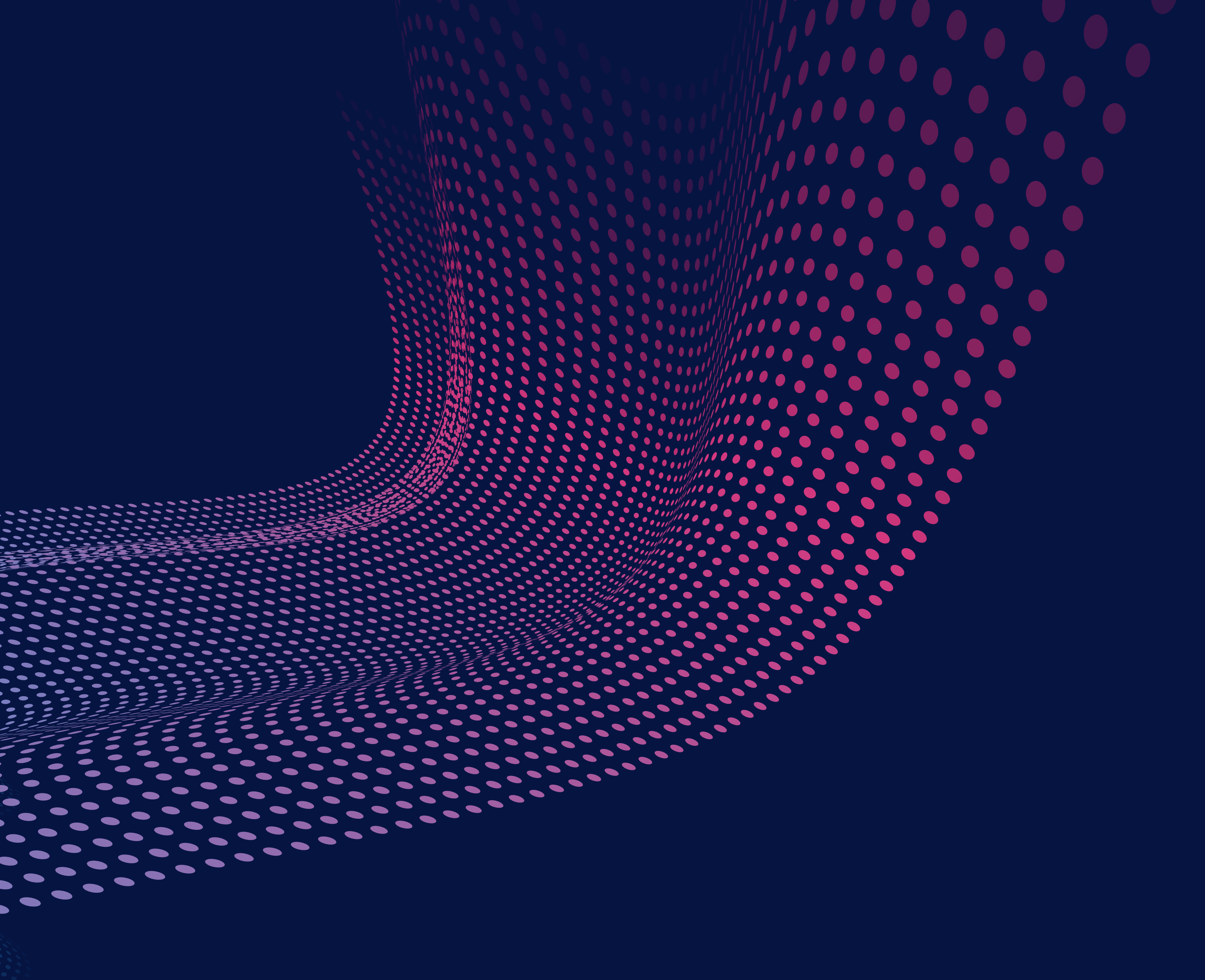
ManageEngine
Log360

ISO 27001

Alert profile recommendations for Log360



This document provides a list of alerts that must be configured in a SIEM solution to meet the ISO 27001 standard.

It is important to note that the priority levels assigned to each alert are based on general guidelines related to the ISO 27001 standard. However, each organization's specific context and circumstances may vary, and it is their responsibility to determine appropriate priority levels for their own alerts based on their individual risk assessment and security policies.

To ensure the effectiveness of security measures, it is recommended that organizations regularly review and update their security policies, procedures, and incident response plans to effectively detect, mitigate, and respond to potential security incidents.

Unauthorized access attempts

- ALERTS for unauthorized access attempts - network, systems, applications.
- ALERTS should also be generated for any events showing sensitive data has been accessed without proper authorization.
    - 5.15 Access control Control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
    - 5.18 Access rights Control Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed according to the organization’s topic-specific policy on and rules for access control.
    - 5.33 Protection of records Control Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
    - 8.12 Data leakage prevention Control Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information

Unauthorized access attempts

Unauthorized access attempts		
Windows		
	Failed software installations due to privilege mismatches	Attention
	Firewall Spoof Attack	Trouble
	Firewall SYN Attack	Trouble
	Locked users due to repeated logon failures	Trouble
	Replay Attack	Trouble
	Terminal Server Attacks	Critical
	Terminal Server Exceeds Maximum Logon Attempts	Trouble
	User Account Locked Out Error	Trouble
Windows Workstation		
	Failed Logons due to Bad Password	Trouble
	Failed Logons due to Bad UserName	Trouble
	Failed logons due to account expiry	Trouble
	Failed logons during non-working hours	Critical
	Failed Network Logons	Trouble
	Failed Remote Interactive Logons	Trouble
	Failed software installations due to privilege mismatches	Attention
	Firewall Spoof Attack	Trouble
	Firewall SYN Attack	Trouble
	Replay Attack	Trouble
	Terminal Server Attacks	Critical
	Terminal Server Exceeds Maximum Logon Attempts	Trouble
	User Account Locked Out Error	Trouble
Unix/Linux		
	Password Changes Failed	Attention
	Failed user additions	Attention
	FTP/SFTP Failed Logons	Attention
	Invalid User Login Attempt	Attention
	Repeated Authentication Failure	Attention
	Unsuccessful logon Failure with Long Password	Attention
AS400		
	Logon failure due to invalid passwords	Trouble
Barracuda, CheckPoint, Fortinet, Juniper, NetScreen, PaloAlto, Sophos		
	Possible Attacks	Trouble
	Critical Attacks	Critical

SonicWall		
	User Privilege Changed	Trouble
	Possible Attacks	Trouble
	Critical Attacks	Critical
ForcePoint		
	Attack	Critical
WatchGuard, H3C, F5, Stormshield, Huawei		
	All Attacks	Critical
FirePower, Meraki, pfSense		
	Possible Attacks	Trouble
Cisco		
	Bad authentication	Trouble
	Routing Table Attack	Trouble
	All Attacks	Critical
SQL Server		
	Unauthorized Copies of Sensitive data	Critical
	Credential Altered	Critical
	Password Reset Failed	Attention
	Password Changes Failed	Attention
	Privilege Abuse	Attention
	All Password Changes	Trouble
IIS W3C Web Server		
	Authentication Changes	Attention
	Password Changes	Attention
IIS W3C FTP		
	Authentication Changes	Attention
	AuthorizationRule Changes	Attention
	Password Changes	Attention
SAP ERP Audit Logs		
	Password Changes	Attention
PostgreSQL Logs		
	Password Changes	Attention
Linux File Monitoring		
	File Permission Changes	Attention
Windows File Monitoring		
	File Permission Changes	Attention

ESXi		
	Password Changes Failed	Attention
Nessus		
	Credential Failures Report	Attention
	Elevated Privilege Failures Report	Trouble

Malicious activity/events

- ALERTS for suspicious network activity, such as malware infections, data exfiltration, and malicious code execution.
  - 8.7 Protection against malware Control Protection against malware shall be implemented and supported by appropriate user awareness.

Malicious activity/events		
Barracuda		
	Possible Attacks	Attention
	Critical Attacks	Critical
	Email Attacks	Trouble
CheckPoint, Fortinet, Juniper, NetScreen, SonicWall, Sophos		
	Possible Attacks	Attention
	Critical Attacks	Critical
Unix/Linux		
	DoS Attack	Trouble
FirePower, Meraki, pfSense		
	Possible Attacks	Attention
Cisco		
	Routing Table Attack	Trouble
	All Attacks	Critical
SAP ERP audit Logs		
	Attack	Critical
PaloAlto		
	Possible Attacks	Attention
	Critical Attacks	Critical
	Spyware Download Detection	Trouble
	Vulnerability Exploit Detection	Trouble

Windows		
	Defender Malware Detection	Trouble
	Audit Events Dropped	Trouble
	DoS Attack Entered Defensive Mode	Trouble
	DoS Attacks	Trouble
	Downgrade Attacks	Trouble
	Event Logs Cleared	Critical
	Failed software installations due to privilege mismatches	Attention
	Firewall Flood Attack	Trouble
	Firewall Internet Protocol half-scan attack	Attention
	Firewall Ping of Death Attack	Trouble
	Firewall Spoof Attack	Trouble
	Firewall SYN Attack	Trouble
	Infected files detected by Symantec Endpoint Protection	Critical
	Replay Attack	Trouble
	Threat Detections by Mcafee	Attention
	Threats Detection by Microsoft Antimalware	Attention
	Threats Detection by Norton AntiVirus	Attention
	Threats Detection by Sophos Anti-Virus	Attention
	Threats Detections by ESET Endpoint Antivirus	Attention
	Threats Detections by Kaspersky	Attention
	Terminal Server Attacks	Critical
Windows Workstation		
	Audit Events Dropped	Trouble
	Defender Malware Detection	Critical
	DoS Attack Entered Defensive Mode	Trouble
	DoS Attacks	Trouble
	Downgrade Attacks	Trouble
	Event Logs Cleared	Critical
	Failed software installations due to privilege mismatches	Attention
	Firewall Flood Attack	Trouble
	Firewall Internet Protocol half-scan attack	Trouble
	Firewall Ping of Death Attack	Trouble
	Firewall Spoof Attack	Trouble
	Firewall SYN Attack	Trouble
	Infected files detected by Symantec Endpoint Protection	Critical
	Replay Attack	Trouble
	Threat Detections by Mcafee	Attention
	Threats Detection by Microsoft Antimalware	Attention

ForcePoint		
	Malicious Content Access	Trouble
ForcePoint		
	Malicious URL Request	Trouble
IIS W3C Web Server		
	cmd.exe and root.exe file executions	Trouble
	DoS Attack	Trouble
	Possible Malicious File Execution	Critical
	Possible Malicious URL Request	Trouble
SQL Server Audit Logs		
	Denial of Service	Trouble
	Dropped Database Audit Specifications	Attention
	Dropped Server Audit Specifications	Trouble
	Privilege Abuse	Critical
	Unauthorized Copies of Sensitive Data	Critical
	SQL Injection	Critical
Oracle		
	Denial of Service	Trouble
	SQL Injection	Critical
Printer		
	Insufficient Privilege to Print Documents	Attention
Linux FIM		
	File Permission Changes	Attention
	System File Changes	Attention
Windows FIM		
	File Permission Changes	Trouble
FireEye		
	Malware Object Events	Trouble
	Web Infection Events	Critical
Malwarebytes		
	Detected Exploits	Critical
	Detected Threats	Trouble
	Malicious Websites Blocked	Attention
	Quarantined Threats	Trouble
Symantec Endpoint Protection		
	Security Risk Found Reports	Critical
Trend Micro		
	Intrusion Prevention Event	Trouble
	Anti-Malware Event	Trouble

Nessus		
	Elevated Privilege Failures Report	Critical
Nexpose		
	Exploited Vulnerability	Critical
Qualys		
	Confirmed vulnerabilities	Critical
	Potential vulnerabilities	Attention

Configuration changes

- ALERTS for changes to important network devices, systems, and applications.
  - 8.9 Configuration management Control Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed

Configuration changes		
Unix/Linux		
	Cron Edit	Attention
	Password Changes	Trouble
	Syslog Stopped	Trouble
Barracuda		
	Clock Update	Attention
	Rules Added	Trouble
	Rules Deleted	Trouble
	Rules Modified	Trouble
CheckPoint		
	Clock Update	Attention
	Configuration Change	Critical
Cisco		
	Added Group policies	Trouble
	Changed user privilege levels	Trouble
	Clock Update	Attention
	Configuration Change	Critical
Fortinet		
	Admin Added	Attention
	Admin Deleted	Trouble
	Admin Modified	Trouble

	Configuration Change	Critical
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
HP		
	Clock Update	Attention
	Configuration Change	Critical
Huawei		
	Clock Update	Attention
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
NetScreen		
	Admin Added	Attention
	Admin Deleted	Trouble
	Admin Modified	Trouble
	Clock Update	Attention
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
PaloAlto		
	Package Installed	Attention
	Package Upgraded	Attention
SonicWall		
	Clock Update	Attention
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
	Rules Added	Attention
	Rules Deleted	Trouble
	Rules Modified	Trouble
	Rules Restored	Attention
	User Privilege Changed	Trouble
Sophos		
	Clock Update	Attention
	Rules Added	Attention
	Rules Deleted	Trouble
	Rules Modified	Trouble

WatchGuard		
	Admin Added	Attention
	Admin Deleted	Trouble
	Admin Modified	Trouble
	Clock Update	Attention
	Configuration Change	Critical
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
Windows		
	Event Logging Service Shutdown	Critical
	Kerberos policy changes	Trouble
	Registry Created	Trouble
	Registry Deleted	Trouble
	Registry Permission Changes	Trouble
	Registry Value Modified	Trouble
	Windows Firewall Group Policy Changes	Critical
	Windows Firewall Rule Added	Attention
	Windows Firewall Rule Deleted	Trouble
	Windows Firewall Rule Modified	Trouble
	Windows Firewall Settings Changed	Trouble
	Windows Firewall Settings Restored	Attention
	Windows Time Change	Trouble
H3C		
	Clock Update	Attention
	Configuration Change	Critical
	Rules Added	Attention
	Rules Deleted	Trouble
	Rules Modified	Trouble
Arista, ForcePoint, SAP ERP Audit Logs		
	Configuration Change	Critical
F5		
	Configuration Change	Critical
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
	Policy Status	Attention

IBM AS/400		
	Authority changes	Trouble
	Device Configuration	Attention
	Job changes	Attention
	Objects deleted	Trouble
	Ownership changes	Trouble
	System time changes	Trouble
	System value changes report	Attention
Stormshield		
	Admin Added	Trouble
	Admin Deleted	Trouble
	Admin Modified	Trouble
	Clock Update	Attention
	Rules Added	Attention
	Rules Deleted	Trouble
	Rules Modified	Trouble
Windows Workstation		
	Event Logging Service Shutdown	Critical
	Privilege Assigned to New Logon	Critical
	Registry Created	Trouble
	Registry Deleted	Trouble
	Registry Permission Changes	Trouble
	Registry Value Modified	Trouble
	System Restored	Critical
	Windows Firewall Group Policy Changes	Attention
	Windows Firewall Rule Added	Trouble
	Windows Firewall Rule Deleted	Trouble
	Windows Firewall Rule Modified	Trouble
	Windows Firewall Settings Changed	Trouble
	Windows Firewall Settings Restored	Attention
	Windows Time Change	Trouble
DB2 Logs		
	DB Configuration Changes	Trouble
	DBM Configuration Changes	Trouble
PostgreSQL logs		
	Database Maintenance Statements	Attention
	DataBase Role Altered	Trouble
	DataBase Role Created	Attention
	DataBase Role Dropped	Trouble

	Permission Granted	Trouble
	Permission Revoked	Trouble
IIS W3C FTP		
	AllConfiguration Changes	Trouble
	Authentication Changes	Attention
	AuthorizationRule Changes	Attention
	IPDOMAIN Changes	Attention
	Logging Changes	Attention
	RequestFiltering Changes	Attention
	SSL Changes	Attention
	UserIsolation Changes	Attention
	Password Changes	Attention
IIS W3C Web Server		
	Admin Authority Changes Report	Trouble
	All Password Changes	Critical
	Alter Database Permission	Trouble
	Altered Database Audit Specifications	Trouble
	Altered Server Audit Specifications	Trouble
	Altered server audits	Trouble
	Altered server roles	Trouble
	Application Role Altered	Trouble
	Application Role Created	Attention
	Application Role Dropped	Trouble
	Created Database Audit Specifications	Attention
	Created Server Audit Specifications	Trouble
	Created Server Audits	Trouble
	Created server roles	Attention
	Dropped Database Audit Specifications	Trouble
	Dropped Server Audit Specifications	Trouble
	Dropped Server Audits	Trouble
	Dropped server roles	Trouble
	Security Changes Report	Trouble
MySQL Logs		
	Account Management Statements	Attention
	Component and Plugin Statements	Attention
	DDL Statements	Trouble
	DML Statements	Trouble
	Other Administrative Statements	Trouble
	Replication Statements	Trouble

Oracle		
	Alter System	Trouble
	Altered roles	Trouble
	Dropped roles	Trouble
	Roles created	Attention
	System Grant	Trouble
	System Revoke	Trouble
Sysmon		
	Config Modification	Trouble
	Registry Key Created	Trouble
	Registry Key Deleted	Trouble
	Registry Object Renamed	Trouble
	Registry Value Created	Trouble
	Registry Value Deleted	Trouble
	Registry Value Set	Trouble
Linux FIM		
	File Modified	Trouble
	File Permission Changes	Trouble
	System File Changes	Trouble
Windows FIM		
	File Modified	Trouble
	File Permission Changes	Trouble
Symantec Endpoint Protection		
	Admin Added	Attention
	Admin Deleted	Trouble
	Admin Modified	Trouble
	Policy Changes	Trouble
Trend Micro		
	Policy Added	Attention
	Policy Deleted	Attention
	Policy Modified	Trouble
vCenter		
	Cluster Created	Trouble
	Cluster Destroyed	Critical
	Cluster Reconfigured	Trouble
	Permission Created	Attention
	Permission Removed	Trouble
	Permission Updated	Trouble

	Role Added	Attention
	Role Removed	Trouble
	Role Updated	Trouble
ESXi		
	Syslog Restarted	Attention
	Syslog Stopped	Attention

Privilege escalation

- ALERTS for incidents where user's privileges are escalated without proper authorization.
  - 8.3 Information access restriction Control Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

Privilege escalation		
Windows		
	Failed software installations due to privilege mismatches	Trouble
	Exe/Dll Files Not Allowed to Run due to Enforced rules	Trouble
Windows Workstation		
	Privilege Assigned to New Logon	Trouble
	Failed software installations due to privilege mismatches	Trouble
AS 400		
	User Profile changes	Trouble
Cisco		
	Changed user privilege levels	Trouble
SonicWall		
	User Privilege Changed	Trouble
SQL Server		
	Privilege Abuse	Critical
Oracle		
	Granted roles	Attention
	Altered roles	Attention
PostgreSQL Logs		
	Database role altered	Attention
Trend Micro		
	Policy Modified	Attention
	Users Modified	Attention

Nessus		
	Elevated Privilege Failure reports	Trouble
vCenter		
	Role Updated	Attention
Unix/Linux		
	Denied NFS mounts based on users	Trouble
Printer		
	Insufficient Privilege to Print Documents	Attention

User account management

- ALERTS for changes to user accounts -account creation/deletion/password changes.

User account management		
Unix / Linux		
	Users Added	Trouble
	Users Deleted	Trouble
	Users Renamed	Trouble
	Failed User Additions	Attention
	Password Changes	Trouble
	Password Changes Failed	Trouble
Cisco		
	Users Added	Trouble
	Users Deleted	Trouble
	Changed user privilege levels	Trouble
SonicWall		
	Users Added	Trouble
	Users Deleted	Trouble
	Users Modified	Trouble
	Disabled Users	Trouble
	Enabled Users	Trouble
	User Privilege Changed	Trouble
Fortinet		
	Admin Added	Critical
	Admin Deleted	Critical
	Admin Modified	Critical
	Users Added	Trouble

	Users Deleted	Trouble
	Users Modified	Trouble
Sophos		
	Group Added	Trouble
	Group Deleted	Trouble
	Group Modified	Trouble
	Users Added	Trouble
	Users Deleted	Trouble
	Users Modified	Trouble
	Disabled Users	Trouble
	Enabled Users	Trouble
Barracuda		
	Admin Added	Critical
	Admin Deleted	Critical
	Admin Modified	Critical
	Group Added	Trouble
	Group Deleted	Trouble
	Group Modified	Trouble
	Users Added	Trouble
	Users Deleted	Trouble
	Users Modified	Trouble
Huawei		
	Group Added	Trouble
	Group Deleted	Trouble
	Group Modified	Trouble
	Users Added	Trouble
	Users Deleted	Trouble
CheckPoint		
	Users Added	Trouble
	Users Deleted	Trouble
	User Group Added	Trouble
	User Group Removed	Trouble
SQL Server		
	User Created	Trouble
	User Dropped	Trouble
	User Altered	Trouble
	Disabled Users	Trouble
	Enabled Users	Trouble
	Password Changes Failed	Trouble

	Password Reset	Trouble
	Password Reset Failed	Trouble
	Password Changes	Trouble
	All Password Changes	Trouble
	Application Role Altered	Trouble
	Application Role Created	Trouble
	Application Role Dropped	Trouble
	Credential Altered	Trouble
	Credential Created	Trouble
	Credential Dropped	Trouble
	Failed Own password changes	Trouble
	Failed Own password resets	Trouble
	Login Altered	Trouble
	Login Created	Trouble
	Login Dropped	Trouble
	Own Password Changes	Trouble
	Own password resets	Trouble
Oracle		
	Altered roles	Trouble
	Dropped roles	Trouble
	Granted roles	Trouble
	Revoked roles	Trouble
	Roles created	Trouble
	User Created	Trouble
	User Dropped	Trouble
	User Altered	Trouble
IIS W3C Web Server		
	Password Changes	Trouble
IIS W3C FTP		
	Password Changes	Trouble
SAP ERP audit Logs		
	User Locked	Trouble
	User Unlocked	Trouble
	User Created	Trouble
	User Deleted	Trouble
	Password Changes	Trouble

PostgreSQL Logs		
	User Created	Trouble
	User Dropped	Trouble
	User Altered	Trouble
	Password Changes	Trouble
	Permission Granted	Trouble
	Permission Revoked	Trouble
Trend Micro		
	Users Added	Trouble
	Users Deleted	Trouble
	Users Modified	Trouble
ESXi		
	Users Added	Trouble
	Users Deleted	Trouble
	Users Renamed	Trouble
	Password Changes	Trouble
NetScreen, WatchGuard, Stormshield, Symantec Endpoint Protection		
	Admin Added	Critical
	Admin Deleted	Critical
	Admin Modified	Critical
Windows		
	Access denied to users	Trouble
	Access granted to users	Trouble
	Special groups assigned to new logon	Trouble
	User Account Locked Out Error	Attention
	User Based Activity	Trouble
IBM AS/400		
	User Based Activity	Trouble
	User Profile changes	Trouble
Widows Workstation		
	Privilege Assigned to New Logon	Critical
vCenter		
	Permission Created	Trouble
	Permission Removed	Trouble
	Permission Updated	Trouble
	Role Added	Trouble
	Role Removed	Trouble
	Role Updated	Trouble

ESXi		
	Group Added	Trouble
	Group Deleted	Trouble
	Group Modified	Trouble
	Users Added	Trouble
	Users Deleted	Trouble
	Users Renamed	Trouble

Log tampering

- ALERTS for incidents where log data is modified, deleted to conceal malicious activities
    - 8.15 Logging Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.

Log tampering		
Windows System Events (Alerts)		
	Audit Logs Cleared	Critical
Windows - Eventlog Reports (Reports)		
	Event Logs Cleared	Critical
	Security Logs Cleared	Critical
	Audit Events Dropped	Trouble
SonicWall (Reports)		
	Logs Cleared	Trouble
SAP ERP audit Logs (Reports)		
	Logs Deleted	Critical
Unix/Linus		
	Syslog Restarted	Trouble
	Syslog Stopped	Trouble
IBM AS/400		
	Unable to write audit record	Trouble
Windows Workstation		
	Audit Events Dropped	Trouble
	Event Logging Service Shutdown	Critical
	Event Logs Cleared	Critical
	Security Logs Cleared	Critical
DHCP Windows Logs		
	DHCP logging paused due to low disk	Trouble

IIS W3C FTP		
	Logging Changes	Trouble
IIS W3C Web Server		
	Logging Changes	Trouble
SQL Server Audit Logs		
	Altered Database Audit Specifications	Trouble
	Altered Server Audit Specifications	Trouble
	Altered server audits	Trouble
	Changed Audit Sessions	Trouble
	Created Server Audit Specifications	Attention
	Created Server Audits	Attention
	Created Database Audit Specifications	Attention
	Dropped Database Audit Specifications	Trouble
	Dropped Server Audit Specifications	Trouble
	Dropped Server Audits	Trouble
	Started Trace Audits	Attention
	Stopped Trace Audits	Trouble
ESXi		
	Syslog Restarted	Trouble
	Syslog Stopped	Trouble

Network anomalies

- ALERTS for unusual network activity - high network traffic/unusual port scans/large data transfers.
    - 8.20 Networks security Control Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.

Network anomalies		
Unix/Linux		
	Data transfer stall timeouts	Attention
	No transfer timeouts	Trouble
Barracuda		
	Denied Connections	Trouble
	Email Scanned Reports	Attention
CheckPoint, FirePower, Cisco, Fortinet, Huawei, Juniper, Meraki, NetScreen, SonicWall, Sophos, WatchGuard, pfSense, H3C, Arista, F5, StormShield		
	Denied Connections	Trouble

PaloAlto		
	Data Filtering Detection	Trouble
	Denied Connections	Trouble
	Flood Detection	Trouble
	Scan Detection	Attention
	Spyware Download Detection	Critical
	Virus Detection	Trouble
Windows, Windows Workstation		
	Firewall Flood Attack	Trouble
	Firewall Internet Protocol half-scan attack	Trouble
	Firewall Ping of Death Attack	Trouble
	Firewall Spoof Attack	Trouble
	Firewall SYN Attack	Trouble
	IP Conflicts	Attention
Dell		
	Port Blocking Report	Trouble
	Port Forwarding Report	Trouble
ForcePoint		
	Denied Connections	Trouble
	Email Rejected	Attention
	Miscellaneous Content Access	Trouble
	Sensitive Content Access	Trouble
	Social Media Access	Attention
	Malicious Content Access	Trouble
	Web Traffic Blocked	Attention
Apache Access Logs		
	Malicious URL Request	Trouble
DHCP Windows Logs		
	Network Failure	Attention
IIS W3C FTP		
	Security Data Exchange	Trouble
IIS W3C Web Server		
	IP Address Rejected	Trouble
	Possible Malicious File Execution	Critical
	Possible Malicious URL Request	Trouble
	Site Access Denied	Attention
SQL Server Audit Logs		
	Storage Media Exposure	Trouble

FireEye		
	Malware Object Events	Trouble
	Web Infection Events	Trouble
Malwarebytes		
	Malicious Websites Blocked	Attention
Trend Micro		
	Intrusion Prevention Event	Trouble
	Web Reputation Event	Trouble
Nexpose, Nmap		
	Open Ports	Trouble
Qualys		
	Open TCP Ports	Trouble
	Open UDP Ports	Trouble
vCenter		
	Device IP Changed	Trouble

ManageEngine
Log360

ManageEngine Log360, a unified SIEM solution with integrated DLP and CASB capabilities, helps enterprises thwart attacks, monitor security events, and comply with regulatory mandates. The solution comes bundled with a log management component that provides better visibility into network activity, an incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents, an ML-driven user and entity behavior analytics add-on that baselines normal user behaviors and spots anomalous user activities, and a threat intelligence platform that leverages dynamic threat feeds for security monitoring and helps enterprises stay on top of attacks.

For more information about Log360, visit manageengine.com/log-management

$ Get Quote

⤓ Download