Proactive Businesses Understand the Importance of Threat Hunting in Cyber Security

Cybercriminals constantly evolve their attack methods, developing new tools that bypass traditional security methods. Consequently, security strategies that wait for threats to trigger alarms no longer provide adequate protection, underscoring the importance of threat hunting in cyber security.

To protect vital digital assets, companies need to move away from reactive security and take a more proactive approach. Like the hunter tracking her prey, threat hunting relies on human expertise to identify the subtle, unusual patterns that may indicate a compromise.

This approach delivers several key benefits. First, it enables security teams to identify and mitigate threats early, thus reducing the risks of data breaches. Secondly, the process helps security teams understand hackers' tactics and adjust their defenses accordingly. And finally, it improves the ability to discover sophisticated attacks that slip past automated defenses.

Challenges to Traditional Cyber Security Approaches

Traditional cyber security strategies tend to rely on established security measures such as antivirus software, firewalls, and intrusion detection. These tools, while essential, operate on the principle of signature-based detection. That is, they identify threats based on known patterns, or signatures, of malicious software.

As a result, traditional security measures may miss more sophisticated threats. These include Advanced Persistent Threats (APTs) that spread unnoticed through the target network. They also include zero-day attacks that exploit vulnerabilities that the vendor does not know about and has not addressed.

Thus, traditional security measures on their own leave dangerous gaps. Enter threat hunting. By including offense as a form of defense, it shifts cyber security from a purely defensive activity to a more balanced approach.

Importance of Threat Hunting in Cyber Security Understood, But How Does It Work?

Threat hunting assumes that breaches have already occurred somewhere in the network. Using a combination of manual and automated techniques, human threat hunters sift through large amounts of data looking for patterns that may indicate a breach.

The process begins when the hunter uses their expert knowledge of threat actors' known tactics, techniques, and procedures (TTPs) to form a hypothesis regarding potential threats. Based on that hypothesis, the hunter then conducts a detailed search of endpoints, networks, and datasets to identify anomalies that might indicate compromise.

Human Expertise Combined with the Right Tools

Threat hunting blends intuition and experience with advanced analytics and machine learning. Successful threat hunters must possess a deep understanding of the network environment and security tools, as well as current threat tactics. And they must combine cyber security expertise with critical thinking, curiosity, and the ability to adjust tactics as threats evolve.

Sophisticated technologies support human expertise. These include a variety of tools such as Security Information and Event Management (SIEM) solutions that collect, analyze, and correlate security data from various sources in real time. Data analytics platforms will help in processing large datasets.

Applicable tools also include Endpoint Detection and Response (EDR) solutions to monitor endpoints and tools to analyze network traffic. And they include threat intelligence feeds to provide context regarding known threats. Hunter-trained AI and automation will prove essential, though they cannot replace human expertise.

Incorporating Threat Hunting into Small Business Cyber Security Strategies

For small businesses with limited resources, implementation of threat hunting can seem daunting. However, with the right strategies, even smaller enterprises can effectively integrate threat hunting into their cyber security program.

Start small. This might involve monitoring for specific types of threats that are most relevant to your industry. It may also involve focusing on the most critical assets within the organization. Additionally, leverage existing security tools such as SIEM systems, antivirus logs, and network traffic analyses to provide valuable insights.

A combination of tactics can provide necessary expertise. First, upskill existing staff by investing in training and certification programs. Next, collaborate with other small businesses to share information and insights, thus building a broader perspective.

Finally, consider outsourcing threat hunting to specialized service providers. Cyber security providers such as eMazzanti offer scalable services tailored to the needs and budgets of small businesses.