CAS Cyber Security Analytics & Defense Expert («CSACAS»)

In diesem CAS-Lehrgang gehen Sie den Analytics- & Defense-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: 15.5 Tage
Preis: 15'900.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursunterlagen und Begleitbücher

Inhalt

Die Schweizer Wirtschaft ist auf eine sichere Digitalisierung angewiesen, um Wettbewerbsvorteile zu erhalten und auszubauen. Das CAS Cyber Security Analytics & Defense Expert bereitet mit seinem hohen Praxisbezug auf in der Wirtschaft gefragte Rollen in der Cybersicherheit vor, insbesondere in Security Operation Centres (SOC). Besonders gefragt sind Cyber Security Analysten mit technischen und methodischen Fähigkeiten. Wir kombinieren beides, sowohl das Technische als auch das Methodische. Unsere Absolventen können Ergebnisse unternehmenstauglich kommunizieren und präsentieren. Wir fordern Ergebnisse und Empfehlungen, die für das Business geeignet sind (ISO 27001).

Im CAS Cyber Security Analytics & Defense Expert erwerben berufserfahrene IT-Spezialisten das notwendige Rüstzeug, um komplexe Angriffsszenarien zu erkennen und schnell zu bewerten. Wir verbinden die Analyse von Vorfällen mit offensiven Angriffstechniken aus Überzeugung, denn nur so können wir gezielt geeignete Abwehrmassnahmen empfehlen. Gerade hier differenzieren wir uns stark. Wir erlernen aktuelle Angriffsmethoden auf Linux- und Windows-Umgebungen (mobil und stationär). Auch aktuelle Angriffsszenarien über Hardware-Implantate und Funktechnologien werden aufgezeigt.

Mit unserem offensiven Hands-on-Ansatz erlernen die Teilnehmer die gleichen Hacking-Skills wie die Angreifer und erhalten so ein geschultes Auge für die Analyse komplexer Angriffsmuster. Die OSSTMM Professional Security Analyst (OPSA)-Zertifizierung erfordert darüber hinaus die methodische Auswertung der Ergebnisse und damit die Umwandlung in unternehmenstaugliche (RAV (Risk Assessment Value) und STAR (Security Test Audit Report) Kennzahlen. Nur so können Risiken gemäss ISO 27001 bewertet und behandelt werden.

Key Learnings

- Anwenden von nützlichen Hackingtools und Frameworks und Einschätzen der Gefahren, die davon ausgehen
- Prüfen von IT-Systemen, Netzwerken und Webapplikationen auf Verwundbarkeiten
- Gezielte Simulation und Analyse von Angriffen auf Mitarbeitende, IT-Systeme, Netzwerke und Webapplikationen
- Finden von gezielten Artefakten und Bestimmen von Indicators of Compromise (IoC)
- Einbeziehen von offensiven Erkenntnissen in Cyber-Security-Strategien
- Umsetzen von bekannten und neuartigen Exploiting-Techniken
- Prüfen von Sicherheitsmassnahmen gegenüber Exploits in Testumgebungen (Hacking-Labs)
- Schärfen der analytischen Fähigkeiten gegenüber gezielten Angriffen
- Verständnis und rasches Erkennen von Angriffsmustern
- In Betrieb nehmen einer Lab-Umgebung (Windows Active Directory), um gängige Angriffe zu simulieren/üben
- Identifikation der einzelnen TTP (Tactics, Techniques & Procedures) eines Cyberangriffs und diese der Enterprise Matrix des MITRE ATT&CK® Framework zuweisen
- Analyse und Interpretation der Testergebnisse der Security Tester nach OSSTMM, um beispielsweise den Benchmark Risk Assessment Value (RAV) zu berechnen oder falsche Ergebnisse zu erkennen
- Fähigkeit die Prüfung zum OSSTMM Professional Security Analyst zu bestehen

Methodik & Didaktik

Der Lehrgang ist in einem Blended-Learning-Format konzipiert. Das Lerndesign berücksichtigt vorbereitende Selbststudienarbeiten, Hausaufgaben, Prüfungsvorbereitung, Prüfungen und Transferarbeiten. Die Kurse bestehen aus interaktivem Training mit Gruppenarbeiten, Diskussionen und Präsentationen. Das Studienkonzept legt besonderen Wert auf die praktische Umsetzung.

Folgende Lernmethoden werden im Trainingsprogramm eingesetzt:

- Praxisorientierter Unterricht mit vielen Labs
- 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 einen Gesamtaufwand von 15 ECTS-Punkten, also 450 Arbeitsstunden. Davon werden ca. 1/3 im Unterricht geleistet, der Rest ist Selbststudium, Prüfungsvorbereitungen und die CAS-Arbeit
- Die CAS-Arbeit selbst beträgt ca. 90 Arbeitsstunden

Zielpublikum

Dieser CAS Lehrgang richtet sich an Security Analysten, Security Tester, Security Engineers, Security Consultants wie auch verantwortungsvolle Systemadministratoren. Der Lehrgang eignet sich mit seiner Wissensbreite und den praxisorientierten Hands-On Vertiefungen insbesondere auch für Führungskräfte und Mitarbeitende in Cyber Defense und Security Operation Center (SOC) Organisationen.

Zertifizierung

Zulassung zur CAS Prüfung

Alle CAS Module absolviert und die Prüfung zum OSSTMM Professional Security Analyst bestanden.

Prüfung und Präsentation

Die 2-tägige Prüfung im Prüfungs-Lab ist praxisorientiert und sehr anspruchsvoll. Es werden alle erworbenen praktischen Fähigkeiten in verschiedenen Angriffssimulationen verlangt. Zusätzlich zur Prüfung muss ein entsprechender OSSTMM-konformer Analysebericht mit Empfehlungen als Transferaufgabe erstellt und den Prüfungsexperten vorgelegt werden. Am Ende der Prüfung haltet das Analyseteam eine managementtaugliche Präsentation mit den Analyseergebnissen und entsprechenden Empfehlungen vor den Prüfungsexperten ab. Die Endnote wird aus dem Analysebericht und der Präsentation gebildet.

ECTS-Punkte

Das CAS und die 15 ECTS-Punkte werden bei zufriedenstellender Note durch die Hochschule für Wirtschaft Zürich (HWZ) verliehen.

Infoabend

- Cyber Security Experts («INFCSE»)

Zusatzinfo

Modulreihenfolge / -termine

Die Reihenfolge der Module ist aufbauend und einzuhalten. Die Termine für die Module können Sie frei wählen.

Anrechnung und Anwesenheitspflicht

Die Anrechnung von Modulen anderer Institutionen für die Zulassung zum Zertifikatskurs ist nicht möglich. Es besteht eine 100%ige Anwesenheitspflicht.

Streckung des Abgabetermins

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

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

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-defense/lehrgang-cas-cyber-security-analytics-defense-expert