SC190 Information Security Incident Management

Kurzbeschreibung:

Teilnehmer erhalten eine praxisnahe Einführung in Incident Handling. Vermittelt werden Grundlagen zur Erkennung und Analyse von Vorfällen, zum Aufspüren von Angriffen im Netzwerk sowie zum Umgang mit Clients und Servern. Behandelt wird, wie Supportfälle von Fehlbedienungen und Angriffen unterschieden werden und wie durch Übungen effektive Reaktionsfähigkeit trainiert wird.

Zielgruppe:

Das Training **SC190 Information Security Incident Management** richtet sich an:

- Verantwortliche für Informationssicherheit
- Verantwortliche von IT-Operations
- Incident Manager
- Prozessverantwortliche

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Workshops **SC190 Information Security Incident Management** gut folgen zu können, sollten Sie Vorkenntnisse aus folgenden Bereichen mitbringen:

- Grundkenntnisse der Informationssicherheit
- Kenntnisse des Tagesgeschäfts von IT-Operations

Sonstiges:

Dauer: 2 Tage

Preis: 1400 Euro plus Mwst.

Ziele:

Nach Abschluss des Workshops sind Sie in der Lage, Sicherheitsvorfälle bzw. Störungen zu erkennen und geeignete Maßnahmen einzuleiten, um den Betrieb schnellstmöglich wiederherzustellen. Sie erhalten ein vertieftes Verständnis und lernen vor allem die Umsetzung und den Betrieb eines Information Security Incident Management Prozesses.

Darüber hinaus lernen Sie aktuelle Best Practices aus Fast-Response-Konzepten, die strukturierte Arbeit mit Playbooks und Runbooks sowie die Analyse von Malware- und Ransomware. Sie trainieren die Zusammenarbeit mit internen und externen Rollen, um auch in komplexen Vorfällen souverän handlungsfähig zu bleiben.

Inhalte/Agenda:

- ♦ **Grundlagen und First Response**
  - ♦ ◊ Darstellung eines mehrstufigen Angriffes auf einen Informationsverbund
  - ◊ Gegenseitiges Wirken von Angriff und Abwehr
  - ◊ Bedeutung der Timeline für die schnelle Erkennung eines Vorfalls
  - ◊ Grundsätze und Richtlinien des IR-Managements
  - ◊ Aufbau einer zuverlässigen Meldekette und First Response
  - ◊ Vorstellung eines Fast-Response-Konzepts basierend auf den Rollen Ersthelfer, SIRT und Notfallstab

  ♦ **Forensik und Incident Handling in der Praxis**
  - ♦ ◊ Livedemo von Angriffen auf Windows- und Linux-Maschinen
  - ◊ Triageprozess durch IT-Ops und nachgelagertes SOC und CSIRT
  - ◊ Sec-Ops-Forensik 1: Spurensuche in Windows-Maschinen
  - ◊ Sec-Ops-Forensik 2: Spurensuche in Linux-Maschinen
  - ◊ Sec-Ops-Forensik 3: Spurensuche in OT
  - ◊ Remediation von infizierten Systemen
  - ◊ Workshop: Arbeiten mit Playbooks und Runbooks in einem selbstgehosteten Notfallsystem
  - ◊ Malware- und Ransomwareanalyse: typische Spuren, Verhalten, Indicators of Compromise (IoCs)

  ♦ **Netzwerkangriffe und Eskalation:**
  - ♦ ◊ Angriffe auf das Netzwerk von außen und innen
  - ◊ Die Bedeutung von Delivery- und Comand&Control-Servern
  - ◊ Sec-Ops-Forensik 4: Spurensuche in verteilten LDAP und AD-Diensten
  - ◊ Sec-Ops-Forensik 5: Spurensuche in Netzwerken und Firewalls
  - ◊ Sec-Ops-Forensik 3: Aufspüren von ICMP/DNS-Tunneln und Backdoors
  - ◊ Best Practices und Validierung von Angriffsquellen
  - ◊ Rollen und Funktionen im Vorfallmanagement: Zusammenspiel von Ersthelfer, Incident Manager, SIRT, IT-Ops und Notfallstab

  ♦ **Vertiefung, Übungen und Zusammenarbeit mit externen Partnern:**
  - ♦ ◊ Individueller DeepDive von Themen der Module 1-3
  - ◊ Praxisübung: Behandlung von Sicherheitsvorfällen
  - ◊ Erfahrungsaustausch
  - ◊ Zusammenarbeit mit externen situativen Erweiterungen wie Cyberversicherern, forensischen Dienstleistern und Kriminalisten

  ♦ Bei Inhouse-Schulungen/Geschlossenen Kursen, die online stattfindet, gehen wir gern auf Ihre individuellen Terminwünsche ein. So können wir den Kurs anstatt an zwei Tagen mit jeweils 8 Stunden auch an 4 Tagen mit jeweils 4 Stunden durchführen. Sprechen Sie uns an!

  ♦