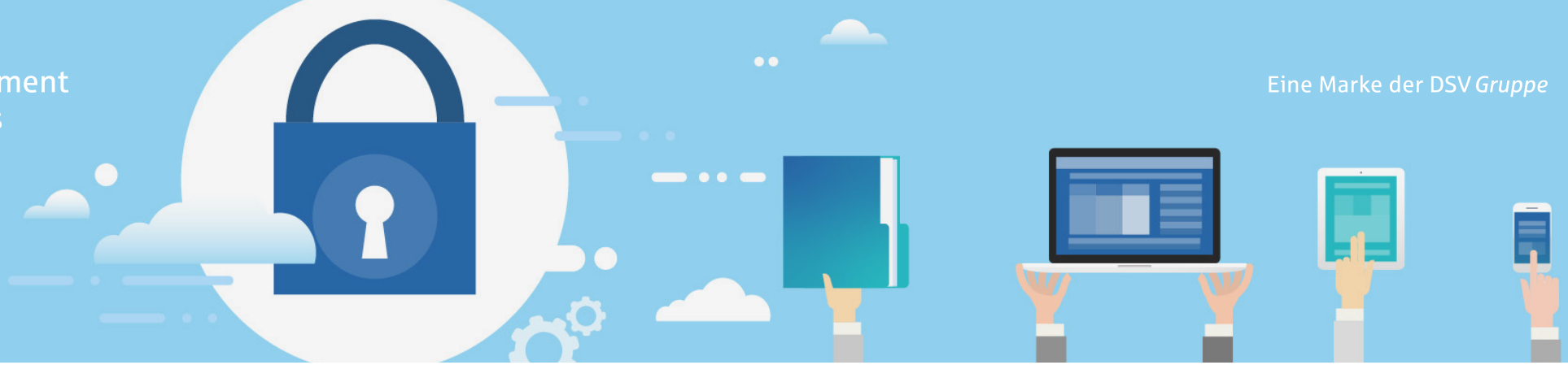
Management Services

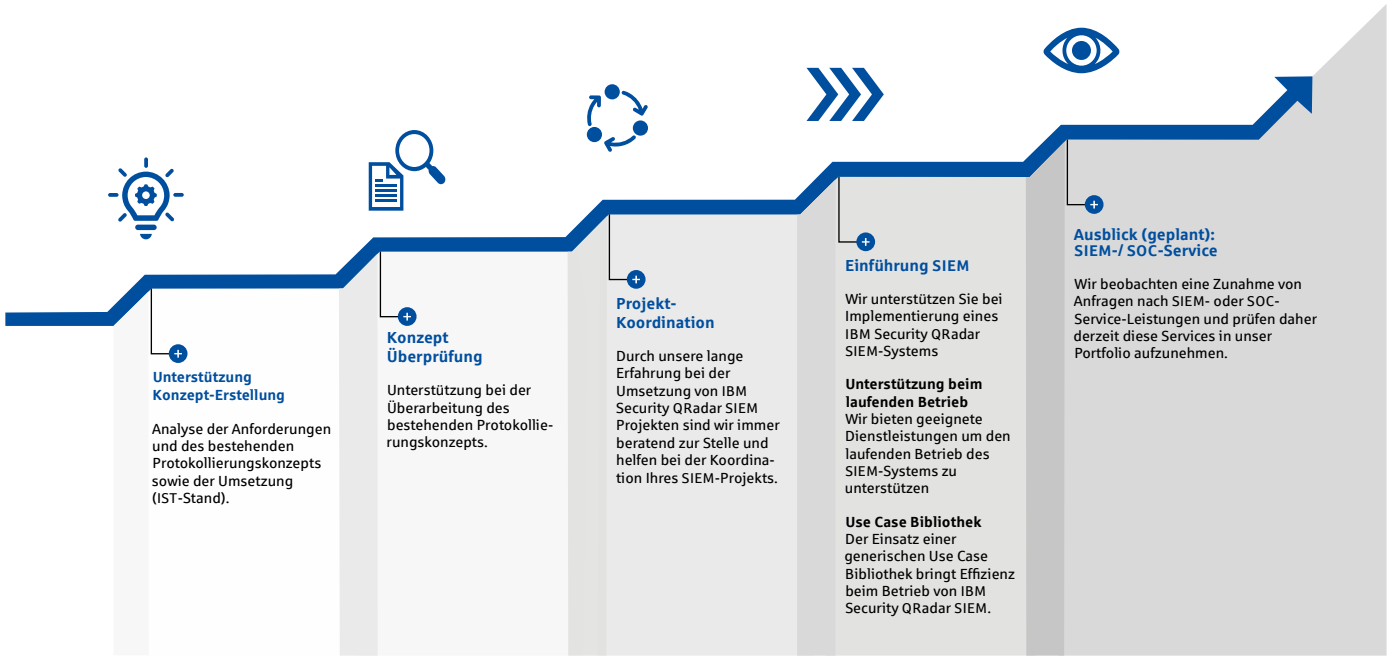
Eine Marke der DSV *Gruppe*



Unser Beratungsangebot zu SIEM.

IBM Security QRadar SIEM.

Aufsichtsrechtliche Anforderungen sowie die sich ständig ändernde Bedrohungslage durch Cyber-Angriffe sind häufig genannte Treiber für den Einsatz einer SIEM-Plattform. Wir bieten unseren Kunden hierzu die marktführende IBM Security QRadar SIEM Software und passende Services an. Unsere Lösung kombiniert persönliche Beratung und kostengünstige Bereitstellung der IBM Software-Lizenzen sowie dauerhafter Service und Support vor, während und nach dem Projekt.



Unterstützung Konzept-Erstellung

Analyse der Anforderungen und des bestehenden Protokollierungskonzepts sowie der Umsetzung (IST-Stand).

Konzept Überprüfung

Unterstützung bei der Überarbeitung des bestehenden Protokollierungskonzepts.

Projekt-Koordination

Durch unsere lange Erfahrung bei der Umsetzung von IBM Security QRadar SIEM Projekten sind wir immer beratend zur Stelle und helfen bei der Koordination Ihres SIEM-Projekts.

Einführung SIEM

Wir unterstützen Sie bei Implementierung eines IBM Security QRadar SIEM-Systems

Unterstützung beim laufenden Betrieb
Wir bieten geeignete Dienstleistungen um den laufenden Betrieb des SIEM-Systems zu unterstützen

Use Case Bibliothek
Der Einsatz einer generischen Use Case Bibliothek bringt Effizienz beim Betrieb von IBM Security QRadar SIEM.

Ausblick (geplant): SIEM-/ SOC-Service

Wir beobachten eine Zunahme von Anfragen nach SIEM- oder SOC-Service-Leistungen und prüfen daher derzeit diese Services in unser Portfolio aufzunehmen.

Protokollierung und SIEM Best Practice.

Kundenbeispiel.

Die bisherige Lösung war bei unserem Referenzkunden mit sehr viel manuellem Aufwand verbunden, was eine konsequente Prüfung der Logs in „Echtzeit“ stark erschwert.

Hingegen ist mittels IBM Security QRadar SIEM eine echtzeitnahe Korrelation und Alarmierung von Sicherheitsvorfällen zu realisieren.

Somit muss keine manuelle Auswertung der Logs, sondern lediglich eine manuelle Prüfung und Bewertung der durch IBM Security QRadar erstellten Alarme erfolgen.

Dienstleistungen der S-MS.

- Persönliche Beratung bei Konzept-Erstellung und bei der Hersteller-Auswahl
- Kostengünstige Bereitstellung der Lizenzen
- Dauerhafter Service und Support vor, während und nach dem Projekt

Effiziente Identifikation von Bedrohungen.

Die Situation: Schwächen bei Log-Auswertungen

- Sicherheitsanforderungen des Payment Card Industry Data Security Standard (PCI-DSS).
- Die bisherige Lösung erforderte hohen manuellen Aufwand.
- Die IBM Security QRadar SIEM-Plattform ermöglicht eine zeitnahe Prüfung der IT-Protokolle (Logs) der Systeme und die Korrelation von Sicherheitsereignissen.

Die Lösung: Einführung einer SIEM Umgebung

- Workshops und Beratung zeigten, dass IBM Security QRadar SIEM preislich und funktional überzeugt.
- Die IBM-Lösung zeichnet sich durch eine automatisierte, zentrale Protokollierung und Auswertung der Logs aus. Durch eine Regel- und verhaltensbasierte Erkennung sicherheitsrelevanter Ereignisse erfolgt eine Alarmierung in Echtzeit.
- Sämtliche Sicherheitsereignisse werden revisionssicher gespeichert. Compliance-Berichte wie Reports werden mit der Lösung erstellt.

Auf einen Blick.

Unser Referenzkunde unterliegt dem Payment Card Industry Data Security Standard, kurz PCI-DSS, der die Notwendigkeit von Log-Auswertungen definiert. Ziel war die Performance-Verbesserung und eine Korrelation der Logs zu ermöglichen. Durch das umfassende Beratungs- und Unterstützungsangebot zu SIEM der S-Management Services wurde eine neue Lösung gefunden, die die bestehenden Probleme behebt und zusätzlich die Berichterstellung erleichtert.

Kontaktpersonen

Martin Karpa | Fachberater

Telefon +49 711 782-22056
martin.karpa@s-management-services.de

Matthias Wüchner | Produktmanager

Telefon +49 711 782-21839
matthias.wuechner@s-management-services.de

S-Management Services GmbH
Am Wallgraben 115
70565 Stuttgart
www.s-management-services.de

Stand 05.2022