Global Service Group GmbH

Sicherheit für KMUs in 5 Teilen

Teil 4: Installation des G-SIEM-Systems

Einführung

Die Implementierung eines Security Information and Event Management (SIEM)-Systems ist gerade im KMU-Umfeld ein entscheidender Schritt zur Stärkung der Cybersicherheit, denn in der Regel werden solche Systeme weitestgehend im oberen Unternehmensbereich angeboten.

Diesem Problem hat sich die Fa. GSG GmbH, mit Sitz in Ober-Ramstadt Hessen, bereits seit einiger Zeit angenommen und ist nun in der Lage sogar für kleine als auch für mittelständische Unternehmen (KMUs) eine komplette Implementierung entweder direkt vor Ort (On-Premise) oder über eine Private Cloud anbieten, je nach den spezifischen Bedürfnissen und Ressourcen des Unternehmens.

Implementierung

1. **On-Premise**
   Unternehmen, die eine vollständige Kontrolle über ihre Sicherheitssysteme wünschen, können sich für eine On-Premise Implementierung entscheiden. In diesem Fall kann das SIEM-System entweder eigenständig von den internen IT-Teams oder mit Unterstützung durch den Service der GSG installiert, konfiguriert und betrieben werden.
2. **Private Cloud**
   Für Unternehmen, die Flexibilität und Skalierbarkeit bevorzugen, bietet GSG die Implementierung des SIEM-Systems in einer privaten Cloud-Umgebung an. Dieser Service umfasst die komplette Einrichtung und Wartung durch das GSG-Fachpersonal, wodurch Unternehmen von

reduziertem administrativen Aufwand und einer skalierbaren Infrastruktur profitieren können.

Vorteile der Virtualisierung

Durch die Wahl einer Virtualisierungs- und Kubernetisierungs-Lösung für das SIEM-System können Unternehmen die Vorteile der Cloud-Technologie voll ausschöpfen, einschließlich:

- **Kostenreduktion**
  Minimierung der Vor-Ort-Hardwareanforderungen und damit verbundener Kosten.
- **Elastizität**
  Schnelles Skalieren der Ressourcen nach Bedarf, ideal für KMUs, die mit variablen Datenmengen arbeiten.
- **Einfache Wartung und Updates**
  Da die Wartung und Updates von GSG durchgeführt werden, können sich die Unternehmen auf ihr Kerngeschäft konzentrieren.

Auswahlkriterien

Bei der Auswahl des SIEM-Systems hat sich GSG für eine Open-Source Lösung entschieden, denn neben der Funktionalität und den Kosten sind auch die Unterstützung und die angebotenen Dienstleistungen der Community in Betracht gezogen worden. Damit bietet diese Lösungen nicht nur eine robuste Technologie, sondern auch vollständige Unterstützung bei der Implementierung und dem laufenden Betrieb, egal ob On-Premise oder in der privaten Cloud.

Zusammenfassung

Ein effektiv implementiertes SIEM-System trägt wesentlich zur Verbesserung der Cybersicherheit bei, indem es kontinuierliche Überwachung und detaillierte Einblicke in die Sicherheitslage bietet. Durch die Optionen der On-Premise Implementierung oder der Einrichtung in einer privaten Cloud bietet die Fa. GSG für KMUs eine flexible und kosteneffiziente Möglichkeit, ihre Cybersicherheit massiv zu stärken.

Global Service Group GmbH

Konfiguration

Die Implementierung eines effektiven SIEM-Systems ist entscheidend für die proaktive Überwachung und Sicherheit von Unternehmensnetzwerken. Dieser Abschnitt erläutert, wie das G-SIEM installiert und konfiguriert wird, um eine umfassende Sicherheitslösung zu bieten

Systemanforderungen

Bevor eine Installation begonnen werden kann, muss die Entscheidung über die geeignete Plattform erfolgt sein, daraufhin ist es wichtig, die Systemanforderungen zu überprüfen. Das G-SIEM ist entwickelt, um auf einer Vielzahl von Plattformen zu laufen, einschließlich dedizierter Hardware und virtualisierten Umgebungen. Es erfordert:

- Ausreichende CPU- und Speicherkapazitäten, um Echtzeitanalysen zu unterstützen.
- Eine stabile Netzwerkverbindung für die kontinuierliche Datenerfassung.
- Betriebssystemkompatibilität, typischerweise mit gängigen Linux-Distributionen.

Installationsprozess

1. **Vorbereitung der Umgebung**
   Es muss sichergestellt sein, dass alle Server und Geräte, die in die SIEM-Lösung einbezogen werden sollen, korrekt konfiguriert und vernetzt sind.
2. **Software-Installation**
   Die Installationsdateien für das G-SIEM müssen von der offiziellen Website heruntergeladen und der Installationsassistenten ausgeführt werden. Dieser Prozess führt durch die erforderlichen Schritte zur Einrichtung der Datenbanken und Benutzeroberflächen.
3. **Konfiguration der Agenten**
   In einem letzten Schritt werden die Sicherheitsagenten auf den zu überwachenden Systemen Installiert und konfiguriert, um die Datenerfassung starten zu können. Diese Agenten werden genutzt, um Log-Daten zu sammeln und an das G-SIEM zu senden.

Einrichtung und Feinabstimmung

- **Einstellung von Regeln und Alarmen**
  Konfigurieren der Sicherheits- und Compliance-Regeln, die auf Ihre Unternehmensrichtlinien und Sicherheitsanforderungen abgestimmt sind. Sicherstellen, dass die Alarme korrekt eingestellt sind, um bei verdächtigen Aktivitäten Benachrichtigungen zu senden.
- **Testen und Validieren**
  Durchführen von Tests, um sicherzustellen, dass das System korrekt konfiguriert ist und alle Komponenten wie erwartet funktionieren. Dies beinhaltet die Überprüfung der Kommunikation zwischen Agenten und dem Server sowie die Effektivität der konfigurierten Regeln.

Inbetriebnahme

Nachdem das G-SIEM erfolgreich installiert und getestet wurde, kann das System in Betrieb genommen werden. Die Leistung des Systems muss überwacht und bei Bedarf Anpassungen vorgenommen werden, um die Sicherheit kontinuierlich zu verbessern und den Schutz gegen neu entstehende Bedrohungen zu gewährleisten.

Die Installation und Konfiguration des G-SIEM ist ein entscheidender Schritt zur Stärkung der Cyber-Resilienz Ihres Unternehmens. Mit der richtigen Vorbereitung und Einrichtung bietet das G-SIEM eine robuste Plattform zur Erkennung und Reaktion auf Sicherheitsbedrohungen.

Zusammenfassung

Die Installation und Konfiguration des G-SIEM ist ein entscheidender Schritt zur Stärkung der Cyber-Resilienz Ihres Unternehmens. Mit der richtigen Vorbereitung und Einrichtung bietet das G-SIEM eine robuste Plattform zur Erkennung und Reaktion auf Sicherheitsbedrohungen.