GUIDE

Seeker and PCI DSS Compliance

Building real-time security and compliance at the speed of business

How Seeker helps you meet PCI DSS requirements

Seeker is the tool of choice for those needing to meet PCI DSS and other compliance obligations.

6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	Seeker provides a continuous vulnerability and remediation process for web applications. Risk rankings are based on industry best practices, consideration of CVSS base score, and/or classification and potential impact by Synopsys. When Seeker discovers new security vulnerabilities, it categorizes them by impact/risk (high, medium, or low). Developers can sort and view defects based on impact/risk.
6.3: Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	Based on industry standards and best practices, Seeker enables you to “build security in” throughout the SDLC, whether you’re developing internal or external applications. Seeker provides the strongest means of achieving the necessary level of information security assurance. It generates strong documentation to assist with compliance activities in accordance with PCI DSS.
6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.	Seeker continuously monitors, detects, and verifies common application security weaknesses during functional testing to ensure changes do not adversely affect the security of applications.
6.5: Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.	One of the best ways to teach developers how to address coding vulnerabilities is to explain why a vulnerability was flagged as exploitable (including the source code) and give them information on the flow of tainted data from source to sink. Seeker provides these details, as well as remediation advice based on secure coding guidelines. It also offers contextual learning with built-in eLearning support. Developers can attain in-depth knowledge and stay up-to-date on secure coding practices for many programming languages.
6.5.1: Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Seeker checks for these injection flaws (including second-order injection): 6.5.1 SQL INJECTION 6.5.1 REFLECTION INJECTION 6.5.1 LDAP INJECTION 6.5.1 XPATH INJECTION 6.5.1 HIBERNATE INJECTION 6.5.1 NoSQL INJECTION 6.5.1 REMOTE FILE INCLUSION 6.5.1 LOCAL FILE INCLUSION

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.