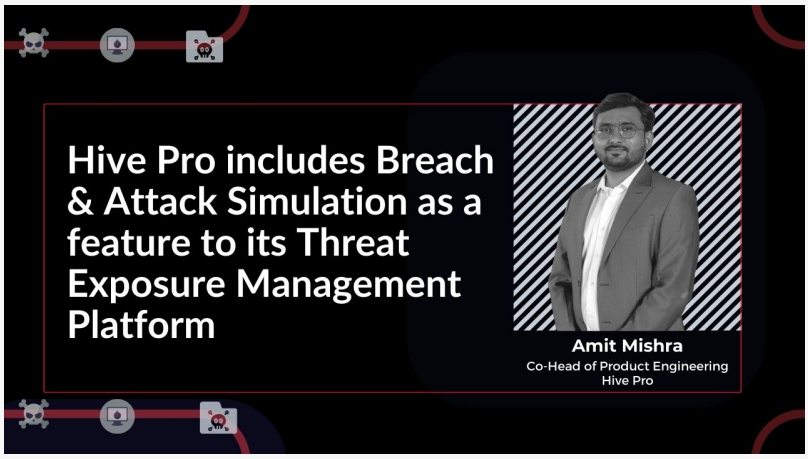
Hive Pro includes Breach & Attack Simulation as a feature in its Threat Exposure Management Platform

MILPITAS, CALIFORNIA, UNITED STATES, December 13, 2022 / EINPresswire.com/ -- Although the Gartner Hype Cycle for Security Operations 2022 has positioned Breach and Attack Simulation (BAS) solutions at the peak of inflated expectations, a new platform is taking BAS to a whole new level.



Hive Pro includes Breach & Attack Simulation as a feature to its Threat Exposure Management Platform

In a digitally transforming world, cyber-security has continued to grow in importance, as organizations recognize the danger posed by the proliferation of threat actors. Thus, it is unusual that Breach and Attack Simulation (BAS) solutions – despite being a technology that is almost a decade old – remain far from maturity.

In fact, the Gartner Hype Cycle for Security Operations 2022 has positioned BAS at the peak of inflated expectations. Clearly, customers are still not satisfied with the offerings of traditional BAS vendors.

> BAS will help customers to make decisions based on the simulation results, while at the same time, making them cognizant of the tangible risk of vulnerabilities in their infrastructure."
>
> *Amit Mishra*

This gap between customer expectations and traditional BAS solutions is the primary reason for a next generation BAS, explains Amit Mishra, Head of Products (SaaS, BAS & Integrations) at Hive Pro, one designed to address both what customers want today, as well as possible future expectations. This, in turn, creates an opportunity to innovate, to address problems differently and to look beyond the obvious.

"Gartner defines BAS technologies as tools 'that allow enterprises to continually and consistently simulate the full attack cycle, including insider threats, lateral movement and data exfiltration,

against enterprise infrastructure – using software agents, virtual machines and other means',"
adds Amit.

"BAS tools are able to run attack simulations unceasingly, systematically and automatically. Their role is to assess validity and efficacy, such as which types of vulnerabilities are accessible. Their other role is to ensure that security tools are operating as designed. Most crucially, BAS tools also provide a view of multiple, if not all, stages of the cyber kill chain, as well as of those areas where threat campaigns will likely be successful."

Essentially, BAS tools utilize simulations to identify vulnerabilities in security environments by mimicking the likely attack paths and techniques used by cyber-criminals – you could describe its operation as being akin to having a continuous, automated penetration test running.

It must be understood, however, continues Amit, that BAS tools are simulations — not real attacks — and are thus often not recognized as a real threat by cyber-security systems. More to the point, these solutions are not informed by threat intelligence. The problem this creates is that security teams do not know what threats are most relevant to test against.

"More pertinently, BAS technology is unable to fully replace activities such as manual testing, and it focuses only on known attacks, without providing remediation. In today's cyber-security environment, having a tool available only to provide diagnostics is simply not enough – it is imperative that the tool is also capable of driving remediation of identified threats."

"We have made an effort to address these challenges, by developing BAS as a feature in HivePro Uni5 Threat Exposure Management platform. This has been designed to work in conjunction with a customer's asset management, vulnerability management and threat management solutions, providing context and intelligence to customers about which attacks to run and on which assets to run these."

It is this unique approach, suggests Amit, that helps customers to make decisions based on the simulation results, while at the same time, making them cognizant of the tangible risk of vulnerabilities in their infrastructure.

"Being a Threat Exposure Management platform, it means there is a comprehensive inventory of the customers' assets, so – drawing from our vulnerability analysis engine and actionable threat advisories – we are able to understand which version and type of a particular threat you may be impacted by. This context helps us pinpoint the exact attack that must be simulated and in the same environment which has the impacted assets. Decisions derived based on these simulations are undoubtedly more accurate and efficient."

"By providing a unified view of the true risk of all vulnerabilities and helping to fix these, our platform delivers a combination of asset criticality, external threat context, internal compensatory control, and patch intelligence, thereby giving customers a unique view of the

actual threat that a vulnerability presents," concludes Amit.

Dharminder Parmar
Hive Pro
email us here