is dependent on the optimization of how routinely and how effectively you can carry out a hunts and feed the information you gather back into your automated detection systems.

Overlaying the Hunting Maturity Model with the Hunting Loop can give organizations a more granular view as to what parts of the hunting process they still need to be improving to reach the next stage of hunting maturity. Looking for information on how to increase hunting maturity? Check out our [White Paper on Threat Hunting Platforms](#) below.