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.
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.