CBT Training & Consulting GmbH
www.cbt-training.de
www.it-informationssicherheit.de

Informationssicherheit

Teilnahmebestätigung

Angela Baruth

hat am Seminar

SIEM nach ISO 27001

Security Information and Event Management

vom 10.05.2023 bis 12.05.2023

teilgenommen.

Continuing Professional Education Hours Earned: 24 CPE

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

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

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

Knackpunkt: Audit-Policy
- IT-typische Inhalte einer Audit-Policy
- Compliance Anforderungen
- Anforderungen aus Unternehmensrichtlinien
- Definition der zu überwachenden Objekte
- Definition der zu überwachenden Ereignisse
- Reporting

Implementierung eines SIEM Systems
- Typische Projektphasen
- Schritte zur Einführung eines SIEM Systems
- Typische Fragestellungen
- Herausforderung: Noise-Reduc

Dozent: Dipl.-Inf. Christian Brinz
Senior Security Architect

Gabriela Bücherl
CEO
CBT Training & Consulting GmbH

Manuela Krämer
Leitung Informationssicherheit
CBT Training & Consulting GmbH