CORE SECURITY

Core Vulnerability Insight

Consolidate and Prioritize Vulnerabilities

Product Overview

By consolidating and prioritizing vulnerability scan data, matching known exploits, and simulating real-world cyber-attacks, Core Vulnerability Insight® enables you to focus on the most vulnerable points of your IT infrastructure to keep critical business assets secure.

Advanced Attack Strategy

Core Vulnerability Insight gives you greater scalability and advanced attack path analytics helping you to accurately identify the vulnerabilities that pose the greatest threat to critical business assets, regardless of the size and complexity of your IT landscape. Once critical vulnerabilities are prioritized, you can get to work on fixing what needs to be fixed first.

Interactive Attack Path Mapping

Through attack path mapping, Core Vulnerability Insight reveals how adversaries can traverse multiple vulnerabilities across layers of infrastructure to reach and expose your most valuable business assets.

Tailored for complex environments, Core Vulnerability Insight provides you with a holistic view of your organization's threat risk. You can quickly model potential threat scenarios according to risk criteria most relevant to your business, such as network connectivity, location, vulnerability type, or potential business impact. You can adjust which exploits and resulting attack paths are displayed based on the risk they pose to your organization.

This display highlights the most urgent attack paths, and de-emphasizes lower priority paths, allowing you to quickly modify attack path characteristics to see exactly how an attack could propagate across your network. After high-risk attack paths have been identified, ranked, and eliminated you can immediately visualize and report your improved risk state.

Consolidate and prioritize vulnerabilities

- Single instance asset store for fast data import, analytics, and queries
- Pre-defined connectors to popular vulnerability assessment solutions

Model threat scenarios using configurable risk criteria

- Demonstrate how attackers can chain vulnerabilities across vectors to move through your environment
- Consider all possible exploits, including "in-the-wild," private, theoretical, wormified, virus and malware

(In addition to Core Security and metasploit exploits)

Identify and eliminate attack paths to critical assets

- Reveal specific assets and exposed resources
- Validate systems and devices that may lead to critical business assets

Leverage flexible reporting

- Granular filtering, grouping, and configuration of large amounts of data
- Customize with templates and share

Adjust, prioritize, and validate remediation efforts

- Measure the effectiveness of remediation efforts
- Compare and track results over time

Centralized Asset Repository

Core Vulnerability Insight leverages a centralized single-instance asset store for simpler data import, faster analytics, and flexible queries. You can sort and filter results by vector type, IP, CVE, server type and other criteria. This customization enables you to consolidate and normalize data in one location, facilitating powerful analytics and reporting.

Core Vulnerability Insight categorizes assets and identifies their value through direct integration with common asset management, network configuration and vulnerability management tools. This automated classification, along with the ability to perform custom labeling during the implementation process, allows you to grade assets based on data sensitivity, location, user, and other important operational characteristics.

Network Scanning

Delivering unrivaled scalability and performance, Core Vulnerability Insight actively (or passively) canvasses all things on your network. You can uncover hidden devices like smartphones, tablets, and laptops that "come-and-go" between scheduled scans.

In addition to Core Vulnerability Insight's embedded scanning capabilities, many third-party network vulnerability scanners are supported out of the box.

*Network Vulnerability Scanners**

- McAfee® Vulnerability Manager
- Qualys® Vulnerability Management
- Tenable SecurityCenter™
- Tenable Nessus®
- Tripwire IP360™
- Rapid7 Nexpose
- GFI Languard

*Additional scanners can be added through service engagements

Web Application Scanning

Core Vulnerability Insight can identify and assess risk at all stages of the software development life cycle, and most importantly in production, so your applications are protected against new threats even after being deployed. This applies to web applications residing on premise or in the cloud.

Web Application Vulnerability Scanners

- Trustwave® App Scanner
- HP WebInspect®
- Qualys Web Application Scanning
- IBM AppScan®
- Rapid7 AppSpider

Distributed Penetration Testing

You can execute penetration tests from a remote location—no matter where the target system resides—avoiding additional resources and costs.

Flexible and Configurable Reporting

Core Vulnerability Insight features a flexible reporting engine that facilitates granular filtering, grouping, and extensive configuration of amounts of data. This engine allows you to choose out- of-the-box reports or to create your own reports. Reports are easily customized (branding, pivot tables, visual charts, etc.) with templates. With Core Vulnerability Insight, you can quickly distribute important risk assessments to your stakeholders.

Smart Card Authentication

Core Vulnerability Insight supports digital certificate authentication through web browsers and smart cards. Smart cards (known as Common Access Cards in the public sector) are used on a daily basis by private organizations and federal agencies. When accessing sensitive data, they provide an additional layer of security with embedded certificates.

ABOUT CORE SECURITY

Courion has rebranded the company, changing its name to Core Security, to reflect the company's strong commitment to providing enterprises with market-leading, threat-aware, identity, access and vulnerability management solutions that enable actionable intelligence and context needed to manage security risks across the enterprise. Core Security's analytics-driven approach to security enables customers to manage access and identify vulnerabilities, in order to minimize risks and maintain continuous compliance. Solutions include Multi-Factor Authentication, Provisioning, Identity Governance and Administration (IGA), Identity and Access Intelligence (IAI), and Vulnerability Management (VM). The combination of these solutions provides context and shared intelligence through analytics, giving customers a more comprehensive view of their security posture so they can make more informed, prioritized, and better security remediation decisions.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

CORE SECURITY