LOGmanager

> Central Log and Machine Data Repository

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager and PCI Data Security Standard v3.2 compliance

Whitepaper how deploying LOGmanager helps to maintain PCI DSS regulation requirements

Many organizations struggle to understand what and where PCI DSS controls are required and how to recognize, which systems and solutions help them to become truly compliant. This whitepaper explains, how some important parts of the PCI DSS requirements can be achieved by implementing proper Security Event Management based on LOGmanager.

Brief overview for CISO/CIO – PCI DSS and LOGmanager relation

PCI Security Standards Council®

The **PCI DSS** (Payment Card Industry Data Security Standard) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. Shortly, it is a set of requirements, testing procedures and guidance's for those procedures, that each organization maintaining and processing payment card data need to comply with. PCI-DSS is divided into 12 areas and full document is freely available online on this website: https://www.pcisecuritystandards.org/ for review and study.

LOGmanager was developed as a „single pane view" system for centralised logmanagement for all machine generated data within organization. In a first step, LOGmanager listen, read, unifies and provide long term storage for logs and events from active network elements, security devices, operating systems and application software. Then it, in near real time, transform data into well-defined powerful database that is accessed by operators via set of predefined dashboards and structured and fulltext searches with graphical display of results. It also provides strong application interface to allow integration with other tools that company use for monitoring and security purposes.

LOGmanager helps organization mostly with, but not restricted to, PCI DSS area of Requirement 10: "Track and monitor all access to network resources and cardholder data". It provides logging mechanisms and the ability to track user activities which are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of all machine data in LOGmanager „single pane view" allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without full system activity logs engine which LOGmanager delivers. Shortly, it is an all-in-one log collection, storage and analysis appliance for cost-effective automation of PCI audits and proactive protection of cardholder data.

PCI DSS requirements and how LOGmanager helps to achieve them

AREA 1 - Build and Maintain a Secure Network and Systems

#	PCI DSS Requirement	LOGmanager response
1.2.x	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	With the LOGmanager capacity to parse and analyze firewall rule logs and router access list logs, LOGmanager can help to identify which network flows are blocked or permitted. By delivering fast analysis how to tune configuration of those devices, it helps to restrict any flows that are not mandated by trusted operations.
1.4.x	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.	With the LOGmanager capacity to observe operations of personal firewall software, it can help to detect improper operations including malfunction, configuration changes and alteration from company personal firewall policy. It also allows to centrally collect and analyze logs and event from those solutions and create proper alerts.

AREA 2 - Do not use vendor-supplied defaults for system passwords and other security parameters

#	PCI DSS Requirement	LOGmanager response
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	LOGmanager can detect and create an alert on using default accounts, that should not be used or have a special or privileged access rights not allowed on systems.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	LOGmanager parse machine data from major Wireless vendors including its SNMP traps. It can detect and alert on configuration changes, improper modifications and violations of wireless access policies. Brute force attacks can be detected and notified.

#	PCI DSS Requirement	LOGmanager response
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	LOGmanager can help to detect various sources using multiple services.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	LOGmanager can create a report of systems detected in defined security zone and notify about new systems appearing in monitored zones in PCI DSS scope.

AREA 5 - Protect all systems against malware and regularly update anti-virus software or programs

#	PCI DSS Requirement	LOGmanager response
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 .	LOGmanager can detect and notify when logs contain information about malfunction or disabled features on common antivirus software. Dashboard displaying in the near real-time can be created to present status of antivirus software deployed in PCI DSS environment.
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.	Same as above.

AREA 6 - Develop and maintain secure systems and applications

#	PCI DSS Requirement	LOGmanager response
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.	LOGmanager can detect uptime of server platforms, installation of security patches and create a dashboard displaying the least updated systems.
6.3	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	LOGmanager can detect and create an alert on using test or custom application accounts, that should not be used on production systems.

AREA 10 - Track and monitor all access to network resources and cardholder data

Area, where LOGmanager add the most value to PCI DSS regulatory scope.

#	PCI DSS Requirement	LOGmanager response
10.1	Implement audit trails to link all access to system components to each individual user.	If LOGmanager is designated destination for audit trails, security operator can quickly determine resources, each individual user access from system components under PCI DSS scope.
10.2.x	Implement automated audit trails for all system components to reconstruct the following events: .1 All individual user accesses to cardholder data .2 All actions taken by any individual with root or administrative privileges .3 Access to all audit trails .4 Invalid logical access attempts .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 .6 Initialization, stopping, or pausing of the audit logs .7 Creation and deletion of system-level objects.	If properly implemented on system event sources, LOGmanager collect, parse and properly display those events. Subsequently, alerts can be created on required events appearance, so security operator is promptly notified.
10.3.x	Record at least the following audit trail entries for all system components for each event: .1 User identification .2 Type of event .3 Date and time .4 Success or failure indication .5 Origination of event .6 Identity or name of affected data, system component, or resource.	If properly implemented on system event sources, LOGmanager record those audit trail entries.
10.4.x	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	LOGmanager by default do not trust the time received from sources and add its own timestamp based on exact time obtained from redundant NTP time sources. Both originator timestamp and LOGmanager timestamp are recorded with each event received.

#	PCI DSS Requirement	LOGmanager response
10.5	Secure audit trails so they cannot be altered.	LOGmanager does not allow any modifications or erase of collected logs and events. It operates in read only mode, once data are written to its database. Only option to delete the collected data is via “Factory-default” function under super-admin access rights with full physical access to the LOGmanager. If LOGmanager database storage space is reached, LOGmanager operator is notified and roll-over storing of the event start. LOGmanager is designed to store data for at least 12 month while reaching its full input performance.
10.5.1	Limit viewing of audit trails to those with a job-related need.	LOGmanager provide possibilities to constrain user interface as well as data sources, available to users with limited rights.
10.5.2	Protect audit trail files from unauthorized modifications.	Same as in # 10.5 .
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	LOGmanager is the solution providing such functionality.
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	LOGmanager is the solution providing such functionality.
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).	Same as in # 10.5 .
10.6.x	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*.	LOGmanager is the platform designed for such activity.

AREA 11 - Regularly test security systems and processes

#	PCI DSS Requirement	LOGmanager response
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Modern wireless access systems provide a functionality to detect and log unauthorized devices. LOGmanager can collect such information and create automated alert.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	LOGmanager collect change notifications and can alert security operator. Dashboard for config change logs is present.