



Sicherheit für KMUs in 5 Teilen

Teil 3: Entscheidungsfindung und Auswahl

Die nächsten Schritte zur Implementierung

Nachdem die Bedeutung von Log-Daten und die Rolle spezialisierter Agenten für die Datensammlung und -analyse diskutiert wurden, ist der nächste Schritt die Implementierung eines SIEM-Systems. Diese Systeme sind entscheidend für die Sicherheitsstrategie von Unternehmen jeder Größe, bieten aber besonders für kleine und mittelständische Unternehmen (KMUs) wesentliche Vorteile.

Vorteile eines SIEM-Systems

1. **Kosteneffizienz**

Viele SIEM-Lösungen, besonders im Open Source-Bereich, bieten KMUs eine kostengünstige Möglichkeit, ihre Cybersecurity zu stärken, ohne die Budgets stark zu belasten.

2. **Einfache Usability**

Moderne SIEM-Systeme sind so gestaltet, dass sie mit minimaler Einarbeitungszeit effektive Benutzung ermöglichen, was Unternehmen schnell auf potenzielle Bedrohungen reagieren lässt.

3. **Skalierbarkeit**

SIEM-Systeme können an das Wachstum und die sich ändernden Anforderungen eines Unternehmens angepasst werden, was sie zu einer langfristigen Investition macht.

Verbesserte Compliance

Durch die automatisierte Log-Verarbeitung und -Analyse helfen SIEM-Systeme, regulatorische Anforderungen wie DSGVO, IT-Sicherheitsgesetz oder NIS 2 einfacher zu erfüllen.



Auswahl eines SIEM-Systems

Bei der Auswahl eines SIEM-Systems sollten Unternehmen besonders auf Lösungen achten, die nicht nur funktional und erschwinglich sind, sondern auch eine Community und Unterstützung bieten, um die Integration und den Betrieb zu erleichtern. Open Source-SIEMs sind oft besonders attraktiv, da sie regelmäßige Updates von einer aktiven Community erhalten und die Möglichkeit bieten, die Lösung an spezifische Bedürfnisse anzupassen.

Nachfolgend sind einige Kerneigenschaften eines fortschrittlichen SIEM-Systems zusammengestellt:

1. **Umfassende Datenerfassung**

Das System sollte in der Lage sein, Log-Daten aus einer Vielzahl von Quellen, einschließlich Netzwerkgeräten, Servern und Endpunkten, zu erfassen und zu aggregieren. Es muss verschiedene Protokolle und Formate unterstützen, um eine lückenlose Überwachung zu gewährleisten.

2. **Erweiterte Analysefunktionen**

Neben der Basisloganalyse sollte das System fortschrittliche Analysewerkzeuge bieten, um Muster zu erkennen und Anomalien zu identifizieren. Dies schließt maschinelles Lernen und Verhaltensanalyse ein, um proaktive Bedrohungserkennung und -abwehr zu ermöglichen.

3. **Echtzeit-Ereignisüberwachung und -reaktion**

Das System muss in der Lage sein, Ereignisse in Echtzeit zu verarbeiten und bei der Erkennung von verdächtigen Aktivitäten sofortige Alarme auszulösen. Automatisierte Reaktionsfähigkeiten können dabei helfen, Bedrohungen schnell zu neutralisieren.

4. **Konfigurations- und Compliance-Überwachung**

Das SIEM sollte Sicherheitskonfigurationsbewertungen (Security Configuration Assessments, SCA) durchführen können, um sicherzustellen, dass alle Systeme gemäß den besten Sicherheitspraktiken und Compliance-Vorschriften konfiguriert sind.

5. **Integration und Skalierbarkeit**

Eine effektive SIEM-Lösung sollte sich nahtlos in bestehende Sicherheitsinfrastrukturen integrieren lassen und skalierbar sein, um mit den wachsenden Anforderungen des Unternehmens Schritt zu halten.



6. **Benutzerfreundliches Dashboard und Reporting**

Ein intuitives Dashboard, das eine klare Visualisierung von Daten und Trends bietet, ist entscheidend für die Benutzerakzeptanz und effektive Sicherheitsüberwachung. Umfassende Reporting-Funktionen unterstützen nicht nur die tägliche Überwachung, sondern auch die Auditierung und Compliance-Überprüfung.

7. **Community und Support**

Für Open Source-basierte Systeme ist eine aktive Entwickler- und Nutzergemeinschaft von Vorteil, die kontinuierliche Verbesserungen, Patches und Unterstützung bietet.