EXTRAHOP

WHITE PAPER

Threat Hunting Across the Network

A Field Guide

TABLE OF CONTENTS

The Network Is Your Hunting Ground

Just as a master hunter identifies a predator by the subtle indentations left in a field of snow, the modern SOC must identify threats by the behavioral tracks left across the network. While EDR agents and firewalls provide a piece of the puzzle, the network is the ground truth—the place where an adversary cannot hide their tracks.

Modern threat hunting is the high-stakes, human-driven pursuit of predators that have already bypassed your automated defenses. It operates under a singular, sobering assumption: **The compromise has already occurred.**

This is a move from passive observation to active defense. It is the process of scouring the wire for adversaries who are "living off the land," weaponizing your own legitimate tools to move laterally and bleed data over time. Hunting isn't a review of logs—it is an iterative, creative interrogation of your data to unmask the "unknown unknowns" lurking in the shadows of your environment.

Why spend time hunting when you're already drowning in alerts?

Yes, the SOC is drowning in alerts. But the difference between investigating and hunting is the difference between **reacting to a fire** and **clearing the brush**. Investigating is **reactive**, while threat hunting is proactive. And if you're doing it right, doing the former will positively impact the latter. This is not philosophical or hypothetical. In the organizations that participated in the SANS 2024 Threat Hunting Survey, for every dollar invested in proactive hunting, they saw a measurable drop in dwell time as hunters found the "Silent 20%"—the threats that bypass automated EDR and SIEM filters—within an average of **14 to 28 days**, compared with the global average of **200+ days**. This translates to finding a threat **55% faster** than when relying on notifications alone. Just as a hunter who is intimately familiar with the landscape is more effective at finding and tracking prey, familiarity with the network and what's on it will make your SOC much more effective at finding the things that shouldn't be there.

More importantly, those significant reductions in dwell time equate to reductions in the cost of security incidents. In the IBM Cost of a Data Breach Report 2024, organizations with active hunting programs saved an average of **$1.12 million** in total breach costs compared to those without. In fact, proactive threat hunting is cited as **one of the top 3 factors** in reducing the total cost of a breach. This isn't hard to understand; less time in the network = less data exfiltrated = lower recovery and regulatory costs.

Threat Investigation (Reactive):
Triggered by alerts from SIEM, EDR, or NDR to validate known incidents and lead to containment.

Threat Hunting (Proactive):
A hypothesis-driven exploration designed to find "unknown unknowns" and emerging threats that automated tools miss.

The Outcome:
Hunting doesn't just close cases; it improves future detections, increases visibility, and drastically reduces attacker dwell times.

Three Good Reasons to Go on a Hunt Today

A quick internet search will turn up a plethora of threat hunting scenarios, many of them specific to a particular industry, malware, or vulnerability—but let's start with 3 broad reasons to go **into the network** on a hunt today.

REASON #1
The Enemy Is Behind the Gate

Perimeter defense is no longer a 100% effective solution. In 2026, attackers are just as likely to log in using stolen credentials as they are to hack in. But regardless of the method of entry, attackers MUST use the network to do reconnaissance, move laterally, communicate back to C2 infrastructure, and exfiltrate data—and each of these activities leaves tracks across the network that a skilled hunter can follow. ExtraHop is purpose-built for this. Not only does ExtraHop watch high-value assets like critical servers and endpoints, but it also allows you to decode the communication between them so you can determine if something is normal vs. abnormal. A wolf in sheep's clothing still doesn't walk, talk, or act like a sheep.

REASON #2
Detections Are Just a Start, Not the Finish, to Finding Threats

Adversaries stay stealthy by using legitimate tools for malicious reasons. PowerShell, Sharphound, and many more examples exist that resist the signature-based approach. ExtraHop also has many behavioral detections that compare historical baselines to current behavior to spot anomalies that indicate malicious intent. But few of these detections in any of your security tools are good for identifying zero day attacks. For all of those types of attacks where signatures do not yet exist or are easy to evade, **threat hunting** is your best defense.

- **Example:** PowerShell is a favorite for lateral movement because it is a trusted, native tool.
- **The Failure of Signatures:** Simple signature-based defenses are easily bypassed when attackers use string manipulation (e.g., `'inv'+'oke'`) or highly encoded commands (`powershell.exe -e`).

REASON #3
The EDR Blind Spot

EDR is essential, but it isn't a silver bullet. Between shadow IT, unmanaged IoT, and legacy servers, "100% coverage" is an aspirational goal, not a practical reality.

In an ever-shifting attack surface, the network is the only **ground truth**. While an attacker can disable an agent or hide in a blind spot, they cannot hide their communications. Every lateral leap, every command, and every exfiltrated byte happens on the wire. This turns the network into the hunter's advantage.

Data Sources for Threat Hunting

Just as an experienced hunter relies on all their senses, a mature hunt program integrates data from multiple layers to be effective. This typically starts with threat intelligence feeds to provide the necessary Indicators of Compromise (IOCs) and behavioral TTPs. This is layered with endpoint data to track process execution, registry changes, and file modifications. However, to capture the full picture, this must be correlated with network data, including packets, flow records (NetFlow/IPFIX), logs, identity (IAM data), as well as cloud and SaaS logs (such as VPC flow logs and CloudTrail). ExtraHop uses virtual or physical sensors to collect and parse this data. Without this diverse telemetry, hunters are often left trying to reconstruct a jigsaw puzzle with only a few of the smallest pieces. ExtraHop brings all this data together for you in the recordstore, but any modern NDR solution needs the ability to centralize, normalize, and analyze this diverse data set.

Three Ways to Hunt Your Network

Risk-Based Threat Hunt: Stalking the Weak and Vulnerable

In the wild, predators don't work harder than they have to—they target the weak. Your network is no different. Every environment—on-prem or cloud—contains "targets of opportunity": legacy servers, deprecated cipher suites, and unpatchable vulnerabilities that offer attackers the path of least resistance. Knowing your own security vulnerabilities means knowing the targets of opportunity the predators themselves will seek out, and this helps you focus your hunts.

Focus: Proactively searching for suspicious behavior related to assets with known vulnerabilities.

- **Hypothesis:** "We patched our Cisco Unified Communications Manager two months after the vulnerability was released. We hypothesize an adversary has targeted our Cisco UCM."
- **Identify the Trail:** Identify if there are or were any holes in your ACLs that may have allowed for external HTTP packets to hit internal management subnets, so you can narrow in your searches on exposed IPs or CIDRs. Review threat blogs and proof of concepts to help craft your searches.
- **The Hunt:** Scrutinize traffic from URI strings that may indicate scanning.

```
type="~http" and (uri ~ "/ccmadmin/" or uri ~ "/cucm-uds/" or uri ~ "/cmplatform/" or
uri ~ "/cucreports/") and ex.isExternal = true
```

- **Pivot:** Sometimes, in threat hunting, the initial search may not return results. This does not mean that the threat doesn't exist. Just like with hunting, learning when and how to pivot is crucial to covering all tracks and catching or evading predators. With this next search, we will adjust how we search for scanning activity.

```
type="~http" and uri~"/cucm-uds/users" and (rspBytes>5000 or method="GET")
```

- **The Final Trail:** It is always good to ensure there were no unwanted actions taken. Sometimes logs age out, or our searches don't reveal scanning and exploitation that leads us to identifying the initial entry. We can search for POST and PUT methods to identify if there were any unwanted interactions.

```
type="~http" and (uri~"/ccadmin/" or uri~"/cucm-uds") and method in ("POST","PUT")
```

Anomaly-Based Hunt: Finding the "Wolf in Sheep's Clothing"

Focus: Identifying outliers that deviate from standard asset behavior.

- **Hypothesis:** "Adversaries are using unauthorized applications to communicate with external infrastructure."
- **The Hunt:** First, cast a wide net to get an idea of what the group of internal hosts (i.e., finance subnet) is making high-frequency connections to external IPs on ports that do not have standard ALPNs. Due to this being a widecast, it is important to do filtering to include the specific subnet you are hunting on.

```
type = "~ssl_open" and serverIsExternal = true and clientAlpn not_in ("h2",
"http/1.1") and clientAddr in (<CIDR RANGE>) | summarize count() by clientAddr,
serverAddr, clientAlpn, host, serverPort
```

- **Narrow the Hunt:** Initial query refinement can be adding more ALPNs to exclude. For example, if your network uses Apple products, you may want to update the query to exclude the Apple ALPN and CIDR ranges.

```
type = "~ssl_open" and serverIsExternal = true and clientAlpn not_in ("h2",
"http/1.1") and clientAddr in (<CIDR RANGE>) and (clientAlpn != "apns-security-v3"
and serverAddr not_in (17.0.0.0/8)) | summarize count() by clientAddr, serverAddr,
clientAlpn, host, serverPort
```

- As you review the results listed, you can expand the query to exclude external IP ranges and hosts that are acceptable to your network.

  Note: Sorting in ascending order will identify the rare values quickly. Which may be more interesting to investigate and drill into.

Intelligence-Based Hunt: Hunting with Known TTPs

Focus: Using global threat intelligence to find specific tactics used by known adversary groups.

- **Hypothesis:** "Chinese APT groups (like *Flax Typhoon*) are using **SoftEther VPN** to quietly access infrastructure. While it looks like legitimate HTTPS, its JA4x signature is unique."
- **Specific Tracks:** Hunt for the **SoftEther VPN** JA4x fingerprint: `t13d880900_fcb5b95cb75a_b0d3b4ac2a14`.
- **The Hunt:** Indicators of Compromise (IOCs) hunts are the most common type of threat hunt because it is easier to figure out where to start. For this specific case, we will be searching for the JA4 Fingerprint associated with SoftEther VPN.

```
type="~ssl_open" and ja4Fingerprint = "t13d880900_fcb5b95cb75a_b0d3b4ac2a14" |
summarize count() by clientAddr, serverAddr
```

Regardless of the type of hunt you choose to go on, the network gives you an advantage that agents and logs can't, especially for lateral movement, privilege escalation, and data exfiltration. Attackers can't hide from the network—they **must** use the network to move around. Put this advantage to work for your SOC.

RevealX™ Gives You More Tools for Your Hunt

RevealX by ExtraHop is a fully functional NDR, IDS, NPM, and packet forensics solution with a treasure trove of data waiting to be leveraged by threat hunters. By leveraging **ExtraHop RevealX**, you can integrate:

- **JA4+ Fingerprinting:** To identify malicious toolkits by their handshake DNA.
- **Threat Intelligence:** From your vendor of choice, with Hunt.io built in.
- **Advanced PowerShell Analysis:** To see the actual commands executed remotely, even when encryption is used.
- **Out-of-Band Decryption:** To inspect payloads for malicious content without disrupting business operations, for no additional cost and no additional hardware needed.
- **90+ Network Protocol Decodes:** Your NDR needs to speak the same language as your applications. ExtraHop understands SQL, LDAP, DNS, Modbus, HTTP, and virtually all other commonly used network protocols, so you can differentiate normal vs. abnormal behavior. For anything custom to your network, custom parsers can be created to meet your unique needs.

Hunt Upstream to Go from Reactive to Proactive

Don't wait for the alert to find you. Use ExtraHop to move from a reactive investigation mindset to a proactive hunting posture. Hunting for threats puts you on the offensive, often looking at the most vulnerable parts of your environment for signs of attack. Lastly, using NDR to hunt for threats in your network will make you much more familiar with your network and the traffic on it, which will make you a more valuable security resource.

Learn more

The Global Threat Landscape: A Guide to Today's Most Active Threat Actors

- Discover how threat actor tactics and patterns have shifted in the last year, driving expanded impact.
- Analyze top ransomware threat actors and how they operate, enabling you to stop them faster.
- Explore how you can detect threats early, preventing data exfiltration and dramatic disruptions.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com