LOGPOINT

Meeting Information Security Logging Standards with SAP Security

Overview

Lack or deficiencies in logging and analysis may prevent organizations from being compliant towards legislation and regulations as well as allowing attackers to hide their location, malicious software, and activities on victim machines.

Purpose & Objectives

The primary objective with this Security Logging standard is to ensure individual accountability and to enable investigation and collection of evidence for incidents, such as access violations, malware and intrusion attacks and fraud. The secondary objective is to provide the ability to provide evidence of compliance against legal requirements and internal as well as external demands. The standard defines the logging requirements to support the primary and secondary objective.

Scope

This standard is valid for all Business Applications and IT Infrastructure owned or used by organizations classified with MEDIUM, HIGH or ENTERPRISE criticality level. All Internet facing systems as well as any systems containing personal data, confidential or strictly confidential information need to enable logging in accordance with this standard.

The following limitations apply for this standard:

- Logging of clients and mobile devices are not included
- Detailed legal requirements are not included – each site and business application should ensure that they fulfill any legal requirements applicable

The reason for logging Business Applications is to enable detection of application logic tampering and data breach investigations.

The reason for logging IT Infrastructure is to enable detection of things like lateral movement, common hacker tools (e.g., Mimikatz), ransomware, command and control software, and phishing campaigns.

References

Document	Chapter, section
ISO 27001:2013 provides control A.12.4	Annex A.12.4 Logging and monitoring
ISF The Standard of Good Practice 2020	TM1.2
NIST Special Publication 800-92	Section 3 and 5
Information Classification Standard	Section 2: Information Classes

Definitions

The following terms are used in this standard.

Term	Description
Should	This word is used to express an obligatory requirement that should be fulfilled.
Recommend	This word is used to express that there may exist valid reasons to ignore a particular item, but the full implications should be understood and carefully weighed before choosing a different course.
Malware	Malware can include computer viruses, worms, trojan horses, spyware, rootkits, botnet software, keystroke loggers, ransomware, crypto miners, adware and malicious mobile code.
Server	Servers are computers that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.
Security Application	Security Applications is the system of hardware, software, facilities and service components that ensures the security of Business Applications and IT Infrastructure. Security Applications includes but are not limited to: • Antimalware • Firewall • IDS/IPS
Business Application	A Business Application is any software or set of computer programs used by the business to perform various business functions. Business Applications includes but are not limited to: • Application • API • Web service
IT Infrastructure	IT infrastructure is the system of hardware, software, facilities and service components that support the delivery of Business Applications and IT-enabled processes. IT infrastructure includes but are not limited to: • Remote Access Gateway • Wireless Access Point • Proxy-Server • Authentication Server / Identity Store • NetFlow • Printer • SMTP • Active Directory • DNS • DHCP • IIS • Server HW • Server OS • Database
Entry management system	A tool that authorizes a person's identity before being admitted entrance to e.g., organizations' premises, Server room or other sensitive area, to avoid security breaches.
Industry-Standard Encryption Protocols	By Industry-Standard Encryption Protocols we point towards the latest NIST's Cryptography Standardization.

Logging Requirements

General

Administrators or any other system actor should not be allowed to delete or deactivate logs of their own activities, where possible. Logs should be stored in a tamper free environment, separate from the log source, to ensure the integrity of the logs at all times.

Stored log data should be protected against:

- Modification
- Deletion
- Insertion
- Unauthorized reading

All activities in the log system should be fully traceable. Any logs containing sensitive information and personally identifiable information should be handled in accordance with organizations' Data Protection Policy and Privacy by Design Standard.

All security logs are recommended to be transferred to organizations' central SIEM-solution, if possible.

The following general logging requirements should apply when applicable:

Requirement	Description	LogPoint for SAP
Event logging	Event logging should always be turned on and protected from accidental or deliberate overwriting. Mechanisms should be established to ensure that event logging continues with as little or no disruption at all times. For explanation of what should be covered by the event logging, see "Actions included in logging" and "Logging identifiers".	LogPoint for SAP Extended checks System parameters and other system settings regarding logging infrastructure settings. ➔ Product coverage: **LogPoint for SAP Extended** LogPoint for SAP HANA queries and chack (among others) the existence and settings of SAP HANA database audit trail. ➔ Product coverage: **LogPoint for SAP HANA**
Entry management system	All entry management systems should log both entry logs, access logs to the system itself as well as any changes made in the system.	n/a
Time	It is important that accurate time is recorded in the logs. Therefore, the following requirements regarding time recording should be secured, when possible: • System clocks should be synchronized from NTP • UTC-time should be utilized in all logs • Timestamps should be identified with time zone	LogPoint for SAP extracts events in UTC format ➔ Product coverage: **LogPoint for SAP Extended, LogPoint for SAP Light and LogPoint for SAP HANA**
Extend logging	It is recommended that there is a possibility to increase logging, for example if a breach of security is investigated.	In LogPoint for SAP Extended, with the help of Enhancement Spots, the Log Extraction of e.g. Change Logs can vary and can be increased in time when the system is open for changes. This does only apply for log extraction, but not for changing logging settings in SAP ➔ Product coverage: **LogPoint for SAP Extended**
Language	All loggings should be done in English	All logging is done in English ➔ Product coverage: **LogPoint for SAP Extended, LogPoint for SAP Light and LogPoint for SAP HANA**
Log transfer	Any log transfer done outside of organizations' internal network should utilize encrypted communication using industry-standard encryption protocols to ensure confidentiality. Log transfer done on organizations' internal network should be encrypted if it contains strictly confidential information.	LogPoint for SAP temporarily stores events in log files on the CORE server. Forwarding the logs can be done via SIEM forwarder technology, syslog forwarder like syslog-ng or LogPoint for SAP forwarder technology. Encryption possible via underlying infrastructure's options.

Requirement	Description	LogPoint for SAP
Criticality Level	The lowest information classification for all collected log files should be Confidential Information. This implies that all handling of collected log files and information should be treated accordingly. Specifically, it should be secured that captured log data should be protected against: • Modification • Deletion • Insertion • Unauthorized reading	LogPoint for SAP collects and immediately forwards log information to SIEM when receiving the log information on the Core Server. The storage of logs on the CORE server is only temporarily, and mainly handled by the SIEM system.
Actions included in logging	The logging should make it possible to identify the following actions: • Authentication successes and failures • Authorization successes and failures • Addition, modification, or deletion of users - What has been changed, when and by whom? • Use of system administrative privileges • Access by application administrators • All actions by users with administrative privileges • Activation and deactivation of security applications such as antimalware and intrusion detection systems • Actions done in applications by users • What Confidential Information has been changed (added, modified, deleted), by whom, when, and from where • What Strictly Confidential Information that has been viewed, by whom, when, and from where	Authentication (success, failure) is protocolled in e. g. Security Audit Log or STAD data (transaction access log) ➔ Product coverage: **LogPoint for SAP Extended** and **LogPoint for SAP Light** Addition, modification or deletion of users are stored in the Security Audit Log ("that" something happened: e.g. Authorization of user changed). What exactly happened (assignment of which Roles and Profiles) are stored in Change Documents ➔ Product coverage: full details (Change Documents) via **LogPoint for SAP Extended** Administrators or Firefighter access can be monitored by Light as well as Extended. Extended will allow more detailed report of activities resp. identification of activities as it extracts more log sources than Light. ➔ Product coverage: **LogPoint for SAP Extended** and **LogPoint for SAP Light** (more details available) Confidential information changed: This is protocolled in SAP Table Change Logs, SAP Change Documents (only available by Extended) ➔ Product coverage: **LogPoint for SAP Extended** Read Access of Confidential information: Precisely only available via the SAP Read Access Log (SRALMANAGER). LogPoint for SAP Extended extracts the SAP Read Access Log LogPoint for SAP helps with deployable configuration of the SAP Read Access log in terms of GDPR (access to personal data).

Requirement	Description	LogPoint for SAP
Logging identifiers	The logging should contain the following **identifiers**: • Unique ID of user, which should make it possible to identify a physical person or when that is not possible, used account • Accessed resources, e.g., IP-addresses, System-IDs, Documents, Webpages, Images • Source of access, e.g., IP-address, System-ID • Date and Time as well as Time Zone • Log Source System ID, e.g., IP-address, Server-name • Log Source Location, when applicable • Log Source Application Name, when applicable • Assigned user privileges, when applicable • Accessed files and access types: o Read o Modify o Delete o Create	The logs contain the SAP User Id. Dialog accounts are mapped to physical persons. With a cross-correlation of AD information in SIEM, the SAP User can be correlated with a physical person. Or usage of obsolete SAP accounts can be detected SAP logs the e. g. access to transactions, download of data. Only Extended can extract the entire information of the Security Audit Log information (source IP/terminal, Transaction Code for all events, Program name for all events). The remote API (Light uses) for the SAP Security Audit Log does partially not provide terminal information (not at all), TCODE information or Program names (for certain events). ➔ Product coverage: Full details in Security Audit Log only available in **LogPoint for SAP Extended**

Log Format

In case there is a possibility to select or design the log format, the recommended log format to use is JSON (JavaScript Object Notation). This log format is compact and lightweight, and simple to read and write for both humans and machines. It can be parsed by nearly all programming languages, even those that don't have built-in JSON functionality. JSON is a universal format using Unicode encoding and thereby supporting almost any operating system.

Additional Requirements for Business Applications

The additional requirements and recommendations for Business Applications should be applied to production environments or environments where production data containing personal data or Strictly Confidential is used.

Requirement	Description	
Input validation	Input validation failures e.g., protocol violations, unacceptable encodings, invalid parameter names and values	
Output validation	Output validation failures e.g., database record set mismatch, invalid data encoding	
Session management failure	Session management failures e.g., cookie session identification value modification	
Startup and shutdown	Application and related system startups and shutdowns should be logged.	
Use of higher-risk functionality	The following high-risk functionality should be logged: • changes to privileges • assigning users to tokens • adding or deleting tokens • access to payment cardholder data when applicable • use of data encrypting keys when applicable • data encryption key changes when applicable • creation and deletion of system-level objects • data import and export including screen-based reports • submission of user-generated content - especially file uploads	SAP security Audit Log only protocols "that" something happened to accounts. – Authorizations of user changed The details what exactly happened to the account (Assignment of privileges, changes of user type, …) is available in Change Documents of user and Change Document Object (SCDO) IDENTITY. ➔ Product coverage: Details of Change Documents are only available via **LogPoint for SAP Extended**
Legal and other Opt-ins	Legal and other opt-ins e.g., permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications	
Code changes in production	Addition, modification, or deletion of application code/configurations – What has been changed, when and by whom?	Code changes are deployed via SAP STMS (SAP Transports) LogPoint for SAP Extended scans released and imported transports using the SAP Code Inspector LogPoint for SAP Extended scans Transports for critical objects, such as R3TR ACGT (Assignment of Roles) ➔ Product coverage **LogPoint for SAP Extended**

Recommendation	Description	LogPoint for SAP
Errors	It is recommended to log application errors and system events e.g., syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection.	SAP Basis near error log is the SAP System Log (SM21), ➔ Product coverage: **LogPoint for SAP Extended** and **LogPoint for SAP Light** System Dumps, RFC Connection failure, system resource bottlenecks, job failure and others are important aspects of monitoring SAP availability and system health. ➔ Product coverage: Enterprise (IT Service Intelligence for SAP) SAP Application logs contain e.g. Authorization failure in digital signature processes which points to erroneous process or manipulation ➔ Product coverage: **LogPoint for SAP Extended**
Others	It is recommended that the following events are logged if it will provide useful information: • Sequencing failu re • Excessive use • Data changes	Data changes are protocolled in Table Change Logs or Change Documents ➔ Product coverage: **LogPoint for SAP Extended**

High Privileged Accounts

Activities of high privileged accounts, with extra ordinary capabilities in an environment, such as Azure Global Administrators or Domain Admins, should have extensive logging.

Log Retention Requirement

Log Retention, as well as analysis of logs inside SAP is a difficult task. Log retention is recommended to be realized in external Log Management and SIEM systems like LogPoint SIEM. This technology ensures the performant access to log data, not only near-real-time analysis but also the performant analysis of "old" data, e.g. for forensic analysis reasons.

The default log retention period at any organizations is 365 days, except for financial systems which is 18 months, but legal requirements and regulatory compliance should always have precedence. Even though logs are stored on a separate system, the logs should be retained locally on the system for a minimum of 14 days. Exceptions to the default log retention period can be approved by Information Security Department. Additional demands can be decided by Information Security Department based on risk assessment.

Below are log retention requirements for some of the major compliance regulations.

Regulation	Retention Requirement
HIPAA	7 years
PCI DSS	1 year
SOX	7 years
ISO 27001	3 years
FISMA	3 years
GPG 13	3 + months
NERC CIP	3 years
GLBA	6 years
DoDI 8500.2	5 years
NIST	3 years

Handling of Collected Logs

The logging function needs to meet the following requirements on storage and storage media:

- Storage media that is no longer used should be destroyed or erased so that the information is impossible to recreate.
- During external transportation, log information should be encrypted

Logs should be reviewed periodically.
Reviews of event logs should be:

- Supported by documented standards/procedures
- Based on an informed assessment of the potential business impact of particular events
- Conducted using as much automated tools as possible

It is the system owner's responsibility to plan and perform reviews of their logs. It is the Information Security Department's responsibility to advice and agree on the handling of collected logs.

Reviews of logs should be done minimum every 6 months, but legal requirements, regulatory compliance and security requirements should always have precedence. For example, The Payment Card Industry Data Security Standard (PCI DSS) mandates daily log review procedures.

The purpose and goal of the log reviews is to detect abnormal or suspicious activities as well as adherence to regulatory requirements or compliance towards an organizations' standards or external standards.

All detected security breaches should be reported in accordance with an organizations' Incident Management routines.

Reporting and Auditing

All logs should be readily available for auditing purposes whenever necessary upon request.

LOGPOINT

About LogPoint

LogPoint is committed to democratizing data insight and making the complex accessible. Our innovative SIEM and UEBA ML technology accelerate cybersecurity detection and response, giving customers the freedom to collaborate and the insight to adapt. We enable organizations to convert data into actionable intelligence: supporting cybersecurity, compliance, IT operations and business analytics. Our commitment to quality and security is documented by our EAL 3+ certification. LogPoint is receiving stellar reviews by cybersecurity professionals and is recognized by leading industry analysts. For more information, visit **www.logpoint.com**

Contact LogPoint

Contact LogPoint If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution, don't hesitate to contact us at **www.logpoint.com/en/contact/**

For more details on LogPoint for SAP please visit **https://www.logpoint.com/en/product/logpoint-for-sap/**

TRUSTED BY MORE THAN 1,000 ENTERPRISES

KONICA MINOLTA CAPTIVATE BOEING GoSecure RÉMY COINTREAU

AWARDS AND HONORS

Gartner peerinsights customers' choice 2019 ™

Gartner Peer Insights

Gartner

Gartner Magic Quadrant

GOLD MEDALIST Software Reviews 2020

SoftwareReviews Data Quadrant

For more information, visit logpoint.com
Email: sales@logpoint.com

LOGPOINT