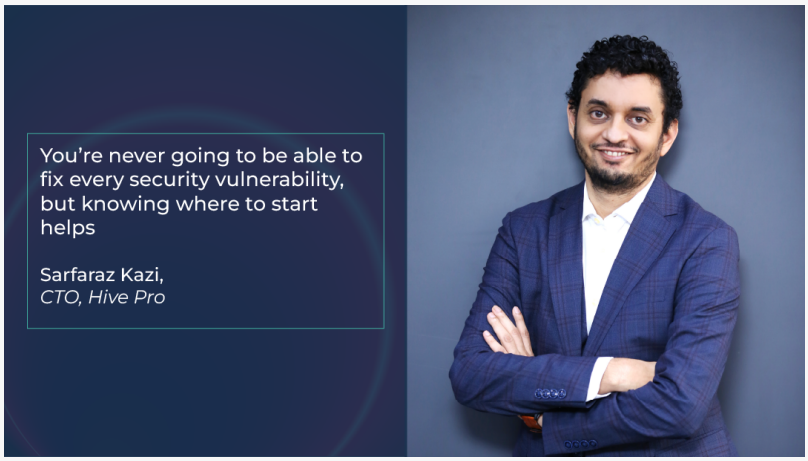
You’re never going to be able to fix every security vulnerability, but knowing where to start helps

MILPITAS, CALIFORNIA, UNITED STATES, August 30, 2022 /EINPresswire.com/ -- IT security operations, risk management and infrastructure teams face a daily challenge: do more with less. And in the face of increasing threats from cybercriminals and exponentially expanding attack vectors, teams are going to have to turn to intelligent technology to overcome even a small part of the threat – or risk becoming overwhelmed and vulnerable.



You’re never going to be able to fix every security vulnerability, but knowing where to start helps - Sarfaraz Kazi

With cyber threats increasing not only in velocity but also in variety and complexity, it is almost impossible for organizations to address every vulnerability. Sarfaraz Kazi, Chief Technology Officer at Hive Pro, a leading provider of cybersecurity solutions aimed at prevention, detection, response and prediction, says that organizations require new strategies to combat this inevitable threat.

> With cyber threats increasing not only in velocity but also in variety and complexity, it is almost impossible for organizations to address every vulnerability.”
>
> *Sarfaraz Kazi*

“The rapid adoption of remote work, increased use of personal assets on organizational networks and expanded requirements for organizations to track risk and threats across their asset base have resulted in an environment that will never be 100% protected from threats, but SecOps is increasingly required to understand the total risk,” says Kazi.

According to Kazi, security operations (SecOps) have had to move swiftly to include people, technology, and processes, but even this is not enough nowadays when at any given time, only 15% of active vulnerabilities will be remediated. Adding, “SecOps faces the added challenge of which 15% constitute the most

critical vulnerabilities, and how they need to be addressed especially since operational technology and internet of things environments are prime targets for orchestrated attacks nowadays." An out-of-date printer driver or incomplete patch on a long-forgotten device can provide the access point for severe, crippling cyberattacks.

SecOps has had to rely on various technologies which monitor and report on vulnerabilities and threats across the organization's attack surface, but none provide any team with a consolidated view and context-aware insights on what vulnerabilities require the most critical remediation.

Effective security and identity management require a layered and collaborative approach. Many of today's solutions address vulnerabilities in siloes, operating with insufficient knowledge of other tools, leaving gaps that can be exploited. A single platform to consolidate security capability appears to be the only solution.

Hive Pro has offered single platform continuous threat exposure management solutions to organizations long before they were identified as critical elements of the Gartner Hype Cycle for Security Operations, 2022. HivePro Uni5 is a Continuous threat exposure management solution built on the foundation of providing organizations with a view of the criticality of their assets, current priority vulnerabilities and attack vectors; and also provides a dashboard that allows CISOs to make better-informed decisions and proactive strategies to bolster defenses.

It's hard enough for large SecOps strategies to adequately address challenges that large organizations face today, leaving small to medium-sized businesses overwhelmed by the existential threat posed by cybercriminals.

HivePro Uni5 changes how organizations, large and small, consume, plan and implement threat mitigation measures and strategies. "The intelligent reporting provided by HivePro Uni5 provides contextually-relevant reporting to current threats and exposure, including guidance on remediation."

When it's not only infrastructure but also resources that are buckling under the constant threat of cybercrime, SecOps benefits from every bit of insight, reporting and help that no team of humans could ever collate and address in such a short space of time.

"HivePro Uni5 is the only reasonable chance that many organizations have of even addressing the 15% of the most critical vulnerabilities, and then steps up with greater insight and remediation tactics so that SecOps has a fighting chance of addressing the ever-increasing number of attacks daily, with less," concludes Kazi.

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
marketing@hivepro.com
Visit us on social media:
Twitter
LinkedIn
