A Framework for Cyber Threat Hunting Part 2: Advanced Persistent Defense

August 5, 2015 by
Sqrrl Team

A Framework for Cyber Threat Hunting Part 2: Advanced Persistent Defense

In part 1 of this series , we discussed the six categories of Indicators of Compromise (IoC) that can be used as trailheads for structured threat hunting trips. In this post, we will focus specifically on how security organizations can build intelligence-driven hunting loops to detect the Tactics, Techniques, and Procedures (TTPs) of advanced threats.

In order to hunt threats, it is important to understand the method of the attacker. The cyber kill chain is the well known framework created by Lockheed Martin to track the steps an attacker goes through to exploit, compromise, and carry out an attack against a targeted system or organization. Disrupting this process at any point in the chain prevents (or at least seriously degrades) an attacker's ability to accomplish their mission.

Figure 1. Cyber Kill Chain

But why let our adversaries be the only ones with cool deployment models? Sqrrl's Security Architect, David Bianco, has developed a cyber defense methodology (inspired by John Boyd's OODA loops) focused on impeding an attacker's movement down the Kill Chain. When defenders are able to more quickly maneuver than an adversary, Advanced Persistent Defense can be achieved. The goal of the Advanced Persistent Defense model is to build a defense structure that evolves with every attack against it. As defenders catalog observations about attackers' TTPs, weak points in their defenses, and any obstructions in the investigative workflow, they can streamline response times and offset the challenge of persistence. Analysts can present information they gather to their security team, and use the interpretations to consistently improve defensive technologies and refine detection/response techniques. Improving on failures of the past and increasingly investing in effective strategies allows your team to stay one step ahead of attackers, rather than one step behind them.

The APD framework consists of three major cycles: Intelligence, Hunting, and Response.

1. **Intelligence Cycle:** *Direct, Collect, Analyze, Disseminate*

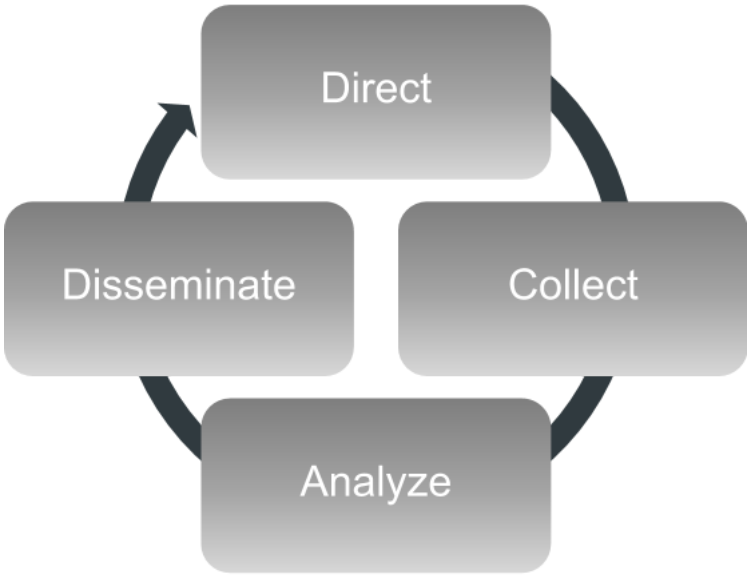

Figure 2. The Intelligence Cycle

The Intelligence Cycle is focused on developing full situational awareness of your threats, vulnerabilities, and assets. It consists of the following steps:

- **Direct** the construction of your defenses by knowing what kinds of intel you want to collect about potential attackers, identifying core assets, and considering potential vulnerabilities; these are fundamentally important considerations.
- **Collect** as much data as possible, keeping in mind what type of data each protective control provides, and store it for as long as possible.
- **Analyze** your data with automated tools as you prepare to maintain your defenses and, down the line, investigate and respond to attacks.

- **Disseminate** the analysis of information collected and use that analysis to influence the construction of your defenses and the trailheads that will be used to orient threat hunting trips.

2. **Hunting Cycle:** *Orient, Query, Analyze, Revise*

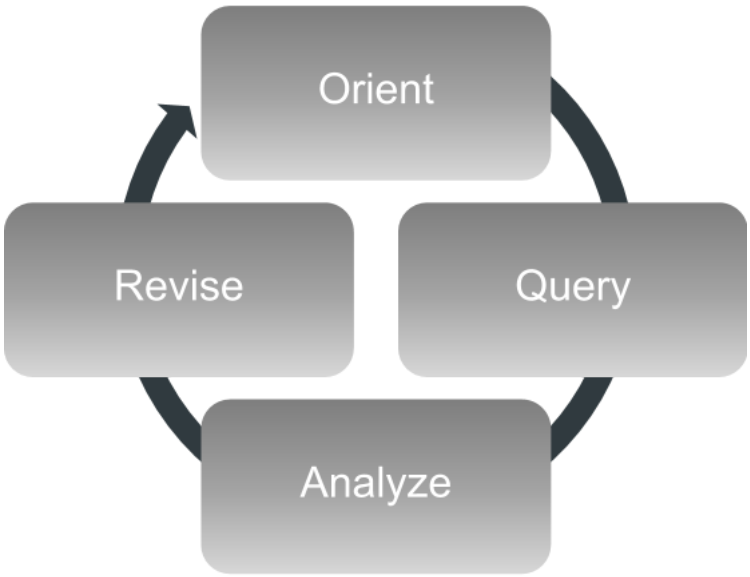

Figure 3. The Hunting Cycle

The Hunting Cycle focuses on proactively and iteratively searching through your data to find advanced threats hidden inside your network and systems. It consists of the following steps:

- **Orient** the direction of your hunt. Each "hunting trip" begins with a trailhead that serves as the starting point for a hunt. Sqrrl defines three different types of trailheads: hypotheses, indicators of compromise, and algorithm results.
- **Query** the information that you will need in order to reconstruct the progression and context of an attack, pivoting across netflow, application, and endpoint sources. Advanced attack narratives will only be fully visible across multiple security datasets. At this stage, Linked Data Analysis is a powerful tool for the kind of pattern analysis and anomaly detection that will shorten the time necessary to reconstruct the TTPs of a given attack.
- **Analyze** patterns and be vigilant in identifying signals of an attacker in a late stage of the Kill Chain (i.e., C2 or Act of Objectives phases). Compare your observations along the hunt with what you would expect to find in normal conditions.
- **Revise** your queries throughout your hunt as you weed out less useful information and hone-in on the attack narrative.

3. **Response Cycle:** *Contain, Investigate, Remediate*

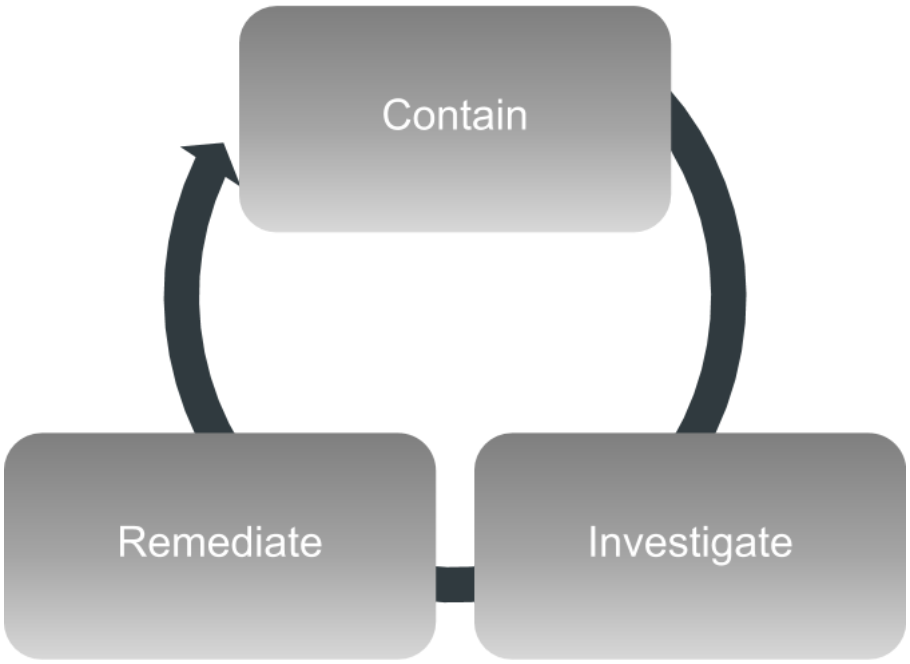

Figure 4. The Response Cycle

The Response Cycle is focused on mitigating the damage of an identified incident. The steps in this cycle include the following:

- **Contain** a threat by restricting its access (either human or automated) to internal systems.
- **Investigate** the extent of the threat's reach by fully developing the narrative of the attack, which will provide feedback to the Hunting Cycle in terms of the depth and quality of the hunt.
- Finally, **R emediate** the effects of the breach and pass newly discovered indicators back into the Intelligence Cycle.

Bringing It All Together

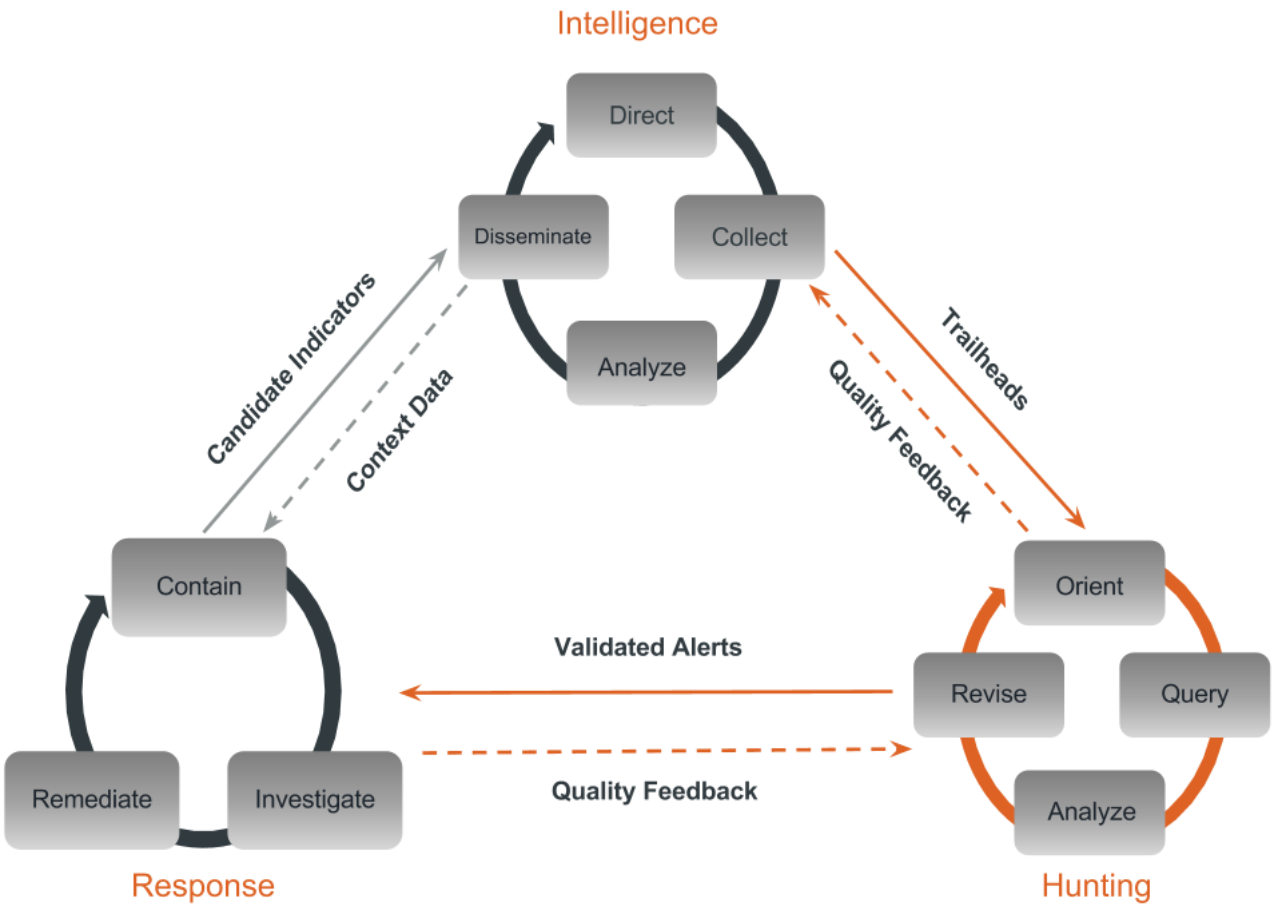

Figure 5. The Advanced Persistent Defense Framework

Together, these cycles form an Advanced Persistent Defense framework that evolves as analysts collect more and more data about attacks. Trailheads produced by the Intelligence Cycle feed the Hunting Cycle where false positives are filtered out and alerts and indicators are investigated across multiple datasets. After threat hunters are able to determine that an incident has occurred/is occurring, it is escalated to the Response Cycle where it can be fully investigated, remediated, and contained.

One important quality of the Advanced Persistent Defense framework is that it is uniquely equipped to detect TTPs. As you may recall from the Pyramid of Pain framework, TTPs are the most powerful indicator of compromise to detect and stop advanced attacks. With its focus on intelligence-driven threat hunting and response, Advanced Persistent Defense goes beyond a reliance on simple indicators and is a framework for digging deeper into adversaries' actions by leveraging an understand of their behavior (TTPs) to help defenses evolve faster than attacks.

Advanced Persistent Defense requires the ability to quickly, efficiently navigate netflow, application, and endpoint data sets in order to piece together the full extent of the attack, from Weaponization and Delivery to Act on Objectives. Sqrrl provides a single pane of glass for analysts to perform Linked Data Analysis across their security datasets, making it uniquely effective at discovering TTPs in the Hunting and Response Cycles. In our third and final part of this series , we will take a deeper look at how discovering TTPs is so important and how to use them effectively. Click the link below to learn more about Linked Data.