ManageEngine
Log360

Training Agenda

About Log360

Log360 is a comprehensive security information and event management (SIEM) solution that performs exhaustive log management, Active Directory auditing, and user behavior management.

Course agenda

Getting started and installing Log360

- System pre-requisites and requirements
- Installing Log360 as an application and as a Windows service
- Starting and setting up Log360 from the web console

Integrating the different components of Log360

- Integrating products installed in other machines in Log360
- Setting up all the components of Log360
- Synchronizing the data between the integrated components

Setting up log collection

- Automatic log collection from devices
- Setting up agent-based and agentless log collection
- Log collection filters

Searching the logs

- Types of search queries and their functionalities
- Building basic and advanced search queries
- Log parsing
- Tagging search queries
- Mapping search results as incidents

Security analytics

- Viewing reports on network activities, Active Directory, Exchange Server, and Office 365 from one place
- Exporting reports in various formats
- Mapping reports as incidents

Active Directory Auditing

- Account Logon auditing
- Logon/Logoff auditing
- AD user object auditing
- AD computer object auditing
- AD group object auditing
- AD Organizational Unit auditing
- Permission change auditing
- GPO auditing
- Other AD object auditing – Containers/Contacts/DNS etc.,

File Server Auditing

- Auditing Windows File Servers
- Windows failover server clusters audit
- NetApp Filer auditing
- EMC storage auditing
- File integrity monitoring

Account Lockout

- Analyze Windows Services/Schedule tasks
- Network Drive Mappings/logon sessions/Process list
- Analyze logon activity – DC and local
- OWA and ActiveSync analysis
- Radius server logins

Member Server Auditing

- Audit logon activity on Servers
- Track process activity
- Audit policy changes
- Monitor system events
- Account management on Servers

- Printer auditing
- ADFS auditing
- Removable storage (USB) auditing
- AD LDS auditing

Dashboard

- Customizing the dashboard and embedding it in external sites
- Adding new widgets to the dashboard

Setting up security alerts

- Viewing pre-built alerts and correlation based alert profiles
- Building custom alert profiles
- Exporting alerts

Event correlation

- Viewing pre-built correlation rules
- Building custom correlation rules

Response workflows

- Configuring workflows for alerts
- Creating workflow profiles

Incident tracking

- Creating incidents for alerts, reports, and search results
- Tracking the incidents

User and entity behavior analytics (UEBA)

- Viewing, scheduling, and exporting reports
- Configuring alerts in Log360 UEBA

Logon settings

- Configuring single sign-on, smart card, and two-factor authentication for secure login

Centralized administration settings for Log360 and integrated components

- Setting up high availability
- Configuring automatic database backup and build update
- Configuring mail server, SMS, and proxy settings
- Applying SSL certificate and enabling HTTPS
- Settings up Log360 as a reverse proxy server for enhanced security

General settings

- Enabling license expiration and product downtime notifications
- Migrating from the built-in database to other databases
- Personalizing language and time zone settings
- Customizing logo, title, etc.