ManageEngine
Log360

Umfassende **SIEM-Lösung** mit **integrierten DLP-** und **CASB-**Funktionen

www.manageengine.de/log360

Erleben Sie Cybersicherheit wie nie zuvor.

5 Gründe für Log360

Zentrale Konsole für Cybersicherheit:

Eine umfassende Lösung, die Log-Management, Active-Directory-Berichte, User Behaviour Monitoring, Data Loss Prevention, Cloud-Sicherheit und IT-Compliance-Management in einer Benutzeroberfläche vereint.

Analysiert nahezu alle Arten von Daten:

Unterstützt über 700 Arten von Log-Quellen.
Mit dem Custom Log Parser können Sie automatisch aussagekräftige Informationen aus jedem menschenlesbaren Log-Format extrahieren.

Einfaches, umfassendes SIEM:

Log360 lässt sich schnell und einfach einrichten. Mit dieser intuitiven SIEM-Lösung benötigen Sie weniger als eine Woche für Bereitstellung, Konfiguration und Training.

Technischer Support für maximalen Nutzen:

Lesen Sie bei Gartner Peer Insights, wie uns unsere Kunden bewerten! Unser Support-Team setzt alles daran, damit Sie Log360 optimal nutzen können.

Erschwingliche, erstklassige SIEM-Lösung:

Ein flexibles Lizenzmodell, bei dem Sie nur für das bezahlen, was Sie nutzen.
Sie wählen – und bezahlen – nur die Komponenten, die zu Ihren Sicherheitszielen passen.

Log-Management

- **Intuitive Sicherheits-Dashboards** mit Diagrammen und Berichten helfen dabei, Angriffe zu erkennen, verdächtiges Benutzerverhalten zu entdecken und potenzielle Bedrohungen zu stoppen.
- **Agentenbasierte und agentenlose Log-Erfassung** ermöglicht es, Protokolle aus über 750 Quellen zu sammeln. Jedes Protokoll in einem menschenlesbaren Format lässt sich mit dem integrierten Custom Log Parser analysieren.
- **Analysieren Sie Logs eingehend und gewinnen Sie umsetzbare Erkenntnisse** über interaktive Dashboards, die Informationen grafisch oder in intuitiven Berichten darstellen.

Bedrohungserkennung und -modellierung

- **Die leistungsstarke Korrelation Engine** mit mehr als 30 vorkonfigurierten Regeln hilft bei der Erkennung bekannter Angriffe wie SQL-Injection, Denial-of-Service- und Firewall-Angriffe.
- **Threat Intelligence Updates** aus vertrauenswürdigen unabhängigen Quellen unterstützen dabei, APTs zu erkennen und Compliance-Vorschriften einzuhalten.
- **User Entity and Behavioral Analytics (UBA)** legt Basiswerte für normales Benutzerverhalten fest und erkennt Anomalien, um APTs effektiv zu identifizieren.
- **Durch die Unterstützung des MITRE-ATT&CK-Frameworks** für die Bedrohungs-Modellierung lassen sich in Kombination mit Sicherheitsanalysen komplexe Angriffstechniken leichter erkennen.

Data Loss Prevention und Datensicherheit

- **Nutzen Sie die Discovery-Funktion und das Activity Tracking,** um sensible Daten, einschließlich personenbezogener Daten, Sozialversicherungs- und Kreditkartennummern auf Dateiservern sowie in Speichern zu schützen.
- **Überwachen Sie die Dateiintegrität,** um bei kritischen Dateien und Ordnern jeden Zugriff und jede Aktion (z. B. Erstellung, Löschung, Änderung und Berechtigungsänderung) zu verfolgen.
- **Erhalten Sie Echtzeit-Benachrichtigungen** per SMS und E-Mail, wenn unbefugte Aktionen oder Anomalien entdeckt werden.

Sicherheits- und Risiko-Management

- **Gewährleisten Sie die Sicherheit Ihres AD** mit der integrierten Sicherheits- und Risiko-Management-Funktion, die auf den Sicherheitsrichtlinien von Microsoft basiert.
- **Überprüfen Sie Ihre AD-Umgebung** kontinuierlich auf Risiken und erhalten Sie Empfehlungen zu deren Behebung.

Incident-Response und -Behebung

- **Automatisieren Sie Ihre Incident Response** mit integrierten Workflows, die mit Incidents verknüpft werden können.
- **Führen Sie schnelle Log-Forensik** durch, um Post-Attack-Analysen durchzuführen, Angriffsmuster zu identifizieren und die Auswirkungen von Sicherheitsvorfällen zu analysieren.
- **Verwenden Sie das integrierte Incident Ticketing Tool,** um Prozesse zu verfolgen, und integrieren Sie es in Ticketing Tools von Drittanbietern.

Integriertes Compliance-Management

- **Nutzen Sie vorkonfigurierte Audit-Berichte** für eine umfassende Liste gesetzlicher Vorschriften wie DSGVO, ISO 27001, PCI DSS, SOX, FISMA, GLBA, HIPAA und viele mehr.
- **Überwachen Sie die Compliance in Echtzeit** mit Dashboards für jede Vorschrift und Echtzeit-Compliance-Warnungen.
- **Verwenden Sie den Compliance Rule Builder** mit seiner einfachen Drag-and-Drop-Oberfläche, um individuelle Regeln für interne Audits zu erstellen.

CASB-Implementierung

- **Verschaffen Sie sich einen umfassenden Überblick** über Ihre AWS-, Azure-, Salesforce- und Google-Cloud-Plattform-Infrastrukturen in der Cloud.
- **Erkennen Sie Schatten-IT,** indem Sie Benutzerzugriffe auf nicht genehmigte Cloud-Anwendungen überwachen.
- **Gewährleisten Sie die Sicherheit von Cloud-Daten,** indem Sie Änderungen an Benutzern, Netzwerksicherheitsgruppen, virtuellen privaten Clouds, Berechtigungen und mehr in Ihrer Cloud-Umgebung in Echtzeit überwachen.
- **Erkennen Sie anomales Verhalten** in Cloud-Umgebungen mit Maschine-Learning-basiertem Behavior Analytics.

Vigil IQ

- **Nutzen Sie die Funktionen von Vigil IQ,** einem fortschrittlichen TDIR-System (Threat Detection, Investigation & Response) innerhalb von Log360.
- **Die leistungsstarke Engine bietet sofortige Einblicke** in Sicherheitsbedrohungen durch Echtzeit-Korrelation und adaptive Warnungen, die auf maschinellem Lernen basieren.
- **Hohe Abdeckung wichtiger Sicherheitsbedrohungen,** intuitive Analysen und automatisierte Playbooks helfen, die durchschnittliche Zeit bis zur Erkennung (MTTD) und die durchschnittliche Zeit bis zur Reaktion (MTTR) zu verbessern, und ermöglichen so ein zeitnahes Handeln.

ManageEngine
Log360

Produkt-Highlights

Profitieren Sie von einer eingehenden Bedrohungserkennung durch regelbasierte Angriffserkennung, forensische Analysen und Unterstützung des MITRE-ATT&CK-Frameworks.

Nutzen Sie User and Entity Behaviour Analytics, um komplexe Bedrohungen und APTs zu identifizieren.

Schützen Sie vertrauliche Daten mit dem DLP-Modul, das sensible Daten aufspürt, Benutzeraktivitäten verfolgt und Warnmeldungen bei unbefugtem Datenzugriff und Datendiebstahl generiert.

Beschleunigen Sie die Bedrohungserkennung durch eine umfassende Bedrohungssuche und umsetzbare Threat Intelligence Updates.

Sichern Sie Ihre Cloud-Infrastruktur mit tieferen Einblicken in Schatten-IT, Richtlinienverstöße, inhaltsbezogene Datensicherheit und andere CASB-Funktionen.

Sorgen Sie mit Echtzeit-Warnungen und Workflows für die Sicherheitsorchestrierung und automatisierte Reaktion Ihres SOC.

AUSZEICHNUNGEN

GARTNER
2025

Zum siebten Mal in Folge in den
„Gartner Magic Quadrant for SIEM“
aufgenommen.

TOP INFOSEC INNOVATOR WINNER CYBER DEFENSE MAGAZINE 2025

Gartner Peer Insights™

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2025

Kontakt

Website:
www.manageengine.de/log360

Ihr ManageEngine-Partner:
MicroNova AG | Unterfeldring 6 | D-85256 Vierkirchen
E-Mail: sales-ManageEngine@micronova.de

Support:
www.manageengine.de/support

30 Tage kostenlos testen:

> Log360 has made my job a cinch. The real-time reports and alerts make sure I don't have to spend a lot of time worrying about threats.
>
> **Victor,**
> IT Security Admin, SHM, London

> Log360 is a complete solution for all of the needs in events auditing! Subcomponents like EventLog Analyzer and ADAuditPlus are really helpful during reviews and audits.
>
> **Arvind Kumar,**
> Verantwortlicher für IT-Sicherheit,
> HCL Technologies, Noida