SC480 Secure Operations

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Einführung in Security Operations (SecOps). Vermittelt werden Grundsätze zur Integration von Sicherheitsaspekten in tägliche Betriebsprozesse sowie Ansätze zur erfolgreichen Einführung von SecOps im Unternehmen. Behandelt werden zudem die Wechselwirkungen zwischen Informationssicherheit, Betrieb und anderen Prozessen, um Reaktionsfähigkeit und Effizienz zu steigern.

Zielgruppe:

Das Training **SC480 Secure Operations** richtet sich an:

- Administratoren
- Security Engineers
- Security Architects
- DevOps Engineers
- Informationssicherheitsbeauftragte / CISOs

Voraussetzungen:

Grundsätzliche Kenntnisse in der Informationssicherheit sind empfehlenswert, jedoch keine zwingende Voraussetzung. Um den Kursinhalten und dem Lerntempo im Workshop **SC480 Secure Operations** gut folgen zu können, sind praktische Erfahrungen im Bereich IT-Administration nötig.

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

- Verständnis der Bedeutung von Secure Operations (SecOps) für Organisationen
- Kennenlernen der Unterschiede zwischen traditionellen Sicherheitsansätzen und SecOps
- Grundlegendes Verständnis von Sicherheitskonzepten wie Zero Trust und Least Privilege
- Sensibilisierung für aktuelle Sicherheitsbedrohungen und -risiken
- Fähigkeit zur Echtzeitüberwachung und Erkennung von Sicherheitsanomalien im Betrieb
- Vertrautheit mit SIEM-Systemen und deren Rolle bei der Bedrohungserkennung
- Integration von Automatisierungstools zur Effizienzsteigerung in SecOps
- Verständnis der Rolle von SecOps bei der sicheren Bereitstellung von Anwendungen
- Fähigkeit zur Bewertung der Effektivität von SecOps-Maßnahmen
- Erwerb von Fähigkeiten zur Datenerfassung und -analyse für kontinuierliche Verbesserung
- Anpassung an sich wandelnde Bedrohungen und Geschäftsanforderungen

Inhalte/Agenda:

- ♦ **Modul 1: Grundlagen von Secure Operations**
  - ♦ ◊ Einführung in SecOps: Bedeutung, Ziele und Vorteile
  - ◊ Evolution der Sicherheitspraktiken: Von Silos zu Integration
  - ◊ Wichtige Begriffe und Konzepte: Zero Trust, Least Privilege, usw.
- ♦ ◊
- ♦ **Modul 2: Sicherheitsbewusstsein und Bedrohungslandschaft**
  - ♦ ◊ Sensibilisierung für aktuelle Sicherheitsbedrohungen
  - ◊ Phishing, Social Engineering und andere Angriffstechniken
  - ◊ Wie Sicherheitsbewusstsein die Unternehmenssicherheit stärkt
- ♦ ◊
- ♦ **Modul 3: Grundlagen der Informationssicherheit im Betrieb**
  - ♦ ◊ Identitätsmanagement und Zugriffskontrolle
  - ◊ Netzwerksicherheit und Überwachung
  - ◊ Änderungs- und Patchmanagement
  - ◊ Cloud-Sicherheit und moderne Technologien
  - ◊ Anforderungen aus der Regulatorik
  - ◊ Definition von Maßnahmen, Umsetzungsplänen und Wirtschaftlichkeitsbetrachtungen
  - ◊ Bereitstellung von personellen und finanziellen Ressourcen
- ♦ ◊
- ♦ **Modul 4: Incident Response und Krisenmanagement**
  - ♦ ◊ Aufbau eines Vorfallreaktionsplans: Vorbereitung auf den Ernstfall
  - ◊ Identifikation, Reaktion und Wiederherstellung nach Vorfällen
  - ◊ Kommunikation und Koordination in Krisensituationen
- ♦ ◊
- ♦ **Modul 5: Automatisierung, Tooling und DevSecOps**
  - ♦ ◊ Integration von Automatisierung in SecOps-Praktiken
  - ◊ Übersicht über Automatisierungstools und deren Einsatz
  - ◊ Verknüpfung von Sicherheit und DevOps für effektive Bereitstellung
- ♦ ◊
- ♦ **Modul 6: Evaluierung und kontinuierliche Verbesserung**
  - ♦ ◊ Bewertung der Effektivität von SecOps-Maßnahmen
  - ◊ Datenerfassung und -analyse zur Identifizierung von Schwachstellen
  - ◊ Anpassung an sich wandelnde Bedrohungen und Geschäftsanforderungen
  - ♦ ◊