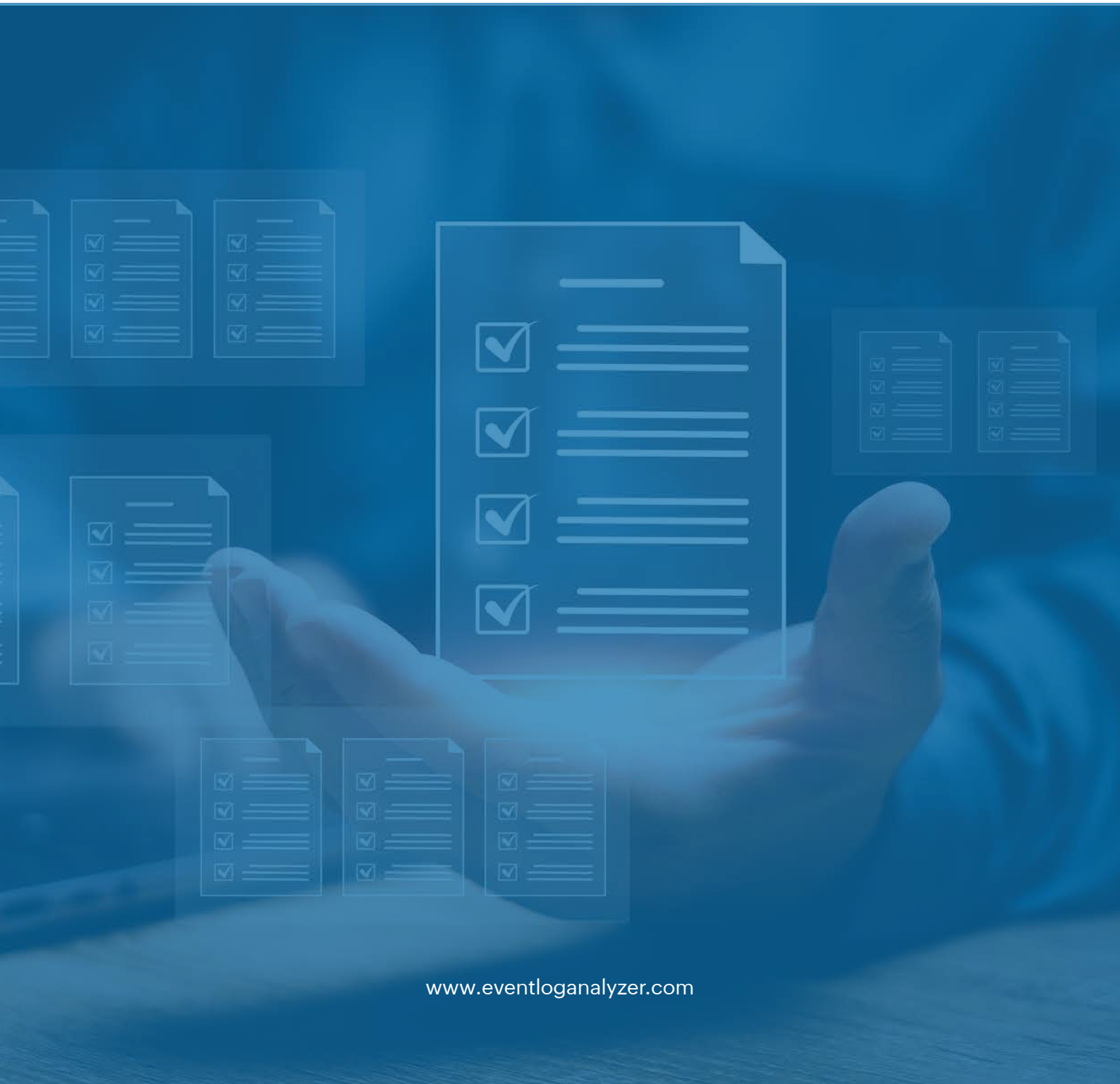
ManageEngine
EventLog Analyzer

CMMC Compliance



www.eventloganalyzer.com

CMMC sections	Description of requirement	Some of EventLog Analyzer's reports that can help fulfill the CMMC's requirements
C001 - AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).	**Detailed Windows Logon Reports** • Windows Successful User Logons • Interactive Logon • Remote Interactive Logon • Network Logon • Logon Attempt Using explicit Credentials • Privilege Assigned to New Logon **Windows Logoff Reports** • Windows Successful User Logoffs • User Initiated Logoffs • Interactive Logoffs • Remote Interactive Logoffs • Network Logoff **Windows Failed Logon Reports** • Windows UnSuccessful User Logons • Failed Interactive Logons • Failed Remote Interactive Logons • Failed Network Logons • Failed logons due to password expiry • Failed logons due to account expiry • Failed logons due to account lock outs • Failed logons due to disabled accounts • Failed logons during non-working hours • Failed Logons due to Bad Password • Failed Logons due to Bad UserName **Windows Events** • User Based Activity **Unix Logon Detailed Reports** • User Logons • SU Logons • SSH logons • FTP/SFTP Logons • Unix UnSuccessful User Logons **Unix Logoff Reports** • User Logoffs • SU Logoff • SSH Logoff • FTP/SFTP Logoff

		Unix User Account Management • Users Added • Users Deleted • Users Renamed • Group Added • Group Deleted • Group Modified • Password Changes • Password Changes Failed • Failed user additions **IAM Activity** • IAM Errors • IAM User Activities • IAM Unauthorized Activities • IAM User Report • IAM Group Report • IAM Role Report • IAM Policy Report • MFA Report • Access Key Report **AWS Failed/Unauthorized Activity** • AWS Error events • AWS Login Failures • AWS Authorization Failures **Cloud User Login Activity** • Successful Logins • Failed logins
C003 - AC.2.013	Monitor and control remote access sessions.	**Detailed Network Device Logon Detailed** • Successful Logons • Failed Logons • Logoff Events • Successful VPN Logons • Failed VPN Logons • VPN Logoff
C007 - AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	**Detailed Windows Logon Reports** • Windows Successful User Logons • Interactive Logon • Remote Interactive Logon • Network Logon • Logon Attempt Using explicit Credentials • Privilege Assigned to New Logon

		Windows Logoff Reports • Windows Successful User Logoffs • User Initiated Logoffs • Interactive Logoffs • Remote Interactive Logoffs • Network Logoff **Windows Events** • User Based Activity **Unix Logon Detailed Reports** • User Logons • SU Logons • SSH logons • FTP/SFTP Logons • Unix UnSuccessful User Logons **Unix Logoff Reports** • User Logoffs • SU Logoff • SSH Logoff • FTP/SFTP Logoff **SQLServer Auditing Server Reports** • SQL Server Admin Authority Changes • SQL Server Owner Changes • SQL Server Database Backup • SQL Server Database Restore • SQL Server Transaction Log Backup • SQL Server Permission Changes • SQL Server Startup • SQL Server Shutdown • SQL Server Logons • SQL Server Failure Logons • SQL Server Logout Account **MySQL Logon Reports** • MySQL Logon Success • MySQL Logon Failures **Detailed Network Device Logon Detailed** • Successful Logons • Failed Logons • Logoff Events • Successful VPN Logons • Failed VPN Logons • VPN Logoff

- **Network Device Configuration Reports**
  - Configuration Errors
  - Interface Up
  - Interface Down
  - Command Executed
  - Command Failed
  - Configuration Changes
- **IAM Activity**
  - IAM Errors
  - IAM User Activities
  - IAM Unauthorized Activities
  - IAM User Report
  - IAM Group Report
  - IAM Role Report
  - IAM Policy Report
  - MFA Report
  - Access Key Report
- **AWS User Activity**
  - AWS User Activity
- **AWS Failed/Unauthorized Activity**
  - AWS Error events
  - AWS Login Failures
  - AWS Authorization Failures
- **File Changes Audit**
  - AWS Accessed Files
  - AWS Deleted Files
  - AWS Created Or Modified Files
- **Route 53**
  - Failed Route 53 Events
  - Route 53 Activity
  - Hosted Zone Configuration Changes
  - Changed Resource Record Sets
  - Traffic Policy Configuration Changes
  - Traffic Policy Instance Configuration Changes
  - AWS Domain Configuration Changes
- **VPC Activity**
  - VPC Changes
  - Network Gateway Changes
  - VPC Endpoint Changes
  - VPC Route Table Changes
  - VPC Route Changes
  - Subnet Changes

		Storage Activity Reports • Modified Buckets • Deleted Buckets • AWS Failed Events **WAF Reports** • WAF Error Events • WAF Rule Changes • IP Set Configuration Changes • SQL Injection Match Set Changes • Web ACL Configuration Changes **AWS Network Security Groups** • Security Group Configuration Changes • Network ACL Changes **AWS Config Reports** • AWS Config Errors • AWS Config Rules Changes • AWS Configuration Recorder Activity **Database Reports** • RDS Error Events • DB Security Group Configuration Changes • RDS Instance Activity • DB Cluster Activity • DB Snapshot Activity **EC2 Reports** • EC2 Instance State Changes • Key Pair Activity • AWS Assigned Addresses • AWS Unassigned Addresses • Network Interface Configuration Changes • Elastic IP Address Activity **Cloud User Login Activity** • Successful Logins • Failed logins
C007 - AU.3.045, AU.3.046, C008 - AU.2.042, AU.3.048, C010 - AU.2.044, AU.3.052	AU.3.045 Review and update logged events. AU.3.046 Alert in the event of an audit logging process failure. AU.2.042 Create and retain system audit	**Windows System Events** • Audit Logs Cleared • System Startup • System Shutdown • Software Installed • Software Updated • Software Uninstalled

	logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity. AU.3.048 Collect audit information (e.g., logs) into one or more central repositories. AU.2.044 Review audit logs. Audit and Accountability. AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting.	• Failed software installations • Failed software installations due to privilege mismatches • New Service Installed • Error in EventLog Service • AD Backup Error • Event log automatic backup • Failed hotpatching **Detailed Windows Software Update Reports** • Installed • Downloaded • Detected • Connectivity • Availability • Windows update process failed • Update Packages Installed **CMMC Windows Threat Detection** • Audit Events Dropped • Security Log Full
C013 - CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.	**MSSQL Account Changes** • SQL Server User Created • SQL Server User Deleted • SQL Server User Modified • SQL Server Login Created • SQL Server Login Deleted • SQL Server Login Modified • SQL Server Role Created • SQL Server Role Deleted • SQL Server Role Modified • SQL Server Credentials Created • SQL Server Credentials Deleted • SQL Server Credentials Modified • SQL Server Enabled Users • SQL Server Disabled Users **Oracle Account Changes** • Oracle Profile Created • Oracle Profile Deleted • Oracle Profile Modified • Oracle User Created • Oracle User Deleted • Oracle User Modified • Oracle Role Created • Oracle Role Deleted • Oracle Role Modified

- Oracle Granted Roles
- Oracle System Grant
- Oracle System Revoke
- Oracle Revoked Roles
- Oracle Alter System

IIS Admin Configuration

- IIS Authentication Changes
- IIS DefaultDocument Changes
- IIS ErrorPage Changes
- IIS Logging Changes
- IIS Modules Changes
- IIS RequestFiltering Changes
- IIS SSL Changes
- IIS AllConfiguration Changes

SAP ERP Configuration

- SAP ERP Configuration change

DB2 Configuration

- DB2 DB Configuration Changes
- DB2 DBM Configuration Changes

Detailed Network Device Logon Detailed

- Successful Logons
- Failed Logons
- Logoff Events
- Successful VPN Logons
- Failed VPN Logons
- VPN Logoff

Network Device Attack Reports

- Attacks
- EndPoint Health

Network Device Configuration Reports

- Configuration Errors
- Interface Up
- Interface Down
- Command Executed
- Command Failed
- Configuration Changes

Detailed Network Device Security Reports

- Website Traffic
- Denied Connections
- Allowed Traffic

- **Network Device Account Management Reports**
  - User Added
  - User Deleted
  - User Modified
  - User Enabled
  - User Disabled
  - Group Added
  - Group Deleted
  - Group Modified
- **Network Device Rule Management Reports**
  - Rules Added
  - Rules Modified
  - Rules Deleted
  - Rules Enabled
  - Rules Disabled
- **IAM Activity**
  - IAM Errors
  - IAM User Activities
  - IAM Unauthorized Activities
  - IAM User Report
  - IAM Group Report
  - IAM Role Report
  - IAM Policy Report
  - MFA Report
  - Access Key Report
- **AWS User Activity**
  - AWS User Activity
- **AWS Failed/Unauthorized Activity**
  - AWS Error events
  - AWS Login Failures
  - AWS Authorization Failures
- **File Changes Audit**
  - AWS Accessed Files
  - AWS Deleted Files
  - AWS Created Or Modified Files
- **Route 53**
  - Failed Route 53 Events
  - Route 53 Activity
  - Hosted Zone Configuration Changes
  - Changed Resource Record Sets
  - Traffic Policy Configuration Changes
  - Traffic Policy Instance Configuration Changes
  - AWS Domain Configuration Changes

- **VPC Activity**
  - VPC Changes
  - Network Gateway Changes
  - VPC Endpoint Changes
  - VPC Route Table Changes
  - VPC Route Changes
  - Subnet Changes
- **Storage Activity Reports**
  - Modified Buckets
  - Deleted Buckets
  - AWS Failed Events
- **WAF Reports**
  - WAF Error Events
  - WAF Rule Changes
  - IP Set Configuration Changes
  - SQL Injection Match Set Changes
  - Web ACL Configuration Changes
- **AWS Network Security Groups**
  - Security Group Configuration Changes
  - Network ACL Changes
- **AWS Config Reports**
  - AWS Config Errors
  - AWS Config Rules Changes
  - AWS Configuration Recorder Activity
- **Database Reports**
  - RDS Error Events
  - DB Security Group Configuration Changes
  - RDS Instance Activity
  - DB Cluster Activity
  - DB Snapshot Activity
- **EC2 Reports**
  - EC2 Instance State Changes
  - Key Pair Activity
  - AWS Assigned Addresses
  - AWS Unassigned Addresses
  - Network Interface Configuration Changes
  - Elastic IP Address Activity
- **Amazon ELB Reports**
  - ELB Error Events
  - Load Balancer Configuration Changes

		Cloud User Login Activity • Successful Logins • Failed logins **Trend Micro Policy Management Reports** • Trend Micro Policy Added • Trend Micro Policy Deleted • Trend Micro Policy Modified **Trend Micro User Account Management Reports** • Trend Micro User Account Added • Trend Micro User Account Deleted • Trend Micro User Account Modified **Symantec End Point Reports** • Admin Added • Admin Deleted • Admin Modified • Policy Changes • Commercial Application Detected • Port Scan • Threat Activity • Virus Report • HIPS Activity Report
C013 - CM.2.063	Control and monitor user-installed software.	**Detailed Windows Software Update Reports** • Installed • Downloaded • Detected • Connectivity • Availability • Windows update process failed • Update Packages Installed **Windows and software reports** • Software Installed • Software Updated • Failed software installations • Failed software installations due to privilege mismatches • Non valid Windows license • Failed Windows license activations • Non activated windows products • New Kernel Filter Driver **Windows Services - Detailed Reports** • Service Started • Service Stopped • Service Failed • New Service Installed

C015 - IA.1.076	Identify information system users, processes acting on behalf of users or devices.	**Detailed Windows Logon Reports** • Windows Successful User Logons • Interactive Logon • Remote Interactive Logon • Network Logon • Logon Attempt Using explicit Credentials • Privilege Assigned to New Logon **Windows Events** • User Based Activity **Unix User Account Management** • Users Added • Users Deleted • Users Renamed • Group Added • Group Deleted • Group Modified • Password Changes • Password Changes Failed • Failed user additions **Detailed Network Device Logon Detailed** • Successful Logons • Failed Logons • Logoff Events • Successful VPN Logons • Failed VPN Logons • VPN Logoff **IAM Activity** • IAM Errors • IAM User Activities • IAM Unauthorized Activities • IAM User Report • IAM Group Report • IAM Role Report • IAM Policy Report • MFA Report • Access Key Report **AWS User Activity** • AWS User Activity **AWS Failed/Unauthorized Activity** • AWS Error events • AWS Login Failures • AWS Authorization Failures

		Cloud User Login Activity • Successful Logins • Failed logins
CO41 - SI.5.222	Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.	**Detailed Windows Software Update Reports** • Installed • Downloaded • Detected • Connectivity • Availability • Windows update process failed • Update Packages Installed **Windows and software reports** • Software Installed • Software Updated • Failed software installations • Failed software installations due to privilege mismatches • Non valid Windows license • Failed Windows license activations • Non activated windows products • New Kernel Filter Driver **Process Tracking** • Process Created • Process Terminated • Process Accessed • Process Duplicated **Windows Services - Detailed Reports** • Service Started • Service Stopped • Service Failed • New Service Installed **Windows Threat Detection from Antivirus Detailed Reports** • Threats Detections by ESET Endpoint Antivirus • Threats Detections by Kaspersky • Threats Detection by Microsoft Antimalware • Threats Detection by Sophos Anti-Virus • Threats Detection by Norton AntiVirus • Threat Detections by Mcafee • Infected files detected by Symantec Endpoint Protection

		CMMC Windows Threat Detection • Audit Events Dropped • Security Log Full
		Detailed Registry Changes • Registry Accessed • Registry Created • Registry Deleted • Registry Value Modified • Failed Registry Access • Failed Registry Creations • Failed Registry Modifications • Failed Registry Deletions • Registry Permission Changes
		Network Device Attack Reports • Attacks • EndPoint Health

Our Products

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus | DataSecurity Plus | SharePoint Manager Plus

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease. For more information about EventLog Analyzer, visit manageengine.com/eventloganalyzer.

$ Get Quote Download