Cyber Security Analyst & Investigator – Hands-On/AI («CSA1»)

In diesem Hands-On Kurs erlangen Sie einen fundierten Überblick über die Analyse konkreter Cyber-Bedrohungen, die von kriminellen Hackern ausgehen. Zusätzlich werden neue Ansätze der Artificial Intelligence (AI) sowie deren Nutzen und Gefahren behandelt.

Dauer: 2 Tage
Preis: 1'900.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursmaterial

Inhalt

Fachkundige Cyber-Security Analysten nutzen konventionelle Methoden und AI-basierte Ansätze, um Cyberangriffe frühzeitig zu erkennen, zu untersuchen und rasch Gegenmassnahmen zu ergreifen. Diese investigativen Fähigkeiten sind in der IT und in Cybersecurity Incident Response Teams (CSIRT) ebenfalls gern gesehen. Zusätzlich sind offensive Hacking Fähigkeiten und das Wissen betreffend aktueller Angriffsszenarien für die Aufdeckung gezielter Angriffsmuster elementar. Gemeinsam erarbeiten wir die notwendigen Grundlagen und setzen uns Hands-On im Hacking-Lab damit auseinander. Der beste Lerngewinn entsteht bekanntlich, wenn Angriffsszenarien selbst erlebt werden.

- Einführung in die SOC-Thematik (Incident-Response, IoC und IoA, TTPs, Playbooks, XDR, SIEM/SOAR, Threat Intelligence, APT, usw.)
- Grundlagen der Analyse und Zuordnung von Tactics, Techniques and Procedures (TTPs) mittels MITRE ATT&CK®
- Bedeutung von YARA, Sigma und Snort für das gezielte Threat Hunting
- Analyse diverser Arbeitsweisen, Techniken und Tools im Hacking-Lab
- Exposition von IT-Systemen und Personen analysieren (OSINT)
- Schwachstellen-Scanning durchführen und analysieren (CVE/CVSS/Exploits)
- Grundlegende Social Engineering Angriffe erkennen
- Grundlegende AI-gestützte Cyberangriffe erkennen
- Grundlegende Cyberangriffe auf IT-Systeme mittels Malware und Exploits erkennen
- Grundlegende Cyberangriffe in Netzwerken erkennen
- Grundlegende Cyberangriffe auf Webapplikationen erkennen (OWASP)
- Grundlegende Cyberangriffe mittels Living-off-the-Land Techniken verstehen
- Hardware Hackingtools erkennen (Keylogger, Bad-USB Stick, Bad-USB Kabel, usw.)
- Gezielte Mitigation der im Hacking-LAB gezeigten Szenarien vorschlagen

* MITRE ATT&CK® is a registered trademark of The MITRE Corporation.

Key Learnings

- Kennen der Grundlagen von SOC, CSIRT und Incident Management
- Kennen bewährter Analysetools und Frameworks einschliesslich der Unterstützung durch Artificial Intelligence
- Prüfen von IT-Systemen, Netzwerken und Webapplikationen auf verwundbare Stellen
- Analysieren von gezielten Angriffen auf Mitarbeitende, IT-Systeme, Netzwerke und Web-Applikationen im Hacking-Lab
- Verstehen aktueller AI-basierter Cyber-Angriffe
- Nutzen von Indicators of Compromise (IoC) und Indicators of Attack (IoA) im Threat Hunting
- Empfehlen von Massnahmen zur gezielten Mitigation

Methodik & Didaktik

Im Kurs wird neben KALI LINUXTM mit verschiedenen Erweiterungen, Online-Tools und AI-Modellen gearbeitet. Für alle Teilnehmenden steht eine entsprechende Lab-Umgebung zur Verfügung. In verschiedenen Hands-On Übungen werden Sie in die Thematik der Cyber Security Analyse eingeführt und lernen zusätzlich verschiedene Hacking Tools näher kennen. Mit dem erlernten Wissen können Sie anschliessend Schwachstellen in eigenen IT-Umgebungen aufdecken, konkrete Angriffsmuster erkennen und sowohl konventionelle als auch AI-gestützte Analysen durchführen. Alle Teilnehmenden verpflichten sich ausdrücklich, das erlernte Wissen nicht missbräuchlich zu verwenden. Vor Beginn des Kurses ist daher eine entsprechende schriftliche Vereinbarung zu unterzeichnen.

* KALI LINUXTM is a trademark of Offensive Security.

Zielpublikum

Dieser Kurs richtet sich an Cybersecurity- und Informatikfachleute, sowie IT-Führungskräfte und IT-Projektleitende, die einen fundierten und praxisorientierten Einstieg in die Analyse von Cyberbedrohungen mittels offensiven Angriffstechniken und Artificial Intelligence suchen. Ebenso angesprochen sind Personen, welche sich eine grundlegende fachliche Übersicht verschaffen wollen.

Anforderungen

Erfahrungen im täglichen Einsatz von Informationstechnologien sowie grundlegende Netzwerkkenntnisse werden vorausgesetzt. Der Umgang mit Linux Shells ist von Vorteil, aber keine Bedingung. Grundkenntnisse der Begrifflichkeiten der Informationssicherheit analog zum folgenden Kurs sind von Vorteil, aber ebenfalls keine Bedingung:

- Informationssicherheits-Grundlagen («P1S»)

Weiterführende Kurse

- Cyber Security Tester – Hands-on Professional («HAK2»)

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/kurs-cyber-security-analyst-investigator-hands-onai