ANGRIFFSSZENARIEN DER CYBER-KRIMINELLEN

Lehrgangsnummer: CS-3-01

ZIEL

Sie lernen die aktuellen Vorgehensweisen der Cyber-Kriminellen kennen, um zu wissen, wo überhaupt potenzielle Bedrohungen vorliegen könnten.

ZUGANGSVORAUSSETZUNG

Mehrjährige Erfahrung im Bereich IT- bzw. Cyber-Security.

LERNMETHODIK

Lehrvortrag, Diskussion, Gruppenarbeit, Projektarbeit

LEHRGANGSMATERIALIEN

Als seminarbegleitende Unterlage erhalten Sie ein Lehrgangsskript in digitaler Form oder auf Wunsch auch auf Papier.

ZERTIFIKATSERWERB

Zum Abschluss des Lehrgangs erhalten Sie eine Teilnahmebescheinigung. Sofern der Lehrgang mit einer bestandenen Prüfung endet, wird Ihnen ein Zertifikat ausgestellt.

LEHRGANGSINHALTE

- Grundlagen des betroffenen IT- / OT-Umfeldes
  - Schutzziele der IT-Sicherheit
  - Das Purdue Referenz-Modell
  - Besonderheiten IT / OT im Vergleich
  - Anforderungen an vernetzte und spezifische Systeme
  - Kritische Infrastrukturen
- Angreifer und Bedrohungen
  - Beispiele der Vergangenheit
  - Täter und Motive
  - Psychologie der Angreifer
  - Angriffsvektoren
  - Werkzeuge des Angreifers
- Angriffsszenarien
  - Cyber Kill Chain
  - Malware, Phishing und Exploits
  - Hacking von Webservern
  - Identitätsdiebstahl
  - Drive-by-Exploits
  - Schadsoftware-Infiltration
  - Distributed Denial of Service (DDoS)
  - Advanced Persistent Threat (APT)

FACHLICHER ANSPRECHPARTNER

Prof. h.c. PhDr. Stefan Loubichi
CISO-MCSE-MCDBA-MCAD-CCNA
Telefon 0201 4862-201 | E-Mail s.loubichi@ksg-gfs.de

ANMELDUNG

Daniela Ruhrus
Telefon 0201 4862-151 | E-Mail d.ruhrus@ksg-gfs.de

DATEN UND FAKTEN

Dauer	1 Tag
Teilnehmer*innen	min. 12 - max. 20
Termine	15.06.2020 und 01.12.2020 oder auf Anfrage
Zeit	8.00 - 16.30 Uhr
Gebühren	750,00 € zzgl. MwSt.
Ort	Simulatorzentrum in Essen oder Siemens Energy Standort Karlsruhe oder Erlangen oder als Inhouse-Seminar bei Ihnen vor Ort

WICHTIGER HINWEIS

Wir empfehlen, dieses Seminar mit dem Seminar CS-3-02 „Abwehrmöglichkeiten gegen Cyber-Attacken“ zu kombinieren