Marktvergleich SIEM-Software Anbieter 2024

BIESER

Anbieter	Vorteile	Nachteile	Cloud	Lizenzmodelle
Splunk	Leistungsfähig und skalierbar, Benutzerfreundlich, Flexible Datenaufnahme, Starke Community, Erweiterbarkeit	Teuer, Komplex für kleinere Organisationen, Hohe Hardwareanforderungen	Splunk Cloud bietet die gesamte Funktionalität der Splunk Enterprise-Plattform. Es handelt sich um eine verwaltete Lösung, die von Splunk gehostet und betrieben wird.	Abo (Subscription) Klassisch Cloud-based (Cloud Usage) Usage Based
IBM QRadar	Gute Integration, Starke Automatisierungsfunktionen, Skalierbarkeit, Umfangreiche Regelbibliothek	Hohe Lizenzkosten, Weniger intuitive Benutzeroberfläche, Komplex in der Verwaltung	Cloud von IBM	Abo (Subscription) Klassische Lizenz
ArcSight (Micro Focus)	Starke Erkennung und Reaktion, Skalierbarkeit, Gute Unterstützung für Compliance	Teuer, Steile Lernkurve, Schwierigkeiten bei der Integration mit nicht-Micro Focus-Produkten	Micro Focus bietet ArcSight als Software-as-a-Service (SaaS) an	Abo (Subscription) Klassische Lizenz
LogRhythm	All-in-One-Lösung, Benutzerfreundlich, Kosteneffektiver, Starke Automatisierungsfunktionen	Weniger leistungsfähig in sehr großen Umgebungen, Inkonsistenter Kundensupport, Komplex für kleinere Unternehmen	LogRhythm bietet eine SaaS-Cloud-Lösung an, bekannt als LogRhythm Axon	Abo (Subscription) Klassische Lizenz Cloud-based (Cloud Usage)
Microsoft Azure Sentinel	Cloud-basiert, Gute Integration mit Microsoft-Produkten, Kosteneffizient, Starke AI- und ML-Funktionen	Abhängigkeit von Azure, Weniger ausgereift, Erfordert spezielle Kenntnisse in Azure	Cloud-Native	Pay-as-you-go Subscription
RSA NetWitness	Starke Bedrohungserkennung und,reaktion, Gute Integration, Skalierbarkeit	Teuer, Komplex in der Verwaltung, Weniger intuitive Benutzeroberfläche	NetWitness Detect AI	Subscription, Perpetual

BIESER