

Hive Pro Announces Release of Version 3.0.1 of Threat Exposure Management Platform

Introducing Self-Service SaaS for HivePro Uni5 Flagship Product and Enhanced Visualizations for Improved Cybersecurity Insights

MILPITAS, CALIFORNIA, UNITED STATES, July 6, 2023 /EINPresswire.com/ -- [Hive Pro](#), a pioneer in the [Threat Exposure Management](#) market, is thrilled to announce the release of version 3.0.1 of the Hive Pro: Threat Exposure Management Platform. This major update includes several innovative features, including a self-service SaaS for their flagship product HivePro Uni5, enhanced hierarchical views, and improved visualizations, empowering organizations with greater control and insights to combat evolving cyber threats.



Hive Pro Announces Release of Version 3.0.1 of Threat Exposure Management Platform

“

We're excited to launch HivePro Uni5's version 3.0.1. With its self-service SaaS, superior visualization, and upgraded VPT, we're ushering in a new era of cyber resilience and proactive defense.”

Jeelan Poola

The highlight of this release is the introduction of the self-service Software-as-a-Service (SaaS) offering for HivePro Uni5. The HivePro Uni5 SaaS platform provides users with a seamless, quick to deploy and easy to use Security experience. With the self-service SaaS model, organizations can easily access and deploy HivePro Uni5, gaining comprehensive threat exposure management capabilities while enjoying the flexibility and scalability of a cloud-based solution. To accompany this launch, Hive Pro is offering a [30-day free trial](#) of the HivePro Uni5 SaaS platform to allow customers to experience the platform's robust features firsthand.

The new version of Hive Pro's Threat Exposure Management Platform also includes enhanced data visualization and dashboard configurations made to provide users with intuitive and easy-to-read representations of attacks, threat actors, vulnerabilities, and remediation priorities.

Users can now scan for a specific vulnerability in their asset environment, or for a specific asset of concern. Additionally, users can now navigate through hierarchical structures to analyze data from multiple angles, gaining deeper insights into the evolving threat landscape and making informed decisions to mitigate risks. These visual, data-rich representations will enable Security teams to quickly identify critical areas of concern and prioritize their response strategies to cyberthreats effectively.

In addition to the hierarchical views, the updated version introduces new visualizations for improved data interpretation. Users can now explore data based on priority, exploitability, asset category, vulnerability category, and vulnerability or threat actor type. These visualizations empower organizations to identify patterns, uncover hidden relationships, and understand the impact of cyber threats more comprehensively. The new visualizations make it easier to communicate insights and collaborate across security teams, streamlining the decision-making process and driving proactive threat management strategies.

Product enhancements have also been made to the Vulnerability Prioritization and Tracking (VPT) dashboard, enabling users to access actionable and downloadable reports. The VPT dashboard provides organizations with real-time insights into their vulnerability landscape, allowing them to prioritize remediation efforts effectively. With the ability to generate 20+ detailed reports (e.g., unscanned assets; vulnerabilities targeted by threat actors; prioritized vulnerabilities; etc.), users can now dive deeper into vulnerability data, track progress, and present comprehensive findings to stakeholders.

"We are excited to announce the release of version 3.0.1 of our Threat Exposure Management Platform," said Jeelan Poola, CPO of Hive Pro. "With the introduction of the HivePro Uni5 self-service SaaS as well as several product enhancements, organizations will be empowered to gain deeper insights into their cybersecurity posture, make informed decisions, and take proactive measures to protect their valuable assets."

Version 3.0.1 also includes several new integrations, enhanced access controls, and the most recent recorded bugs and required fixes. Hive Pro remains committed to providing cutting-edge cybersecurity solutions to organizations across industries. The release of version 3.0.1 of the Threat Exposure Management Platform represents another significant step forward in delivering innovative features and capabilities to strengthen cybersecurity defenses.

About Hive Pro, Inc.

The Hive Pro Threat Exposure Management (TEM) Platform is a comprehensive, all-in-one platform designed to track threats, streamline vulnerability management, enhance collaboration, and improve security posture. From security assessment workflow orchestration to actionable AI-driven threat prediction and vulnerability remediation, TEM empowers organizations to build their organizational resilience by identifying, prioritizing, and resolving security threats and

vulnerabilities. We automate and orchestrate the security remediation process dynamically and at scale, so you have one less thing to worry about. Experience seamless security improvements with Hive Pro's fully integrated TEM platform.

To learn more, visit www.hivepro.com.

All trademarks contained herein are the property of their respective owners.

Hive Pro Marketing

Hive Pro

marketing@hivepro.com

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/643079182>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.