INTSIGHTS
Defend Forward™

Empower PCI DSS Continuous Compliance with Vulnerability Risk Analyzer

If your organization processes, stores, or transmits payment cardholder information, it must comply with the Payment Card Industry Data Security Standard (PCI DSS). The 12 Requirement sections included in the prescriptive standard define a minimum level of security protections that your organization must implement. Organizations must be compliant or face fines and penalties.

PCI Compliance and IT Risk Management Goals:

- Protect critical systems from threat exposure and security vulnerabilities.
- Validate and provide integrity of threat intelligence sources.
- Provide compensating control support for security requirement gaps.
- Prove vulnerability prioritization program aligns with risk mitigation goals.
- Automate patch enrichment and context to audit reporting requirements.

IntSights Vulnerability Risk Analyzer attains continuous compliance and automates risk prioritization

The IntSights vulnerability prioritization and risk enrichment solution, Vulnerability Risk Analyzer (VRA), goes above and beyond the underlying compliance requirement of basing vulnerability patching and mitigation solely on industry-standard CVSS scores. CVSS scores often miss critical security gaps, putting the security posture of the organization in jeopardy and exposing the enterprise to increased risk of attack. VRA adds essential threat and risk measures to the PCI assessment process and enables continuous compliance.

VRA enables organizations to solve three important provisions embedded within PCI DSS Requirement 6.1:

Identify and assign a risk ranking to newly discovered security vulnerabilities:
IntSights VRA provides point-in-time prioritized vulnerability inspection that reflects the real risk of the security vulnerability, beyond the CVSS ranking score.

Ensure that sources for vulnerability information (i.e., vendor websites, industry news groups, mailing list, RSS feeds) are trustworthy:
IntSights VRA provides comprehensive context for supporting security vulnerability information to validate trustworthiness and support mitigation decisions.

Continuously evaluate vulnerabilities and assign risk rankings by deploying a process to actively monitor industry sources for vulnerability information:
IntSights VRA provides real-time or point-in-time evaluation of vulnerabilities with context-rich threat intelligence to ensure the findings are based on real risks specific to any proprietary business processes or gaps within the enterprise (i.e., unpatchable EOL systems supporting critical business).

Key Benefits

VRA for PCI Vulnerability-Centered Requirements:

- Immediate scoring of PCI Scope system CVEs based on severity, dramatically improving alerting confidence and patching time for proven critical vulnerabilities
- Ability to surface relevant intelligence from the clear, deep, and dark web, allowing auditors and QSAs to review, confirm, and validate compliance risk criteria and scoring
- Complete CVE lifecycle management with focus on relevant technologies, BAUs, industry sectors, and more, helping to accelerate the PCI quarterly audit cycle
- Robust integrations with leading vulnerability management solutions and an advanced API to ease implementation into the compliance stack and audit process
- Individual CVE trendlines to demonstrate whether activity is increasing or decreasing over time, empowering PCI scoping, gap analysis, and validity of threat mitigation plans

PCI DSS Requirement 6.1		
Develop and maintain secure systems and applications	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities and file assets. **The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment.** **Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds.**	Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. **The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information.**

Obtain continuous compliance and align with PCI DSS requirements with IntSights VRA

- Stop security threats that stem from malicious software and targeted attacks.
- Protect and secure in-scope and out-of-scope systems.
- Establish a process to identify security vulnerabilities and assign a risk ranking prioritization.
- Create critical asset policies to reduce the amount of data to analyze and associated administrative efforts.
- Receive real-time targeted alerts protecting all of your critical data and assets.

Prioritizing remediation of system vulnerabilities that create gaps in security infrastructure is a vital component of any compliance program. A good vulnerability enrichment and prioritization program should provide evidence to auditors that the appropriate controls are in place with context for the supporting intelligence.

Proactive vulnerability identification and risk ranking are requirements in the current version of the PCI DSS (v.3.2.1) to support patch mitigation plans, growing PCI DSS Compensating Controls, and remediations. This will become even more important in the near future as version 4.0 of PCI DSS is expected to call for further enrichment and validation of intelligence that informs security mitigation planning. Organizations will need to adopt proactive vulnerability identification and intelligence-based prioritization processes, which are fully served by IntSights VRA.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

Learn More about **IntSights Compliance Assessment and Advisory Services**