CAS Cyber Security Expert («CSECAS»)

In diesem CAS-Lehrgang gehen Sie den Offensive-Security-Aspekt in Hands-on-Übungen an und lernen die Werkzeuge für IT-Administratoren und Security-Analysten kennen. Diese haben zum Ziel, die Wirksamkeit Ihrer IT-Security-Massnahmen zu erhöhen.

Dauer: 17.5 Tage
Preis: 17'200.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursmaterial und Begleitbücher

Inhalt

Cyber-Security-Spezialisten sind momentan sehr gesucht. Gerade offensive Security-Ansätze sind zur Abwehr moderner Angriffsszenarien von äusserster Wichtigkeit. Daher erhalten Sie mehrere Tage Ethical Hacking Hands-on-Training mit KALI LINUX™ und weiteren Penetration Testing Tools. Sie verfügen nach Abschluss des CAS über tiefgreifende Fähigkeiten im Bereich der offensiven Informationssicherheit und können damit verbunden Cyber-Security-Massnahmen nach deren Wirksamkeit überprüfen. Im Studienkonzept wird besonderen Wert auf die praktische Umsetzung gelegt.

Prüfungsvorbereitung und Präsentation CAS-Abschlussarbeit und OPST-Prüfung (3.5 Tage):

Die Teilnehmer führen alleine oder in Gruppen ein OSSTMM-konformes Security Audit einer Infrastruktur durch. Die im Rahmen der Ausbildung erlernten Methoden und Techniken werden praktisch in einem Penetration-Testing-Szenario angewendet und geprüft. Zusammen mit dem Auftraggeber wird der Rahmen des Audits definiert und mittels der OSSTMM-Methode durchgeführt. Der Abschluss der CAS-Arbeit stellt eine Präsentation der Audit-Ergebnisse vor den Mitstudenten dar. Es wird ebenfalls ein Vertreter der Geschäftsleitung und ein Techniker des Auftraggebers anwesend sein.

Key Learnings

- Kennen von Definitionen und Grundsätzen des Informationssicherheitsmanagementsystems (ISMS)
- Kennen der Stellung der ISO/IEC 27001 im Rahmen des Informationssicherheitsmanagementsystems (ISMS)
- Kennen der Konzepte und Inhalte des Informationssicherheitsmanagementsystems (ISMS)
- Überblick über die Security Controls des ISO/IEC 27001
- Kennen aktueller Szenarien von Angriffen auf Netzwerke und Systeme
- Aktuellhalten Ihres Wissens mit fundierten Quellen
- Vorschlagen von Massnahmen zum Schutz der Netzwerk- und Systemsicherheit
- Praktische Umsetzungshilfen zur Implementierung von Schutzmassnahmen
- Selbstständige Anwendung der wichtigsten Hackingtools und Einschätzen der Gefahren, die davon ausgehen
- Erläutern von Advanced-Hacking-Methoden und Vorschlagen von Gegenmassnahmen
- Prüfen der Sicherheit des eigenen Unternehmens in Testumgebungen (Hacking-Labs) mit Ethical-Hacking-Methoden auf der Grundlage von KALI Linux
- Kennen von kreativen Ansätzen zur Kombination von Hacking-Methoden
- Einbeziehen offensiver Erkenntnisse in Cyber-Security-Strategien
- Ideale Vorbereitung auf die offizielle OPST-Zertifizierungsprüfung, die vom Institute for Security and Open Methodologies (ISECOM) sowie von der La-Salle-Universität in Barcelona anerkannt wird
- Kennen der Grundlagen des OSSTMM
- Kennen der praktischen Anwendungen eines Security Testers
- Kennen der Tools für das Security Testing und Umgang damit
- Kennen verschiedener Angriffe auf Webapplikationen (inkl. dahinterliegende Datenbanken und Backends), die Sie anschliessend selbst ausführen
- Kennen der Grundzüge der sicheren Softwareentwicklung (OWASP)
- Eingehende Auseinandersetzung mit verschiedenen potenziellen Gefährdungsszenarien
- Zielgerichtetes Adressieren und Präsentieren von Security-Abschlussberichten nach OSSTMM

Methodik & Didaktik

Im Rahmen der Ausbildung kommen folgende Lernmethoden zum Einsatz

- Aktive Lehrgespräche mit den Teilnehmenden
- Reflexion und Austausch von Erfahrungen aus der eigenen Praxis im Kontext der Theorie
- Diskussion und Analyse von Beispielen aus dem Lernstoff
- Praxisaufgaben zum Transfer des erworbenen Wissens und der Kompetenzen auf die eigene Person
- Bearbeiten von diversen praxisorientierten Labs, die Sie während dem Lehrgang lösen (Der Umfang variiert je nach Kompetenzlevel)
- Das CAS hat gemäss HWZ einen Gesamtaufwand von 15 ECTS, also 450 Arbeitsstunden. Davon werden ca. 1/3 im Unterricht geleistet und der Rest ist Homework, Prüfungsvorbereitungen und die CAS Arbeit.
- Die CAS Arbeit selber hat in etwa einen Umfang von 90 Arbeitsstunden inkl. Präsentation.
- Beim restlichen Homework kommt es stark auf die Vorkenntnisse an.

Zielpublikum

Dieser Lehrgang richtet sich an Informationssicherheitsverantwortliche, Informationssystemarchitekten, Sicherheitstester, Sicherheitsrevisoren, Sicherheitsberater, Sicherheitsingenieure, Netzwerkingenieure, Systemadministratoren.

Anforderungen

Eidg. Fachausweis, ein eidg. Diplom, ein Diplom HF, ein Hochschulabschluss (Uni oder FH, Bachelor oder Master) oder mindestens 3 Jahre Berufserfahrung in der IT.

Erfahrungen in Projekten und im täglichen Einsatz von Informationstechnologien, IT-Systemen und Netzwerken werden vorausgesetzt. Wünschenswert sind zudem Grundkenntnisse der Informationssicherheit, analog dem folgenden Kurs:

- IT-Grundschutz («P2S»)

Zertifizierung

1. ISO/IEC 27001 Foundation
    - wird nach dem 1. Modul «Kurs: ISO/IEC 27001 Foundation («IS27F»)» absolviert
2. EXIN Ethical Hacker Foundation
    - nach dem 4. Modul «Kurs: Cyber Security Tester – Hands-on Professional («HAK2») » separat zu absolvieren. Wir empfehlen zwischen dem HAK, HAK2 und HAK3 jeweils eine 2-monatige Pause dazwischen zu machen, damit Sie genügend Zeit zum Lernen/Vorbereiten haben.
3. OSSTMM OPST
    - Wird am letzten Kurstag absolviert
    - Die erworbenen Fähigkeiten muss der Prüfungskandidat in einem Penetration-Testing-Szenario nachweisen.
    - Die OPST-Zertifizierung wurde zudem für das Diplom «Master in Information Technology Security» der La-Salle-Universität in Barcelona anerkannt. Diese Einrichtung gehört zum internationalen La-Salle-Bildungsnetzwerk, dem auch das Manhattan College in New York und die La Salle University in Philadelphia angehören. Alle OPST-Zertifikate sind sowohl mit dem ISECOM- als auch dem La-Salle-Siegel versehen, als Zeichen des damit verbundenen Prestiges.
4. Prüfung und Präsentation CAS-Abschlussarbeit an der Digicomp Academy
    - Prüfungszulassung: Alle CAS Module besucht / Prüfungen: ISO-27001 Foundation und e OSSTMM Professional Security Tester absolviert
    - Separater Termin nach Vereinbarung
5. Insgesamt werden 15 ECTS Punkte von der HWZ verliehen

Infoabend

- Cyber Security Experts («INFCSE»)

Zusatzinfo

Modulreihenfolge / -termine
Die Reihenfolge der Module ist aufbauend und einzuhalten. Dies gilt jedoch nicht für die Module «ISO/IEC 27001 Foundation» und «Web Application Security – Foundation». Sie können diese Kurse zu einem späteren Zeitpunkt innerhalb des Lehrgangs absolvieren. Die Termine für die Module können Sie frei wählen.

Folgende Themen werden in diesem CAS nicht behandelt:

- Vertiefung von Informationssicherheits-Mangementsystem (ISMS)
- Unternehmens-Risikomanagement
- Informatik-Recht (Datenschutzgesetzt, ...)
- Leadership in der Informationssicherheit

Das CAS und die ECTS Punkte werden verliehen durch die Hochschule für Wirtschaft Zürich (HWZ).

Streckung des Abgabetermins
Verspätet eingereichte Arbeiten & Berichte werden als nicht bestanden gewertet. Bei einem erneuten Versuch muss ein neues Thema eingereicht werden.

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-offense/lehrgang-cas-cyber-security-expert