InformationWeek
DARKReading

Threat Hunting: 5 Tips To Bag Your Prey

Knowing the lay of the land and where attackers hide is a key element in hunting, both in nature and in the cyber realm.

The days when Security Operations Center analysts could sit back and wait for alerts to come to them have long passed. A year of breaches and attacks at Fortune 100 banks, retailers, and government agencies have shown that traditional measures like firewalls, IDS, and SIEMs are not enough. While these measures are still important, today's threats demand a more active role in detecting and isolating sophisticated attacks. It's hunting season, so here are five tips to make your efforts more productive.

TIP 1: EMBRACE BIG DATA

Since hunting is a data-driven process, it is not surprising that the collection of large amounts of data is critical. You should be collecting logs from each of the three major security data domains (network transactions, operating system events, and application logs). This is potentially a lot of data, but you don't have to do it all at once. Start with a subset of sources and then grow your data collection incrementally as your monitoring program matures. Authentication logs for operating systems and applications are a good place to start, as are some of the more common types of network transactions, like HTTP server and proxy logs and netflow records. Emails and employee data, like HR information and access privileges, can also be useful to detect internal threats and anomalies.

These datasets make for productive hunting, but may be more than your SIEM can handle. Given that advanced attacks can often evade observation for weeks or months, we often see organizations that want to store all this data for a year or more. To house and use it efficiently, you're going to need some kind of big data platform like Apache Hadoop.

TIP 2: ASK QUESTIONS

It's important to remember that hunting is not an automated process; it's driven by questions and hypotheses. One question might be "Is data exfiltration happening?" A starting hypothesis might be "If there is data exfiltration happening, it is most likely going on through this part of the network." So, you may want to check to see whether there is any exfiltration going through that subnet, and then you might try to figure out what protocols the attacker would use and what that activity would look like in the logs. An adversary could steal data by FTPing it straight out or using HTTP to bypass possible firewall restrictions. A savvy hunter understands that the attackers can accomplish their goals in many ways and examines the data from several viewpoints to compensate.

TIP 3: PIVOT… AND THEN PIVOT AGAIN

Hunting consists of spending a lot of time searching for something that is elusive by nature. To locate entrenched threats, your hunt needs to be dynamic and adaptable. Plus, you need to be able to easily pivot from one dataset to the next to evaluate the full context of the attacker's digital footprints. This might include moving from operating system events to netflow data and then to application logs. Your hunting toolset needs to be able to support this kind of nimble data exploration. Once you've identified an item of interest, you'll also need to be able to quickly identify all the context associated with that item, including its relationships to other entities on your network, its historical activity, how it correlates with threat intelligence, or how it relates to non-technical data, like HR information.

TIP 4: ALWAYS HAVE A STRATEGY

Knowing the lay of the land and where attackers may hide is a key element to hunting. Kill chain mapping provides a useful framework to plan your hunting trips for maximum impact. Typically, you will want to focus on the last two phases of the kill chain (Command and Control and Act on Objectives) first, since the farther along the kill chain the adversary is, the worse the incident is for you. It is also where attackers typically leave the largest digital footprints, so starting your hunts near the end of the kill chain makes a lot of sense. Beginning with even a simple strategy like this can save you a lot of time that might otherwise have been wasted chasing leads that either don't pan out or that you don't have enough data to investigate properly.

TIP 5: GET YOUR DATA SCIENCE ON

Making sense of Big Data is no easy task, and it's no secret among security professionals that data science is becoming increasingly important in security efforts. In general, an enterprise is going to want to keep as much data as it will be able to store. If you want to actually capitalize on terabytes or even petabytes of information, you will need a smart and effective way of making sense of it all. Modern machine learning and statistical tools have the potential to multiply the effectiveness of a hunter's powers by automating common tasks such as producing activity summaries or finding the "weird" entities in a dataset. Hunters need tools that provide data science without requiring the users to be data scientists.

Obviously, there is a lot more to hunting than just these five steps. The most important tip, though, is just to dive in! Start by making the most of the data you already collect, no matter what it is. As you hunt, you'll naturally learn the limitations of your data collection and your analysis toolsets. Use this feedback to prioritize improvements. Hunting is an iterative process, and so is the process of improving your hunting platform.

What are you waiting for? Go out and find the threats before they find you.

AUTHORED BY:
David J. Bianco,
Lead Security Technologist at Sqrrl