

# **Security Information and Event Management (SIEM)**

**- Konzept -**

## Inhaltsverzeichnis

Prüfung und Freigabe .....	2
Änderungshistorie .....	3
Dokumentensteuerung und Verteilerkreis .....	4
1 Ziel und Zweck .....	7
2 Geltungsbereich .....	7
3 Verantwortlichkeiten für das Management dieser Regelung .....	7
4 Begriffe .....	8
5 Management von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen .....	9
5.1 Änderungsmanagement .....	9
5.2 Planung .....	9
5.2.1 Allgemeines .....	9
5.2.2 Risikomanagement .....	10
5.2.3 Ressourcen .....	12
5.2.4 Beschaffung .....	12
5.2.5 Datenschutz und Arbeitnehmerrechte .....	12
5.2.6 Informationssicherheitsvorfall .....	13
5.2.7 Schulung und Unterweisung .....	13
5.3 Umsetzung .....	14
5.3.1 Allgemeines .....	14
5.3.2 Anforderungen an Aktivitäten des Security Information and Event Management .....	14
5.3.3 Verantwortungsbereiche für das Monitoring und die Behandlung von Events .....	16
5.3.3.1 Use Case Designer .....	16
5.3.3.2 Content Engineer .....	16
5.3.3.3 Security Incident Manager .....	17
5.3.3.4 Security Analyst .....	17
5.3.3.5 Security Operations Center (SOC) .....	17
5.3.4 Korrelierende Konzepte für den Betrieb der SIEM-Lösung .....	18
5.3.4.1 Einbindung des Monitoring und Event Management .....	18
5.3.4.2 Einbindung des Incident Management .....	19
5.3.4.3 Einbindung des CERT und CSIRT .....	20
5.3.4.4 Einbindung der Lenkung eines Informationssicherheitsvorfalls .....	20
5.3.4.5 Einbindung des Business Continuity Management / Business Continuity Planning .....	21
5.3.5 Entwicklung, Design und Modellierung der Use Cases .....	22
5.3.5.1 Identifikation und Festlegung der Datenquellen für das Monitoring .....	24
5.3.6 Kategorisierung und Klassifizierung von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen .....	25
5.3.7 Priorisierung der Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle .....	26
5.3.8 Detektion von sicherheitsrelevanten Ereignissen und Vorfällen .....	27
5.3.8.1 Besonderheiten der Protokollierung beim Betrieb einer SIEM-Lösung .....	27

5.3.8.2 User and Entity Behavior Analytics (UEBA) .....	27
5.3.8.3 Vorgehensweise und Ablauf der Detektion .....	28
5.3.9 Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle .....	30
5.3.9.1 Security Orchestration, Automation and Response (SOAR) .....	30
5.3.9.2 Vorgehensweise und Ablauf der Reaktion .....	30
5.3.9.3 Reaktionsstruktur .....	31
5.3.9.4 Management der Information und der Kommunikation .....	32
5.3.9.5 Management der in Kenntnissetzung, der Meldung einer Warnung oder eines Alarms sowie der Benachrichtigung .....	33
5.3.10 Auswahl und Beschaffung des SIEM-Tools .....	35
5.3.10.1 Allgemeines .....	35
5.3.10.2 Security Orchestration, Automation and Response (SOAR) .....	36
5.3.10.3 Kriterien für die Auswahl des SIEM-Tools .....	36
5.3.10.4 Kriterien für die Beschaffung des SIEM-Tools .....	38
5.3.10.5 Kriterien für den Betrieb des SIEM-Tools .....	38
5.4 Überwachung .....	39
5.4.1 Allgemeines .....	39
5.4.2 Maßnahmen der Überwachung .....	39
5.5 Aufrechterhaltung und Verbesserung .....	40
5.5.1 Allgemeines .....	40
5.5.2 Maßnahmen der Aufrechterhaltung und Verbesserung .....	40
6 Sanktionen .....	41
7 Referenzierte Dokumente .....	41

Bitte dieses Dokument an Ihre Organisation anzupassen