EINPRESSWIRE

The current cybersecurity challenge: All the threat data in the world, but no idea how to leverage it

MILPITAS, CALIFORNIA, UNITED STATES, August 5, 2022 /EINPresswire.com/ -- Organizations today are facing a deluge of automated cybersecurity threats that are increasing exponentially every day, not only in velocity but in variety and complexity. This makes it virtually impossible for organizations to address every vulnerability. In addition to this, chief information security officers (CISOs) are faced with a siloed approach to understanding and addressing cyber security threats, leaving organizations of all sizes – simple and complex – exposed, vulnerable and under constant threat, focusing on trying to remediate in the wrong areas, says Sarfaraz Kazi, CTO Hive Pro, a leading provider of cybersecurity solutions aimed at prevention, detection, response and prediction.

The current cybersecurity challenge All the threat data in the world, but no idea how to leverage it

> “
> We have changed the way CISOs consume, plan, & implement threat mitigation measures for their cybersecurity strategies! Consequently, this helps organizations fix vulnerabilities that matters to them.”
>
> *Sarfaraz Kazi*

Typically, any organization's ability to remediate vulnerabilities today is only 15% of the active vulnerability count. Given this reality, it’s time for organizations to move away from trying to fix all vulnerabilities and instead focus on the ones that matter. Except, they struggle with multiple sources of "what really matters".

Using various siloed tools like Vulnerability Management, Vulnerability Prioritization, Breach and Attack Simulation, PenTesting, customers consume multiple vulnerability ratings but are still unable to find a single console to represent the actual risk

At a recent symposium, Gartner Director Analyst, Sam Olyaei, reiterated that treating threats and remediation the same way as has been done in the past, is no longer good enough. The thinking, philosophy, programmes and architecture need to change.

In addition, in its Top 10 Security Projects for 2020-2021 report, Gartner suggests that the most efficient route to addressing this challenge is to focus on the vulnerabilities that are actually exploitable, and to go beyond a bulk assessment of threats. Threat intelligence, attacker activity and internal asset criticality provide better views of the real risk that organizations face.

Many solutions follow the Cybersecurity and Infrastructure Security Agency's binding directive as a guide on what vulnerabilities to address, but what they lack is asset criticality and contextual threat intel in order to take truly transformative steps to address vulnerabilities.

Hive Pro solutions are built on the foundation of providing organizations with a view of the criticality of their assets, current priority vulnerabilities and attack vectors, while also providing a dashboard that allows CISOs to make better-informed decisions and proactive strategies that bolster defenses.

Kazi explains that this is something Hive Pro provided well before Gartner identified it as a priority in the face of the rising levels of threats. "We have changed the way that CISOs consume, plan, and implement threat mitigation measures for their cybersecurity strategies. It has become clear that there are not enough resources available to address all the threats, and most solutions lack the intelligence to guide what vulnerabilities need to be addressed, how they need to be addressed, and how to do so at speed."

Intelligent reporting, allows CISOs to see whether tasks that have were prioritized for action by other departments, have actually been addressed. The seamless integration of Hive Pro's solutions mean that deployment and onboarding provide a near-zero time to value with results delivered in hours.

Using vulnerability as a pivot, Hive Pro can pre-empt attack surfaces and provide a pre-breach analysis specific to an organization's risks. Advanced machine learning models are deployed which identify unique threats specific to the environment and industry. And finally, patch intelligence covering more than 80 000 common vulnerabilities and exposures and 100 000+ patches provides teams with the actionable insight to act on and remediate the most critical threats before they become costly exploitations.

Where cybercrime has become more advanced than ever before, and CISOs and their organizations have more at stake, those that turn to proven technology to address the most critical challenges will be the ones that survive. Indeed, having access to data without the insight and context, can be as risky as the threats themselves.

About Hive Pro Inc.

Hive Pro Inc is a cybersecurity company specializing in Cyber Threat Exposure Management. Its product HivePro Uni5 provides a Cyber 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 Inc
marketing@hivepro.com
