Achieve PCI 3.2 Compliance with WhiteHat Sentinel

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard set by the five major payment brands and industry stakeholders to protect user data from exposure. It is a "self-regulating" industry standard, which means there are no governmental regulations covering compliance and enforcement is left to the individual payment brands. Any organization that deals with credit card information must take steps to protect this information as it is used, stored and transmitted. Organizations that suffer a breach and have not taken steps
to ensure compliance can be penalized, and in some cases may even be prohibited from working with specific payment brands.

Recent changes in the PCI DSS regulation (v3.0, v3.1, and v3.2) provide a set of suggested best practices and methodologies that make it possible to comply with PCI on an ongoing basis. These changes will have an impact on how organizations go about ensuring compliance. This solution brief looks at the requirements that apply to application security and discusses the issues that should be considered during the Software Development Lifecycle (SDLC).

WhiteHat Security:
Your PCI Compliance Partner

- **Reliable:**
  All vulnerabilities are manually verified by a member of our Threat Research Center (TRC)
- **Dependable:**
  Near zero false positives
- **Fast:**
  Actionable advice
- **Accessible:**
  24x7 access to a security expert with specific advice about each vulnerability identified
- **Seamless:**
  Easy integration into SDLC
- **Helpful:**
  Computer Based Training (CBT) offerings that meet PCI 6.5 and 12.6 standards

Who has to comply?

Perhaps a better question is "Who doesn't have to comply?" The PCI DSS applies to every aspect of credit card processing.

Today, many companies with internal or public-facing websites fall under some section of the Payment Card Industry Data Security Standard. Any company that collects, stores or transmits credit card data is subject to PCI DSS. If any aspect of a business has anything to do with credit card processing, including but not limited to credit card terminals, credit card imprinters, mobile payment devices, online payments, paper forms, payment-enabled software or point of sale (POS) solutions, PCI DSS applies and it would need to be determined which standards apply. The regulations are especially applicable in certain high-profile industries such as healthcare, financial services, retail and service providers.

Principal issues for compliance in application security

The recent enhancements to PCI DSS call for changes in the way organizations do secure in-house application development, and ensure the security of their internal and external applications. This solution brief covers the principal areas related to application security, providing an explanation of each relevant standard, and a description of how WhiteHat can be a partner for successful PCI compliance. This document is not meant to be a replacement for a formal PCI DSS audit, but rather an overview of how WhiteHat Security can help businesses become compliant based on our work with hundreds of customers who have successfully implemented PCI DSS in their own environments.

WhiteHat Security for PCI Compliance

Requirement	Brief Explanation	How WhiteHat can Help:
2.4	Maintain an inventory of all systems and their components – and understand what each component is doing.	During configuration, the WhiteHat Sentinel scanner rapidly identifies all website assets and inventories existing applications.
6.1	Establish a process to identify security vulnerabilities and assess risk ranking.	Vulnerabilities that are identified by WhiteHat Sentinel are verified for accuracy and then prioritized based on risk, to target high priority issues.
6.2	Ensure that all components and software are protected from known vulnerabilities; install patches	WhiteHat Sentinel provides integration with Web Application Firewalls (WAFs) to create virtual patches and fix vulnerabilities.
6.3	Develop internal and external applications securely; incorporate security throughout SDLC: ▪ Remove development and test accounts before moving code to production ▪ Review custom code for vulnerabilities before production	WhiteHat Sentinel enables ongoing, continuous assessment with guidance that is easily integrated into the SDLC. WhiteHat Sentinel evaluates source code in test and development environments, searching for vulnerabilities before the code goes into production.
6.4	Ensure that change control processes are followed: ▪ Separate development/test environments from production ▪ Production data (live PANs) must not be used for testing or development ▪ Remove test data and accounts before production	WhiteHat Sentinel identifies development artifacts such as testing code and configurations.
6.5	Address common vulnerabilities throughout the SDLC: ▪ Injection flaws ▪ Buffer overflows ▪ Insecure cryptographic storage ▪ Insecure communications ▪ Improper error handling ▪ All “high risk” vulnerabilities identified ▪ Cross-site scripting ▪ Improper access control ▪ Cross-site request forgery ▪ Broken authentication / session management	WhiteHat Sentinel tests for the most common vulnerabilities including the OWASP Top 10, the Web Application Security Consortium’s Threat Classification, as well as performing additional custom testing.
6.6	Address threats and vulnerabilities related to public-facing web applications on an ongoing basis.	WhiteHat Sentinel provides continuous and concurrent vulnerability assessments.
11.3	Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification	WhiteHat Sentinel PE satisfies the application security testing requirements of 11.3 by finding vulnerabilities that cannot be discovered by automated scanners alone.
12.6	Implement a formal security awareness program and educate personnel.	WhiteHat Security offers Computer Based Training (CBT) to give developers the skills they need to write secure code in fast-paced production environments. These CBT courses also map one-to-one for Continuing Professional Education (CPE) credits.

WhiteHat Security – Your Partner for PCI Compliance

Our patented methodology exceeds the strictest industry standards for application security as established by the PCI Security Standard Council by providing ongoing, verified vulnerability assessments for both internal and public websites. With WhiteHat, you have access to the world’s largest team of security experts who can help you become PCI DSS compliant and maintain it.

About WhiteHat Security

WhiteHat Security combines advanced technology with the expertise of its global Threat Research Center (TRC) team to deliver application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company’s flagship product, WhiteHat Sentinel, is a SaaS platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in Santa Clara, Calif. Learn more at www.whitehatsec.com.

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com

021317