LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

ISO 27001:2013 and LOGmanager

Integration guide

Abstract

Every organization uses multiple security measures to establish and maintain protections against threats such as malicious actors, natural disasters, or IT operational incident. Unfortunately, due to the complexity of the subject and sheer number of controls to implement, security tends to be disorganized or even lacking in critical areas.

ISO 27001:2013 is an international standard aimed to provide clear requirements for establishing, implementing, maintaining, and continually improving Information Security Management System (ISMS). Having an ISMS implemented in accordance with ISO 27001:2013 is a proof of organization security maturity. There are multiple reasons to go for ISO certification – some companies use it to comply with various laws and regulations, standards, SLAs - others just to prove to their clients that they take security seriously.

Whatever the reason, fulfilling every objective of ISO 27001:2013 is not an easy task. There are over 100 objectives described by the standard, covering multiple areas of organization operations, ranging from policies and procedures, human resources, physical control, assets security, to more IT focused controls such as logging and monitoring, access control, cryptography, or malware.

There is no single solution which will solve all the problems you might face during implementation process. Generally, there is no easy way to do it – only the right way, which is going step by step. Of course, that does not mean we should not be looking for external solutions to help us. SIEM systems such as LOGmanager, due to their holistic view into many parts of the IT infrastructure, are known to be a great aid in achieving compliance with various standards and regulations, by helping us meet some of the controls, or even fulfilling them completely.

Goals of this document

The goal of this document is to provide clear instructions which ISO 27001:2013 objectives can be fulfilled or at least supported by LOGmanager.

LOGmanager is a SEM/SIEM tool, which gathers logs from every device in the infrastructure, stores them in secure and unmodifiable way for long time, and enables fast search and visualization. It can also alert on defined conditions and correlate between events coming from different sources. Thanks to described capabilities it is a perfect system for storing audit trails of activities (which is required by multiple ISO objectives), alert on threats and provide fast and secure access to log data .

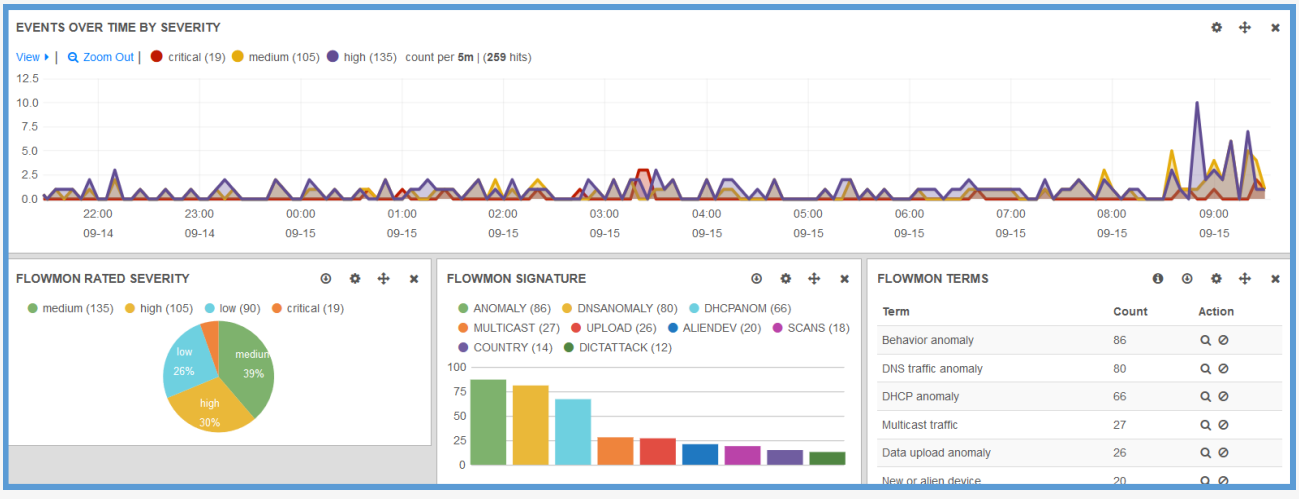

Figure: Preview of Flowmon data visualization in LOGmanager

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.6.2 Mobile Devices and Teleworking		
Objective: To ensure the security of teleworking and use of mobile devices.		
A.6.2.1 Mobile device policy	A policy and supporting security measures need to be adopted to manage the risks introduced by using mobile devices.	Gather logs from MDM/VPN/Directly to track device usage and location.
A.6.2.2 Teleworking	A policy and supporting security measures must also be imple-mented to protect information accessed, processed, or stored at teleworking sites.	Gather logs from VPN and devices to track user logon/ logoff and location. Gather logs from AV to monitor for threats. Alert on critical events such as brute force logging attempts or suspicious logon source IP (ex. unexpected country).
A.9.1 Business requirements of access control		
Objective: To limit access to information and information processing facilities.		
A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Gather logs from Domain Controller/VPN/Wireless Devices to track successful/unsuccessful authentica-tion events and confirm access control work as expected. Alert on unauthorized access attempts.

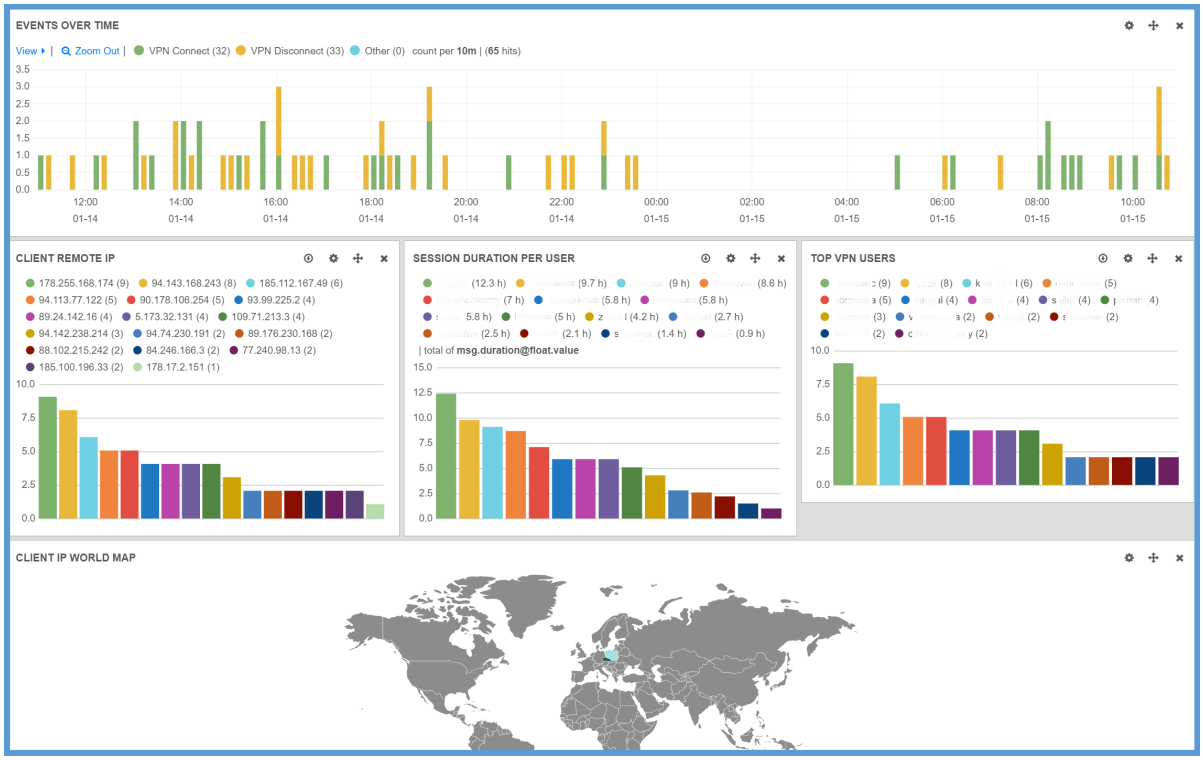

Figure: SSL VPN statistics—session duration, top VPN users, GeoIP.

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.9.2 User access management		
Objective: To ensure users are authorised to access systems and services as well as prevent unauthorised access.		
A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Gather logs from Domain Controller to track account registration/de-registration/suspension. Alert on usage of suspended or deleted accounts. Forward a copy of audit log confirming a registration/de-registration/suspension action to be saved in ticketing system as proof.
A.9.2.2 User Access Provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Gather logs from Domain Controller to track account rights provisioning/de-provisioning. Forward copy of audit log confirming a provisioning/de-provisioning action to be saved in ticketing system as proof.
A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Gather logs from Domain Controller to track privileged account rights provisioning/de-provisioning. Monitor privileged account logon/logoff. Schedule privileged accounts usage report to satisfy review process (revoke elevated access if unused). Forward copy of audit log confirming a provisioning/de-provisioning action to be saved in ticketing system as proof.
A.9.3 User responsibilities		
Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1 Use of Secret Authentication Information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Monitor for accounts being used by more than one user (shared accounts).

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.9.4 System and application access control		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Monitor if data is being accessed by authorized users. Alert on unauthorized use.
A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Gather logon/logoff success/failure. Alert on account lockouts or brute force attempts.
A.9.4.4 Use of Privileged Utility Programmes	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Log usage of privileged utility programmes.
A.9.4.5 Access control to program source code	Access to program source code shall be restricted.	Collect access and change logs to code repositories.
A.10 Cryptography		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Log key management activities.
A.11.1 Secure areas		
Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.		
A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Log site entry/exit data from physical entry controls to provide audit trail.

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1 Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Gather logs from multiple security devices to monitor for threats in single console. Gather logs from AV and generate scheduled reports to prove periodic AV scanning process. Alert on detection of threats by security devices. Perform periodic threat hunting activities (ex. network traffic logs review for Command&Control channel). In case of incident use LM to perform root cause analysis (who, where, when, how).
A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Use LOGmanager to gather logs from any source in your infrastructure. Store them for as long as you need (depending on available LM disk space – but archivization on external storage is also possible). Use available or custom dashboards for logs visualizations to help with review process. Create own or use available alert templates to proactively monitor for threats.
A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Logs stored in LOGmanager database cannot be deleted or modified in any way.
A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged, and logs protected and regularly reviewed.	Use LOGmanager to gather privileged user audit logs from any source in your infrastructure. Monitor LOGmanager usage and changes. Use available or custom dashboards for logs visualizations to help with review process.
A.12.4.4 Clock synchronization	The clock of all relevant information processing systems within an organization or security domain shall be synchronised to single reference time source.	LOGmanager adds its own timestamp to every received message, thus ensuring time synchronization between all gathered logs.

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Gather logs from network devices. Alert on critical events. Correlate data from multiple sources to detect anomalies in network traffic.
A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network service agreements, whether these services are provided in-house or outsourced.	Gather logs from network devices. Using log visualizations review technical parameters and firewall rules. Alert on critical events and abuse (example: multiple failed logon attempts).
A.14.1 Security requirements of information systems		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Gather logs from Domain Controller and network devices. Alert on GPO changes and errors which could impact public services. Monitor for the unencrypted data communication over public network (example: FTP).

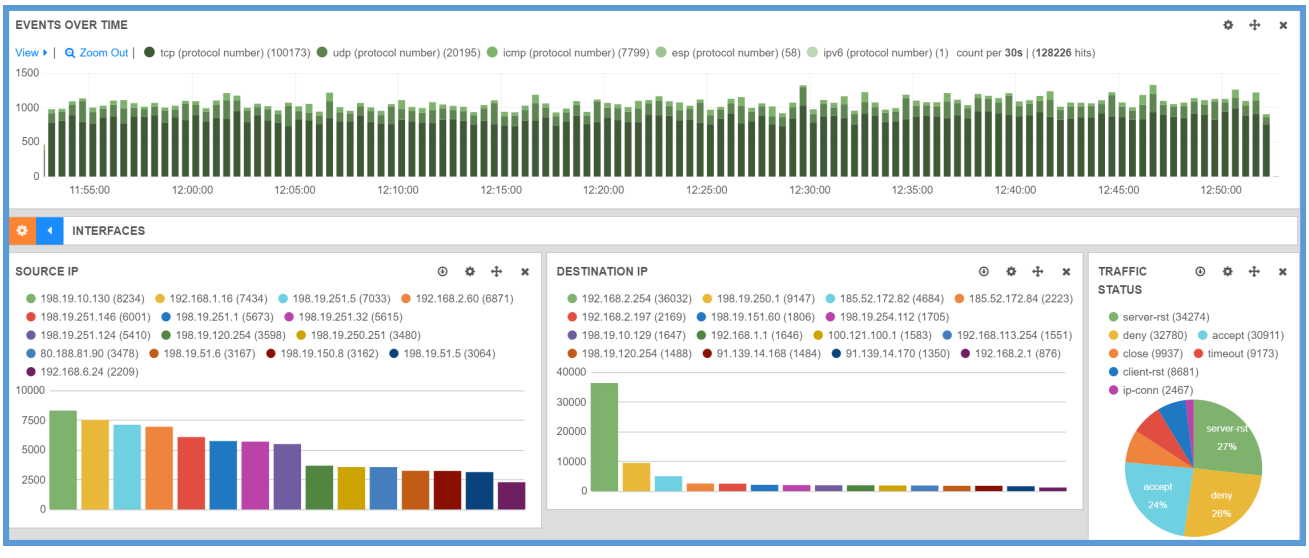

Figure: Network traffic visualization.

ISO27001 Control	Control Description	How LOGmanager helps achieve compliance
A.14.3 Test data		
Objective: To ensure protection of data used for testing.		
A.14.3.1 Protection of test data	Test data shall be selected carefully, protected, and controlled.	Gather appropriate operation data logs to prove when it was copied for testing purposes. Track state of the data (who is accessing it and when).
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Gather Network Devices/Domain Controller/File Access logs (and others if applicable) to monitor supplier activity.
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and affective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Alert on selected security events. Correlate between sources to detect potential security incidents. Gather logs from all security devices and aggregate them. Receive configured security alerts via email. Generate daily security incident report.
A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.	Logs gathered by LOGmanager cannot be tampered and hence can be used in incident investigation effort (root cause analysis). Access to sensitive information can be restricted to authorized personnel only.

Please, provide feedback and suggestions on this guide to: security-team@logmanager.com.

ABOUT THE MANUFACTURER

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. You can find selected customer references at www.logmanager.com. Our customers include not only government authorities, but also businesses of all sizes from all sectors, business corporations, banking organizations and more. Do not hesitate to contact us for more detailed customer references directly from your area of business. We will be happy to provide contacts to existing customers, who have agreed to be included on our list of references.