WHITE PAPER

Threat Hunting 101

Cyberthreats are Changing

What you do not know about the security of your network really will hurt you. For instance, Cybersecurity Ventures estimates that by 2021, cybercrime is likely to cost the world $6 trillion annually, which is more than the combined GDP of the UK and France.

Today, businesses need to go beyond the traditional perimeter security provided by firewalls, intrusion prevention systems, data loss prevention systems, and intrusion detection systems to actively search for threats that have infiltrated the network. This means deploying a threat hunting solution that uses deep packet inspection (DPI) to look for threats early in the cyber kill chain processes of delivery, exploitation, and installation.

Cybersecurity Ventures estimates that by 2021, cybercrime is likely to cost the world $6 trillion annually, which is more than the combined GDP of the UK and France.

This white paper summarizes four fundamental aspects of threat hunting:

1. Making a Commitment: Adopting a Proactive Security Practice
2. Finding the Right Data: Packets Are Key
3. Building Your Infrastructure: A Challenge and the Solution
4. Starting the Hunt: An Organized Approach

KEYSIGHT TECHNOLOGIES

Making a Commitment: Adopting a Proactive Security Practice

New security exploits are getting harder — and more costly — to find. The number of advanced threats doubled in 2018, according to respondents cited in the 2018 Threat Hunting Report from Crowd Research Partners. Sixty percent of companies surveyed plan to build out their threat hunting defenses over the next three years, in part because of the increase in advanced threats.

The first step to beginning a threat hunting practice is to commit to adopting proactive security practices. This is not a trivial decision. Proactive cyber defense and threat hunting take considerable investments in money and time. However, once you have created and implemented a proactive plan, you will detect more hidden cyberattacks and be a less-likely victim.

Threat hunting can look at both data at rest (for example, data lakes) and data in motion (data flowing in and out of servers), allowing you to deploy solutions that analyze data in real time or at a later date.

Artificial intelligence (AI) and machine learning (ML) can contribute greatly to threat hunting. These technologies are good at finding the relatively few threats that may be hiding in very large sets of data. While differing in underlying technologies, both approaches can establish a baseline for “normal” behavior on a network allowing the identification of anomalous behavior.

New security exploits are getting harder — and more costly — to find. In addition, the number of advanced threats doubled in 2018.

Finding the Right Data: Packets are Key

Before you start threat hunting, you need to have the right data. This is true for any security approach. Your data must be both complete and reliable. The wrong data will lead to false positives (finding threats that do not really exist) while missing data can lead to false negatives (reporting all is well when in fact a threat is present).

While this may sound rudimentary, hidden traps are everywhere. First, many enterprises use SPAN ports on their network switches to capture monitoring data. The problem with this is that SPAN ports can drop packets when switches become heavily loaded. Also, SPAN ports automatically drop malformed and improper packets that could contain key pieces of information about when, where, and how a threat started.

Another approach, using metadata to summarize data flows, can be helpful in certain applications or when bandwidth is a concern. However, metadata is like lossy compression in that small but important details may be lost.

However, these are not the only concern. Surprisingly, even some leading network monitoring solutions drop packets under load or when multiple features or filters are employed.

The best source of data for threat hunting is packet data. While meta data like flow data can be useful, packet data is the gold standard.

This data can come from anywhere across your network. Once collected, it requires aggregation and filtering for irrelevant material before analysis for security threats.

Data can come from anywhere across your network. Once collected, it requires aggregation and filtering for irrelevant material before analysis for security threats.

Building Your Infrastructure: A Challenge and the Solution

As mentioned earlier, getting better insight into traffic on your network may sound easy, but it is not.

Here are some areas where many organizations face challenges:

- data capture at wire speed and scale
- SPAN technology that does not scale — even though networks are getting faster, no packet loss is acceptable
- complex network topologies
- too many distributed data capture points and the use of data encapsulation
- virtual network blind spots caused by east-west traffic and private clouds
- duplicate or unnecessary data (for example, backups, redundant packets, low-value data)
- compliance mandates such as PCI, GDPR, and HIPAA
- encrypted traffic that limits the ability to detect threats

Additional challenges exist when choosing and collecting the proper data to review for security threats. Here are some common challenges, broken down by area:

Log data

- Because of the large number of log files to review, you need to decide how many and which ones to examine.
- Certain threats can evade log capture.
- On-premises logging can be inconsistent.

Endpoint data

- This gives you visibility into system processes only.
- The context of the threat is lacking; it requires correlation later on.
- It is heavily dependent on response capability in this area.

Network data

- The network contains a huge amount of data to sift through.
- You do not see internal system information.

Active network intelligence delivers quick and actionable results

Active network intelligence can help overcome many data collection and analytics challenges. Taps are the start of any visibility solution.

Taps provide access to the right kind of packet data. They are passive devices that you can install anywhere in the network. Taps make a copy of all data passing through that point on the network and forward it to another location, typically a network packet broker (NPB) or a security analysis tool.

An NPB is a tool that can segment different types of monitoring data for different types of monitoring tools. The segmentation is based on Layer 2–4 or Layer 7 parameters. This device ensures that the right security or analytics tool gets the right data.

An NPB grooms the monitoring data to optimize the following:

- the quality of the data (packets, NetFlow, geolocation metadata)
- the volume of the data (data at rest, in motion, across time)
- the reach of your data collection (such as core, perimeter, server farm, private data center, and public cloud)

The best architecture is to send data from the tap to an NPB placed between the tap and a security analysis tool, as shown in Figure 1.

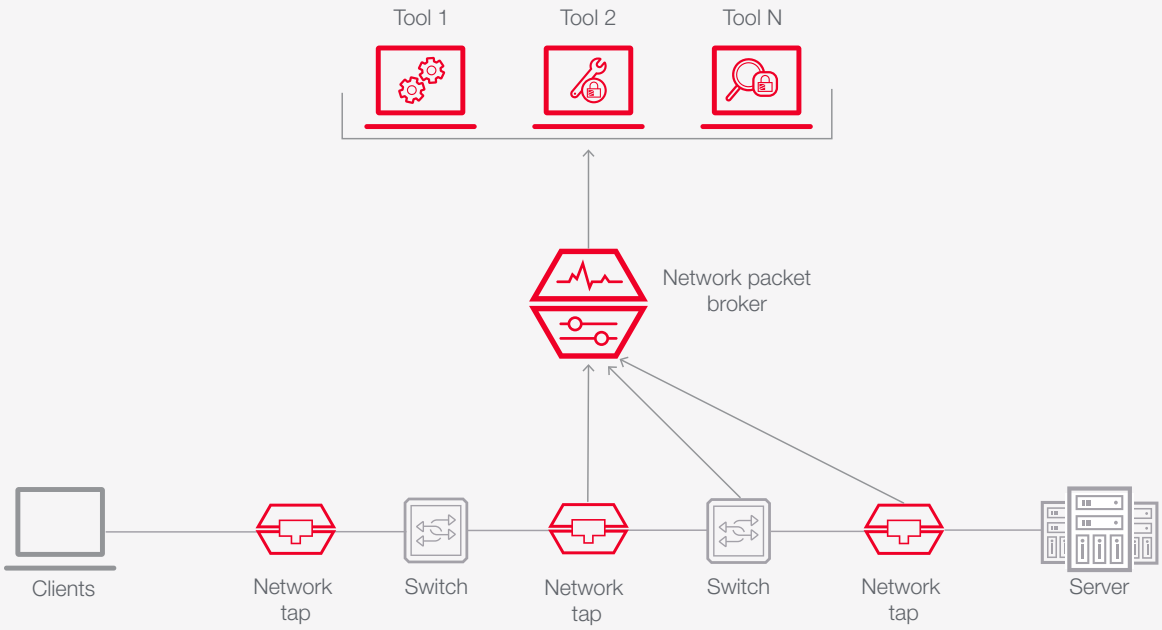

Figure 1. Data filtering provided by an NPB for out-of-band security threat tools

An NPB is a purpose-built filtering solution that lets you easily segment different types of out-of-band monitoring data for different types of monitoring tools. This device ensures that the right security tool gets the right data.

A well-built NPB delivers wire-speed data to threat hunting appliances for analysis. However, not all NPBs and taps are created equal. It is important to select taps and packet brokers that can process data at wire speed and do not drop packets. You can remove unnecessary data, but you do not want your data collection architecture to randomly drop data, since that lost data might have been critical to your analysis process.

Packet brokers have many features, including data filtering, header stripping, load balancing, SSL decryption, and application intelligence such as NetFlow-based metadata. Automation from the NPB to orchestration systems can also be deployed using a RESTful interface to a security information and event management tool (SIEM), unified threat management tool (UTM), or another type of solution. This allows threat hunting solutions to react without constant manual intervention, quickening the search.

Starting the Hunt: An Organized Approach

Now that you have the correct data, your job is almost done. However, the final steps are key. You will need to derive context from the correct data as fast as possible to identify and remediate threats.

Now that you have the correct data, your job is almost done. However, the final steps are key.

Here are five basic steps to help you organize your way forward:

1. Determine what kind of threat information you are after — command and control, data destruction, data encryption, data exfiltration, unauthorized access, anomalous behavior, or something else.
2. Determine what specific data sources you need for the threat(s) you are after and where to get the data from your network intelligence architecture.
3. Use a threat hunting tool to actively look for the specified threat(s).
4. Review the anomalies your threat hunting tool flagged and compare snapshots over time and established baselines.
5. Make a determination about the anomaly or decide to investigate it further.

As an example, if you decide that you want to look for command and control compromises, first see if any internal systems are persistently communicating with one or more IP addresses (systems) on the internet.

In this case, you would typically use this four-point process:

1. Identify any communication channels leaving your network for the same IP address.
2. Analyze the protocol on which the communication is taking place.
3. Identify the internal originating host and evaluate whether the type of communication is suspicious for that device.
4. Identify and evaluate the reputation for the destination address. Is it a known bad IP address, or is there anything suspicious about the destination?

While you can perform this process manually, a dedicated threat hunting tool makes it easier to do. In the early days, threat hunting could be as simple as creating a static baseline of "normal" functions (x number of HTTP requests). Anything more than 10% over this mark was suspicious. However, as networks have grown more sophisticated, the process has evolved. First came dynamic baselines, but these are difficult to update manually. Now you need ML to perform the investigations, so you can spend your precious time on anomaly evaluation.

Typical threat hunting tools provide the following benefits:

- complete visibility with auto-discovery of even encrypted interactions
- real-time detection that finds anomalies fast using ML and wire data
- guided investigation, which establishes root cause in seconds instead of days

Conclusion

Threat Hunting 101 requires a commitment to building an active, effective security practice, getting the right data, building the infrastructure to capture and transport that data to the right tools, and taking an organized approach to your hunt. Dynamic network intelligence is the foundation for success. It starts with taps and NPBs to give IT an advantage against cyberthreats by correctly filtering data and delivering it to threat detection solutions for analysis. In contrast to legacy solutions, such as SPAN port or last-generation packet brokers, active network intelligence ensures full visibility without dropping packets, even with features and filters turned on.

Specifically, this approach enables security operations teams to:

- detect hidden network security threats as fast as possible
- use AI to increase the mean time to detection from days or weeks to minutes
- use NPBs to deliver packet data, flow data, and metadata to the threat hunting appliance
- filter out irrelevant L2–7 data using an NPB in order to increase the speed of analyses
- utilize integrated TLS decryption within NPBs to remove the threat of hidden malware in encrypted traffic
- access data from any location in your network using taps and an NPB

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES