Hive Pro

WHITE PAPER

The ‘Exposure Management’ Dictionary

Introduction

In cybersecurity, new concepts, techniques, and technologies are constantly evolving and emerging due to the rapidly changing threat landscape, advancements in technology, and ongoing research and development efforts. 'Exposure Management' is one of the most recent concepts released by Gartner, Inc. and carries with it an overwhelming burden of learning new acronyms and words.

Even though it may seem impossible to keep up, it's necessary to help you communicate with teammates, clients, and/or customers. To enhance your cybersecurity expertise, we've curated a list of essential terms, acronyms, their meanings, and relevance to the emerging 'Exposure Management' technology market.

Asset:

Any valuable resource, component, or entity within an organization's IT infrastructure that needs to be protected from potential threats and vulnerabilities. Assets can take various forms like data, hardware, software, networks, infrastructure, IP, user accounts, and third-party services.

Attack Path:

The series of steps or vulnerabilities that an attacker can exploit to gain unauthorized access to a computer system, network, or specific asset. Understanding attack paths is crucial for cybersecurity professionals as it allows them to identify vulnerabilities, model threats, reduce their cyber risks, plan defenses, respond to incidents, and protect their digital assets.

Attack Path Mapping:

A methodology that involves identifying, visualizing, and documenting the various steps, vulnerabilities, and tactics that an attacker might use to compromise a target system, network, or organization. It provides a clear, graphical representation of how an attacker could progress through a series of vulnerabilities and access points to achieve their malicious objectives.

Attack Surface:

Refers to the sum of all the points or entry points through which an attacker could potentially gain unauthorized access to a system or application. It represents the external and internal interfaces, services, and components that are exposed to potential threats, including but not limited to open ports, network services, APIs, user interfaces, hardware interfaces, and more.

Attack Surface Management (ASM):

A proactive cybersecurity practice and a set of strategies and tools aimed at identifying, monitoring, and managing the attack surface of an organization. It involves assessing and reducing the exposure of potential vulnerabilities and entry points that could be exploited by cyber threats.

Blue Team:

Blue Teams are cybersecurity professionals in an organization who defend against cyber threats. They collaborate with Red Teams (offensive) or Purple Teams (both) to enhance security. Blue Teams safeguard information systems, networks, data, and assets by managing vulnerabilities, monitoring security, and responding to incidents.

Breach & Attack Simulation (BAS):

A technology that involves simulating various real-world cyberattacks and security breaches to assess an organization's security posture, identify vulnerabilities, improve security controls and evaluate its ability to detect and respond to threats effectively. It provides a controlled and safe environment for an organization to test their defenses and incident response capabilities for better preparation against evolving cyber threats.

Business Context:

The understanding and consideration of an organization's specific business goals, operations, processes, and objectives when making security-related decisions and implementing security measures. Business context helps organizations assess and prioritize cybersecurity risks based on their potential impact on critical business functions. It enables decision-makers to allocate resources effectively to mitigate the most significant risks.

Cloud Security Posture Management (CSPM):

A cybersecurity practice and toolset that assesses, monitors, and enhances the security of an organization's cloud infrastructure. It identifies and addresses misconfigurations, vulnerabilities, and compliance issues, ensuring secure and compliant cloud environments while supporting multi-cloud setups and real-time monitoring.

Common Vulnerability Scoring System (CVSS):

A standardized framework for rating the severity of software vulnerabilities. CVSS assigns a numerical score typically ranging from 0.0 (no impact) to 10.0 (maximum impact), with higher scores indicating more severe vulnerabilities based on factors like exploitability and impact to help organizations prioritize and address security issues effectively. VSS provides a common language and methodology for organizations to communicate and make informed decisions about addressing security vulnerabilities.

Configuration Management Database (CMDB):

A central database that stores and manages detailed information about an organization's IT assets, configurations, and their relationships. It is a crucial tool in cybersecurity, providing a comprehensive inventory of digital assets and their security attributes. CMDBs serve as a foundation for asset management, configuration control, and security governance, aiding cybersecurity teams in assessing risks, responding to incidents, and ensuring compliance.

Continuous Controls Monitoring (CCM):

Continuous Controls Monitoring (CCM) is a cybersecurity practice that continuously assesses and monitors an organization's internal controls, security policies, and compliance measures in real-time. It relies on automated tools to collect and analyze data from various sources, providing operational insights into the effectiveness of security controls and ensuring compliance with industry regulations and standards.

Continuous Integration & Continuous Delivery/ Continuous Deployment (CI/CD):

A set of practices and automation processes aimed at improving the security of software and systems throughout their development, testing, and deployment lifecycle. CI/CD practices integrate security into every phase of the software development and deployment pipeline, ensuring that security is not an afterthought but an integral part of the development process.

Continuous Threat Exposure Management (CTEM):

A proactive approach to cybersecurity that involves continuously monitoring, assessing, and managing an organization's exposure to various threats, vulnerabilities, and risks. This practice focuses on real-time and ongoing threat visibility, risk assessment, and mitigation efforts, enabling organizations to adapt quickly to changing cyber threats and protect their digital assets effectively.

Common Vulnerabilities and Exposures (CVE):

A system for uniquely identifying and naming known software vulnerabilities and security weaknesses. Each CVE entry comes with a standardized identifier (e.g., CVE-YYYY-NNNN) and contains detailed information about the vulnerability, including its description, affected software or systems, and references to relevant security advisories or patches. CVE provides a consistent way to catalog vulnerabilities, making it easier for organizations and security professionals to track and share information about security issues.

Cyber Asset Attack Surface Management (CAASM):

A cybersecurity practice and set of strategies aimed at identifying, analyzing, and managing the attack surface of an organization's digital assets. It relies on comprehensive asset identification to measure and reduce the exposure of potential vulnerabilities and entry points that could be exploited by cyber threats with a specific focus on the organization's assets.

Cybersecurity Mesh Architecture (CSMA):

An emerging cybersecurity concept and strategy that focuses on flexible and decentralized security. Instead of relying solely on a central defense, it spreads security measures across an organization's digital assets, devices, and services. This approach prioritizes user identity, adapts access controls based on context, and continuously monitors for threats. It's like a web of interconnected security, offering better protection for today's complex IT environments, including remote work and cloud services, while putting the user at the center of security efforts.

Cyber Threat Intelligence (CTI):

Information and insights collected, analyzed, and disseminated regarding potential and current cyber threats to help organizations understand the tactics, techniques, procedures, motivations, and infrastructure employed by cyber threat actors. CTI assists with identifying and mitigating cybersecurity risks by providing actionable intelligence that enables proactive threat detection, incident response, and the development of effective security strategies.

Cyber Validation (CyVal):

A cybersecurity practice that focuses on evaluating and validating an organization's cybersecurity capabilities, controls, and strategies through various assessments and testing methodologies like breach and attack stimulation and penetration tests. CyVal aims to identify vulnerabilities, measure resilience, and enhance overall cybersecurity posture and preparedness against cyber threats.

Dynamic Application Security Testing (DAST):

A cybersecurity testing method that assesses the security of web applications and APIs by actively examining them during runtime. It simulates real-world attack scenarios to identify vulnerabilities and weaknesses that may be exploited by malicious actors. DAST is valuable for identifying vulnerabilities in live applications, helping organizations detect and remediate security flaws to protect their web-based assets.

Development-Security-Operations (DevSecOps):

An integrated approach to software development that places a strong emphasis on security. It involves seamlessly integrating security practices and tools into the development pipeline, allowing for early detection and mitigation of security issues. DevSecOps emphasizes automation, continuous monitoring, and shared responsibility among development, security, and operations teams to deliver secure software efficiently while fostering a security-conscious culture.

Exposure Assessment (EA):

The process of systematically evaluating and quantifying an organization's potential security risks and vulnerabilities, both internal and external. This assessment considers various factors, including vulnerabilities in systems and applications, misconfigurations, data exposures, and other potential threats that could impact an organization's security posture. Exposure assessments aim to provide organizations with a comprehensive understanding of their risk landscape, enabling informed decisions regarding risk mitigation, resource allocation, and security strategy development.

External Attack Surface Management (EASM):

A cybersecurity practice and set of strategies aimed at identifying, monitoring, and managing an organization's digital assets and vulnerabilities that are exposed and accessible from external sources, such as the internet. EASM focuses on assessing and reducing the attack surface that cyber threat actors could potentially exploit. It involves continuous monitoring, vulnerability scanning, threat intelligence analysis, and risk assessment to enhance an organization's overall security posture and protect against external threats and attacks.

Exploit Prediction Scoring System (EPSS):

A cybersecurity framework and methodology designed to predict the likelihood and impact of potential cyber exploits on an organization's digital assets and vulnerabilities. EPSS assesses the risk posed by specific vulnerabilities by considering factors such as their severity, exploitability, and the presence of known threats targeting them. By quantifying the risk associated with vulnerabilities, EPSS helps organizations prioritize and allocate resources for vulnerability remediation and security efforts, allowing them to focus on addressing the most critical and likely-to-be-exploited security weaknesses to proactively enhance their cybersecurity defenses.

Exploit:

A piece of software, code, or technique that takes advantage of a vulnerability or weakness in a computer system, software application, or network to gain unauthorized access, perform malicious actions, or compromise the security of the targeted system.

Exposure Management (EM):

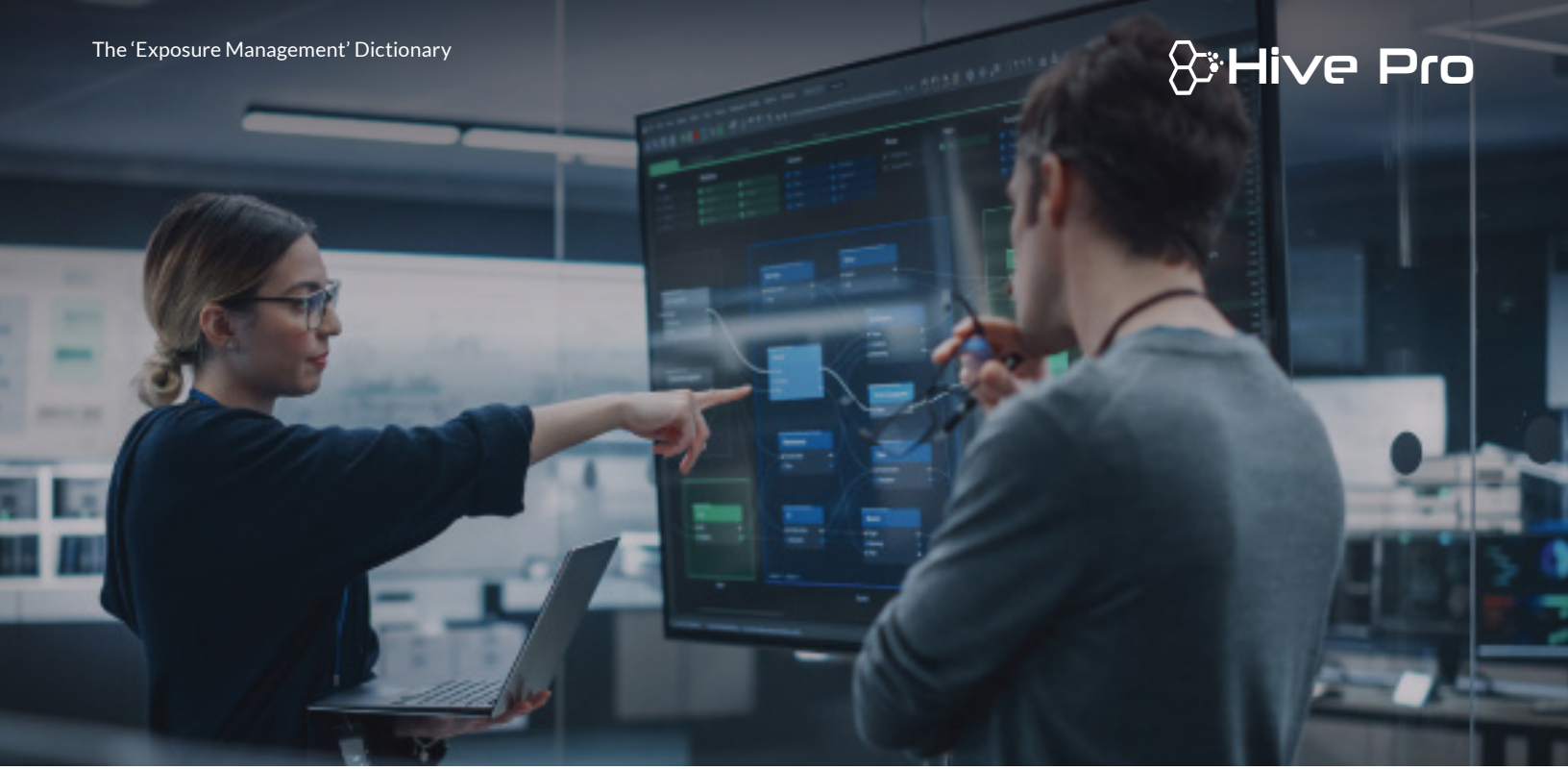
The ongoing process of identifying, evaluating, and proactively addressing an organization's exposure to various cybersecurity threats and vulnerabilities. It encompasses activities such as vulnerability assessments, risk evaluations, and threat monitoring to gain a comprehensive view of an organization's threat landscape and the potential impact of security vulnerabilities. Exposure Management focuses on reducing an organization's attack surface and minimizing its susceptibility to cyber threats by implementing mitigation strategies, security controls, and remediation measures. This continuous and proactive approach helps organizations enhance their cybersecurity resilience and reduce the potential impact of security incidents.

Governance, Risk Management and Compliance (GRC):

A comprehensive framework that ensures an organization's cybersecurity aligns with business objectives, effectively manages risks, and complies with regulations. GRC encompasses policies, risk assessments, and adherence to legal requirements to protect digital assets and maintain a secure and compliant cybersecurity posture.

Infrastructure & Operations (I&O):

Refers to the collective management and maintenance of an organization's IT infrastructure, including hardware, software, networks, and associated processes as owned by the IT team. It involves the design, deployment, and ongoing operation of the technology stack that supports an organization's digital operations.



IT Service Management (ITSM):

A set of practices and processes backed by technology focused on efficiently and securely delivering and managing IT services within an organization. ITSM encompasses strategies for incident management, problem resolution, change management, and service request fulfillment while also integrating cybersecurity considerations.

Mean Time to Detect (MTTD):

A key metric in cybersecurity that represents the average amount of time it takes for an organization to identify and recognize a security incident or anomaly after it has occurred. A shorter MTTD indicates a more efficient detection process, enabling faster response to threats and reducing potential damage. MTTD is critical for effective cybersecurity as it directly influences an organization's ability to mitigate and contain security breaches, minimize the impact of incidents, and safeguard its digital assets and data from unauthorized access or compromise.

MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE® ATT&CK):

A comprehensive knowledge framework and resource in cybersecurity that provides a structured and detailed view of the tactics, techniques, and procedures (TTPs) used by cyber threat actors during various stages of an attack. ATT&CK helps organizations understand and counteract cyber threats by categorizing and describing real-world attack patterns and methods. It serves as a valuable reference for threat detection, threat hunting, and security assessments, allowing organizations to align their defenses, monitor for specific attack indicators, and improve their cybersecurity posture based on a deep understanding of adversary behavior and tactics.

Patch:

Refers to a software update or fix that is specifically designed to address security vulnerabilities, weaknesses, or flaws in a software application, operating system, or system component.

Patch Management:

The process of planning, implementing, and maintaining updates and patches for software, operating systems, and applications within an organization's IT environment. It involves identifying and prioritizing software vulnerabilities, acquiring and testing patches or updates, and then deploying them to address these vulnerabilities efficiently and securely.

Penetration Testing (Pen Test):

A controlled and systematic process of evaluating the security of computer systems, networks, applications, or environments by simulating real-world attacks. During a penetration test, skilled professionals, known as ethical hackers or penetration testers, attempt to identify and exploit vulnerabilities, weaknesses, or misconfigurations in the target system's defenses. The primary goal of a penetration test is to uncover security issues before malicious hackers can exploit them, allowing organizations to proactively strengthen their cybersecurity posture, remediate vulnerabilities, and enhance their overall security defenses.

PTaaS – Pentest As A Service:

A cloud-based or managed penetration testing service that organizations can subscribe to for conducting regular and comprehensive security assessments of their systems, networks, and applications. PTaaS providers offer skilled penetration testers who simulate real-world cyberattacks to identify vulnerabilities and weaknesses within an organization's digital infrastructure. These services often follow established methodologies and provide detailed reports outlining the findings, potential risks, and recommended remediation measures.

Purple Team:

A collaborative approach that combines elements of both Red Team and Blue Team activities to improve an organization's overall security posture. The Purple Team operates by fostering communication and cooperation between offensive security (Red Team) and defensive security (Blue Team) personnel. While Red Teams simulate cyberattacks and attempt to breach the organization's defenses, the Blue Team actively defends against these simulated attacks. The Purple Team facilitates knowledge sharing and feedback, allowing the Blue Team to learn from the tactics and techniques used by the Red Team and adjust their security measures accordingly.

Risk-Based Vulnerability Management (RBVM):

A strategic approach to identifying, prioritizing, and addressing vulnerabilities in an organization's IT environment based on their potential impact and the associated risks. Instead of treating all vulnerabilities equally, RBVM assesses them in the context of the organization's specific risk tolerance, business objectives, and threat landscape. It involves evaluating vulnerabilities not only by their technical severity but also by considering factors such as their exploitability, the value of the affected assets, and the potential impact on business operations.

Red Team:

A group of skilled professionals or ethical hackers who simulate malicious cyberattacks and offensive operations against an organization's systems, networks, applications, and defenses. The primary goal of a Red Team is to identify vulnerabilities, weaknesses, and potential security risks within an organization's digital infrastructure by using tactics, techniques, and procedures (TTPs) similar to those employed by real cyber adversaries. Red Teams conduct comprehensive security assessments, including penetration testing, vulnerability assessments, and social engineering attacks, to help organizations understand their security weaknesses, improve their incident response capabilities, and enhance their overall cybersecurity defenses.

Secure Operations Center (SOC):

A centralized facility or team responsible for monitoring, detecting, analyzing, and responding to security incidents and threats within an organization's IT infrastructure. A SOC operates 24/7 and is staffed with security analysts and experts who use specialized tools and technologies to actively monitor network traffic, log data, and security alerts in real-time. The primary goal of a SOC is to proactively identify and mitigate security breaches, anomalies, and vulnerabilities, ensuring the confidentiality, integrity, and availability of an organization's data and systems.

Static Application Security Testing (SAST):

A cybersecurity testing method that focuses on identifying security vulnerabilities and weaknesses in software applications during the development or source code review phase. SAST tools analyze the application's source code, bytecode, or binary code without executing it, searching for coding practices, design flaws, or vulnerabilities that could be exploited by attackers. Common security issues detected by SAST tools include code injection, authentication and authorization flaws, input validation errors, and other vulnerabilities that may lead to security breaches.

Security Operations (SecOps):

A collaborative approach that merges security and IT operations to manage and respond to security threats effectively. It closes the gap between security and operational teams by emphasizing real-time monitoring, incident response, threat intelligence integration, and automation, seamlessly integrating security into daily operations. This alignment improves threat detection, investigation, and mitigation, ultimately strengthening cybersecurity and minimizing the impact of security incidents.

[Security] Service Level Agreement (SLA):

A formal and contractual commitment between a security service provider and its client or organization. The SLA outlines specific terms, expectations, and guarantees regarding the security services being provided. These services may include threat detection and response, incident management, vulnerability assessments, and other cybersecurity-related functions. The SLA typically defines key performance indicators (KPIs), response times, incident severity levels, and reporting requirements to ensure that the security service provider delivers the agreed-upon level of protection and meets the organization's security needs.

Security Posture Management (SPM):

A comprehensive approach and set of practices that focus on assessing, monitoring, and enhancing an organization's overall security posture. SPM involves continuous evaluation of security controls, configurations, and vulnerabilities across an organization's IT infrastructure, including networks, systems, cloud environments, and applications. This practice aims to identify and address security gaps, misconfigurations, and potential risks by providing real-time insights into the security status of digital assets.

Threat:

Any potential danger, risk, or circumstance that has the capability to exploit vulnerabilities in computer systems, networks, applications, or data, potentially causing harm or damage. Threats can take various forms, including cyberattacks, malware infections, unauthorized access attempts, data breaches, and other malicious activities that aim to compromise the confidentiality, integrity, or availability of digital assets.

Threat Actor:

An individual, group, organization, or entity that carries out deliberate actions to compromise the security of computer systems, networks, applications, or data. Threat actors can have various motivations, including financial gain, political objectives, espionage, hacktivism, or personal reasons. These actors employ a range of tactics, techniques, and procedures (TTPs) to achieve their goals, which may include cyberattacks, malware distribution, social engineering, and exploiting vulnerabilities.

Threat Assessment (TA):

A systematic evaluation that identifies, analyzes, and prioritizes potential threats and vulnerabilities facing an organization's digital assets and operations. It involves considering factors like known vulnerabilities, emerging threats, threat actors, and attack vectors. The primary goals include identifying and cataloging risks, evaluating their likelihood and potential impact, prioritizing them based on risk tolerance, and developing mitigation strategies. Threat assessments play a crucial role in helping organizations make informed decisions about cybersecurity investments, resource allocation, and risk management to protect against cyber threats and maintain a strong security posture.

Tactics, Techniques and Procedures (TTP):

The strategies, methods, and specific steps that threat actors or cyber adversaries employ to carry out cyberattacks and achieve their malicious objectives. TTPs encompass a wide range of activities, including attack vectors, exploitation techniques, evasion methods, and post-compromise actions. Understanding TTPs helps organizations recognize and respond to cyber threats effectively by identifying the behaviors and patterns associated with different types of attacks.to help detect, prevent, and mitigate cyber threats and enhance overall cybersecurity resilience.

Vulnerability:

A weakness, flaw, or gap in a computer system, network, application, or device that can potentially be exploited by malicious actors or cyber threats. Vulnerabilities can exist in software code, configurations, design, or even human behavior, making systems susceptible to security breaches or unauthorized access. Cybersecurity professionals often assess and identify vulnerabilities to mitigate or remediate them before they can be exploited. Common examples of vulnerabilities include software bugs, misconfigurations, outdated software, and unpatched systems.

Vulnerability Assessment (VA):

A systematic process of identifying, evaluating, and prioritizing security vulnerabilities within an organization's IT infrastructure, including systems, networks, applications, and devices. The primary goal of a Vulnerability Assessment is to proactively discover weaknesses that could be exploited by cyberthreats or malicious actors. This assessment involves using automated tools and manual techniques to scan, analyze, and categorize vulnerabilities, assigning severity levels based on their potential impact. The results help organizations prioritize and address vulnerabilities by applying patches, implementing security controls, and taking remedial actions to strengthen their cybersecurity defenses and reduce the risk of security breaches.

Zoom Vulnerability Impact Scoring System (VISS):

A cybersecurity tool that prioritizes vulnerabilities based on their real-world impact, shifting the focus away from theoretical worst-case scenarios. VISS employs a web-based interface to calculate scores, taking into account parameters related to platform, infrastructure, and data impact. This scoring system also allows for score adjustments using the Compensating Controls metric, catering to an organization's individual risk tolerance. VISS enhances vulnerability assessment, helping organizations concentrate on high-impact issues and allocate resources more effectively for comprehensive protection.

Vulnerability Management (VM):

A structured and ongoing process that involves identifying, assessing, prioritizing, mitigating, and monitoring security vulnerabilities within an organization's IT infrastructure, including systems, networks, applications, and devices. The primary objective of Vulnerability Management is to proactively address weaknesses that could be exploited by cyberthreats or malicious actors to compromise the confidentiality, integrity, or availability of digital assets and data. The key stages of VM include vulnerability scanning, vulnerability assessment, remediation planning, and continuous monitoring.

Vulnerability Prioritization Technology (VPT):

Advanced tools and methodologies used to evaluate and rank security vulnerabilities based on their potential impact and the associated risks. To be trustworthy and successful, VPT relies on several key inputs, including real-time threat intelligence, asset inventory data, contextual information about the organization's environment, historical data on past vulnerabilities and their exploitation, and industry-specific insights. By leveraging these inputs, VPT can provide organizations with a prioritized list of vulnerabilities that need immediate attention, allowing them to allocate resources effectively and address the most critical security issues first. This approach helps organizations strengthen their cybersecurity defenses, reduce exposure to cyber threats, and optimize their vulnerability management efforts.

Vulnerability Scanning (VS):

The practice of using automated tools and software to systematically identify and assess security vulnerabilities within an organization's IT infrastructure, including systems, networks, applications, and devices. Vulnerability scanning tools actively search for known weaknesses, misconfigurations, and potential threats, typically by comparing the scanned assets to a database of known vulnerabilities. The results of these scans are then used to create a list of identified vulnerabilities, often ranked by severity, which can guide organizations in prioritizing and addressing security issues.

About Hive Pro

Hive Pro is a recognized and trusted vendor in Threat Exposure Management, delivering a purpose-built platform to identify, manage, and resolve vulnerabilities and threats across your entire digital landscape. Only Hive Pro can give Security, IT, Business and DevOps teams the full spectrum of their cyber threat exposure and the means to actionably reduce it from one platform and one interface.

Hive Pro’s corporate headquarters are located in Herndon, Virginia, with presence across the US, EMEA, and APAC.

To learn more about Hive Pro, visit www.hivepro.com.

About Uni5 Xposure

Uni5 Xposure delivers a unified view of your cyber risks and all actionable pathways to resolve vulnerabilities and neutralize threats. By combining the power of infrastructure scanners, vulnerability assessment, risk prioritization, security control validation and remediation, Uni5 Xposure fortifies your cyber resiliency and preparedness.

Read more about Uni5 Xposure here .

Get in Touch

Hive Pro Inc. | info@hivepro.com | www.hivepro.com

Book a Demo

Read our Blog