

---

## Sicherheitsüberwachung

Sicherheitsüberwachung, auch als Security Monitoring bezeichnet, ist ein kontinuierlicher Prozess zur Überwachung von IT-Infrastrukturen, Netzwerken und Systemen auf verdächtige Aktivitäten oder Sicherheitsverletzungen. Das Ziel der Sicherheitsüberwachung ist es, Angriffe frühzeitig zu erkennen, um schnell darauf reagieren und die Auswirkungen minimieren zu können. Dies erfolgt durch den Einsatz von Sicherheitsinformationen und Ereignismanagement-Systemen (SIEM), die Protokolle und Aktivitäten in Echtzeit analysieren und verdächtige Muster identifizieren. Die Sicherheitsüberwachung kann sowohl automatisierte als auch manuelle Analysen umfassen, um Sicherheitsvorfälle zu ermitteln und zu untersuchen.