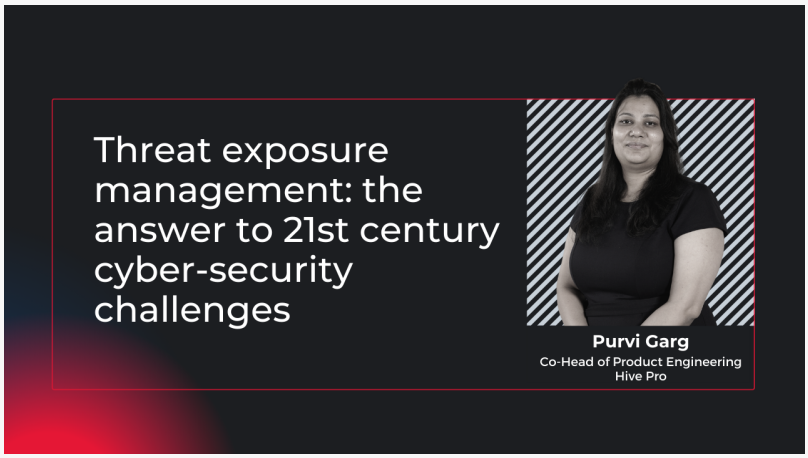
Threat Exposure Management: The answer to 21st century cyber-security challenges

MILPITAS, CALIFORNIA, UNITED STATES, November 1, 2022 /EINPresswire.com/ -- The chief information security officer (CISO) role is one that came into being as a result of an increasing wave of cyber-crime, and is a job that has only increased in importance, as CISOs today face multiple challenges on the security front.



Threat exposure management the answer to 21st century cyber-security challenges

Not only are the threats from cyber-criminals increasing, but digital transformation has also led to a scenario of exponentially expanding attack vectors. These challenges themselves lead to vulnerability fatigue, from constantly searching for new threats and vulnerabilities. In fact, the Gartner Hype Cycle for Security Operations 2022 actually suggests that top CISOs are recognizing the need for a formally defined approach to managing threats and vulnerability.

> Threat exposure management provides richer, more contextual insight that helps organizations proactively identify, prioritize and manage unexpected risks or exposures."
>
> *Purvi Garg*

According to Purvi Garg, Co-Head of Product Engineering at Hive Pro, a leading provider of cybersecurity solutions aimed at prevention, detection, response and prediction, such an approach infers that organizations should seek to undertake a necessary evolution from the more traditional patch and vulnerability management scenarios, by adopting instead the concept of threat exposure management.

"By definition, patch management assists in remediating risk by upgrading software to the most recent versions, whereas vulnerability management is designed to unveil risks and prioritize those risks based upon their levels of severity," she says. The disadvantage of the former is that it becomes a sheer numbers game: CISOs may be looking at, for example, 20 000 vulnerabilities in their system, of which 200 are exploitable, and 100 of these actually present a serious threat.

And it is here that the idea of implementing a threat exposure management approach comes to the fore. This is the proactive identification, assessment, and mitigation of security risks and vulnerabilities within an organization. Threat exposure management aims to protect an organization's information assets, systems, and networks from internal and external threats.

"Threat exposure management provides richer, more contextual insight that helps organizations proactively identify, prioritize and manage unexpected risks or exposures. This approach differs from standard threat management practices, because it responds to an ever-changing threat landscape. In other words, it works to the principle that what might be low risk for an organization today, might in fact be high risk for it tomorrow," Purvi notes.

There are four key components to threat exposure management. The first is risk identification, which involves proactively identifying risks and vulnerabilities through security assessments, threat intelligence, and other means. Secondly, there is risk assessment, or determining the potential impact of identified risks and vulnerabilities.

The third component is risk mitigation, such as implementing controls and countermeasures to reduce risks and vulnerabilities' likelihood and impact, while the final one is risk monitoring – continuously monitoring the environment for changes that could impact the organization's security posture.

"To achieve an effective transition to threat exposure management, it is necessary to firstly undertake a risk assessment to identify which threats pose the most significant risks to your organization," she adds. Once this is known, the business should develop policies and procedures for managing exposure to these threats, and then implement controls to mitigate the risks associated with these threats. The next step is to ensure you monitor and review your exposure to these threats regularly, while also taking action to address any new or increased risks.

However, it is vital to note that the threat exposure management arena is one that is not yet mature and is thus lacking in easily accessible expertise. It is for this reason that it is wise for organizations to entrust their threat exposure management strategy to a vendor that is equipped to combine an organization's existing asset and vulnerability management capabilities with a new suite of tools.

"Essentially, you will want a partner that understands your enterprise's specific needs, can effectively determine what your vulnerabilities are, and will help you to bolster your defenses and fine-tune your proactive cyber-security tactics," Purvi explains.

In this way, you will be positioned to lower the exposure of an attack, reduce an attacker's ability to exploit vulnerabilities, detect and respond to attacks more rapidly and reduce the risk of human error – ultimately leveraging this new approach to reduce the overall risk of an attack.

About Hive Pro Inc.

Hive Pro Inc is a cybersecurity company specializing in Continuous threat exposure management. Its product HivePro Uni5 provides a Continuous threat exposure management Solution to proactively reduce an organization's attack surface before it gets exploited. It neutralizes critical cybersecurity vulnerabilities that really matter to organizations through a single console. Hive Pro has its corporate headquarters in Milpitas, California, a sales office in Dubai, UAE, and a development center in India. For more information, visit www.hivepro.com.

Hive Pro Marketing
Hive Pro
email us here
