TechBridge
Making the World Smarter

tbSIEM: PCI DSS v3.2.1

WHITE PAPER

Contents

1. PCI DSSv3.2.1

PCI DSS Requirements v3.2.1	Milestone	tbSIEM	How it helps
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1 Establish and implement firewall and router configuration standards that include the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	Rootcheck	Rootcheck provides capabilities to inspect firewall and routers configuration files, when those are accessible by the agent.
		Syscheck	Syscheck can be used to detect firewall and router configuration file modifications looking for changes in MD5/SHA1 checksums.
1.2.2 Secure and synchronize router configuration files.	2	Syscheck	Syscheck can monitor router configuration files integrity, when those are accessible by the agent or via SSH (agentless), generating alerts when modifications of these files are detected.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM	How it helps
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices	2	Rootcheck Logcollector - Run commands	Rootcheck can check that local system firewall is enabled, by inspecting configuration settings (registry keys or config files). Logcollector can run commands to ensure firewall is working and alert if it is not active.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM	How it helps
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.	2	Rootcheck Logcollector	Rootcheck can inspect system files and detect if unnecessary user accounts have not been removed or disabled. Logcollector can be used to retrieve system logs and alert if a default account is active.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	3	Rootcheck	Rootcheck module can be used to enforce systems hardening. It implements out of the box rules to enforce CIS benchmarks.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	3	Rootcheck	Rootcheck can detect unnecessary running processes, identifying services that should not be active on the server.
2.2.2 Enable only necessary services, protocols, daemons, etc, as required for the function of the system.	3	Rootcheck	Rootcheck can detect unnecessary running processes, daemons or services. As well, it can ensure that necessary processes are running.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	3	Rootcheck Logcollector - Run commands	A combination of rootcheck and logcollector capabilities can be used to alert if insecure services are enabled.
2.2.4 Configure system security parameters to prevent misuse.	3	Rootcheck	Rootcheck provides security policy enforcement rules that can be customized to prevent misuse.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	3	Rootcheck	Rootcheck policy enforcement rules can check that unnecessary functionality has been removed, by inspecting the file system, running processes or registry keys (when monitoring a Windows server).
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties	2	Rootcheck	Rootcheck policy enforcement rules can be used to ensure security policies and procedures are in use.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM	How it helps
Requirement 3: Protect stored cardholder data			
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data	1	Logcollector Run commands	tbSIEM agents can run commands on monitored servers, alerting when data stored is higher than a defined threshold or when it is not being deleted.

• A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention.			

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS). • Satellite communications	2	Rootcheck Logcollector Run commands	Rootcheck provides enforcement capabilities to confirm that services are configured in a secure manner. Logcollector run commands can be used to check the presence of private keys. In some cases, this can also be done using Rootcheck to inspect the file system.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs			
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	2	Rootcheck	Rootcheck can alert if the Antivirus process is not running.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7	2	Logcollector Syscheck	Logcollector can retrieve antivirus audit logs. Syscheck provides integrity monitoring capabilities based on MD5/SHA1 checksums that can be used to detect archived antivirus logs modifications.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be	2	Rootcheck Syscheck	Rootcheck can alert if the Antivirus process is not running or configured properly. Syscheck can monitor file permissions, alerting if those are modified.

disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.			

PCI DSS Requirements v3.2.1	Milestone	TbSIEM component	How it helps
Requirement 6: Develop and maintain secure systems and applications			
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	3	Rootcheck	Rootcheck rules can be used to inspect software version files and ensure that the latest patches have been applied.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	3	Rootcheck Logcollector	Rootcheck rules can inspect system files (like/etc/shadow) to alert if development user accounts have not been removed. Logcollector can be used to monitor system and application logs to detect the usage of development user accounts.
6.4 Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes. The processes must include the following:	3	Syscheck	Syscheck provides file integrity monitoring capabilities that are used to verify that the changes are made according to the change control process.
6.4.4 Removal of test data and accounts before production systems become active.	3	Rootcheck	Rootcheck rules are used to ensure that test data and accounts have been removed. This can be done inspecting the file system or the contents of system files (/etc/shadow).
6.5 Address common coding vulnerabilities in software development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and • understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 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	3	Analysisd	TbSIEM can analyze Web application log messages, for example from Apache and PHP, and detect attacks, buffer overflow, failure to restrict URL access, etc.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XpPath injection flaws as well as other injection flaws.	3		

6.5.2 Buffer overflows.	3		
6.5.3 Insecure cryptographic storage.	3		
6.5.4 Insecure communications.	3		
6.5.5 Improper error handling.	3		
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	3		
Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):			
6.5.7 Cross-site scripting (XSS).	3	Analysisd	TbSIEM can analyze Web application log messages, for example from Apache and PHP, and detect attacks, buffer overflow, failure to restrict URL access, etc.
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal and failure to restrict user access to functions).	3		
6.5.9 Cross-site request forgery (CSRF).	3		
6.5.10 Broken authentication and session management.	3		
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Performing application vulnerability assessment at least annually and after any changes. Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. Installing an automated technical solution that detects and prevents web-based attacks (for example, a web- application firewall) in front of public-facing web applications, to continually check all traffic.	3	Analysisd	Analsysisd provides a signature-based approach to detect attacks by inspecting Web application log messages.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	3	Rootcheck	Rootcheck provides policy enforcement capabilities that can be used to ensure that security and operational procedures are in use.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 7: Restrict access to cardholder data by business need to know			
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	4	Rootcheck	Rootcheck provides policy enforcement capabilities that can be used to ensure that security and operational procedures are in use.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps

Requirement 8: Identify and authenticate access to system components			
8.1 Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components as follows:			
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	4	Rootcheck	Rootcheck can check account IDs inspecting files or registry keys (when monitoring a Windows server).
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	4	Syscheck	Syscheck can monitor the integrity of system files containing user accounts information.
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: Enabled only during the time period needed and disabled when not in use. Monitored when in use.	4	Analysisd	TbSIEM can analyze logs from different services as FTP or ssh to detect several actions like log out or timeouts.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	4	Rootcheck	On Windows systems, Rootcheck can be used to check lockout policy is configured to lock a user after not more than six attempts. On Linux systems, Rootcheck can be used to ensure a mechanism is in place to lock accounts after the defined number of attempts.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	4	Rootcheck Logcollector - Run commands	On Windows systems, Rootcheck can be used to check the lockout duration. On Linux systems, Rootcheck can check the configuration of lockout duration. In some cases, when running a command is necessary to check this configuration, Logcollector can be used to check it.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	4	Rootcheck	Rootcheck can be used to check user sessions expiration time settings in remote connection services like RDP or SSH.
8.2.3 Passwords/phrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	4	Rootcheck	Rootcheck can check user accounts password policies (e.g. Windows or PAM Unix policies).
8.2.4 Change user passwords/passphrases at least every 90 days.	4		
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	4		
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	4		

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the application (and not by individual users or other non- application processes)	4	Analysisd	Analysis daemon provides mechanisms to analyze databases logs to identify access, queries, service availability, etc.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	4	Rootcheck	Security policies checked by Rootcheck are enforced by this module, ensuring that they are in use.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 9: Restrict physical access to cardholder			
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	5	Logcollector - Run commands	Logcollector can run system commands to ensure backups have been done successfully and are ready to move to a secure location.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 10: Track and monitor all access to network resources and cardholder data			
10.1 Implement audit trails to link all access to system components to each individual user.	4	Rootcheck	Rootcheck can check audit policies and configuration settings.
10.2 Implement automated audit trails for all system components to reconstruct the following events:			
10.2.1 All individual user accesses to cardholder data.	4	Rootcheck Logcollector Analysis daemon	Rootcheck provides mechanisms to ensure audit of user actions, or access attempts, are enabled. If these policies are modified, an alert is generated. Logcollector implements powerful capabilities to collect and centralize log data (audit trails) for systems and applications. Analysis daemon provides mechanisms to analyze the data collected by Logcollector using detection signatures and rules to perform correlation.
10.2.2 All actions taken by any individual with root or administrative privileges.	4		
10.2.3 Access to all audit trails.	4		
10.2.4 Invalid logical access attempts.	4		
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	4		
10.2.6 Initialization, stopping or pausing of the audit logs.	4		
10.2.7 Creation and deletion of system-level objects.	4		
10.3 Record at least the following audit trail entries for all system components for each event:			
10.3.1 User identification.	4		Logcollector can be used to centralize system and application messages in real time. It can read messages from different locations
10.3.2 Type of event.	4		
10.3.3 Date and time.	4		
10.3.4 Success or failure indication.	4		

10.3.5 Origination of event.	4	Logcollector	and forward those to the TbSIEM manager system, where those are processed by the Analysis daemon.
10.3.6 Identity or name of affected data, system component, or resource.	4		
10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP)	4		
10.4.1 Critical systems have the correct and consistent time.	4		
10.4.2 Time data is protected.	4		
10.4.3 Time settings are received from industry-accepted time sources.	4		
10.5 Secure audit trails so they cannot be altered.			
10.5.1 Limit viewing of audit trails to those with a job-related need.	4	Logcollector Analysis daemon Syscheck	Logcollector can read system and application messages and forward them to the manager, where those are centralized for analysis and archiving. Syscheck component can be used to ensure archived log data integrity. It uses MD5/SHA1 checksums to alert if a data file is modified.
10.5.2 Protect audit trail files from unauthorized modifications.	4		
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	4		
10.5.4 Write logs for external-facing technologies onto a log server on the internal log server or media device.	4		
10.5.5 Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	4		

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.			
10.6 Perform the following:			
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD, or that could • impact the security of CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	4	Analysis daemon	Analysis daemon can be used to automatically identify anomalies, suspicious activities, misconfigurations, application errors or possible intrusions by analyzing log messages. It uses rules that are based on string patterns or correlation rules. They can be customized to generate an alert when an event (log message) occurs. Analysis daemon can also be used to store an audit trail history of events received from the deployed agents.
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	4		
10.6.3 Follow up exceptions and anomalies identified during the review process.	4		

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	4		
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	4	Rootcheck	Rootcheck module can be used to ensure audit and security policies are in use, monitoring access to network resources and cardholder data.

PCI DSS Requirements v3.2.1	Milestone	tbSIEM component	How it helps
Requirement 11: Regularly test security systems and processes			
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.	2	Analysisd Rootcheck	Analsysisd detects attacks by inspecting log messages and rootcheck capabilities can be used to alert if malware is detected.
PCI DSS Requirements v3.2.1			
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).			
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.			
Keep all intrusion-detection and prevention engines, baselines,			

and signatures up-to-date.			

PCI DSS Requirements v3.2.1	Milestone	TbSIEM component	How it helps
Requirement 12: Maintain a policy that addresses information security for all personnel.			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	6	Rootcheck	Rootcheck can be used to ensure remote-access technologies are configured to automatically disconnect sessions after a period of inactivity.
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	6	Rootcheck	Rootcheck can be used to alert if a remote-access technology has been activated (e.g. RDP) or deactivated.
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data to be protected in accordance with all applicable PCI DSS Requirements.	6	Logcollector Analysis daemon	A combination of audit policies and centralized logging and analysis can be used to detect personnel accessing cardholder data.
12.10.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	2	Analysis daemon	Analysis daemon is the component that generates intrusion detection, log analysis, rootcheck and file integrity monitoring alerts. As well, it centralizes events and prioritize alerts, making them available for incident response teams.

FOR MORE INFORMATION

About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

Certificates:-

ISO 9001

ISO 27001

ISO 20000

CMMi L3

ISO 15408-1

PinkVERIFY

Mail us at: sales@tech-bridge.biz

Address:- TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana