

SC100 Cyber Security Foundation

Kurzbeschreibung:

Die Teilnehmer erhalten einen kompakten Überblick über die Cyber Security-Landschaft. Sie lernen Angriffs- und Verteidigungsmechanismen in Theorie und Praxis kennen und trainieren das Zusammenspiel von Mensch, Organisation und Technologie. Der Kurs führt in **aktuelle Bedrohungen, KI-gestützte Angriffe und Verteidigungsstrategien** sowie in **tagesaktuelle Sicherheitsvorfälle aus der Infosec-Branche ein**.

Zielgruppe:

Der Workshop **C100 Cyber Security Foundation** richtet sich an erfahrene sowie bereits etablierte und auch neue Mitarbeiter im Bereich Informationssicherheit.

Er ist besonders geeignet für Teilnehmer, die bisher wenig Berührung mit der ganzen Themenbreite der Informationssicherheit hatten, weil Sie zum Beispiel eher Experte in einem bestimmten Themenbereich sind und nun einen Blick über den Tellerrand werfen wollen.

Voraussetzungen:

Es sind keine spezifischen Vorkenntnisse bzgl. Informationssicherheit und IT-Sicherheit für die Teilnahme am Kurs **SC100 Cyber Security Foundation** erforderlich.

Sonstiges:

Dauer: 2 Tage

Preis: 1350 Euro plus Mwst.

Ziele:

- Vertiefen Sie Ihr Wissen über die Wechselwirkung von Angriff und Verteidigung bei den zentralen Komponenten Technologie, Organisation und Mensch.
- Lernen Sie Maßnahmen zur Sicherstellung eines anvisierten Sicherheitsniveaus kennen und erfahren Sie, wie die Häufigkeit, Schadenshöhe und Eintrittswahrscheinlichkeit behandelt werden, um ein Risiko zu minimieren.
- Bekommen Sie einen Überblick über die wichtigsten aktuellen Sicherheitsstandards und deren Zusammenwirken.
- Erleben Sie den Einsatz von Kryptografie im modernen Sicherheitsumfeld – von alltäglicher Datenverschlüsselung bis zu post-quantenresistenten Verfahren.
- Vervollständigen Sie Ihre Grundlagen: Von den Ursprüngen der deutschen Hackerundergroundszene, über die Gründung der ENISA und des BSI, die Best Practices beim Aufbau eines ISMS bis zu den Lieblingscontrols der Auditoren.
- Reflektieren Sie anhand realer, aktueller Vorfälle die Rolle von KI in Angriff und Verteidigung und erlernen Sie Strategien für den Umgang mit neuen Bedrohungen.
- Trainieren Sie mit einem erfahrenen Hacker und Social Engineer Ihre eigenen Social Skills – inklusive Erkennung von Deepfakes und KI-basierten Social-Engineering-Attacken – und kreieren Sie in Gruppenarbeit ein eigenes Awarenessprogramm.
- Bereiten Sie sich und Ihre Kollegen mit Best Practices des Resilienz- und IT-Notfallmanagements auf den Fall der Fälle vor.



Inhalte/Agenda:

- **Erstellung von Angriffsszenarien auf Firmen anhand von öffentlich sichtbaren Vektoren als moderierte Live-Demo**
- ♦ **Diskussion und kreative Auslassung von Angriff und Verteidigung**
 - ♦ Wie wirken Offense und Defense aufeinander?
 - ♦ Neue Dimension: KI-basierte Angriffe (z. B. generative Malware, automatisiertes Phishing, Deepfake-Audios für Social Engineering)
 - ♦ Verteidigung durch KI-gestützte Abwehrmechanismen wie Machine Learning für Anomalieerkennung, automatisierte Threat-Hunting-Systeme
 - ♦ Einbindung aktueller Infosec-Vorfälle (z. B. Ransomware-Trends, Supply-Chain-Angriffe, KI-gestützter Betrug)
- ♦ **Vergrößern der Sicherheitsoberfläche (Technik – Organisation – Mensch)**
 - ♦ Wie stärken Schutzbedarfsklassifizierung, Risikoanalyse, Risk Management, Compliance die Sicherheit?
 - ♦ Besonderheiten bei Clouddienstleistungen (Vendor-Lock, Geo-Risiko, Exit-Strategie)
 - ♦ Vorstellung der Lockheed-Martin Cyber Kill Chain
- ♦ **Welche Standards sind relevant? Wie sind sie aufgebaut und wofür sind sie praktisch nutzbar?**
 - ♦ Wie bauen sie aufeinander auf und ergänzen sich (z.B. Kreuzreferenztabellen IT-Grundschutz zu ISO27001)?
 - ♦ Vorstellung NIST Cybersecurity Framework, ISO 2700X Familie, BSI Grundschutz-Standards, weitere relevante Organisationen wie Teletrust, ENISA oder OWASP
- ♦ **Grundlagen der technischen IT-Sicherheit**
 - ♦ Aufbau des Netzes
 - ♦ Sichere Anbindung von lokalen Netzen an das Internet
 - ♦ Sichere Nutzung von WLAN
 - ♦ Sicherer Einsatz von IPv4 und IPv6
- ♦ **Komponenten im Netz**
 - ♦ Absicherung eines PC-Clients
 - ♦ Absicherung eines Servers
- ♦ **Dienste und Anwendungen im Internet**
 - ♦ Sichere Nutzung von E-Mail
 - ♦ Sicherer Betrieb von E-Mail-Servern
 - ♦ Sichere Nutzung von Webangeboten
 - ♦ Sicheres Bereitstellen von Webangeboten
 - ♦ Sichere Internettelefonie (VoIP)
 - ♦ Sicherer Fernzugriff auf lokale Netze (VPN)
- ♦ **Wie entstehen Vulnerabilitäten und wie werden sie entdeckt?**
- ♦ **Workshop: Entdeckung und Schwächung von Vulnerabilitäten durch technische, menschliche und organisatorische Maßnahmen an verschiedenen Szenarien**
- ♦ **Grundlagen des Social Engineering**
 - ♦ Psychologische Grundlagen
 - ♦ OSINT und Information Gathering
 - ♦ Typische Angriffs-Szenarien (Phishing, Vishing, Lishing, Smishing, Deepfakes, Tailgating, Spoofing)
 - ♦ Verteidigung gegen SE-Angriffe (inkl. Training im Erkennen KI-erzeugter Inhalte)
- ♦ **Lagebild des Cybercrime**
 - ♦ Hacktivisten, State Nation Actors, Commercial Hackers, Skriptkiddies
 - ♦ Darknet, Deepweb, Trojaner/Viren/Würmer, WLAN + USB-Angriffe, DDoS, Ransomware, Lateral Movement in Berechtigungssystemen (am Beispiel von Active Directory)
- ♦ **Aufbau eines resilienten ISMS**
 - ♦ Zweckbestimmung, Sammeln der Stakeholder, Wahl des Systems, Risikoanalyse, Bestimmung der Rollen und Funktionen, Compliance, Governance, Erstellen von Richtlinien, Sicherheitskonzepten und Maßnahmen
- ♦ **Technologie zur Cybersicherheit:**
 - ♦

- ◊ Präventiv: Firewalls, Proxy, Segmentierung, Hardening, IAM, Kryptografie (klassische Verfahren, Schlüsselmanagement, Zero-Trust-Ansätze, Post-Quantum-Kryptografie), Patching, Backup
- ◊ Detektiv: advanced Analytics, Virenschutz (Signatur/Heuristik/nextGen), NBAD (Network Behavior Anomaly Detection), Mailprotection, Honeypots Detection), Mailprotection, Honeypots
- ◊ Reaktiv: Quarantäne, Behaviour Blocking, SIEM, SOC, CERT, Forensik
- ◊ Prädiktiv: • Darknetüberwachung/Underground Spotting, Bug Bounty, BCM, BIA

◆ **BCM – Notfallvorsorge und Maßnahmen zur Resilienz**

- ◆ ◊ Wie bereitet man sich auf das Unerwartete vor (Black Swan, N.N.Taleb)?

◆ **Awareness – Kampagnenaufbau, Fehlerkultur, Teambuilding, Lighthouse-Projekte**