ManageEngine

Log360

Meet GDPR requirements with Log360, a comprehensive SIEM solution

www.manageengine.com/log-management

Table of Contents

Scope of this guide

This document elaborates on the GDPR's IT security requirements, the measures security administrators need to take to meet these requirements, and how Log360, a comprehensive security information and event management (SIEM) solution, can help you meet these requirements.

IT Security requirements of GDPR and Log360 features mapping

Article	What it means	What Log360 offers
Article 5 1(f) "..in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."	To prevent unauthorized processing, set up security configurations and monitor the changes to these configurations to detect unauthorized or unlawful access and processes. Audit all the operations performed on personal data to ensure the processes carried out in a legitimate manner.	Log360 provides out-of-the-box audit reports as below to ensure authorized access to personal data. • SQL server permission information • SQL server security changes • Created, altered, or deleted roles and users in Oracle database server. • Domain level permission changes • Group policy permission changes • Folder permission changes • Access control list (ACL) changes • User permission changes. Also, to audit the changes to privileged groups, the solution provides detailed information on: • Changes to security groups • Recently added members to security groups

<table>
<tr><td></td><td></td><td>These reports help security admins validate whether the change made to the privileged user groups are legitimate.

Further, Log360 offers audit reports on DML and DDL operations performed on SQL and Oracle databases to ensure that the processing of personal data stored in these databases is legitimate.

Available reports
● Selected, inserted, deleted, and updated tables.
● Executed and received commands
● Inserted, selected, updated, and deleted schemas.
● Created, altered, and deleted tables/databases.</td></tr>
<tr><td colspan="3">**Protip:** One of the best methods to prevent unauthorized or unlawful processing of personal data is to keep a check on network intrusions. With most of the security attacks aiming to steal personal data, it is mandatory that you try stop those attacks at its intrusion stage and continue protecting personal data.

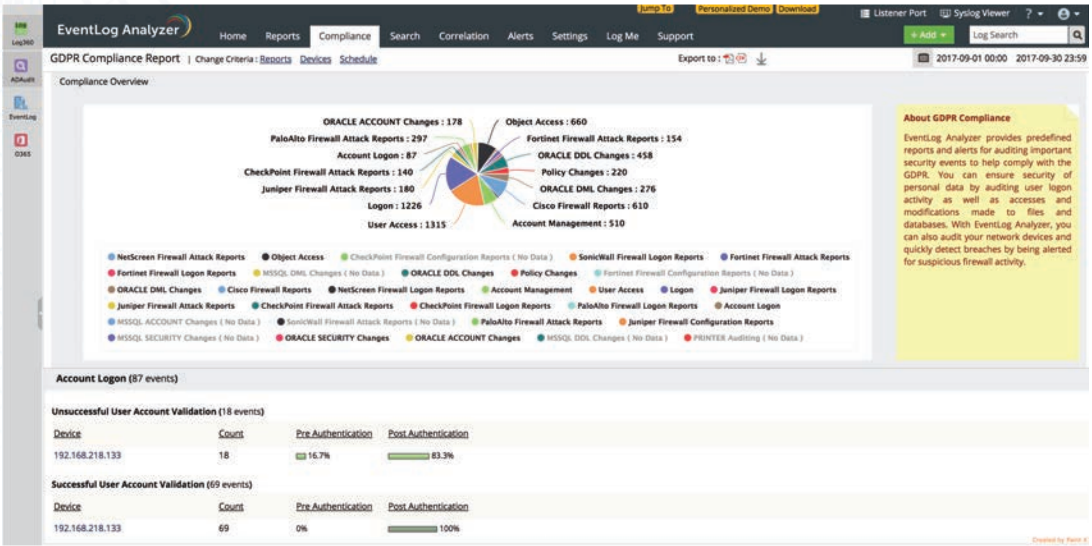
Log360 helps stop security attacks by identifying **malicious traffic into the network.** The solution's threat intelligence feature includes Global IP Threat Database and STIX/TAXII threat feed processor that are dynamically updated with known malicious sources (IP addresses, domains, and URLs). An attempt of intrusion from any of these suspicious sources will result in instant email/SMS notification with which you can block the traffic and safeguard personal data from being mishandled.</td></tr>
<tr><td>Article 25 (2) "...In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."</td><td>Ensure that personal data access is granted only for selected users and is not made accessible to everyone.</td><td>Log360 offers logon reports that help check who accesses the systems and applications that store/process personal data.</td></tr>
</table>

	Monitor the privileged user group that has permissions to access and process personal data.Changes to this group should be tracked and analyzed to avoid unauthorized access to personal data.	Additionally, the permission and security configuration change reports (specified above) will also help validate the personal data access.
Article 32 1(b) "... ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"	Regularly audit the systems (or servers) that store and applications (databases) that process personal data. Get notified in real-time upon any unauthorized access attempts, permission changes, privilege escalations, or unexpected shutdowns of servers and applications that could result in potential threats affecting their confidentiality or integrity.	To ensure confidentiality and integrity, Log360 offers real-time email notifications and exhaustive auditing reports on: • SQL server logon failures • Logon attacks on Windows Servers and SQL/Oracle databases • Reasons for logon failure to ascertain whether the attempt is authorized. To ensure integrity, the solution offers audit reports for: • File permission changes Critical group membership changes • ACL changes • Database role changes • Changes to privileged user accounts. To ensure availability and to speed up troubleshooting process, Log360 offers real-time email and SMS notification when : • A database server goes down. • A file server shuts down. • A service stops unexpectedly.

Article 33 (1) "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it,.."	Data breaches, if any should be detected and reported to supervisory authorities within 72 hours.	Log360, with its real-time correlation engine and threat intelligence platform, helps enterprises detect data breaches in real-time. The solution is capable of detecting data leakages for well-known attacks such as: • SQL injection • Ransomware attacks • Insider data stealing • Cross-site scripting • Denial of Service and Distributed Denial o Service. Further, the solution's custom rule building capability helps security admins create new rules to detect internal security attacks and policy violations as well. Log360's User and Entity Behavior Analytics (UEBA) detects anomalous activities of users and entities.This helps identify and mitigate insider threats, account compromise and data exfiltration attempts at an early stage.
Article 33-3(d) "....describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	Elaborate the efforts taken to mitigate the attacks and its adverse effects.	Log360's forensic analysis capability helps to ascertain the data breach'seffects including: • System/server affected by the breach. • Data that got affected. Further, the log search feature helps ascertaining the method of data breach, which is essential to mitigate the adverse effects and prevent future attacks of similar kind.

The comprehensive GDPR audit report

Apart from the above listed individual reports that help you probe into information that you need for meeting GDPR's security requirements, Log360 provides a comprehensive GDPR audit report, that aggregates and presents events across your network for easy auditing.


Log360
ADAudit
EventLog
O365
EventLog Analyzer
Home
Reports
Compliance
Search
Correlation
Alerts
Settings
Log Me
Support
Jump To
Personalized Demo
Download
Listener Port
Syslog Viewer
+ Add
Log Search
Export to :
ORACLE ACCOUNT Changes : 178
PaloAlto Firewall Attack Reports : 297
Account Logon : 87
CheckPoint Firewall Attack Reports : 140
Juniper Firewall Attack Reports : 180
Logon : 1226
User Access : 1315
Object Access : 660
Fortinet Firewall Attack Reports : 154
ORACLE DDL Changes : 458
Policy Changes : 220
ORACLE DML Changes : 276
Cisco Firewall Reports : 610
Account Management : 510
NetScreen Firewall Attack Reports
Object Access
CheckPoint Firewall Configuration Reports (No Data)
SonicWall Firewall Logon Reports
Fortinet Firewall Attack Reports
Fortinet Firewall Logon Reports
MSSQL DML Changes (No Data)
ORACLE DDL Changes
Policy Changes
Fortinet Firewall Configuration Reports (No Data)
ORACLE DML Changes
Cisco Firewall Reports
NetScreen Firewall Logon Reports
Account Management
User Access
Logon
Juniper Firewall Logon Reports
Juniper Firewall Attack Reports
CheckPoint Firewall Attack Reports
CheckPoint Firewall Logon Reports
PaloAlto Firewall Logon Reports
Account Logon
MSSQL ACCOUNT Changes (No Data)
SonicWall Firewall Attack Reports (No Data)
PaloAlto Firewall Attack Reports
Juniper Firewall Configuration Reports
MSSQL SECURITY Changes (No Data)
ORACLE SECURITY Changes
ORACLE ACCOUNT Changes
MSSQL DDL Changes (No Data)
PRINTER Auditing (No Data)
Created by Parit K

GDPR Compliance Report | Change Criteria : Reports Devices Schedule

2017-09-01 00:00 2017-09-30 23:59

Compliance Overview

About GDPR Compliance

EventLog Analyzer provides predefined reports and alerts for auditing important security events to help comply with the GDPR. You can ensure security of personal data by auditing user logon activity as well as accesses and modifications made to files and databases. With EventLog Analyzer, you can also audit your network devices and quickly detect breaches by being alerted for suspicious firewall activity.

Account Logon (87 events)

Unsuccessful User Account Validation (18 events)

Device	Count	Pre Authentication	Post Authentication
192.168.218.133	18	16.7%	83.3%

Successful User Account Validation (69 events)

Device	Count	Pre Authentication	Post Authentication
192.168.218.133	69	0%	100%

Salient features of Log360

- Auditing activities happening in business critical applications
- User behavior monitoring
- Active Directory change auditing
- Threat intelligence
- Real-time correlation with integrated incident management
- Automated log management
- Best-in-class forensic analysis

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

⤓ Download