With Threat Hunters in High Demand and Limited Supply, Executives Need to Shift from a Culture of Defense to Offense

Research highlights obstacles including talent shortages, management buy-in, and lack of funding

NEW YORK, NY, UNITED STATES, March 2, 2023 /EINPresswire.com/ -- Enterprise-level cybersecurity teams are desperate for trained threat hunters to help improve cybersecurity threat detection and response, but face major challenges including talent shortages, position funding, and organizational understanding of how threat hunting tools work, according to new research from CyberRisk Alliance Business Intelligence, the research and content arm of cybersecurity data and insights company CyberRisk Alliance (CRA).

Despite growing recognition of the value of threat hunting, a survey of over 200 U.S.-based security and IT leaders, practitioners, administrators, and compliance professionals revealed there is still very low organizational awareness of what processes, tools and policies are needed to maximize threat hunting potential. The report was underwritten by ExtraHop.

“No one on my team has any experience, so it’s learning as we go and trial-by-fire,” said one survey respondent. “There isn’t a big enough buy-in from executive management to get additional training or hiring an experienced threat hunter.”

While third-party providers are a viable solution, “The overall cost for third-party managed threat hunting programs can be unrealistic for small- and medium-sized businesses,” said another respondent.

Key findings:

• While more organizations have announced intentions to introduce hunting capabilities in the next year, threat hunting overall remains out of reach to most businesses due to high costs of entry or limited understanding into what value it would bring. More than half (56%) of respondents believe threat hunting is very/extremely important in improving the overall security

posture of their organization. While 32% of respondents said they are currently implementing a threat hunting program today, about half (51%) indicated they will be planning for it or evaluating it in the next 12 months or considering it for the future.

• Respondents point to the difficulty in recruiting and retaining individuals (41%) who have such diverse skills and depth of expertise — a rare blend of technical knowledge, forensic talents and intellectual curiosity. In addition to dealing with such a limited pool of candidates, respondents say threat hunters carry a price tag that many organizations simply lack the budget for (69%).

• Roughly 75% of respondents use SIEM and/or endpoint detection and response tools (EDR) in their threat hunting programs while cyber threat intelligence is only used by about half of these organizations. About 80% of respondents collect at least a moderate level of data that provide the analytics that power their threat hunting programs. Data collected for threat hunting can include endpoint data, network data, and various types of security data (e.g., alerts, threat intelligence, etc.). Not clear what this means.

• Organizations that implemented threat hunting have observed improvements when it came to faster speed and accuracy in threat response, reduced attack surfaces and encounters with bad actors, as well as greater precision in discovering and detecting threats. At the top of respondents' list of objectives for conducting threat hunting are advanced threat detection (63%), reduced exposure to advanced threats (48%), and improving the speed and accuracy of the threat responses (45%).

In addition to survey insights, the report offers guidance to help organizations get started and/or pursue threat hunting initiatives more effectively. For more detailed findings and analysis, the full research report is available for download here.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

About ExtraHop
ExtraHop is on a mission to stop advanced threats. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to threats–– before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised. Learn more by visiting extrahop.com.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here
Visit us on social media:
Twitter
LinkedIn
