SC425 Red Teaming Master Class

Kurzbeschreibung:

In der intensiven fünftägigen **SC425 Red Teaming Master Class** lernen die Teilnehmer, als hocheffektives Red Team zu agieren. Der Schwerpunkt liegt auf der Zusammenarbeit verschiedener Spezialisierungen, der Entwicklung von Soft Skills und der praktischen Anwendung fortgeschrittener Angriffstechniken in realistischen Simulationen gegen ein aktives Blue Team.

Zielgruppe:

- Erfahrene IT-Sicherheitsspezialisten
- Penetrationstester
- Cybersecurity-Experten, die ihre Fähigkeiten in Red Team Operations vertiefen und ihre Zusammenarbeit in einem Team verbessern möchten

Voraussetzungen:

Um den Inhalten und dem Lerntempo des Kurses **SC425 Red Teaming Master Class** gut folgen zu können, empfehlen wir folgende Vorkenntnisse:
Vorherige Teilnahme an mindestens einem der Red Team Lernpfade: Hacking & Pentesting, Social Engineering, OSINT

Sonstiges:

Dauer: 5 Tage

Preis: 3750 Euro plus Mwst.

Ziele:

Dieses Training **SC425 Red Teaming Master Class** kombiniert intensive praktische Übungen mit der Entwicklung essenzieller Soft Skills für erfolgreiche Red Team Operations. Die Teilnehmer werden nicht nur ihre technischen Fähigkeiten verbessern, sondern auch lernen, effektiv in einem hochspezialisierten Team zu arbeiten und auf unerwartete Herausforderungen zu reagieren.

Inhalte/Agenda:

- **Grundlagen und Teambildung**
- ♦ Einführung in Red Team Operations und Rollenverteilung
  ♦ Team-Building-Übungen und Kommunikationstraining
  ♦ Überblick über Angriffstaktiken und die MITRE ATT&CK Matrix
  ♦ Simulation 1: Kleine Angriffsübung mit Fokus auf Teamkommunikation
- ♦
  Aufklärung und erste Angriffe
- ♦ Advanced OSINT-Techniken (Reconnaissance Specialist)
  ♦ Social Engineering Strategien (Social Engineer)
  ♦ Exploitation Grundlagen (Exploit Developer)
  ♦ Simulation 2: Informationsbeschaffung und initiale Kompromittierung
- ♦
  Eindringen und Ausbreitung
- ♦ Fortgeschrittene Exploitationtechniken
  ♦ Laterale Bewegung im Netzwerk (Cyber Red Team Operator)
  ♦ Physical Security Bypass-Methoden (Physical Security Specialist)
  ♦ Simulation 3: Komplexer Angriff mit physischen und digitalen Komponenten
- ♦
  Persistenz und Datenexfiltration
- ♦ Fortgeschrittene Persistenztechniken
  ♦ Datenexfiltration und Verschleierungsmethoden
  ♦ Anpassung an Blue Team-Gegenmaßnahmen
  ♦ Simulation 4: Langfristige Operation mit Anpassung an Verteidigung
- ♦
  Berichterstattung und Lessons Learned
- ♦ Erstellung professioneller Berichte (Reporting Specialist)
  ♦ Präsentation der Ergebnisse vor dem Management
  ♦ Lessons Learned und Verbesserungsvorschläge
  ♦ Abschlusssimulation: Vollständige Red Team Operation
- ♦
  Durchgehende Fokusthemen:
- ♦ Rollenübergreifende Zusammenarbeit
  ♦ Entscheidungsfindung unter Druck
  ♦ Führungskompetenzen (insb. für Red Team Operations Lead)
  ♦ Anpassung an unerwartete Situationen
  ♦ Zeitmanagement und Priorisierung von Aufgaben
  ♦ Ethische Überlegungen und rechtliche Aspekte
- ♦
  Methodik:
- ♦ Interaktive Vorträge und Diskussionen
  ♦ Praktische Übungen in der Laborumgebung
  ♦ Realistische Simulationen gegen ein aktives Blue Team
  ♦ Rollenspiele zur Verbesserung der Soft Skills
  ♦ Tägliche Debriefings und Feedback-Runden
  ♦