ManageEngine
Log360

# 10 Crucial audit reports for IT security

## The fundamentals of security auditing

Ensuring smooth security operations requires regularly reviewing security events occurring in your network. Security reports always have been, and perhaps always will be, a crucial aspect of IT security and compliance. In fact, several IT compliance regulations, such as PCI DSS and ISO 270001, expect organizations to maintain a well-defined system for auditing log data.

Security teams must implement a process to audit security events as part of their daily operations. The best way to achieve this is by scheduling reports using a security information and event management (SIEM) tool. A SIEM tool can parse log data from different event sources—such as servers, domain controllers, firewalls, and databases—and generate reports that help you visualize vital security information. These reports will not only help you stay on top of security threats, but also help you demonstrate compliance to auditors.

# Here are ten crucial audit reports every security team needs:

## 1. Severity-based reports

Logs have severity levels that describe the state of importance of the message. Segregating and reviewing logs based on their severities is a well-established security best practice and is important for meeting different IT compliance mandates.

## 2. Login activity

You need to know who is logging on to workstations, servers, databases, and other systems. Tracking logon events will help you detect many attacks at their earliest stages because most attacks start with or involve logon events. Track both successful and failed logons and look out for repeated failed logons, which could be a security threat like a brute force password attack.

## 3. Administrator actions

Different compliance regulations require organizations to maintain the audit trail of actions performed by privileged users. This is because actions performed by administrators—who have elevated privileges and access rights—can inadvertently result in security violations.

## 4. Data accesses and modifications

Auditing file server activity in real time is a must to ensure integrity and confidentiality of data. File creations, deletions, accesses, modifications, and renames must all be tracked. The same approach should be applied to databases and other systems that store data.

> Make sure you're also tracking changes to file permissions because these types of changes can expose sensitive data if left unchecked.

## 5. Accepted and denied firewall connections

It's important to know the details about the traffic passing through your firewall. Traffic must be analyzed based on the source, destination, and protocol. This data also plays an important role during forensic investigation in the event of a breach.

## 6. System events

System events are an inevitable part of cyberattacks. While there are several system events that must be tracked, server shutdowns/restarts and installations of new software/services in particular are potential indicators of compromise (IoCs).

## 7. Web server activity

Web server usage including site visitors, requests, HTTP status codes, and file uploads/downloads must be audited to detect and mitigate threats as early as possible. Go one step further and track known web server attacks such as cross-site scripting (XSS) and SQL injection.

## 8. Active Directory changes

Active Directory changes should always be audited in real time. Changes made to users, groups, computers OUs, and GPOs can potentially jeopardize the security policy of your organization. For example, if a regular end user is moved to the Domain Admins group, it would result in an unwarranted escalation of privileges, which means this change needs to be reverted immediately.

## 9. Network configuration changes

Firewall policy changes can result in malicious sources gaining access to your network's resources. Ensure that router configuration changes as well as firewall rule additions, deletions, and modifications are all authorized. It's safe to say that any change in general is cause for concern and must be audited and validated.

## 10. User behavior anomalies

In today's threat landscape, you need more than basic, rule-based reports and alerts to comprehensively track insider threats. A comprehensive SIEM solutions comes with a user behavior analytics (UBA) component that uses machine learning techniques to analyze user behaviors and automatically detect anomalous user actions.

## Auditing made easy with ManageEngine Log360

Log360—an integration of EventLog Analyzer, a log management tool, and ADAudit Plus, a real-time Active Directory change auditing tool—is a comprehensive SIEM solution that comes with over 1,000 prebuilt audit reports, including reports from all ten crucial categories of security reports discussed above. Log360's carefully crafted, prebuilt parsing rules extract meaningful information from log messages to provide actionable insights to security teams.

All reports are automatically generated as soon as the devices added for monitoring start generating log messages. Going one step further, all reports can be associated with alerts. For example, you can configure alerts for security events of interest such as account lockouts, members getting added to privileged groups in Active Directory, and more. These alerts will be automatically sent to you via email or SMS.

## Out-of-the-box log auditing and reporting

Below are the typical log sources that customers add to Log360 for auditing:

- Workstations
- Servers (Windows/Unix)
- Domain controllers
- Databases
- Web servers
- Routers
- Switches
- Firewalls
- IDS/IPS
- Threat solutions
- Vulnerability scanners

Log360's features can help in all report categories mentioned above as well as many other categories not discussed here. For more details on where to access and schedule these reports or to learn more about Log360's extensive SIEM capabilities, contact our technical support team at **log360-support@manageengine.com,** or try the product yourself with a free trial.


## Kick-start your evaluation of Log360 with your free, 45-day license,

and instantly start generating reports and triggering alerts to boost the security of your network.

## About the author

Siddharth Sharath Kumar is an IT security and compliance specialist on ManageEngine's product marketing team. He writes articles and e-books, regularly hosts webinars on key IT security topics, and presents at ManageEngine's conferences and other industry events across the globe.