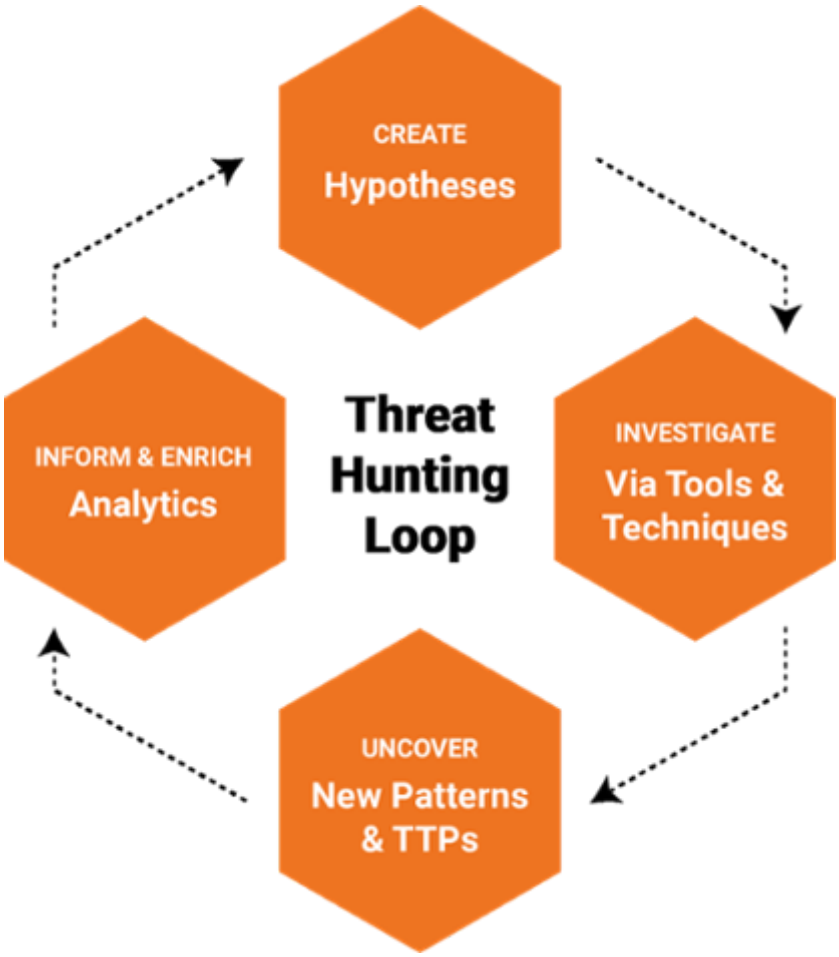
The Threat Hunting Reference Model Part 2: The Hunting Loop

October 28, 2015 by
Sqrrl Team

The Threat Hunting Reference Model Part 2: The Hunting Loop

In our previous post, part 1 of this blog series, we profiled the various stages of an organization's hunting maturity scale . 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.

The Threat Hunting process is meant to be iterative. You will never be able to fully secure your network after just a single hunt. To avoid one-off, potentially ineffective hunting trips, it's important for your team to implement a formal cyber hunting process. The following four stages make up a model process for successful hunting.



The hunting loop illustrates that hunting is most effective when it's habitual and adaptable. Let's break it down step by step, beginning with hunting starting points, or what we call "trailheads":

A hunt starts with **creating a hypothesis** , or an educated guess, about some type of activity that might be going on in your IT environment. An example of a hypothesis could be that users who have recently traveled abroad are at elevated risk of being targeted by state-sponsored threat actors, so you might begin your hunt by planning to look for signs of new malware on their laptops or assuming that their accounts are being misused around your network. Hypotheses are typically formulated by analysts based on any number of factors, including friendly and threat intelligence. There are various ways that a hunter might form a hypothesis. Often this involves laying out attack models and the possible tactics a threat might use, determining what would already be covered by automated alerting systems, and then formulating a hunting investigation of what else might be happening.

A hunter follows up on hypotheses by **investigating via various tools and techniques** , including Linked Data Search and visualization. Effective tools will leverage both raw and linked data analysis techniques such as visualization, statistical analysis or machine learning to fuse disparate cybersecurity datasets. Linked Data Analysis is particularly effective at laying out the data necessary to address the hypotheses in an understandable way, and so is a critical component for a hunting platform. Linked data can even add weights and directionality to visualizations, making it easier to search large data sets and use more powerful analytics. Many other complementary techniques exist, including row-oriented techniques such as stack counting and datapoint clustering. Analysts can use these techniques to discover new malicious patterns in their data and reconstruct complex attack paths to reveal an attacker's **Tactics, Techniques, and Procedures (TTPs)** .

Various tools and techniques are used in **uncovering new malicious patterns of behavior and adversary TTPs** . This step is the definitive success criteria for a hunt. An example of this process could be that a previous investigation revealed that a user account has been behaving anomalously, with the account sending an unusually high amount of outbound traffic. After conducting a Linked Data investigation, it is discovered that the user's account was initially compromised via an exploit targeting a third party service provider of the organization.

New hypotheses and analytics are developed to specifically discover other user accounts affiliated with similar third party service providers.

Finally, successful hunts form the basis for **informing and enriching automated analytics** . Don't waste your team's time doing the same hunts over and over. Once you find a technique that works to bring threats to light, automate it so that your team can continue to focus on the next new hunt. Information from hunts can be used to improve existing detection mechanisms, which might include updating SIEM rules or detection signatures. For example, you may uncover information that leads to new threat intelligence or indicators of compromise. You might even create some friendly intelligence, that is, information about your own environment and how it is meant to operate, such as network maps, software inventories, lists of authorized web servers, etc. The more you know about your own network, the better you can defend it, so it makes sense to try to record and leverage new findings as you encounter them on your hunts.

The hunting loop is a simple but effective step by step process that can radically enhance an organization's control over its own network defense. As noted above, hunting is most effective when it is used together with other more traditional security systems, complementing the detection efforts and perimeter security that most organizations already have in place. In the third and final part of this blog series we will profile how the hunting loop is executed at various stages of an organization's hunting maturity . For more general information on threat hunting, be sure to check out our Threat Hunting eBook below.