Sonatype

WHITEPAPER

Tools & Techniques for Addressing Component Vulnerabilities for PCI Compliance

Component Governance is Now Required for PCI Compliance

Research shows that today's applications are actually "assembled" vs. "written". In fact, in a survey of over 3500 developers, they reported that at least 80% of their applications are comprised of components. Components are like building blocks of code - often downloaded from public open source repositories - which can be easily and quickly assembled together to build applications faster. Therefore the security of components is considered a key aspect of overall application security.

The Payment Card Industry (PCI) and other prominent specifications are being updated to reflect this reality. OWASP, the Open Web Applications Security Project, was recently updated to include a requirement that specifies that untrusted components must be avoided. This relates directly to PCI compliance since the PCI specification requires OWASP vulnerability management be supported. The specification notes that as the OWASP specification is updated, current best practices must be used.

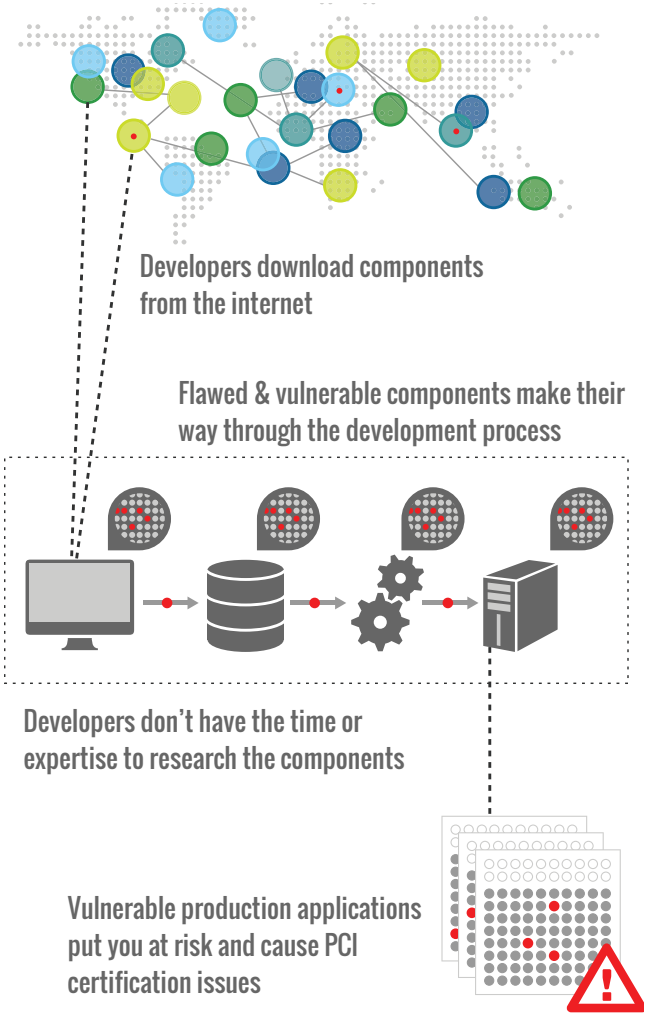
Since components are used to build applications, these requirements require proper governance of open source component usage. The Version 3.0 Change Highlights expand the specification by requiring organizations to maintain an inventory of system components as a way to ensure proper compliance coverage.

Both the existing PCI Version 2.0 and the PCI DSS and PA-DSS Version 3.0 Change Highlights address component usage (please refer to pages 9-14 for details). The existing specification requires that organizations develop and maintain secure systems and applications. It also requires that organizations implement regular monitoring and testing; and specifies that policies are maintained that address information security for all parties. Since components are used to build applications, these requirements require proper governance of open source component usage. The Version 3.0 Change Highlights expand the specification by requiring organizations to maintain an inventory of system components as a way to ensure proper compliance coverage. The Change Highlights also reiterate the

need to update compliance so that it aligns with secure coding practices stated by OWASP, NIST, and SANS.

Recent changes to OWASP put component compliance directly into play. OWASP updated their Top 10 list to include A9, which states that applications should avoid using components with known vulnerabilities. OWASP requires that components and versions be tracked, that component vulnerabilities be monitored and that security policies be used to govern component usage.

Sounds easy right? You can just expand your existing PCI approach to support components. Or can you? Given the volume of applications that organizations use to run their business; the fact that applications are comprised of 80% components; and the volume, variety, complexity and release cadence of components, organizations must take an automated component management approach to feasibly address PCI compliance.



PCI: If You Process Credit Card Data, It Probably Applies to You

As explained in the Payment Card Industry (PCI) Data Security Standard:

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

Since many organizations process payment cards, the PCI standard is applicable to a wide range of industries – not just financial services and retail. The PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. Other cardholder data includes the cardholder name, expiration date, and service code.

The standard includes 12 summary PCI DSS requirements that consist of many detailed requirements that span network, storage, vulnerability management, access control, monitoring and testing, and information security policy. Given the breadth of the requirements; the complexity of today's applications and infrastructure; and the fact that a cardholder data environment is comprised of people, processes, and technology that store, process or transmit cardholder data; organizations can't simply turn to a single vendor or solution to ensure compliance. They must implement a complete program that leverages policies, processes and technologies to ensure compliance.

Visit www.pcisecuritystandards.org for more information.

OWASP New Top 10 List Includes Secure Component Requirement

"OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted… We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas."

OWASP has recognized the critical role that components play in today's applications. OWASP updated their Top 10 list to include A9, which states that applications should avoid using components with known vulnerabilities. The standard includes these best practices:

- Identify the components and the versions you are using, including all dependencies.
- Monitor the security of these components in public databases, project mailing lists, and security mailing lists, and keep them up-to-date.
- Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and acceptable license.

Please refer to page 6 for additional information about application components.

SONATYPE HELPS MEET PCI COMPONENT REQUIREMENTS

Monika Liikamaa, Director of Card Services for Financial Services provider, Crosskey, recently stated, "There is no such thing as 98% compliance. You either are or you aren't". And there is no such thing as "point-in-time" compliance. The best way to ensure compliance is to manage the entire software lifecycle by integrating security and compliance throughout the development process while providing ongoing trust in the production environment.

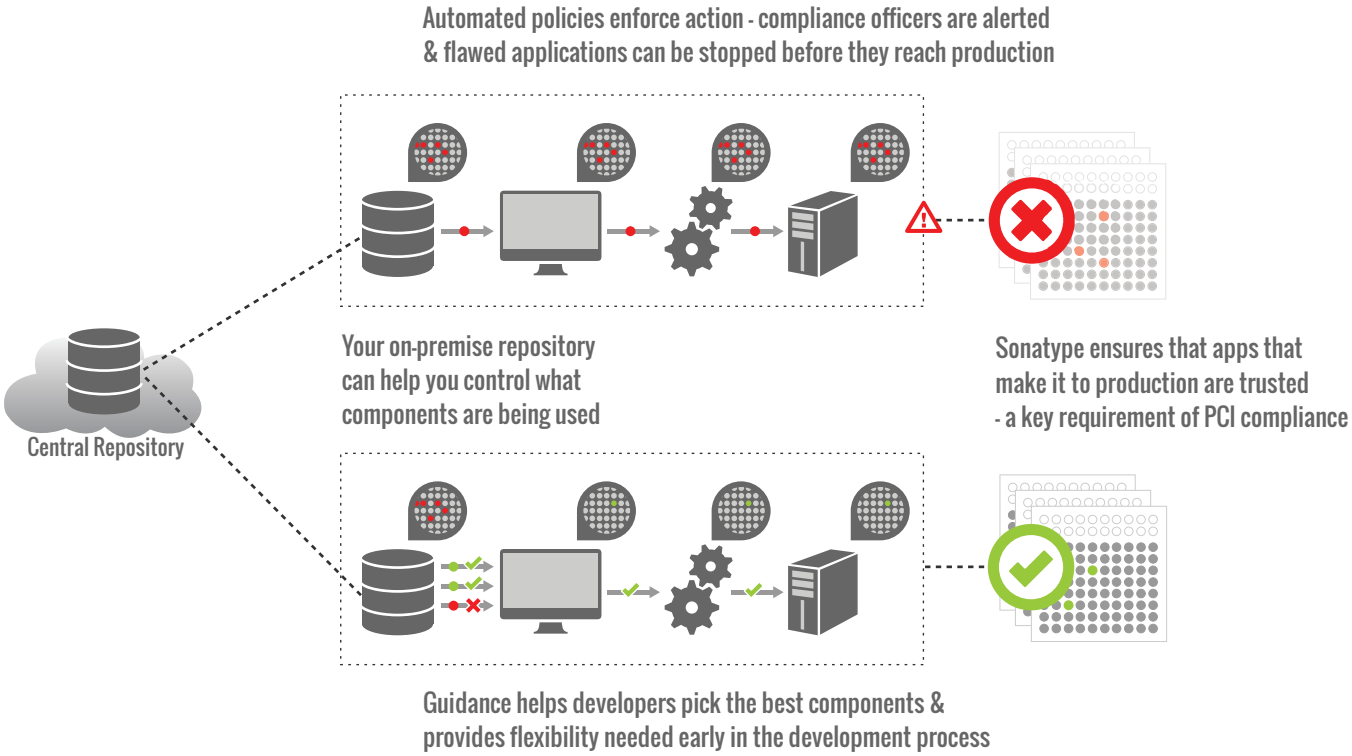
Sonatype helps you cost effectively meet PCI requirements by automating policies that address the volume, complexity, variety, and release cadence of open source components.

Sonatype plays an instrumental role in helping organizations address PCI compliance by ensuring that components that are used to construct applications are secure and remain secure over time. Sonatype helps address PCI requirements in many key ways:

- Sonatype helps ensure that applications are trusted by analyzing application components, identifying vulnerabilities, integrating information and providing guidance throughout the software development lifecycle.
- Sonatype provides a component inventory that helps meet PCI reporting requirements; helps to identify scope and helps to limit scope of compliance assessment efforts.
- Sonatype helps organizations keep applications up to date by providing information about current/best component versions. Sonatype "one click migration" helps developers upgrade their applications quickly with minimal effort.
- Sonatype helps organizations address third party compliance requirements by supporting open source components sourced from the Central Repository.
- Sonatype helps organizations establish and implement poli-

cies that are automatically enforced.

- Sonatype helps organizations identify new vulnerabilities and helps organizations triage and prioritize compliance efforts.



CROSSKEY RELIES ON SONATYPE FOR PCI CERTIFICATION

Like many financial services organizations, Crosskey processes payment card transactions so protecting cardholder data is key to ensuring consumer confidence and trust. Crosskey views PCI as not only a requirement, but views the certification as a competitive advantage over other financial institutions.

But compliance is not easy to attain. In fact, in this day of agile, component-based development - with a heavy reliance on open source components - compliance has become increasingly difficult. To complicate compliance efforts, Crosskey deploys new application functionality frequently, every 6 weeks at a minimum. Crosskey does this to ensure business agility and to deliver new

"Trust is what we strive for. Trust is why PCI was invented. It allows people to trust our brand and know their payments are safe. Crosskey offers trust to the end user. Sonatype is a key component to delivering trust."

Crosskey

Monika Liikamaa,
Director of Card Solutions
Crosskey

What's a Component Anyway?

In the context of PCI DSS, "system components are defined as any network component, server, or application that is included in or connected to the cardholder data environment… Applications include all purchased and custom applications, including internal and external (for example, Internet) applications."

In the context of Sonatype, components are the run-time binary artifacts that are used to assemble applications. These components are the primary building blocks for the applications, which are comprised of 80% open source components.

The PCI system component definition is broader than the Sonatype component definition since it includes "any network, server or application component that is included or connected to the cardholder data environment." Components that are managed by Sonatype are instrumental to the applications that leverage network and server components that fall under PCI.

capabilities to their customers. They determined that it was not feasible to ensure compliance based on the volume of components and applications that they use. And if they attempted to do it manually, they would still lack the ability to prove that they had performed the appropriate checks.

Sonatype helps Crosskey control and manage the components that are used in their applications - and since applications are comprised of 80% components, this goes a long way to ensuring compliance. Sonatype also ensures that the components sourced from the Central Repository, the de facto standard for open source components, are delivered securely, eliminating the possibility that hackers manipulated them. Crosskey is using Sonatype to implement security policies that will help manage the application release process. Crosskey can ensure that only trusted components are used in applications that are deployed to production, applications that process credit card information. Crosskey depends on Sonatype to identify and choose the best and safest components. "This is a big requirement for us as it helps us gain trust in the marketplace," says Likamaa.

For Crosskey, trust is key, says Likamaa. "Trust is what we strive for. Trust is why PCI was invented. It allows people to trust our brand and know that their payments are safe. Crosskey offers trust to the end user. Sonatype is a key component to delivering trust."

PCI VERSION 2.0 APPLICATION REQUIREMENTS APPLY TO COMPONENTS

Since components are now the dominant pattern for developing applications, the existing PCI requirements that relate to applications apply to the components used to assemble the applications. This is primarily evident in the specification details that require organizations to develop and maintain secure systems and applications. To do this, PCI states that organizations must maintain a Vulnerability Management Program. The existing specification also requires that organizations implement regular monitoring and testing; and specifies that policies be maintained that address information security for all parties.

PCI requires that organizations develop and maintain secure systems and applications. Since applications are comprised primarily of components, using secure components is the only way to comply with PCI.

For a detailed view of how Sonatype helps you address specific requirements for the existing PCI Version 2 Specification Details, please refer to the information on pages 9-14.

PCI VERSION 3.0 INCREASES COMPONENT SCRUTINY

Like any active specification, PCI is updated on a periodic basis. Responding to industry feedback, the Council moved from a two-year to a three-year standards development lifecycle in 2010. A document that defines the anticipated changes for version 3.0 that will be introduced in November 2013, was published in August, 2013. Stakeholders that will review and discuss draft versions of PCI DSS and PA-DSS at 2013 Community Meetings will use the Version 3.0 Change Highlights document. Organizations can also use the document to review and understand changes prior to implementation.

Version 2.0 will remain active until December 31st, 2014. Some of the sub-requirements for Version 3.0 will be best practices only until July 1st, 2015, while specifics about implementation dates will be introduced by the Council accordingly.

While some organizations may delay implementation of the standard until it becomes a hard requirement, leading organizations understand that early compliance with the new specification can be used as a differentiator since consumer confidence and trust is key to many businesses.

For a detailed view of how Sonatype helps you address specific requirements for the recently announced Version 3.0 requirements, please refer to the PCI Version 3.0 Change Highlights Specification Details (pages 13 and 14).

PA-DSS Applies PCI Requirements to Packaged Software Vendors

While the PCI DSS standard provides a baseline of technical and operational requirements designed to protect cardholder data that applies wherever account data is stored, processed or transmitted "The PA-DSS (Payment Application Data Security Standard) applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties." The PA-DSS applies to vendors that provide "off the shelf" payment applications.

Organizations that leverage PA-compliant applications are not PCI-DSS compliant unless the application is implemented into a PCI DSS compliant environment.

Version 3.0 will require organizations to maintain an inventory of system components to ensure proper compliance coverage. The Change Highlight requires secure coding practices as stated by OWASP, NIST, and SANS.

Three Steps to Start the PCI Component Journey

Step 1 Build an inventory: It's difficult to manage your components and applications if you don't know what you have. It's also a key PCI requirement. Start by building an inventory of your critical applications by identifying all components (including dependencies) that are used to construct the applications.

Step 2 Determine your threat exposure: As dictated by the PCI specification, prevent common coding vulnerabilities by identifying components that have known vulnerabilities noted in public databases.

Step 3 Prevent vulnerabilities and remediate flaws: Implement a policy mechanism that will ensure developers use the best components from the start. And ensure that you can quickly identify, triage and fix newly discovered vulnerabilities across the application lifecycle.

PCI & COMPONENTS: THE NEW BOTTOM LINE

PCI support is key for any organizations that process payment cards. Consumers must have confidence that their cardholder data is secure and the best way for organizations to do this is to support PCI compliance. Given that the PCI specification is updated every 3 years, organizations that comply during the "best practice" phase can tout PCI compliance as a competitive advantage. But compliance is not easy to attain, and compliance in this day of agile, component-based development that relies on open source components has become increasingly difficult. Complicating compliance is the volume of application requirements and the speed at which development organizations have to deliver to support the business. Sonatype is the only solution capable of helping you meet your compliance goals while speeding application delivery.

- Sonatype speeds development by integrating guidance directly into the development lifecycle.
- Sonatype ensures PCI compliance by automating policy enforcement throughout the lifecycle.
- Sonatype provides ongoing monitoring, alerts, and rapid remediation for protection against newly discovered vulnerabilities.

PCI DSS Requirements and Security Assessment Procedures, Version 2.0		
PCI Specification Number	PCI Specification Text	Sonatype Value Statement
High Level Overview		
	Maintain a Vulnerability Management Program: 6. Develop and maintain secure systems and applications.	The Sonatype solution provides comprehensive support for application components that are key to developing and maintaining secure systems and applications.
	Regularly Monitor and Test Networks: 11. Regularly test security systems and processes.	The Sonatype solution leverages application component vulnerability meta-data that may have been generated by monitoring and testing the application components.
	Maintain an Information Security Policy: Maintain a policy that addresses information security for all parties.	The Sonatype solution provides the ability to define policies that address PCI compliance. The policies provide guidance and enforcement throughout the entire software lifecycle.
Sampling of Business Facilities/System Components	The first step of a PCI DSS assessment is to accurately determine the scope of the review.	Component Lifecycle Management (CLM) inventory capabilty helps identify scope of effort as it relates to component-based applications.
Instructions and Content for Report on Compliance	If there are standard, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that all business facilities/system components are configured per the standard processes.	CLM policies that are applied across a large set of applications can be used as justification to limit the sample size and reduce the compliance effort.
	3. Details about Reviewed Environment: List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each.	CLM inventory capability provides list of critical application components.
	3. Details about Reviewed Environment: List of third-party payment application products and versions numbers in use.	CLM inventory capability and component meta-data provides information about open source components sourced from the Central Repository.

PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (continued)		
Requirement 6: Develop and maintain secure systems and applications		
6. Intro		
6.1	All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.	Sonatype helps ensure that "standard" application components are used based on security policy. Guidance provided in the IDE helps ensure that "secure coding" is leveraged by using components that were securely coded.
6.1 Note	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Sonatype helps organizations stay current with the latest versions or best versions of application components. Initially by guiding the developer to select the best component when developing applications, making it easy to see all relevant component versions, and later by identifying and notifying when new vulnerabilities are discovered.
6.2	An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	Sonatype helps organizations prioritize their efforts based on the degree of policy violation. Information is provided in dashboards that summarize the overall risk, allowing organizations to determine the impact of a component problem by identifying where it is being used. Policies can be created that factor in the criticality of the application - another mechanism that helps support the policy constraints that are violated, and the criticality of the violation.
6.2.b	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	The Sonatype policy mechanism allows the security team to set a threat value based on the severity of the vulnerability, As described in the standard, this threat value can be related to the CVSS base score.
6.3	Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.	Sonatype provides information about the components based on public security vulnerability sources and augments this with additional research. As new vulnerabilities are discovered, they are identified and matched to the component inventory for applications in development or in production.
6.3.2	Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle.	Sonatype provides the ability to apply security policies throughout the development lifecycle. This helps incorporate information secureity throughout the software development lifecycle.

PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (continued)		
6.4.1	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	Sonatype ensures that components that are consumed as binary artifacts are protected. Although Sonatype does not analyze custom source code, it helps bolster application security since applications are now comprised of 80% open source components.
6.4.5	Separate development/test and production environments.	Nexus helps organizations support multiple environments based on its support for staging and promotion. Staging and promotion is strengthened by security policies that can be applied to this release process.
6.4.5.1	Change control procedures for the implementation of security patches and software modifications.	Although Sonatype does not provide change control procedures - Sonatype's ability to help identify the correct version helps ensure that new versions are deployed.
6.5	Documentation of impact.	Sonatype can be used to track updates that have happened, which could be correlated with other data to determine or help measure impact. This "audit trail" of activity related to component activity (vulnerabiliies discovered, vulnerabilities fixed) can help determine activity and impact.
6.5 Note	Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes.	The Sonatype solution helps support the entirety of OWASP, NIST and SANS requirements as they relate to application components. For example, Sonatype helps mitigate issues for application components that specificed as OWASP requirements: SQL Injection, XSS, CSRF, etc."
6.5.1 - 6.5.9	The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	"OWASP has recognized the critical role that components play in today's applications. OWASP updated their Top 10 list to include A9, which states that applications should avoid using components with known vulnerabilities. The standard includes these best practices: - Identify the components and their versions you are using, including all dependencies. - Monitor the security of these components in public databases, project mailing lists, and security mailing lists, and keep them up-to-date. - Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and acceptable license. Sonatype supports each of these best practices.
6.6	The PCI notes that it is necessary to prevent common coding vulnerabilities in software development processes including: Injection flaws, buffer overrlow, insecure crytographic storage, insecure communications, improper error handling, XSS, improper access control, CSRF.	Sonatype analysis and identification of vulnerabilities in application components downloaded from the Central Repository provides protection against these vulnerabilities.

PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (continued)		
Requirement 11: Regularly test security systems and processes.	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks	
11.3.2		
Maintain an Information Security Policy	Application-layer penetration tests	Sonatype's analysis of components fulfills this requirement for the components that exist in an application. This analysis establishes known vulnerabilities that are then matched against the application inventory.
12.1		
12.1.2	Establish, publish, maintain, and disseminate a security policy	Sonatype provides the ability to codify security policies that are created by the security team. These policies can be designed to support the PCI requirements. The policies are automatically enforced with stage appropriate guidance throughout the software lifecycle.
12.5.1	Include an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	Sonatype provides on-going assessment of risk that is visualized in CLM dashboards. This can help support periodic reviews that are required for PCI compliance.
12.5.2	Establish, document, and distribute security policies and procedures.	Sonatype codifies security constraints in the security policies.
12.5.3	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Sonatype provides proactive alerts for new vulnerabilities and distributes this information to appropriate personnel based on the policy definition.
12.9.5	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	It is possible to integrate alerts generated by Sonatype to feed a system that manages incident response and escalation.
	Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	Vulnerabilities that are discovered using these technologies for the applciation components in the Central Repository can result in meta-data that can result in actions specified by CLM policies.

PCI DSS and PA-DSS - Version 3.0 Change Highlights		
Intro	The updated standards will help organizations not by making the requirements more prescriptive, but by adding more flexibility and guidance for integrating card security into their business-as-usual activities.	Sonatype helps support the "business-as-usual" activity of designing, developing, deploying and maintaining applications that run the business. Sonatype helps organizations integrate security directly into the development process, which is a critical aspect of doing PCI correctly.
Intro	At the same time, the changes will provide increased stringency for validating that these controls have been implemented properly, with more rigorous and specific testing procedures that clarify the level of validation the assessor is expected to perform.	The increased stringency for validating PCI controls will put more pressure on organizations to prove compliance. Given the component-based nature of today's applications, the volume, variety, complexity and release cadence of components makes it difficult if not impossible to manage and validate PCI requirements manually. Sonatype support for policy-based automation coupled with the ability to provide proof will help organizations address this increased stringency.
Intro	Overall, the changes are designed to give organizations a strong but flexible security architecture with principles that can be applied to their unique technology, payment, and business environments.	The Sonatype solution provides the flexibility necessary to support different architecture approaches - organizations can implement support based on their most critical need - IDE integration, release management, production monitoring, etc. Sonatype supports various tools and environments, which provides another form of flexibility.
Intro	Help manage evolving risks & threats.	Sonatype continuous monitoring helps manage evolving risks. As new vulnerabilities are discovered, they are identified and related to the component inventory of applications that are in production or in development. Organizations can then remediate these new threats.
Intro	Security as a shared responsibility.	The Sonatype approach facilitates communication and collaboration between the security team and the development and IT Ops organization. This helps ensure that security is a shared responsibility vs. placing all of the responsibility on the security team.
Intro	The PCI DSS and PA-DSS are constructed in a way that their principles can be applied to various environments where cardholder data is processed, stored, or transmitted—such as e-commerce, mobile acceptance, or cloud computing.	Sonatype helps ensure that the best components are selected and re-used across multiple application development efforts. This helps PCI initiatives that span multiple application environments (e-commerce, invoicing, etc.) and also helps applications regardless of how they are deployed (mobile, cloud, etc.).
2	Maintain an inventory of system components in scope for PCI DSS.2	Sonatype provides the ability to create a highly accurate inventory of application components. This inventory capability is nearly instantaneous and is not invasive to the development or runtime environments. This inventory is key to providing component management that is based on security, licensing and usage meta-data.

PCI DSS and PA-DSS - Version 3.0 Change Highlights (continued)		
6	Update list of common vulnerabilities in alignment with OWASP, NIST, SANS, etc., for inclusion in secure coding practices.	OWASP has recognized the critical role that components play in today's applications. OWASP updated their Top 10 list to include A9, which states that applications should avoid using components with known vulnerabilities. The standard includes these best practices: - Identify the components and their versions you are using, including all dependencies. - Monitor the security of these components in public databases, project mailing lists, and security mailing lists, and keep them up-to-date. - Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and acceptable license. The Sonatype solution helps support the entirety of OWASP, NIST and SANS requirements as they relate to security. For example, Sonatype helps mitigate issues for components that specificed as OWASP requirements: SQL Injection, XSS, CSRF, etc.
12	Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity. Service providers to acknowledge responsibility for maintaining applicable PCI DSS requirements.	Sonatype supports the entire software lifecycle and software supply chain. Organizations that leverage service providers to provide applications / components, can use Sonatype to ensure that what they deliver meets their policies.

Sonatype's software protects the world's enterprise software applications from security, compliance, and licensing threats. Every day, millions of developers build software applications from open source building blocks, or components. Customers rely on the Sonatype family of products to accurately identify and analyze component usage and proactively fix flawed components throughout the software development lifecycle so applications are secure and comply with licensing and regulatory requirements. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures.