SOLUTION QUICK CARD

PCI DSS 4.0 Requirement 11.3 - Vulnerability Scanning

Critical Start Vulnerability Management Service with PCI Scanning

KEY BENEFITS

- ✓ Offload burdensome (but required) tasks
- ✓ Achieve and maintain PCI compliance, even as the standard changes
- ✓ Eliminate audit findings and avoid penalties and fines
- ✓ Reduce cyber risk
- ✓ Gain deep insights into your operating environment and security maturity
- ✓ Save on cost and focus your staff on your organization's mission

PCI Compliance is Required – But Do You Have the Resources to Keep Up?

Vulnerability scanning is an essential requirement of the Payment Card Industry Data Security Standard (**PCI DSS**). But scanning alone isn't enough. PCI DSS 4.0 requirement 11.3 requires organizations to perform internal and external scans at least quarterly; identify, prioritize, and resolve high-risk and critical vulnerabilities; and then re-scan to demonstrate compliance. Organizations must also maintain their scanning tools, keep scan profiles and rules updated through environmental changes, and keep track of ongoing PCI compliance efforts. All these tasks must be performed with tools on the approved scanning vendor (**ASV**) list and conducted by "qualified personnel" – domain experts who understand the systems in use and who keep up with the rapidly shifting vulnerability and exposure landscape. While these best practices are intended to protect consumer data, the heavy lift of PCI vulnerability scanning requirements taxes even some of the best staffed organizations.

Ideal Use Cases

For any organization struggling to keep pace with PCI DSS vulnerability scanning compliance, the Critical Start Vulnerability Management Service with PCI Scanning is a game changer.

This Vulnerability Management Service tier is ideal for organizations that fall under PCI compliance, and are:

- MDR or MSSP subscribers, or any organization that has an outsourced SOC.
- In retail/ecommerce, banking/finance, healthcare, or any other industry that processes credit card payments.
- Small-to-medium businesses.
- Small enterprise organizations.
- Any organization that is resource and/or time constrained.
- Organizations that lack tools from the ASV list.

How it works

Critical Start's Vulnerability Management Service with PCI Scanning starts by understanding your environment, including which systems fall under PCI compliance, and identifying which are most at risk. Our domain experts use scanning tools from the ASV list for PCI, tuned to your environment, and then conduct quarterly internal and external scans. After each scan, you receive prescriptive patch lists that detail exactly which patches to use, where to apply them, and why they're important. Once you finish resolving issues, we conduct post-remediation scanning and provide all required scan reports needed for the audit. Additionally, the service includes continuous operational monitoring so that you can trust that your scan jobs are complete and accurate, and that all applicable PCI systems are scanned in accordance with the standard.

Learn more about Critical Start Vulnerability Management Service with PCI Scanning, or schedule a demo at:
www.criticalstart.com/contact/request-a-demo/

CRITICALSTART®