**Threat Exposure Management (TEM)** is a continuous, risk-based program that aims to **manage your security vulnerabilities and minimize your threat exposure.** For TEM to be effective, it is dependent on several factors: wide asset visibility, actionable fit-for-business intelligence, and cooperative collaboration across all stakeholders. Unfortunately for many organizations, TEM is disrupted by poor threat exposure visibility, fractured cross-functional collaboration, siloed tools and weak vulnerability management.

In the wake of compounding annual cyber attacks, Hive Pro believes that it is integral for all organizations to have an effective TEM program. **TEM is possible for enterprises of all sizes and states of maturity.** At the core of this should be one platform that fosters cooperation and collaboration among all stakeholders to manage their vulnerabilities, reduce their threat exposure, strengthen their security posture and build their organizational resilience. This is why we created the **Hive Pro Threat Exposure Management platform.**

Hive Pro: Threat Exposure Management Platform

ArtemisPro is your security assessment orchestration plane and vulnerability intelligence repository.

HivePro Uni5 is your threat-intelligence enrichment engine from where you prioritize your vulnerabilities, test your security controls, and remediate your risks.
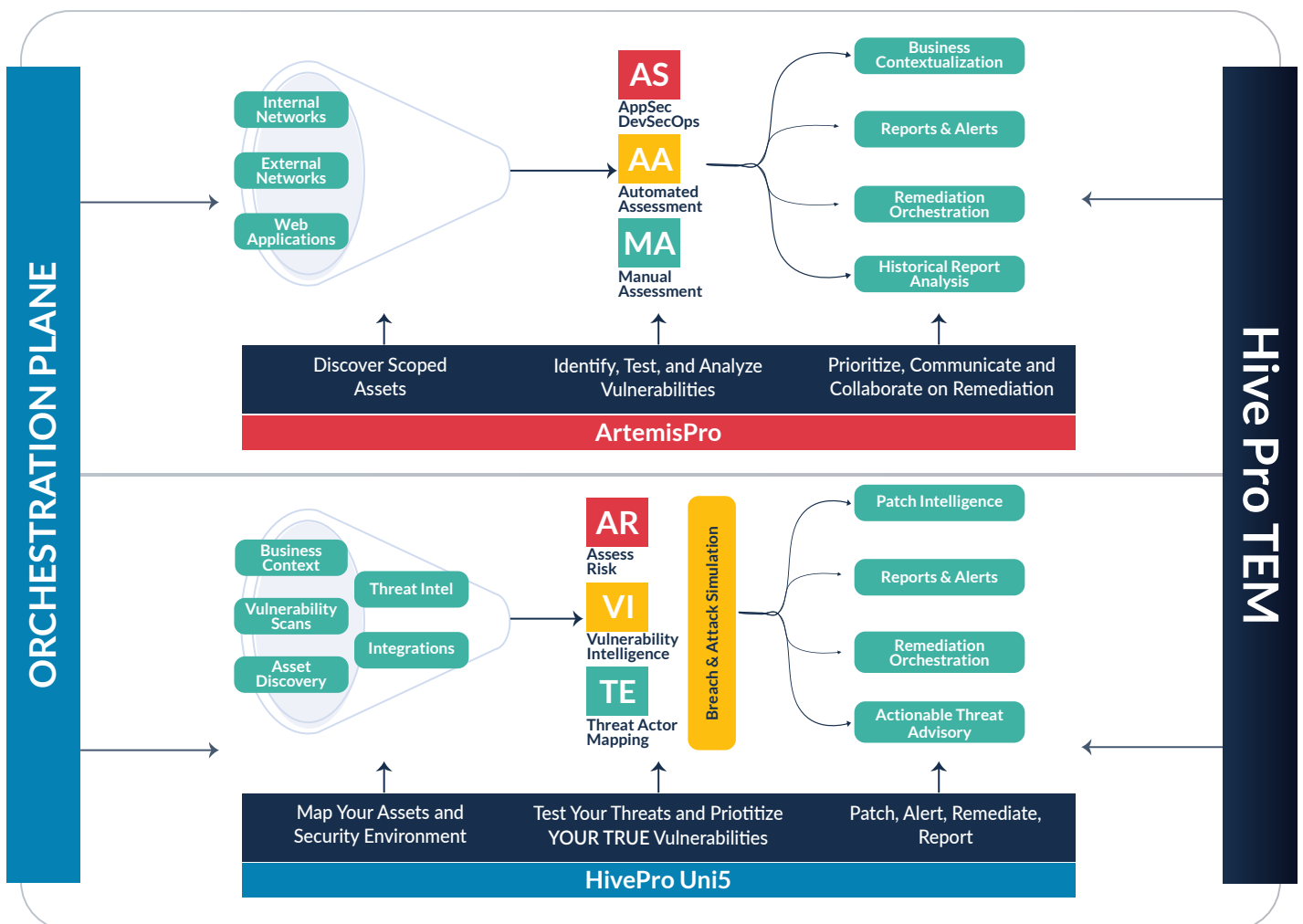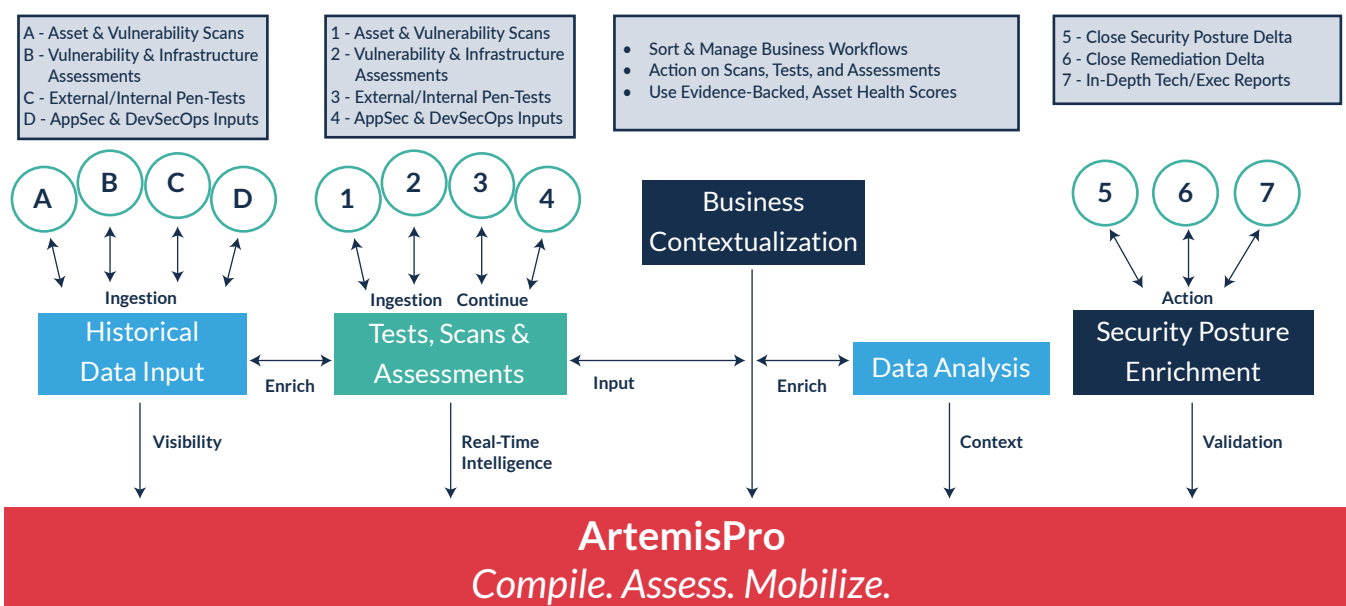
ArtemisPro
Compile. Assess. Mobilize.

ArtemisPro is the workflow orchestration layer of Hive Pro. It is responsible for gathering all vulnerability data from various types of security assessments, workflow orchestration and collaboration over all ongoing and pending security assessments. In Artemis Pro, every scoped, historical and continuous vulnerability scan, assessment, and penetration test data is compiled, assessed and intuitively visualized for all relevant users and stakeholders. For where remediation decisions and exceptions are made, decisions are documented and tracked in ArtemisPro, enabling Security teams to never miss a beat on risk management.

ArtemisPro: TEM Workflow Orchestration

A - Asset & Vulnerability Scans
B - Vulnerability & Infrastructure Assessments
C - External/Internal Pen-Tests
D - AppSec & DevSecOps Inputs

1 - Asset & Vulnerability Scans
2 - Vulnerability & Infrastructure Assessments
3 - External/Internal Pen-Tests
4 - AppSec & DevSecOps Inputs

- Sort & Manage Business Workflows
- Action on Scans, Tests, and Assessments
- Use Evidence-Backed, Asset Health Scores

5 - Close Security Posture Delta
6 - Close Remediation Delta
7 - In-Depth Tech/Exec Reports

(A) (B) (C) (D)   (1) (2) (3) (4)   **Business Contextualization**   (5) (6) (7)

Ingestion   **Ingestion Continue**   **Action**

Historical Data Input —Enrich— **Tests, Scans & Assessments** —Input— —Enrich— **Data Analysis**   **Security Posture Enrichment**

Visibility   **Real-Time Intelligence**   **Context**   **Validation**

ArtemisPro
Compile. Assess. Mobilize.

ArtemisPro solves for fragmented cross-functional team collaboration and the required burden of proof for vulnerability remediation placed on Security Operations by enabling rich data analysis and ongoing workflow management. For all of the intelligence ArtemisPro collects, it shares with HivePro Uni5, wherein remediation priorities are decided, assets are secured, and security controls are optimized.
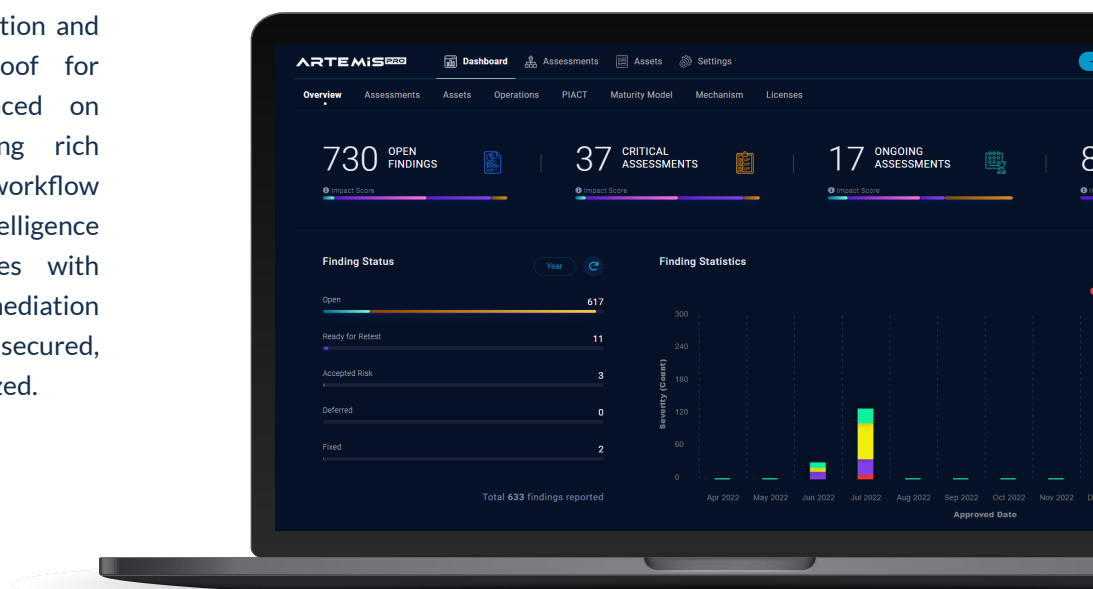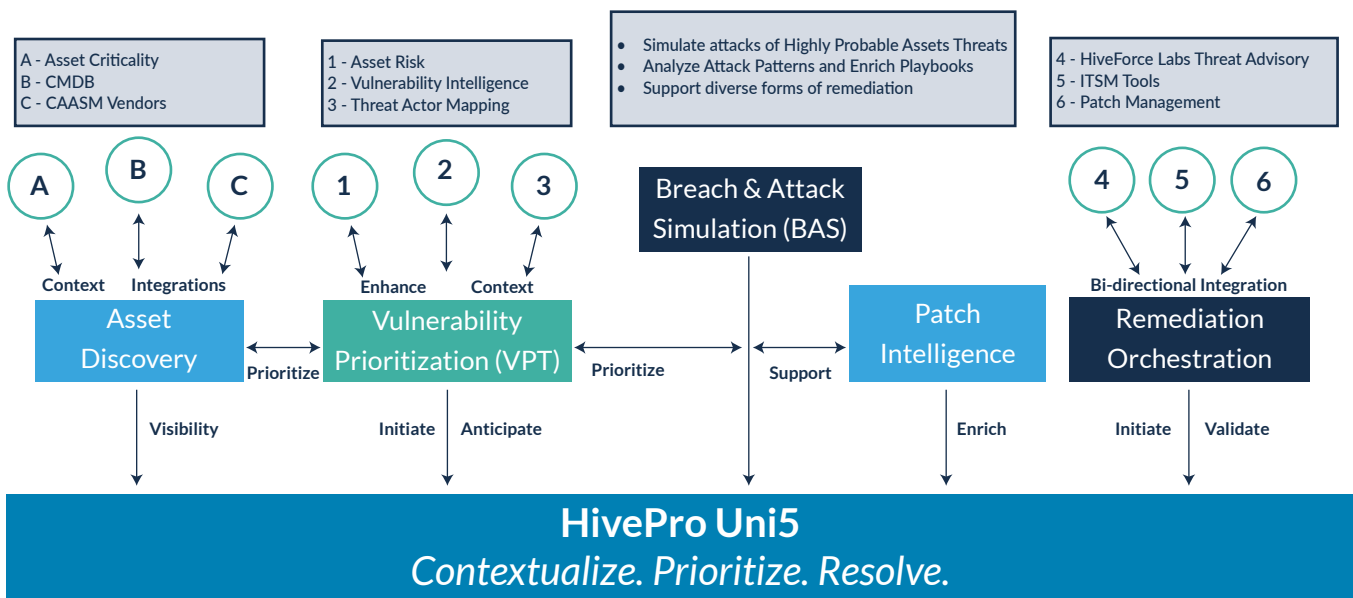
HivePro Uni5
Contextualize. Prioritize. Resolve.

HivePro Uni5 contextualizes business-critical assets against extensive vulnerability and threat intelligence to prioritize your vulnerabilities, manage your threats and deliver actionable courses of remediation. HivePro Uni5's Breach & Attack Simulation module conducts simulated, real-world attacks against scoped parts of an organization's security infrastructure to test security control efficacy and to yield diverse remediation options. Among your remediation options are security tool configurations, patch intelligence, code revisions and suggested compensatory controls. HivePro Uni5 enables remediation orchestration through immediate patch intelligence and rich bi-directional integrations with Asset Management and ITSM platforms. The HivePro Uni5 platform keeps track of all workflows, actioned remediations, and the status of your security posture.

HivePro Uni5: Vulnerability & Threat Exposure Remediation

A - Asset Criticality
B - CMDB
C - CAASM Vendors

1 - Asset Risk
2 - Vulnerability Intelligence
3 - Threat Actor Mapping

- Simulate attacks of Highly Probable Assets Threats
- Analyze Attack Patterns and Enrich Playbooks
- Support diverse forms of remediation

4 - HiveForce Labs Threat Advisory
5 - ITSM Tools
6 - Patch Management

A   **B**   **C**   **1**   **2**   **3**

Context   **Integrations**

Enhance   **Context**

Breach & Attack Simulation (BAS)

4   **5**   **6**

Bi-directional Integration

Asset Discovery

Vulnerability Prioritization (VPT)

Prioritize

Patch Intelligence

Remediation Orchestration

Prioritize   **Support**

Visibility   **Initiate**   **Anticipate**   **Enrich**   **Initiate**   **Validate**

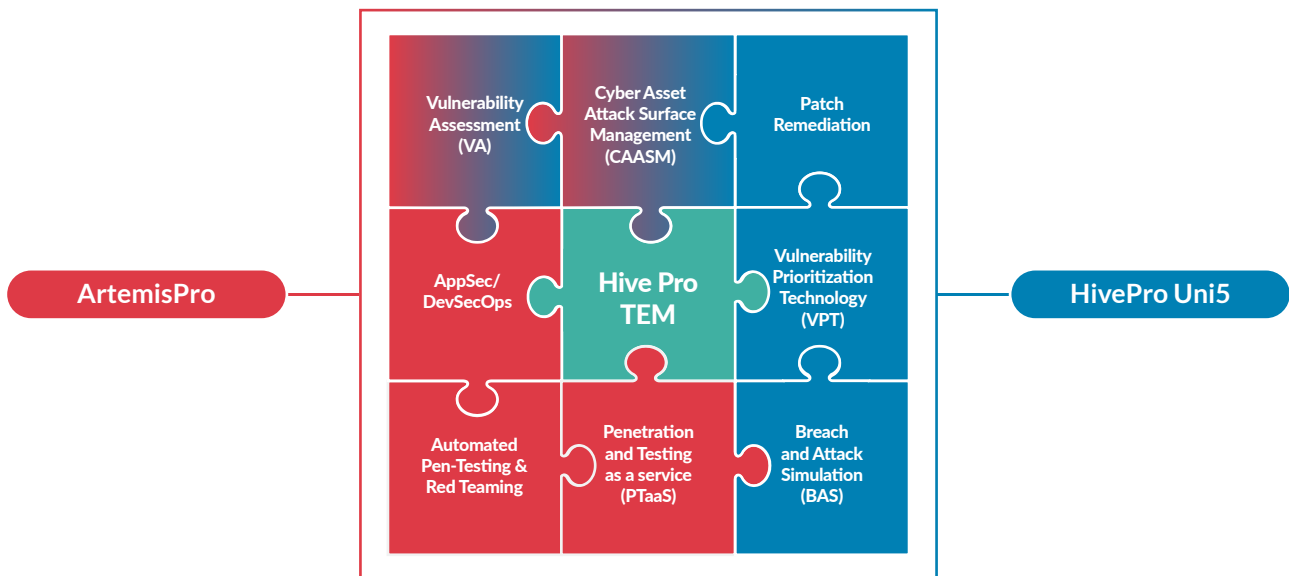### HivePro Uni5
Contextualize. Prioritize. Resolve.

Our goal is to communicate a consistent, actionable and understandable security posture and remediation improvement plan(s) to you and all of our users. **HivePro Uni5** enables you to effortlessly share your security story with relevant stakeholders. With just a click of a button, you can generate actionable strategic, tactical, and operational reports for cross-functional teams.
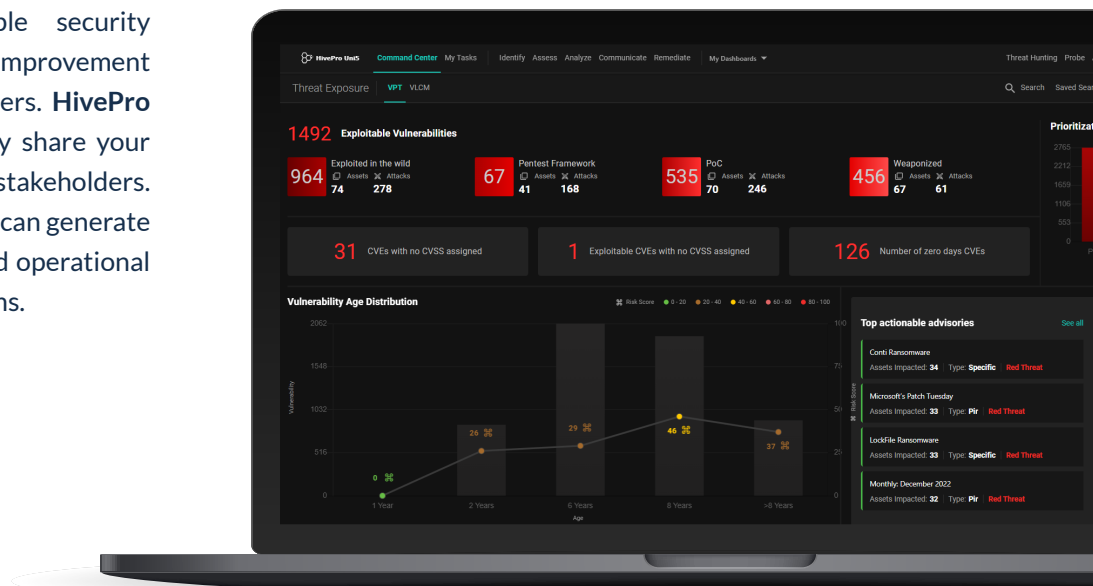
Working Together

The cybersecurity market is rife with point-solutions that solve for single or disparate parts of the vulnerability and threat exposure management story. At Hive Pro, we speak to Security teams with 10+ tools and several consoles, and they have all espoused the need to collapse the most necessary functions for vulnerability and threat exposure management into one platform. We also speak to Security teams who have just started their SOC journey, and they want the most fundamental thing: insight that matters. Hive Pro strives to meet Security Teams' needs, no matter their maturity with Hive Pro: Threat Exposure Management, an all-in-one fully-integrated platform.

Hive Pro TEM: All-In-One Platform

ArtemisPro

Vulnerability Assessment (VA)	Cyber Asset Attack Surface Management (CAASM)	Patch Remediation
AppSec/ DevSecOps	Hive Pro TEM	Vulnerability Prioritization Technology (VPT)
Automated Pen-Testing & Red Teaming	Penetration and Testing as a service (PTaaS)	Breach and Attack Simulation (BAS)

HivePro Uni5

Key Benefits

Tailor-Made For All Organizations

Hive Pro TEM tailors thousands of threat and vulnerability intelligence resources to your business-critical assets, filters through the noise and prioritizes the vulnerabilities that matter the most. Our all-in-one platform tracks your security assessment history, orchestrates workflows to assessment completion, and aligns all risk decisions to the proper business-unit and owners so you can collaborate and reach resolution faster.

Security Optimization

ArtemisPro is the ultimate security assessment workflow orchestration plane and vulnerability intelligence data hub. HivePro Uni5 is your threat-enriched, and risk-based vulnerability prioritization, security control testing, and risk remediation tool. Together, from the Hive Pro Threat Exposure Management platform an all-in-one, intuitive platform that filters through the noise to find and resolve the threats and vulnerabilities that matter to your business.

Rational, Timely, In Sync Workflows

Security Operations teams can track workflows to remedy gaps in out-of-sync periods, and ensure that newly initiated workflows are occurring at optimal frequencies, in line with several factors: remediation cycles, organizational risk tolerance, audit and compliance mandates, and other business-critical events.

Fully Customizable Dashboard

In one easy-to-read interface, Hive Pro TEM maps all of your critical assets, associated vulnerabilities, and the threats most likely to exploit them. Every in-platform user can customize HivePro Uni5 and ArtemisPro's rich intelligence dashboards to their needs.

Strong Cross-Function Collaboration

Hive Pro TEM provides transparent information into your IT exposure, vulnerabilities, threats and enables collaboration in-console through integrated workflows, processes, and decisions.

Build your Cyber Resilience with Hive Pro Threat Exposure Management

Unify your threat exposure management with Hive Pro's all-in-one platform. Gain comprehensive asset visibility, actionable intelligence, and seamless team collaboration. Optimize your risk management decisions and fortify your organization's security posture.

Request a demo today!
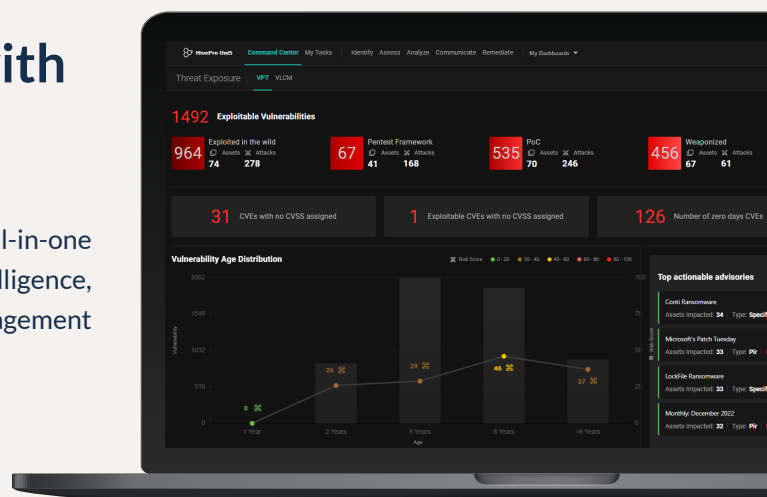
Hive Pro

Contact Us   Schedule a Demo   Read Our Blog