riverbed®

A Guide to Cyber Security Threat Hunting

The art of proactively detecting advanced security threats

EBOOK

Table of Contents

SUNBURST: Lessons Learned

If we learned anything from the SUNBURST breach, it's that today's advanced threats require a more proactive security strategy. Security teams cannot rely solely on passive preventative measures nor operate only in firefighting mode, responding to alerts that suggest potential indicators of compromise. Today's cybercriminals are very sophisticated and are constantly devising new attacks that can quickly evade traditional defenses. Many are not even criminals at all, in the traditional sense, but are agents working for a nation state. By the time your security team discovers a breach, often months later, confidential data has been exfiltrated and moved laterally in the network. The cost of a breach is typically in the millions, not including the hit to your brand.

To detect those threats that slip by your defenses, your organization needs to hunt for cyber threats proactively and regularly. To be optimally effective, threat hunting should not be an ad hoc process, rather it should be performed consistently as a regular part of your cyber security strategy for protecting digital assets.

High-Profile Breaches in 2022

Crypto.com – $18 billion in Bitcoin and $15 million in Ethereum

Microsoft – Compromised Cortana, Bing, and several other products

Ronin Crypto Theft – $625 million in cryptocurrency

Block (formerly known as Square) – PII* from 8 million customers

FlexBooker – PII from 3 million users

Shields Health Care Group – 2 million users affected

Neopets – Exposes data on 69 million accounts

Flagstar Bank – 1.5m customers affected

Red Cross – 500,000 people affected

Marquard & Bahls – Closure of 200+ gas stations across Germany

*PII – Personally identifiable information.

What is Cyber Threat Hunting?

Most threats security analysts deal with are relatively unsophisticated and can be easily detected and mitigated with standard tools and good security hygiene. But, a small, but growing percentage of them are advanced threats that will breach your defenses and gain a foothold in your network. After gaining that foothold, an attacker can remain hidden in your network for months as they quietly collect data, look for confidential material, or obtain login credentials that will allow them to move laterally across the environment.

This is where the cyber threat hunter fits in.

Cyber threat hunting is the practice of proactively and iteratively seeking out, tracking, and disabling the most skilled and dangerous network intruders. It is an analyst-centric process that typically starts with a hypothesis or trigger and proactively and iteratively searches through network, endpoints, and data to detect and isolate threats that have evaded traditional preventative controls.

Unlike security analysts who wait for the intrusion detection system (IDS) or security information and event management (SIEMs) to surface alerts and then react to them, hunting for threats lets your security analyst be proactive and identify them sooner. The process of threat hunting also helps detect vulnerabilities and mitigate associated risks before they affect your organization.

Six Reasons Your Organization Should Cyber Threat Hunt

It's a simple fact: the longer the time to identify a breach, the greater the cost.

277
Days

Average time to identify and contain a breach[1]

75%

of breaches are caused by outsiders[2]

83%

of organizations have had more than one data breach[1]

$4.35M

Average total cost of a breach[1]

89%

of breaches are caused by system intrusion, web application attacks, and social engineering[2]

29
Days

Saved in response time with extended detection and response (XDR) technologies[1]

[1] Ponemon, The Cost of a Breach, 2022

[2] Verizon, Data Breach Investigations Report, 2022

Threat Hunting Requirements

The goal of threat hunting is to use the world's most powerful anomaly detector, the human brain, to unearth undiscovered threats. However, to be successful, threat hunting requires a mature security program with broad visibility, including:

Broad Network Visibility

A clear understanding of your network and infrastructure is essential for threat hunting. Further, establishing a baseline of normal network activity can help identify malicious activity and provide the initial context for initiating a hunt.

Skilled, Dedicated Personnel

Threat hunters should know how to use their security and network visibility tools and understand the mindset of their adversaries. In short, to catch a hacker, you must think like a hacker. Threat hunters who perform regular, structured hunts with clearly defined goals will be more effective.

Rich Threat Intelligence

An understanding of new threat vectors will allow hunters to stay current with the latest techniques. Using public indicators of compromise such as malware signatures, IP addresses and others may help increase detection of new threats.

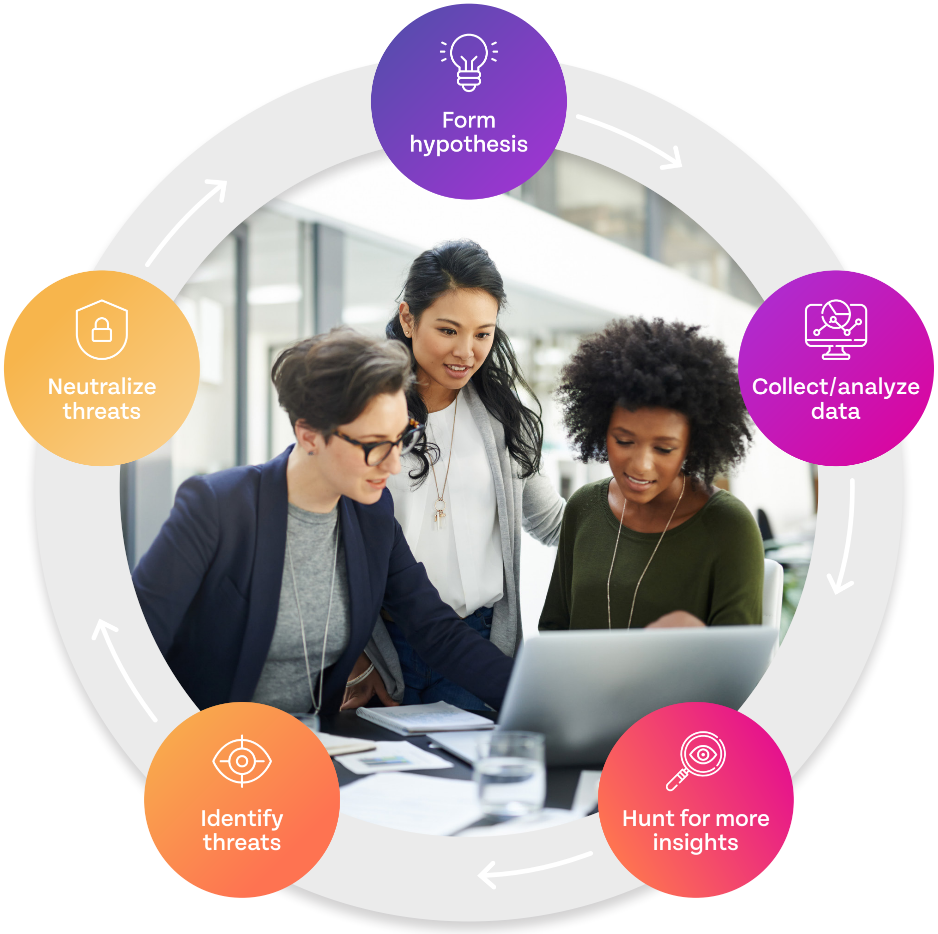
Security Forensics

Once the threat is identified, in the ideal situation, you take the time to capture the proof in a forensically accurate manner so that it holds up in a legal proceeding.

How to Hunt

Effective threat hunting is an iterative process involving regular reviews and adjustments. Threat hunters need to think like their adversaries and build knowledge about where to hunt within the network based on recognized tactics, techniques, and procedures (TTPs). They also must anticipate where an attack is most likely and what targets are at higher risk for attack.

Understanding what the bad guys are doing and where they are likely to strike provides the structure needed to threat hunt beyond relying on hunches or putting out fires when something goes wrong.



The Threat Hunting Process

Common Threat Hunting Tools

There are a variety of tools that can be used for threat hunting. Using multiple, different tools provides distinct perspectives into the data. However, you'll want to integrate this data into common dashboard views to gain unified insights across your security domains. Here are some tools you will want to consider:

Full-fidelity flow monitoring for network traffic reports with port mapping and dependency mapping. The benefit of unsampled flow monitoring is its ubiquity of polling across the entire hybrid enterprise. This broad coverage ensures visibility into all recesses of the network, and with long-term data retention, it's what threat hunters need in a security solution. Sampling, taking intermittent snapshots of network traffic, simply does not provide a complete set of data and therefore cannot provide these same benefits. If you want to be secure 100% of the time, you need full-fidelity, always-on visibility.

Packet capture and analysis with deep packet inspection (DPI) identifies the protocol details and URLs and offers abundant packet storage for forensics analysis. Packets provide the details to investigate exactly what's happening at the data level, for example, what data was stolen in an exfiltration attack.

Infrastructure monitoring provides details into change management, and detects unusual activity on network devices, such as saturation of an interface by an attack. According to analyst firm EMA, network infrastructure is the most common root cause of security incidents.

Endpoint detection monitors desktops and servers, laptops, tablets, smartphones, and even IoT devices to detect and investigate suspicious activities.

Log analysis extracts data from log files for trend and pattern analysis; however, the first thing an adversary does once inside your network is turn off logging. Because of this, it's clear you must always supplement logging with one or more alternative sources.

Anomaly detection recognizes changes in volume and velocity of traffic between IPs. Anomaly detection may be built into your visibility or security solutions or may be a separate AI Ops offering.

Wrap Up

Threat hunting isn't a panacea; security teams must continue to execute on the security fundamentals. Still, organizations that contain valuable data are going to continue to face sophisticated threats. There will always be adversaries whose sole purpose is to infiltrate the network without tripping alerts. Threat hunting is the only means of consistently detecting those advanced threats.

With always-on, full-fidelity capture, Riverbed Network Observability allows you to identify and resolve performance issues and security threats up to 90% faster. Identifying and remediating network concerns always starts with visibility. The adage is truer today than ever: You cannot manage what you can't measure. The corollary is true as well: You can't secure what you cannot see. Any blind spot is ripe for exploitation.

When it comes to network visibility, fighting security threats must employ an all-of-the-above strategy. This includes the ability to capture every packet, every flow, and every device metric, everywhere.

The third component is the ability to collate and apply analytics to derive meaningful and actionable insights. Understanding what constitutes normal traffic patterns, detecting anomalies, accurately identifying correlations versus causations, and being able to quickly respond and mitigate performance problems and cybersecurity threats – all of this depends on your ability to see and analyze what is happening across your distributed network – on-premises, virtual, or in the cloud.

For more information about using Riverbed Network Observability for threat hunting, click here.

About Riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed provides two industry-leading solutions: the Riverbed Unified Observability portfolio, which integrates data, insights, and actions across IT to enable customers to deliver seamless digital experiences; and Riverbed Acceleration, which offers fast, agile, and secure acceleration of any application over any network to users, whether they are mobile, remote, or on-premises. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com.