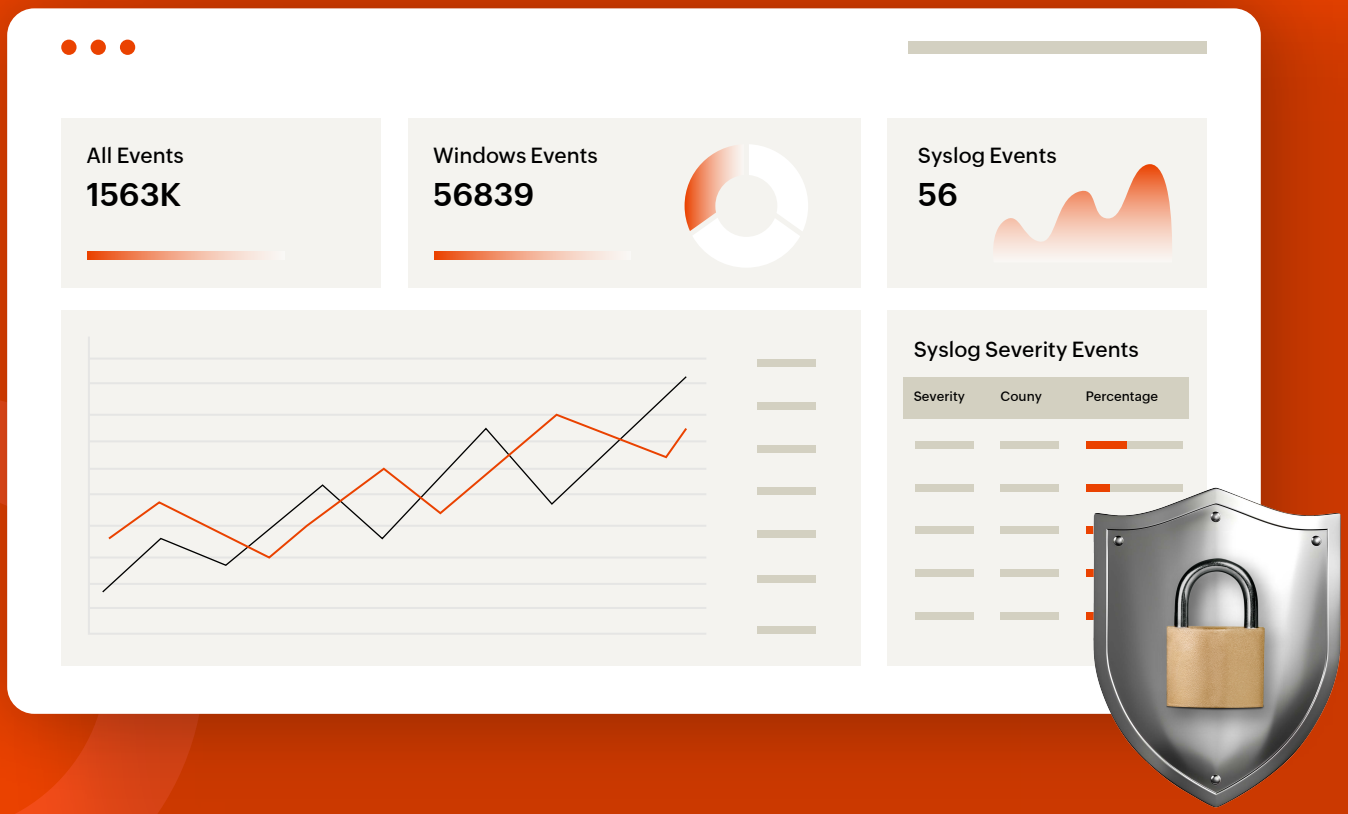
ManageEngine
Log360

10 critical audit reports for **IT security**



www.manageengine.com/log-management/

The fundamentals of security auditing

Ensuring your network's security operations are running smoothly requires regular reviews of security events. Today's threat landscape is characterized by increasing sophistication and frequency of cyberattacks, making security auditing more than a best practice, but a business imperative.

Security reports have always been a crucial aspect of IT security and compliance. In fact, several IT compliance regulations, such as the PCI DSS, the GDPR, and ISO 27001, expect organizations to maintain a well-defined system for auditing log data. To audit security events effectively, security teams should integrate this process into their daily operations. The optimal approach is to schedule reports using a security information and event management (SIEM) tool like ManageEngine Log360.

Log360 can aggregate and parse log data from various sources—servers, domain controllers, firewalls, and databases—and generate comprehensive reports. It provides detailed and actionable insights through a range of specialized reports. These reports not only enhance your visibility into potential security threats but also help demonstrate compliance to auditors.

Here are 10 crucial audit reports every security team needs

1

Privileged user monitoring

Different compliance regulations mandate that organizations maintain an audit trail of actions performed by administrators by logging all activities, such as logins, configurations, and privilege changes. These logs are analyzed for anomalies, ensuring any unauthorized or suspicious behavior is flagged. A transparent audit trail is essential for compliance with regulations like the GDPR and HIPAA and play a critical role in security investigations.

Log360's reports

Administrative User Actions | Privileges Utilized by User | Privilege Escalation

2

Data accesses and modifications

It is important to audit file server activity and track the access and modifications made to the data in it. Logging every interaction with your sensitive data, including who accessed or altered the data, when, and from where, is essential. The same approach should be applied to databases and other systems that store data. Make sure to also track changes to file permissions because these types of changes can expose sensitive data if left unchecked.

Log360's reports

File created | File modified | File deleted | File renamed | File permission changes | System file changes | File moved | Files copied and pasted | Folder permission changes | Folder audit settings changes (SACL) | Folder owner changes | Failed Attempt to Read/Write/Delete File

3

Network device monitoring

Activities across routers, switches, firewalls, and other critical components must be logged, capturing key data such as configuration changes, connection attempts, and traffic anomalies. Understanding the details of traffic passing through firewalls—including source, destination, and protocol—is vital, especially during forensic investigations after a breach. Unauthorized firewall policy changes or router configurations can expose networks to malicious sources. Every change must be audited and validated, as even minor modifications can impact network integrity.

Log360's reports

Router Configuration | Router Logon | Router Accepted/Denied Connections | Router Traffic Errors | Firewall Allowed/Denied Traffic | Firewall Threats | System Events

4

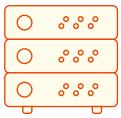
System events

System events, such as a server shutdown, restart, or new software installation, is often a key indicator of compromise (IoC) and must be closely monitored. These events can signal potential compromises and provide early warning signs of unauthorized access or malicious activity. Tracking system events enables organizations to quickly identify IoCs, address vulnerabilities, and prevent security breaches.

Log360's reports

Windows Startup | Windows Shutdown | Windows Restarts | Unexpected Shutdown | Software Installed | Software Updated | Software Uninstalled | Failed Software Installation | AD Database Corruption | Bad Disk Block | Hard Disk Failures

5



Web server activity

Web server activity, including access requests, configuration changes, site visitors, HTTP status codes, and file uploads and downloads, provides critical insights into server health and security. Monitoring web server logs is essential for identifying anomalies such as unusual traffic patterns or repeated failed login attempts, which may indicate an attack. You can go one step further and track known web server attacks such as cross-site scripting (XSS) and SQL injection.

Log360's reports

IIS W3C Web Server and Apache - Client Error | Server Error | SQL Injection | Cross Site Scripting | Directory Traversal | Site-wise Logs Trend | Malicious URL Request

6

Active Directory (AD) changes

AD changes, such as modifications to users, groups, computers, OUs, and GPOs, should always be audited in real time to protect organizational security. Unauthorized or improper changes can jeopardize security policies, such as moving a regular end user into the Domain Admins group, which results in unwarranted privilege escalation. Immediate detection and reversal of such changes are crucial to prevent potential data breaches and ensure the integrity of access controls and overall security posture.

Log360's reports

AD permission changes | AD object changes | DNS changes | Account management | Group management | GPO management

7

User behavior anomalies

UEBA analyzes patterns of user and entity activities to identify deviations from established norms and gives time-based, count-based, and pattern-based reports. For instance, if a user suddenly accesses sensitive data outside their usual scope or logs in from an unusual location, UEBA can flag these anomalies as potential threats. This behavioral analysis is crucial for detecting sophisticated threats that bypass traditional security measures, such as insider threats or compromised accounts, enabling timely responses and strengthening overall security posture.

Log360's reports

Successful Logon Anomalies | Data Upload Anomalies | Data Download Anomalies | Data Deletion | User Account Changes | System and Configuration Changes | Sensitive Data Access | Audit Changes

8

Threat intelligence and dark web monitoring

With evolving threats, it is important to have detailed insights into emerging threats, their source, category, and reputation score. Further, having visibility into the dark web and monitoring illicit forums allows for early detection of potential breaches and compromised credentials.

Log360's reports

External Threat | All Breach Data | Dark Web Breach Data | Botnet Leak Data | Supply Chain Breach | McAfee Threat | Detected Threats | Quarantined Threats | Allowed Threats | Top Threats Based on Source | Top Threats Based on User | Top Target Ports | Top Malware

9

External threat framework-based analysis

In today's threat landscape, you need more than basic, rule-based reports and alerts to monitor your network comprehensively. Reports based on the MITRE ATT&CK® framework correlate and map your network activities to adversarial tactics, techniques, and procedures (TTPs) used in real-world attacks. By analyzing these reports, organizations can identify vulnerabilities and strengthen their security posture against known adversaries. This approach enhances incident response capabilities, improves threat hunting, and ensures a proactive defense strategy.

Log360's reports

Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control

10

Cloud log monitoring

As organizations rapidly transition to cloud and hybrid infrastructures, cloud log monitoring reports become increasingly vital. These reports offer comprehensive visibility into complex, multi-environment setups by tracking user activities, access events, and configuration changes across both cloud and on-premises systems. This visibility is crucial for detecting unauthorized actions, ensuring compliance, and managing security across diverse environments.

Log360's reports

Salesforce | AWS | Azure | Google

Scheduling security reports and setting up alerts for critical issues ensures that threats are promptly identified and addressed. This proactive approach maintains oversight, meets compliance requirements, and strengthens your security posture. With the help of these 10 audit report types, your organization can achieve a resilient and secure IT environment.