SIEM

Inhaltsverzeichnis

SIEM (Security Information and Event Management) sammelt und korreliert Sicherheits- und Systemereignisse zentral. Ziel sind Erkennung, Untersuchung und Nachweis von Incidents.

1 Funktionsweise

Logs und Events aus Firewalls, Servern, Endpoints und Cloud-Diensten werden normalisiert, gespeichert und mit Regeln bzw. Analysen ausgewertet.

- **Collection:** Agenten, Syslog, APIs
- **Correlation:** Auffällige Muster über Quellen hinweg
- **Alerting/Cases:** Priorisierte Hinweise für Reaktion

2 Typische Einsatzbereiche

- Sicherheitsüberwachung und Compliance-Nachweise
- Forensik und Incident Response
- Überblick in heterogenen IT-Landschaften

3 Wichtige Hinweise

- Ohne Use Cases und Tuning entsteht Alert-Müdigkeit.
- Log-Qualität und Uhrzeit/NTP sind entscheidend.
- Aufbewahrung und Datenschutz müssen geregelt sein.

4 Fazit

SIEM ist die zentrale Linse auf Sicherheitsereignisse – wertvoll erst mit klaren Erkennungszielen und betrieblich tragfähigem Tuning.