



## SIEM nach ISO 27001 Security Information and Event Management

Dieser **Praxis Workshop** stellt das Basiswissen und die Grundbegriffe von SIEM Systemen vor und ist somit auch für technisch nicht so versierte Teilnehmer geeignet.

- Einführung und Grundlagen eines SIEM Systems: SIEM vs. Abgrenzung Monitoring, IDS/IPS
- Organisatorische Voraussetzungen und Vorarbeiten: inkl. Herausforderung Incident Response
- Technische Voraussetzungen und Vorbereitung: Benötigte Komponenten, Abschätzen Speicherbedarf
- Audit-Policy: Compliance Anforderungen, Reporting
- Implementierung eines SIEM Systems: Projektphasen, Herausforderung Noise-Reduction

### Listenpreis

2.690,00 € exkl. MwSt

3.201,10 € inkl. MwSt

### Dauer

3 Tage

### Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

### Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

### Ihre Ansprechpartnerin



**Manuela Krämer**  
Leitung  
Informationssicherheit

### Kontakt/Fragen:

[m.kraemer@cbt-training.de](mailto:m.kraemer@cbt-training.de)

Telefon: +49 (0)89-4576918-12

## Inhalte

- **Modul 1: Einführung und Grundlagen**
  - Die Motivation für den Einsatz von SIEM
  - Grundlegende Funktionsweise eines SIEM Systems
  - Abgrenzung: Monitoring vs. SIEM
  - Abgrenzung: IDS/IPS vs. SIEM
  - Vergleich verschiedener Ansätze für SIEM
  - Typische Anwendungsfälle
  - Live Demo eines SIEM Systems
  - Grenzen eines SIEM Systems
- **Modul 2: Organisatorische Voraussetzungen und Vorarbeiten**
  - Inhalte eines Kick-Off Meetings zur Einführung von SIEM
  - Festlegen der Zielsetzung
  - Auswahl und Definition der Anwendungsfälle
  - Herausforderung: Incident Response
  - Betriebsprozesse
  - Rollen innerhalb des SIEM Systems
- **Modul 3: Technische Voraussetzungen und Vorbereitung**
  - Prüfung der Realisierbarkeit
  - Auswahlkriterien für ein SIEM-System
  - Allgemeine technische Voraussetzungen
  - Benötigte Komponenten / Verteilte SIEM Systeme
  - Abschätzen des Speicherbedarfs
  - Herausforderung: Das richtige Maß finden
- **Modul 4: Knackpunkt: Audit-Policy**
  - Typische Inhalte einer Audit-Policy
  - Compliance Anforderungen
  - Anforderungen aus Unternehmensrichtlinien
  - Definition der zu überwachenden Objekte



- Definition der zu überwachenden Ereignisse
- Reporting
- **Modul 5: Implementierung eines SIEM Systems**
  - Typische Projektphasen
  - Schritte zur Einführung eines SIEM Systems
  - Typische Fragestellungen
  - Herausforderung: Noise-Reduction
  - Zusammenfassung, Fragerunde und Diskussionen

---

### Ziele

Dieser Kurs stellt das Basiswissen und die Grundbegriffe von SIEM Systemen vor und ist somit auch für technisch nicht so versierte Teilnehmer geeignet.

- Einführung und Grundlagen
- Organisatorische Voraussetzungen und Vorarbeiten
- Technische Voraussetzungen und Vorbereitung
- Audit-Policy
- Implementierung eines SIEM Systems

---

### Zielgruppe

IT-Sicherheitsverantwortliche, IT-Mitarbeiter, IT-Leiter, Sicherheitsbeauftragte, Geschäftsführer, IT-Manager, Compliance Beauftragte.

---

### Voraussetzungen

Die Teilnehmer sollten über grundlegende Kenntnisse der ISO 27001 Standards und Prozesse innerhalb eines Information Security Management Systems (ISMS) verfügen.

Gute Anwenderkenntnisse von Windows- oder Unix-Systemen sollten vorhanden sein. Erfahrungen aus dem Bereich der System- und Netzwerkverwaltung sind hilfreich.

---