
Sicherheitsinformations- und Ereignismanagement-System (SIEM)

Sicherheitsinformations- und Ereignismanagement-Systeme (SIEM) sind Lösungen, die entwickelt wurden, um Sicherheitsereignisse und -informationen in einem Unternehmen oder einer Organisation zu zentralisieren, zu analysieren und zu verwalten. SIEM integriert Protokolldaten aus verschiedenen Quellen, wie Firewalls, IDS, Antivirensoftware und Anwendungen, um eine umfassende Sicht auf die Sicherheitslage zu erhalten. Durch die Kombination von Echtzeitüberwachung mit der Korrelation und Analyse von Ereignissen ermöglicht SIEM die frühzeitige Erkennung von Sicherheitsvorfällen und die schnelle Reaktion auf Bedrohungen. SIEM bietet auch leistungsstarke Reporting-Funktionen und Dashboards, um Einblicke in die Sicherheitslage und -trends zu gewinnen. Durch die Verwendung von SIEM können Unternehmen ihre Sicherheitsoperationen optimieren und die Effizienz der Incident Response verbessern.