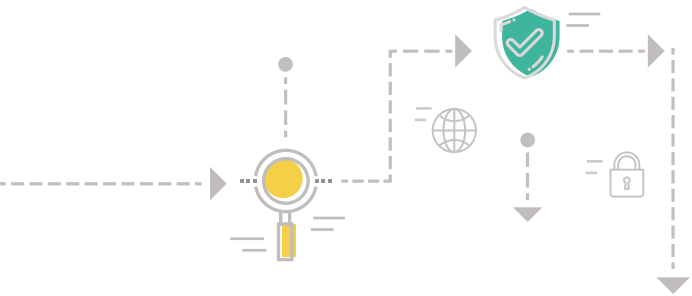
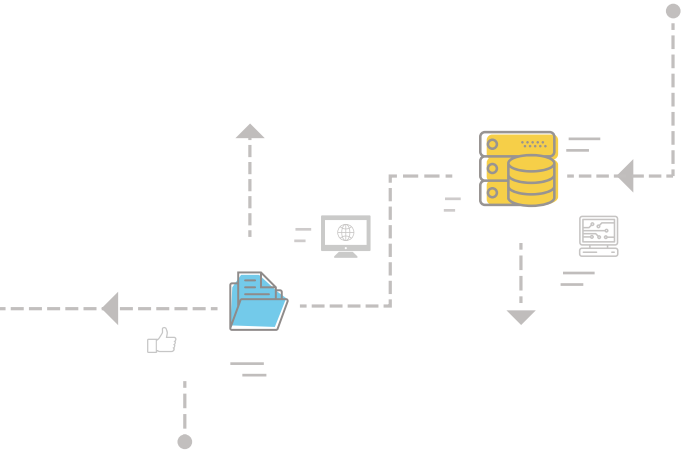
ManageEngine
Log360

www.manageengine.de/log360



Analysieren Sie Log-Dateien und sichern Sie Ihr Netzwerk mit einer **kompletten SIEM-Lösung** rundum ab



Umfassendes Auditing

- **Auditing von Perimeter-Netzwerkgeräten:** Erhalten Sie Antworten auf die wichtigen W-Fragen – das Auditing von Router-, Server-, Switch-, Firewall- und IDP/IPS-Aktivitäten macht's möglich.
- **Kritische Anwendungen überprüfen**: Verfolgen Sie Änderungen in IIS- und Apache-Webservern, SQL-Servern und Oracle-Datenbanken, um Anomalien zu erkennen.
- **Auditieren Sie einfach alles**: Behalten Sie die Aktivitäten im Active Directory, in Office 365, Exchange Online, Amazon Web Services (AWS), Microsoft Azure und Salesforce im Blick.

Detaillierte Active-Directory-Audits

- **Insider-Angriffe erkennen**: Überprüfen Sie die Aktivitäten von Anwendern und privilegierten Benutzern, inklusive An- und Abmeldungen, Ausweitung von Privilegien etc., um eventuelle Insider-Angriffe sofort zu erkennen.
- **AD-Änderungen überwachen**: Dokumentieren Sie kritische Änderungen an Gruppen, Group Policy Objects (GPOs), Organisationseinheiten (OUs) und Computern mit vordefinierten Berichten.
- **Gesperrte Accounts analysieren**: Untersuchen Sie, warum Konten gesperrt wurden und finden Sie so schnell heraus, ob Anmeldedaten gestohlen wurden.

Bedrohungsanalyse

- **Bösartigen Datenverkehr erkennen**: Identifizieren Sie bösartige Quellen, die versuchen, in das Netzwerk einzudringen, mithilfe der integrierten globalen Datenbank für IP-Bedrohungen.
- **STIX/TAXII Threat Feed Processor**: Die Lösung holt sich automatisch die neuesten Informationen aus den STIX/TAXII-Bedrohungsfeeds und warnt Sie in Echtzeit, wenn IP-Adressen oder URLs mit dem Netzwerk interagieren, die auf der Blacklist stehen.
- **Incident-Management-System**: Lassen Sie sich bei anomalen Aktivitäten in Echtzeit benachrichtigen und managen Sie Sicherheitsvorfälle effizient, indem Sie sie bestimmten Technikern zuweisen.

Integriertes Compliance-Management

- **Vorkonfigurierte Reports**: Erfüllen Sie die IT-Vorgaben von PCI DSS, FISMA, HIPAA, GLBA, SOX und GDPR mit vordefinierten Audit-Berichten.
- **Benutzerdefinierte Berichte für interne Sicherheitsrichtlinien:** Passen Sie bestehende Compliance-Berichte an oder erstellen Sie neue, um internen Sicherheits- oder Compliance-Richtlinien gerecht zu werden.
- **Forensische Datenanalyse**: Führen Sie forensische Log-Analysen mit der effizienten Suchmaschine durch und legen Sie fest, wie lange Log-Dateien archiviert werden sollen – so erfüllen Sie Compliance-Vorgaben mühelos.

Automatisiertes Log-Management

- **Umfangreiches Sammeln von Log-Dateien**: Unterstützt sowohl agentenlose als auch agentenbasierte Log-Erfassung aus mehr als 750 Quellen. Durch den integrierten individuellen Log Parser kann Log360 Log Files von jedem Gerät verarbeiten.
- **Detaillierte Log-Analyse**: Analysieren Sie Log-Dateien und gewinnen Sie dank intuitiver Dashboards und aussagekräftiger Berichte konkrete Erkenntnisse über alles, was in Ihrem Netzwerk passiert.
- **Log-Korrelation in Echtzeit**: Nutzen Sie vorkonfigurierte oder eigene Korrelationsregeln, um Log-Dateien aus Ihrem gesamten Netzwerk zu analysieren und potentielle Sicherheitsangriffe zu erkennen.

Drei Jahre in Folge im

Gartner Magic Quadrant

für SIEM ausgezeichnet

Log360 – Ihre SIEM-Lösung für alle Herausforderungen rund um Log-Management und Netzwerksicherheit

5 Gründe für Log360

01

Wir decken alles ab

Es spielt keine Rolle, ob Ihre Geschäftsumgebung in der Cloud oder On-Premise gehostet wird: Mit Log360 haben Sie alles im Griff.

02

Eine zentrale Konsole

Log360 bündelt Log-Management, Active-Directory-Auditing, Monitoring von privilegierten Anwendern, Dateiintegritäts-Monitoring, Event-Correlation, Bedrohungserkennung und Compliance-Management in einer zentralen Konsole.

03

Sofort einsatzbereit und trotzdem flexibel anpassbar

Log360 bietet zahlreiche vorkonfigurierte Berichte, Alarmprofile und Korrelationsregeln, die sich bei Bedarf einfach und schnell an Ihre spezifischen Anforderungen anpassen lassen.

04

Finden Sie die Nadel im Heuhaufen – in Rekordzeit

Dank der leistungsstarken Suchmaschine von Log360 können Sie 25.000 Log-Dateien pro Sekunde durchsuchen – so finden Sie im Handumdrehen das gewünschte Log File.

05

Wir machen SIEM einfach

Log360 ist innerhalb von Minuten einsatzbereit und beginnt mit dem Sammeln der Log-Files, sobald die Geräte zur Überwachung hinzugefügt wurden. Das Lizenzmodell ist einfach und unabhängig von der Größe der zu verarbeitenden Log-Files.

Telefonnummer
+49 8139 9300-456

Weitere Informationen unter
www.manageengine.de/log360

E-Mail
sales-ManageEngine@micronova.de