EXTRAHOP

Hunt Threats Faster Using Network Data and ExtraHop

The network is your perfect hunting ground for advanced, persistent threats

SOLUTION BRIEF

The Challenge

Today's threat actors are increasingly logging in using stolen credentials purchased for as little as $20 on the dark web. 81% of breaches involve compromised credentials now, making it easier than ever for attackers to get a foothold inside the perimeter. Once inside, it is a matter of patience and time to eventually move laterally, act on objective, and exfiltrate. Besides the obvious problem of letting the attacker inside, several other factors conspire against today's cybersecurity professionals:

- Initial access is further threatened by AI-assisted attacks like highly personalized phishing and social engineering, and the abuse of AI agent credentials.
- Encrypted channels deliver 87% of ALL network traffic, not just web traffic. This makes detection of lateral movement particularly difficult, since it is almost always encrypted.
- Attackers often use stolen but legitimate identities and "approved" software like RMM tools that blend in with ordinary traffic.

This is why 41% of attacks successfully bypass ALL your existing defenses. We need to start assuming the enemy is already inside the gate. And we need a way to reveal the contents of many of the encrypted sessions that could be hiding these threats.

The Solution

Just as a master hunter identifies a predator by the subtle indentations left in a field of snow, the defender can identify threats by the behavioral tracks left across the network. The network is your ideal hunting ground because the attacker MUST use the network for reconnaissance, to move laterally, and to exfiltrate data. And just as night vision goggles can aid the hunter spot tracks in the dark of night, a modern network detection and response (NDR) solution can decrypt east/west traffic at scale, in real time, to reveal threats lurking inside that encrypted traffic.

The difference between investigation 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, 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

KEY CAPABILITIES

Decryption, at scale, for east/west traffic reveals threats lurking in encrypted sessions. ExtraHop gives you decryption capabilities at speeds up to 100 Gbps at no extra charge.

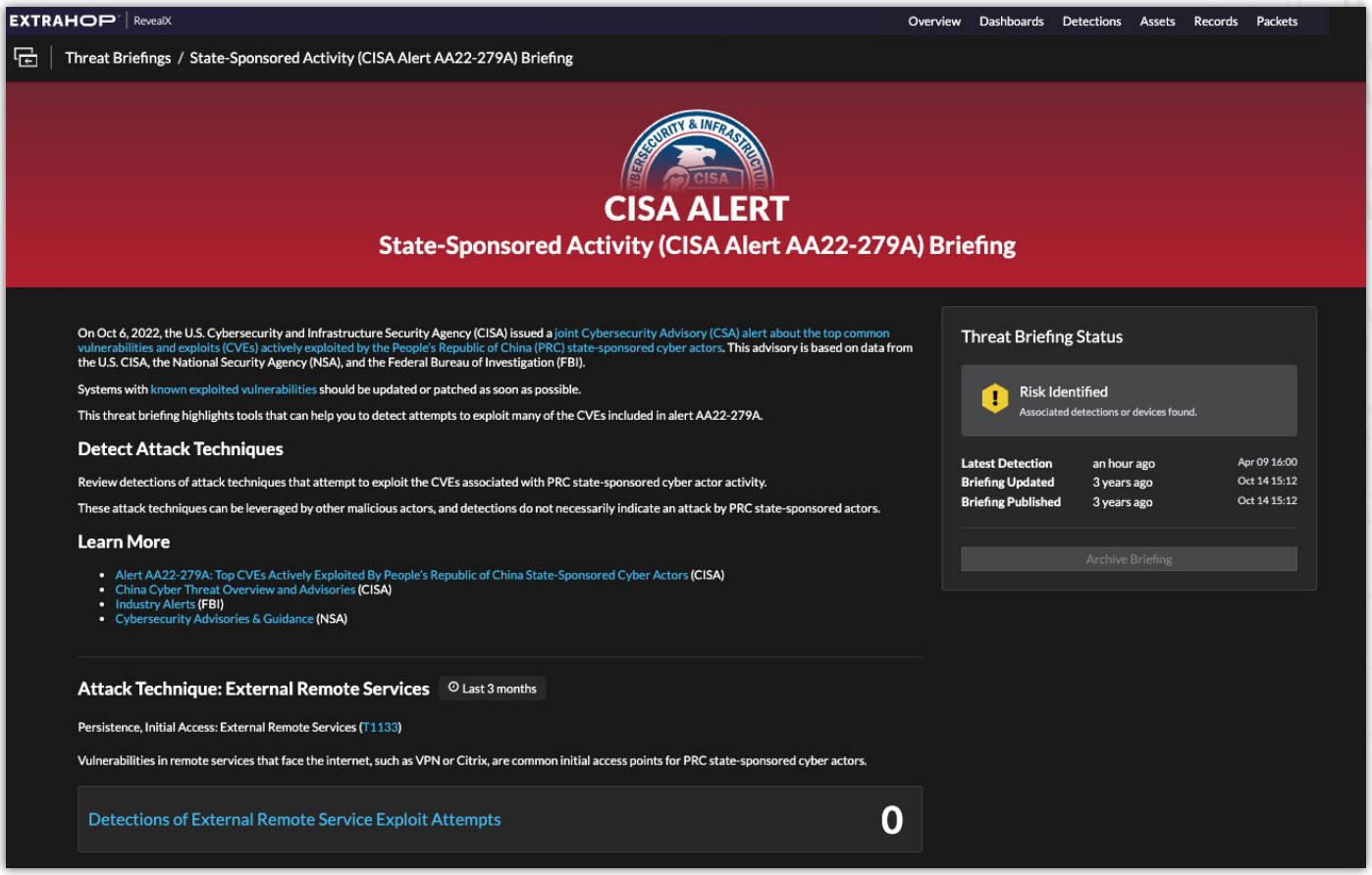
ExtraHop decodes over 90+ protocols. It doesn't do any good to listen in on a conversation if you don't speak the language. ExtraHop is fluent in most network protocols and can tell the difference between normal and malicious behavior.

ExtraHop's recordstore contains detailed data on everything that went over the network, giving you the ground truth on what actually happened.

The ExtraHop query language is the key to leverage the treasure trove of answers inside the recordstore. Use curated queries as a jumping-off point, or start your own custom hunt using your own complex query and aggregations to search, pivot, and iterate until you get your answer.

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 translated to finding a threat **55% faster** than when relying on notifications alone.

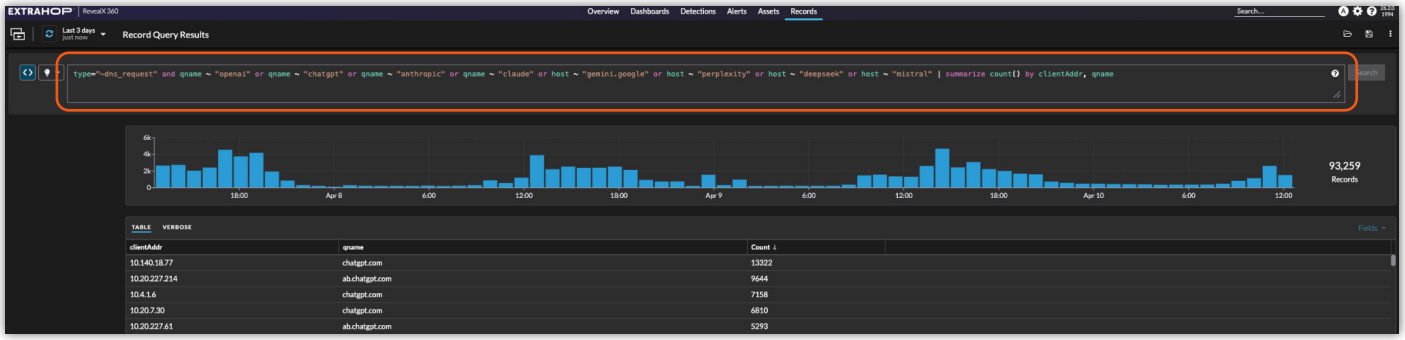
ExtraHop is a force multiplier for every level of threat hunter. Regularly updated threat briefings in the product educate on prevalent threats seen by ExtraHop’s Reveal Labs research team and guide them on beginner hunts.



For more senior threat hunters on the prowl for those novel persistent threats, ExtraHop provides crucial capabilities no other tool can:

1. Decryption at scale for east/west traffic at 100 Gbps throughput. For the servers and applications you host on-prem or in the cloud, ExtraHop can reveal threats lurking in encrypted channels. And not just for web traffic using TLS 1.3, ExtraHop also provides decryption for other protocols like NTLM, LDAP, DNS, MS-RPC, SMB, and WSMAN that are often used by attackers for lateral movement.
2. The detailed recordstore for network data, with retention options from 30 to 365 days. ExtraHop’s recordstore is the high-fidelity data repository for all sessions seen on the network. With ExtraHop’s ability to decode over 90+ protocols, you’ll get the individual commands and responses—giving you the detail you need to spot the malicious activity hiding among the normal traffic.

3. The ExtraHop query language is your direct access to the wealth of information inside the recordstore. Jump into a threat hunt with one of our curated queries, or use them as a jumping-off point into your own custom threat hunt. Build complex queries using aggregation functions to search, pivot, and iterate until you either prove or disprove your hunt hypothesis.



Get Fast Answers to Complex Queries | **Guided or Custom Threat Hunts** | **Use Decryption to Reveal Hidden Threats**

> Watch this webinar on the ExtraHop Community for a more in-depth look at using ExtraHop for threat hunting.

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