GLOBAL CYBERSECURITY ACADEMY

Grünwalder Weg 32
82041 Oberhaching München
Öffnungszeiten des Büros: 9:00 Uhr bis 18:00 Uhr

+49-(0)174-47-47-338
office@gc-group.io
https://www.global-cybersecurity-academy.com

WERDE CYBERSICHERHEITSEXPERT*IN!

Die digitale Welt wächst stetig, und mit ihr auch die Herausforderungen im Bereich der Cybersicherheit. Als IT-Sicherheitsexperte bist du der Schutzschild, der Unternehmen und Organisationen vor den Gefahren des digitalen Zeitalters bewahrt. Du wirst ein gefragter Spezialist, der in der Lage ist, Cyberangriffe zu verhindern, Systeme zu sichern und sensible Daten zu schützen. Die Nachfrage nach qualifizierten Fachkräften im Bereich IT-Sicherheit steigt kontinuierlich, und dieser Kurs bereitet dich optimal auf eine erfolgreiche Karriere in einem zukunftssicheren Berufsfeld vor.

Live Online | Vollzeit | 11 Monaten

EINE AZAV ZERTIFIZIERTE WEITERBILDUNG

AZAV zertifiziert

UNTERRICHTSZEITPLAN

MO. DI. MI. DO. FR.

09:00 – 12:00 Übungen und Laborarbeit mit Mentoring
oder
14:00 – 17:00 Übungen und Laborarbeit mit Mentoring
17:00 – 18:00 Pause
18:00 – 18:45 1. Live Online-Unterricht mit Dozent
18:45 – 19:30 2. Live Online-Unterricht mit Dozent
19:45 – 20:30 3. Live Online-Unterricht mit Dozent
20:30 – 21:15 4. Live Online-Unterricht mit Dozent

Dauer: Der Kurs läuft in Vollzeit mit durchschnittlich 8 UE pro Tag und umfasst insgesamt 1.704 Unterrichtseinheiten (1UE=45 Min), die sich in geleitete Lernstunden (792 UE) und Selbstlernphasen (912 UE) mit Unterstützung eines Mentors aufteilen.

Zielgruppe: IT-Sicherheit-begeisterte, Quereinsteiger, Arbeitslose und Arbeitssuchende, IT-ler, die sich im Bereich IT-Sicherheit spezialisieren möchten.

Voraussetzungen: Keine Vorkenntnisse in der IT erforderlich.

Unterrichtsformat: Der Kurs wird im Live-Online-Format durchgeführt, bestehend aus einer Theoriephase und einer betreuten Selbstlernphase. Die Anwesenheit ist verpflichtend um das intensiven Lernpensum zu schaffen.

Technische Anforderungen: stabiles Internet.

Die Lernumgebung: Live-Video Meetings mit Dozenten, Zugänge zu diversen Laboren, Selbstlernmaterialien, E-Book.

LAPTOP ALS GESCHENK BEI ERFOLGREICHEM ABSCHLUSS DES KURSES.

KURSINHALT

MODUL 1.
Einführung in Computer

Geleitete Lernstunden: 40 UE
Geleitete Selbstlernstunden: 40 UE

Ziel des Moduls:
In diesem Modul lernen die Studierenden eine allgemeine Computerumgebung kennen. Sie werden grundlegende Hardware-, Software- und Betriebssystemkenntnisse erwerben, die fast jeder in seinem täglichen Leben nutzt. Das Ziel ist es, die Studierenden mit den Grundlagen von Computern, Betriebssystemen und Computing-Fähigkeiten vertraut zu machen, damit sie Netzwerk-Lektionen leichter verstehen können.

Lernziele:
1. Verstehen der Computergeschichte und ihrer Entwicklung in der modernen Zeit.
2. Verstehen der grundlegenden Computerkonzepte (Hardware, Software und Betriebssysteme) und wie Computer funktionieren.
3. Verstehen grundlegender Dateisystemkonzepte.
4. Die Fähigkeit zum Installieren virtueller Maschinen.

MODUL 2.
Netzwerk

Geleitete Lernstunden: 140 UE
Geleitete Selbstlernstunden: 140 UE

Ziel des Moduls:
In diesem Modul erlangen die Studierenden grundlegende Kenntnisse und Fähigkeiten im Netzwerkbereich, die für eine Karriere in der Informationstechnologie (IT) unerlässlich sind. Sie können leicht die CompTiA Network+ Zertifizierung erhalten. Diese Zertifizierung bestätigt die Fähigkeit einer Person, verkabelte und drahtlose Netzwerke zu entwerfen, zu konfigurieren, zu verwalten und zu diagnostizieren. Das Ziel des CompTIA Network+ Kurses ist es, Einzelpersonen mit dem Wissen, den Fähigkeiten und den Referenzen auszustatten, die für eine erfolgreiche Karriere in Netzwerken und Informationstechnologie erforderlich sind.

Lernziele:
1. Verständnis des Zwecks und der Funktionen verschiedener Netzwerkkomponenten wie Router, Switches, Bridges, Hubs, Firewalls und Server.
2. Kenntnisse der OSI- und TCP/IP-Modelle, Protokolle und Adressierung.
3. Kenntnisse über die Unterschiede zwischen gängigen Netzwerktopologien und -technologien.
4. Verständnis von Verkabelungsstandards, Netzwerktypen und drahtlosen Technologien.
5. Implementierung und Verwaltung von Netzwerkprotokollen, Netzwerkbetriebssystemen und Netzwerkgeräten.
6. Überwachung und Optimierung der Netzwerkperformance und Sicherstellung einer ordnungsgemäßen Netzwerkauslastung.
7. Verständnis gängiger Netzwerkbedrohungen, Umsetzung bewährter Sicherheitspraktiken und Sicherung von Netzwerkgeräten.
8. Implementierung von Netzwerkhärtungstechniken.
9. Kenntnisse über Authentifizierung, Zugriffskontrolle und Datenverschlüsselungsmethoden.
10. Verwendung verschiedener Tools und Techniken zur Diagnose und Behebung von Netzwerkproblemen. Verständnis gängiger Netzwerkprobleme und Fehlerbehebungsmethoden.
11. Branchenstandards, Praktiken und Netzwerktheorie: Verständnis von Branchenstandards und -protokollen sowie bewährten Praktiken für Netzwerkimplementierung, -verwaltung und -sicherheit.
12. Kenntnisse der Netzwerktheorie, wie Routing- und Switching-Konzepte.
13. Verständnis von Risikominderungstechniken und Umsetzung von Sicherheitsrichtlinien und -verfahren zum Schutz von Netzwerken und Daten.

MODUL 3.
Active Directory

Geleitete Lernstunden: 40 UE
Geleitete Selbstlernstunden: 40 UE

Ziel des Moduls:
In diesem Modul lernen die Studierenden Windows-Server und Active Directory kennen. Active Directory (AD) ist ein von Microsoft entwickelter Verzeichnisdienst zur Verwaltung von Netzwerkressourcen in einer Windows-Umgebung. Es bietet eine zentrale Datenbank zur Speicherung und Organisation von Informationen über Benutzer, Gruppen, Computer und andere Netzwerkobjekte. Das Ziel eines Active Directory-Kurses ist es, Einzelpersonen mit dem Wissen und den Fähigkeiten auszustatten, die erforderlich sind, um Active Directory-Umgebungen in einem auf Windows basierenden Netzwerk effektiv zu entwerfen, bereitzustellen, zu verwalten und zu beheben.

Lernziel:
1. Verständnis des Zwecks, der Funktionen und der Vorteile von Active Directory bei der Verwaltung von Netzwerkressourcen.
2. Erlernen der hierarchischen Struktur von Active Directory, einschließlich Domänen, Bäumen, Wäldern und des globalen Katalogs.
3. Verstehen der Rolle und Funktionen von Domänencontrollern, einschließlich Installations-, Konfigurations- und Verwaltungsaufgaben.
4. Erlernen, wie Benutzer- und Gruppenkonten im Active Directory erstellt, geändert und gelöscht werden, sowie die Verwaltung von Berechtigungen und Zugriffskontrolle.
5. Erkunden von Gruppenrichtlinienobjekten (GPOs) und Erlernen, wie GPOs erstellt, bearbeitet, verknüpft und durchgesetzt werden, um Sicherheitseinstellungen, Softwarebereitstellung und andere Konfigurationen im Netzwerk umzusetzen.
6. Verständnis des Zwecks von Organisationseinheiten (OUs) zur Organisation von Verzeichnisobjekten und Erlernen, wie administrative Aufgaben an bestimmte Benutzer oder Gruppen delegiert werden können.
7. Erlernen von Vertrauensbeziehungen zwischen Domänen und Wäldern sowie Konfigurieren und Verwalten von Vertrauensbeziehungen, um einen sicheren Zugriff auf Ressourcen zu ermöglichen.
8. Verständnis der Integration von Active Directory mit DNS für die Namensauflösung und Dienstlokalisierung.
9. Verständnis von DHCP, Dateiserver-Ressourcenverwaltung, Remote Desktop Protocol in AD.
10. Verstehen, wie Berechtigungen mithilfe von Freigabe- und Sicherheitsfunktionen vergeben werden.

MODUL 4.
Linux

Geleitete Lernstunden: 40 UE
Geleitete Selbstlernstunden: 40 UE

Ziel des Moduls:
In diesem Modul lernen die Studierenden die Linux-Umgebung kennen, die die Basis für Serverinstallationen in der Geschäftswelt dominiert. Das Ziel des Moduls ist es, Systemoperationen und -administration aufzubauen, um Ihnen das Wissen und die Fähigkeiten zu vermitteln, die erforderlich sind, um eine Kali Linux-Umgebung zu konfigurieren, zu verwalten, zu betreiben und zu beheben, indem Sie bewährte Sicherheitspraktiken, Skripting und Automatisierung verwenden.

Lernziele:
1. Benutzer und Gruppen verwalten.
2. Berechtigungen und Besitz verwalten.
3. Speicher verwalten.
4. Dateien und Verzeichnisse verwalten.
5. Kernelmodule verwalten.
6. Den Linux-Startprozess verwalten.
7. Systemkomponenten verwalten.
8. Geräte verwalten.
9. Netzwerke verwalten.
10. Pakete und Software verwalten.
11. Linux-Systeme absichern.
12. Bash-Shell-Skripte schreiben und ausführen.
13. Aufgaben automatisieren.
14. Eine Linux-Installation planen und durchführen.

MODUL 5.
Firewall

Geleitete Lernstunden: 60 UE
Geleitete Selbstlernstunden: 60 UE

Ziel des Moduls:
Der Firewall (FortiGate) Kurs zielt darauf ab, die Teilnehmer mit umfassendem Wissen und praktischen Fähigkeiten in der Konfiguration, Verwaltung und Sicherung von Netzwerken unter Verwendung der Firewall-Lösungen von Fortinet auszustatten. Die Teilnehmer werden grundlegende Konzepte, erweiterte Konfigurationen und praktische Anwendungen durchlaufen und dabei Fachkenntnisse in Netzwerksicherheit, VPN-Konfigurationen, Traffic-Shaping, Bedrohungserkennung und Incident-Response erlangen.

Lernziele:
1. Ein umfassendes Verständnis grundlegender Konzepte der Netzwerksicherheit erlangen, einschließlich Protokollen, Verschlüsselung und Authentifizierung.
2. Erlernen der effektiven Konfiguration und Verwaltung von Firewalls durch Implementierung von Richtlinien und Regeln zur Steuerung des Netzwerkverkehrs.
3. Die Prinzipien von VPNs verstehen und die Fähigkeiten erwerben, sowohl Site-to-Site- als auch Remote-Access-VPNs zu konfigurieren und zu verwalten.
4: Erforschen Sie Techniken zur Erkennung und Verhinderung unbefugten Zugriffs, einschließlich der Verwendung von Intrusion Detection und Prevention Systems (IDS/IPS).
5: Entwickeln Sie die Fähigkeit, Sicherheitsrichtlinien zu erstellen und durchzusetzen, die Industriestandards und bewährte Verfahren einhalten.
6: Erlangen Sie Fähigkeiten im Incident Response und lernen Sie, Sicherheitsvorfälle effektiv zu identifizieren, zu analysieren und darauf zu reagieren.
7: Verstehen Sie die Bedeutung der Sicherung von Endpunkten und erlernen Sie Techniken zum Schutz von Endpunkten vor Malware und anderen Bedrohungen.
8: Entwickeln Sie ein Bewusstsein für bewährte Sicherheitspraktiken und die Bedeutung kontinuierlicher Sicherheitsschulungen für Benutzer und IT-Mitarbeiter.
9: Lernen Sie, Netzwerküberwachungstools zu verwenden und Logdateien zu analysieren, um Sicherheitsvorfälle zu erkennen und darauf zu reagieren.
10: Gewinnen Sie Einblicke in Praktiken zur Risikobewertung und -management und verstehen Sie, wie Sicherheitsrisiken identifiziert, bewertet und gemindert werden können.

MODUL 6.
Sicherheit

Geleitete Lernstunden: 40 UE
Geleitete Selbstlernstunden: 40 UE

Ziel des Moduls:
Dieses Modul umfasst wesentliche Definitionen, Begriffe und Schlüsselkonzepte, um den Studierenden zu helfen, die wichtigsten Bestandteile der Cybersicherheit zu verstehen. Das Ziel dieses Moduls ist es, eine solide Grundlage für die nächsten Module zu schaffen, die die Hauptbausteine der Cybersicherheitsdomänen sind.

Lernziele:
1. Die Schlüsselelemente der Cybersicherheit (CIA-Triad) zusammenfassen.
2. Schlüsselbegriffe und Definitionen im Zusammenhang mit Cybersicherheit zusammenfassen.
3. Arten von Malware zusammenfassen.
4. Angriffsrahmenwerke (MITRE-Kill Chain-Diamond) zusammenfassen.
5. Identitäts- und Zugriffsmanagement-Schlüsselkonzepte zusammenfassen.
6. Die Grundlagen kryptografischer Konzepte und wichtiger kryptografischer Algorithmen zusammenfassen.

MODUL 7.
Pentesting

Geleitete Lernstunden: 288 UE
Geleitete Selbstlernstunden: 288 UE

Ziel des Moduls:
Dieses Modul umfasst wesentliches Wissen und praktische Erfahrungen für Netzwerk- (Infrastruktur) und Webanwendungs-Penetrationstest-Aktivitäten. Das Ziel dieses Moduls ist es, den Teilnehmern zu ermöglichen, zu verstehen und einige Arten von Cyberangriffen durchzuführen, was zu einem umfassenden Verständnis für nahezu alle defensiven Berufsrollen beiträgt.

Lernziele:
1. Gegeben ein Ziel oder eine Domain, passives/aktives Informationsgewinnen verstehen und durchführen können.
2. Die Fähigkeit haben, ein Netzwerk zu kartieren, einschließlich Portscans und Ping-Sweeps.
3. Die Fähigkeit haben, zu enumerieren, einschließlich Null-Sitzungen.
4. Die Fähigkeit haben, Nessus zu installieren und eine Schwachstellenbewertung durchzuführen.
5. Die Fähigkeit haben, das Netzwerk zu sniffen und einen MiTM-Angriff (Layer-2) durchzuführen.
6. Die Fähigkeit haben, eine verwundbare Maschine unter Verwendung des Metasploit-Frameworks einschließlich Meterpreter auszunutzen.
7. Die Fähigkeit haben, nach dem erstmaligen Zugriff auf das Ziel Post-Exploitation durchzuführen.
8. Die Fähigkeit haben, Persistenz auf dem Ziel aufrechtzuerhalten, einschließlich Privilege Escalation.
9. Grundlagen der Social Engineering und Tools wie SET, BlackEye und Gophish verstehen (einschließlich Phishing-E-Mail-Analyse).
10. Das OWASP-Projekt und die OWASP Top 10-Fundamentals zusammenfassen können.
11. Verstehen, wie man den Web Security Testing Guide (OWASP) verwendet.
12. Die Fähigkeit haben, einen OWASP Top 10-Angriff unter Verwendung von entweder PortSwigger Labs oder einer verwundbaren Maschine Metasploitable 2 durchzuführen.
13. Das Schreiben eines Penetrationstest-Berichts und seiner Hauptkomponenten verstehen.

MODUL 8.
Sicherheitsanalyse

Geleitete Lernstunden: 296 UE
Geleitete Selbstlernstunden: 296 UE

Ziel des Moduls:
Das Ziel dieses Moduls ist es, angehende SOC-Analysten umfassend auf ihre Rolle vorzubereiten, indem sie das notwendige Wissen, die Fähigkeiten und die Einstellung erwerben, um Organisationen erfolgreich vor Cyberbedrohungen zu schützen. Durch die Kombination von geführtem Lernen und Selbststudium werden die Teilnehmer in der Lage sein, Sicherheitsvorfälle zu analysieren, zu identifizieren und angemessen darauf zu reagieren. Wichtige Ressourcen wie der CompTIA Security+ Student Guide, die CompTIA CySA+ Materialien sowie praktische Erfahrungen mit SIEM-Lösungen und Plattformen wie Tryhackme werden genutzt, um die Lernergebnisse zu maximieren.

Lernziele:
1. Unterschiede zwischen Malware-Typen erkennen, Schwachstellen identifizieren, Angriffsvektoren erkennen und verschiedene Minderungsstrategien erklären können.
2. SIEM-Plattformen bedienen: SIEMs effektiv nutzen, um Sicherheitsprotokolle zur Bedrohungserkennung und -untersuchung zu sammeln, zu analysieren und zu korrelieren.
3. Netzwerkscanner, Paketerfassungstools und Schwachstellenbewertungstools nutzen, um Sicherheitsschwächen und potenzielle Bedrohungen zu identifizieren.
4. Incident-Response-Workflows verstehen und Plattformen nutzen, um Aufgaben zu automatisieren, Bedrohungen zu priorisieren und die Incident-Response effektiv zu verwalten.
5. Incident-Response-Phasen (Identifizierung, Eindämmung, Ausrottung, Wiederherstellung, Berichterstattung) für eine effektive Incident-Behandlung implementieren können.
6. Digitale Beweise für Incident-Untersuchungen sammeln und analysieren, Ursachen identifizieren und Beweise für rechtliche Zwecke sichern können.
7. Unterschiedliche Quellen für Bedrohungsintelligenz verstehen, ihre Glaubwürdigkeit bewerten und Erkenntnisse zur Informierung von Verteidigungsstrategien anwenden können.
8. Proaktiv nach Anzeichen von Kompromittierung (IOCs) und verdächtigen Aktivitäten suchen, um potenzielle Bedrohungen zu identifizieren, bevor sie eskalieren.
9. Kontinuierlich über neue Bedrohungen, Angriffstaktiken und neue Schwachstellen lernen, um eine effektive Bedrohungserkennung aufrechtzuerhalten können.

MODUL 9.
Cloud-Sicherheit

Geleitete Lernstunden: 40 UE
Geleitete Selbstlernstunden: 40 UE

Ziel des Moduls:
Ziel dieses Moduls ist es, die Teilnehmer mit umfassenden Kenntnissen und Fähigkeiten auszustatten, die für die Organisation des Cybersecurity-Schutzes für die Cloud-Infrastruktur erforderlich sind. Durch diesen Kurs werden die Teilnehmer ein tiefes Verständnis für verschiedene Aspekte der Cloud-Infrastruktur (Amazon Web Services, Google Cloud Platform, Microsoft Azure) erlangen, so dass sie in der Lage sind, Cybersicherheitsmaßnahmen in der Cloud-Umgebung effektiv zu implementieren und zu verwalten.

Lernziele:
1. Verstehen der Cloud-Architektur und der Designkonzepte. Implementierung und Pflege einer sicheren Cloud-Umgebung.
2. Erfolgreiche Bereitstellung und Konfiguration von Cloud-Ressourcen.
3. Demonstration der Fähigkeit, den Betrieb während des gesamten Lebenszyklus der Cloud-Umgebung unter Verwendung von Beobachtbarkeit, Skalierung und Automatisierung zu verwalten.
4. Verstehen grundlegender DevOps-Konzepte in Bezug auf Bereitstellung und Integration.
5. Behebung allgemeiner Probleme im Zusammenhang mit der Cloud-Verwaltung.
6. Sichere Cloud-Infrastruktur (Amazon Web Services, Google Cloud Platform, Microsoft Azure).

MODUL 10.

Informationssicherheitsbeauftragter und Informationssicherheitsmanager

Geleitete Lernstunden: 80 UE
Geleitete Selbstlernstunden: 80 UE

Ziel des Moduls:
Das Ziel dieses Moduls ist es, den Teilnehmern fundierte Kenntnisse und praktische Fähigkeiten zu vermitteln, die für die Rolle eines Information Security Officers (ISO) unerlässlich sind. Im Laufe dieses Moduls werden die Teilnehmer ein tiefes Verständnis für die grundlegenden Aspekte der Informationssicherheit entwickeln und lernen, wie sie ein Informationssicherheitsmanagementsystem (ISMS) effektiv planen, implementieren und aufrechterhalten können. Darüber hinaus wird das Modul einen umfassenden Überblick über die relevanten Normen und Standards, einschließlich der ISO/IEC 27000-Reihe, bieten und die Teilnehmer darauf vorbereiten, diese Standards in ihrer Organisation anzuwenden.

Lernziele:

1. Grundlagen der Informationssicherheit verstehen: Die Teilnehmer erlernen die grundlegenden Prinzipien der Informationssicherheit und deren Bedeutung für den Schutz von Unternehmenswerten und sensiblen Informationen.
2. Ein ISMS entwickeln und umsetzen: Die Teilnehmer erwerben die Fähigkeiten, ein Informationssicherheitsmanagementsystem (ISMS) zu entwerfen, das den spezifischen Anforderungen ihrer Organisation gerecht wird, und lernen die Unterschiede und Schnittstellen zum IT-Servicemanagement kennen.
3. Normen und Standards der Informationssicherheit: Ein umfassendes Verständnis der relevanten Normen und Standards, insbesondere der ISO/IEC 27000-Reihe, wird vermittelt. Die Teilnehmer lernen, wie diese Standards in der Praxis angewendet werden, um ein robustes Sicherheitsmanagement zu gewährleisten.
4. Anforderungen der ISO/IEC 27001: Die Teilnehmer lernen die spezifischen Anforderungen der ISO/IEC 27001 kennen und verstehen, wie diese in einem ISMS implementiert und auditiert werden.
5. PDCA-Zyklus anwenden: Der kontinuierliche Verbesserungsprozess (Plan-Do-Check-Act) wird als grundlegendes Prinzip für die ständige Weiterentwicklung des ISMS vermittelt.
6. Datenschutzrechtliche Anforderungen: Die Teilnehmer erwerben fundiertes Wissen über die rechtlichen und regulatorischen Anforderungen, insbesondere im Hinblick auf die Datenschutz-Grundverordnung (DSGVO) und andere relevante Gesetze, die in der Informationssicherheit eine Rolle spielen.
7. Rollen und Verantwortlichkeiten im ISMS: Die Verteilung von Rollen und Verantwortlichkeiten innerhalb eines ISMS wird erörtert, um sicherzustellen, dass alle relevanten Parteien in den Sicherheitsprozess eingebunden sind.
8. Sicherheitstechnologien und Kryptographie: Die Teilnehmer erhalten einen Überblick über die gängigen Sicherheitstechnologien und die Rolle der Kryptographie im Schutz von Informationen.
9. Asset-Management und Risikobewertung: Die Teilnehmer lernen, wie Informationswerte (Assets) identifiziert, klassifiziert und geschützt werden, sowie wie eine effektive Risikoanalyse und -bewertung durchgeführt wird.
10. SoA (Statement of Applicability) und Scope: Die Bedeutung der Erklärung zur Anwendbarkeit (SoA) und die Festlegung des Anwendungsbereichs (Scope) im ISMS werden erläutert.
11. Maßnahmenziele und Maßnahmen (ISO/IEC 27001 Anhang A; ISO/IEC 27002): Die Teilnehmer lernen die Maßnahmenziele und die konkreten Maßnahmen kennen, die in Anhang A der ISO/IEC 27001 und in der ISO/IEC 27002 beschrieben sind, und wie diese in ihrer Organisation umgesetzt werden können.

MODULE 10

Informationssicherheitsbeauftragter und Informationssicherheitsmanager

Geleitete Lernstunden: 80 UE
Geleitete Selbstlernstunden: 80 UE

ZIEL DES MODULS:

Das Ziel dieses Moduls ist es, den Teilnehmern fundierte Kenntnisse und praktische Fähigkeiten zu vermitteln, die für die Rolle eines Information Security Officers (ISO) unerlässlich sind. Im Laufe dieses Moduls werden die Teilnehmer ein tiefes Verständnis für die grundlegenden Aspekte der Informationssicherheit entwickeln und lernen, wie sie ein Informationssicherheitsmanagementsystem (ISMS) effektiv planen, implementieren und aufrechterhalten können. Darüber hinaus wird das Modul einen umfassenden Überblick über die relevanten Normen und Standards, einschließlich der ISO/IEC 27000-Reihe, bieten und die Teilnehmer darauf vorbereiten, diese Standards in ihrer Organisation anzuwenden.

LERNZIELE:

1.GRUNDLAGEN DER INFORMATIONS-SICHERHEIT VERSTEHEN

Die Teilnehmenden sollen lernen, wie man Sicherheitsrichtlinien und -standards in einer IT-Umgebung implementiert und sicherstellt, dass diese je nach Bedarf eingehalten werden.

1. NETZWERKSICHERHEIT ANWENDEN

Die Teilnehmenden sollen lernen, wie man auf Sicherheitsvorfälle reagiert, diese dokumentiert und je nach Bedarf geeignete Maßnahmen zur Schadensbegrenzung und Wiederherstellung einleitet.

1. NETZWERKSICHERHEIT ANWENDEN

Die Teilnehmenden sollen lernen, wie man Sicherheitsrichtlinien und -standards in einer IT-Umgebung implementiert und sicherstellt, dass diese je nach Bedarf eingehalten werden.

MODULE 11

Praxisprojekt

Geleitete Lernstunden: 160 UE (2 Wo+2Wo (Möglichkeit der Aufteilung) oder im Block: 4 Wochen bei 40 UE Wo)

LERNZIELE:

1. NETZWERKSICHERHEIT ANWENDEN

Die Teilnehmenden sollen das theoretische Wissen zur Netzwerksicherheit auf praktische Szenarien anwenden, um Netzwerke sicher zu gestalten und Schwachstellen je nach Bedarf zu identifizieren.

2. SECURITY OPERATIONS CENTER (SOC) PROZESSE INTEGRIEREN

Die Teilnehmenden sollen die Abläufe und Aufgaben eines SOC praktisch erfahren, indem sie Bedrohungen erkennen, analysieren und entsprechende Gegenmaßnahmen entsprechend dem jeweiligen Aufgabenspektrum ergreifen.

3. IMPLEMENTIERUNG VON SICHERHEITSRICHTLINIEN UND -STANDARDS

Die Teilnehmenden sollen lernen, wie man Sicherheitsrichtlinien und -standards in einer IT-Umgebung implementiert und sicherstellt, dass diese je nach Bedarf eingehalten werden.

4. DURCHFÜHRUNG VON PENETRATIONSTESTS UND SCHWACHSTELLENANALYSEN

Die Teilnehmenden sollen Penetrationstests und Schwachstellenanalysen durchführen, um die Sicherheit von Systemen und Anwendungen entsprechend den jeweiligen Anforderungen zu überprüfen und zu verbessern.

5. EINSATZ VON SICHERHEITS-FRAMEWORKS UND -TOOLS

Die Teilnehmenden sollen verschiedene Sicherheitsframeworks und -tools anwenden, um die IT-Sicherheit im Unternehmensumfeld gemäß dem spezifischen Bedarf sicherzustellen.

6. REAKTION AUF SICHERHEITSVORFÄLLE

Die Teilnehmenden sollen lernen, wie man auf Sicherheitsvorfälle reagiert, diese dokumentiert und je nach Bedarf geeignete Maßnahmen zur Schadensbegrenzung und Wiederherstellung einleitet.

7. SICHERUNG UND ÜBERWACHUNG VON NETZWERKEN

Die Teilnehmenden sollen praktische Erfahrungen in der Sicherung und Überwachung von Netzwerken sammeln, um unautorisierte Zugriffe zu verhindern und Anomalien entsprechend dem aktuellen Bedarf zu erkennen.

8. ANWENDUNG VON KRYPTOGRAPHIETECHNIKEN

Die Teilnehmenden sollen kryptographische Methoden praktisch anwenden, um Daten zu verschlüsseln und deren Integrität gemäß den jeweiligen Anforderungen zu gewährleisten.

9. UMSETZUNG VON DATENSCHUTZMASSNAHMEN

Die Teilnehmenden sollen Datenschutzmaßnahmen praktisch umsetzen, um den gesetzlichen Anforderungen zu entsprechen und die Privatsphäre der Benutzer entsprechend dem Bedarf zu schützen.

10. ERSTELLUNG UND DURCHFÜHRUNG VON SICHERHEITSAUDITS

Die Teilnehmenden sollen lernen, wie man Sicherheitsaudits plant, durchführt und die Ergebnisse dokumentiert, um die Sicherheitssysteme kontinuierlich zu verbessern, je nach Aufgabenspektrum und Bedarf.

MODULE 12

Karriereplanung und -entwicklung

Geleitete Lernstunden: 20 UE
Geleitete Selbstlernstunden: 20 UE

LERNZIELE:

1.BEWERBUNGSUNTERLAGEN RICHTIG ERSTELLEN

Die Teilnehmenden sollen lernen, wie man professionelle und überzeugende Bewerbungsunterlagen erstellt, die den Anforderungen des Arbeitsmarktes entsprechen.

2. SOFT SKILLS TRAINING FÜR DAS ERFOLGREICHE BESTEHEN IM JOB INTERVIEW UND KARRIERE IN DER IT-SICHERHEIT

Die Teilnehmenden sollen wesentliche Soft Skills entwickeln, um in Vorstellungsgesprächen zu überzeugen und eine erfolgreiche Karriere in der IT-Sicherheit zu gestalten.

3. ARBEITSVERTRAG MITSAMT RECHTEN UND PFLICHTEN VERSTEHEN UND GEHALTSVERHANDLUNGEN VORTEILHAFT FÜHREN

Die Teilnehmenden sollen die wichtigsten Aspekte eines Arbeitsvertrages kennen und lernen, wie sie erfolgreich Gehaltsverhandlungen führen.

4. ARBEITSRECHT UND BUSINESS KNIGGE UM DEN BERUFSALLTAG ERFOLGREICH ZU MEISTERN UND DIE RECHTE UND PFLICHTEN ZU KENNEN

Die Teilnehmenden sollen ein fundiertes Verständnis von Arbeitsrecht und Business-Etikette entwickeln, um im Berufsalltag erfolgreich und rechtssicher agieren zu können.

5.VORBEREITUNG AUF BEWERBUNGS-PROZESS

Die Teilnehmenden sollen eine maßgeschneiderte Vorbereitung auf ihren individuellen Bewerbungsprozess erhalten, um ihre Erfolgschancen zu maximieren.

6. INDIVIDUELLES STRESS-JOB-INTERVIEW MIT VIDEOAUFNAHME

Die Teilnehmenden sollen lernen, wie sie mit Stresssituationen in Bewerbungs-gesprächen umgehen und ihre Performance durch Videoanalysen verbessern können.

7. SELBSTLERNPHASEN

Die Teilnehmenden sollen eigenständig Bewerbungsunterlagen erstellen, Verbesserungsvorschläge umsetzen, ihre Soft Skills testen und ihre Online-Profile optimieren, um gut vorbereitet in den Bewerbungsprozess zu starten.

Grünwalder Weg 32
82041 Oberhaching München

+49-(0)174-47-47-338

office@gc-group.io

https://www.global-cybersecurity-academy.com

https://web.arbeitsagentur.de/weiterbildungssuche/suche?sty=0&anbieter=302047

UNSERE ONLINE-SPRACHLERNPLATTFORM

Unsere Online-Sprachlernplattform bietet Ihnen eine maßgeschneiderte Lösung, um Ihre Englisch- und Deutschkenntnisse gezielt auf das Berufsleben in der IT-Branche vorzubereiten. Das Ziel ist, Englisch auf B2-Niveau und Deutsch auf C1-Niveau zu erlernen. Dies wird durch eine Kombination aus selbstgesteuertem Lernen und praxisorientierten Gruppenübungen erreicht, die Ihre Kommunikationsfähigkeiten in realen beruflichen Situationen verbessern.

Einstufungstest/Lernziele: Nach einem Einstufungstest bei unserem Partner können Sie Grammatik- und Vokabelübungen im eigenen Tempo durchgehen. Um Fortschritte zu erzielen, sind mindestens 2 Stunden wöchentlicher Einsatz erforderlich, inklusive Teilnahme an praxisorientierten Gruppenübungen.

Sprachtraining in der Gruppe: In Gruppen von 6-8 Teilnehmern diskutieren Sie berufsrelevante Themen, was Ihre Kommunikationsfähigkeiten verbessert und die Hemmschwelle zur mündlichen Kommunikation senkt. Flexibel wählbare Termine ermöglichen die optimale Integration in Ihren Alltag.

Sprachzertifikat: Am Ende erhalten Sie bei erfolgreicher Teilnahme ein anerkanntes Sprachzertifikat, das Ihre Chancen auf eine Anstellung in der IT-Branche erhöht.
Wir motivieren unsere Studenten, dieses Programm aktiv zu nutzen, um ihre beruflichen Ziele zu erreichen.

INTERNATIONALE ZERTIFIKATE

Unsere Teilnehmenden erhalten nach Abschluss des Kurses folgende internationale Cybersicherheitszertifizierungen die folgende Lernergebnisse dokumentieren:

CompTIA Network+

Das Zertifikat bestätigt Kenntnisse in der Netzwerkinfrastruktur, Netzwerkoperationen, Netzwerksicherheit und Fehlerbehebung, sowie die Fähigkeit, Netzwerke zu konfigurieren und zu verwalten.

CompTIA Security+

Dieses Zertifikat weist fundiertes Wissen in den Bereichen Netzwerksicherheit, Bedrohungen und Schwachstellen, Sicherheitsarchitektur und -design sowie Cybersicherheitstechniken und -tools nach.

CompTIA Linux+

Das Zertifikat bescheinigt Fähigkeiten in der Verwaltung, Konfiguration und Fehlerbehebung von Linux-basierten Systemen und Netzwerken sowie die Nutzung von Linux-Befehlen und -Tools.

CompTIA Pentest+

Dieses Zertifikat bestätigt Kenntnisse in Penetrationstests, Schwachstellenbewertungen und Management sowie die Fähigkeit, Netzwerke und Systeme auf Sicherheitslücken zu überprüfen und zu sichern.

CompTIA Cloud+

Dieses Zertifikat demonstriert Arbeitgebern, dass Sie die technischen Fähigkeiten besitzen, die notwendig sind, um Cloud-Infrastrukturdienste innerhalb umfassender IT-Systeme abzusichern.

CompTIA CySa+

Dieses Zertifikat weist Fähigkeiten in der Cybersecurity-Analyse, Bedrohungserkennung, Incident Response und der Implementierung von Sicherheitsmaßnahmen nach.

Splunk Core Certified User

Das Zertifikat bestätigt die Fähigkeit, Splunk zu navigieren, Daten zu suchen, zu analysieren und Berichte sowie Dashboards zu erstellen.

Fortinet NSE4

Dieses Zertifikat bescheinigt Kenntnisse und Fähigkeiten im Bereich der Netzwerksicherheit, einschließlich der Konfiguration und Verwaltung von Fortinet-Firewalls und -Sicherheitslösungen.

Dekra

Information Security Officer (ISO): Das Zertifikat belegt fundierte Kenntnisse in Informationssicherheitsmanagementsystemen nach ISO-Standards sowie die Fähigkeit, Sicherheitsrichtlinien und -Maßnahmen zu implementieren und zu überwachen.

DER KURS BEREITET DIE TEILNEHMENDEN AUF EINE EXPERTENKARRIERE VOR. DIE JOBTITELN BZW. AUFGABEN SIND VIELFÄLTIG UND VARIIEREN JE NACH AUSGESUCHTEN SCHWERPUNKT:

✓ Cyber Security Analyst/in SOC
✓ Cyber Security Engineer
✓ Cyber Risk Consultant
✓ Information Security Analyst
✓ Vulnerability Analyst
✓ Cloud Security
✓ Penetration Tester
✓ Network Security Engineer
✓ SOC Engineer
✓ IT Security Administrator
✓ Information Security Officer
✓ IT Support
✓ System Administrator

VORTEILE UNSERES BILDUNGSPROGRAMMS:

- Unübertroffene Qualität zu einem fairen Preis.
- Anerkannte internationale Zertifikate, die Ihnen als Türöffner bei der Jobsuche dienen werden.
- Erfahrene Lehrkräfte aus der Praxis, die größten Wert auf die Vermittlung praxisnahen Wissens legen.
- Bequemes und spannendes Lernformat mit interaktiven Übungen und Praxisaufgaben.
- Kurzfristige und intensive Weiterbildung mit Vorbereitung auf Zertifikate.
- Praktische Anwendung und Erprobung des Wissens während der vierwöchigen integrierten Praxisphase.
- Zugang zur Sprachplattform zur Verbesserung Ihrer Englisch- oder Deutschkenntnisse.
- Unterstützung bei der Arbeitsvermittlung und Optimierung der Bewerbungsunterlagen durch erfahrene und gut vernetzte HR-Experten. Bei Bedarf auch nach Beendigung der Weiterbildung.

DER KURS IST AUS MEHREREN GRÜNDEN WICHTIG FÜR DEN ARBEITSMARKT:

ARBEITSMÖGLICHKEITEN:
Offene Stellen im Bereich der Cybersicherheit in Deutschland umfassen eine breite Palette von Rollen und Spezialisierungen, darunter SOC-Analytiker, Incident Responder, Penetrationstester, Sicherheitsarchitekten und Cloud Sicherheitsexperten, um nur
einige zu nennen.

INDUSTRIELLE NACHFRAGE:
Verschiedene Branchen in Deutschland, darunter das Finanzwesen, das Gesundheitswesen, die verarbeitende Industrie und die öffentliche Verwaltung, haben einen hohen Bedarf an Cybersicherheitsexperten. Jede Branche hat ihre eigenen Herausforderungen und Anforderungen an die Cybersicherheit, wodurch sich vielfältige Beschäftigungsmöglichkeiten für Fachleute mit unterschiedlichen Fähigkeiten und Hintergründen und somit auch Quereinsteiger ergeben.

WACHSENDE NACHFRAGE:
In Deutschland, wie auch in vielen anderen Ländern, ist die Nachfrage nach IT-Sicherheit-Fachkräften deutlich gestiegen. Diese Nachfrage wird durch Faktoren wie digitale Transformationsinitiativen, zunehmende Cyber-Bedrohungen und regulatorische Compliance-Anforderungen angetrieben.

QUALIFIKATIONSDEFIZIT:
Trotz der steigenden Nachfrage nach IT-Sicherheit-Fachleuten gibt es einen Mangel an qualifizierten Arbeitskräften, die diese Positionen besetzen können. Diese Qualifikationslücke ist sowohl eine Herausforderung als auch eine Chance für Personen, die in den Bereich der Cybersicherheit einsteigen möchten.

GLOBAL
CYBERSECURITY
ACADEMY

KONTAKT

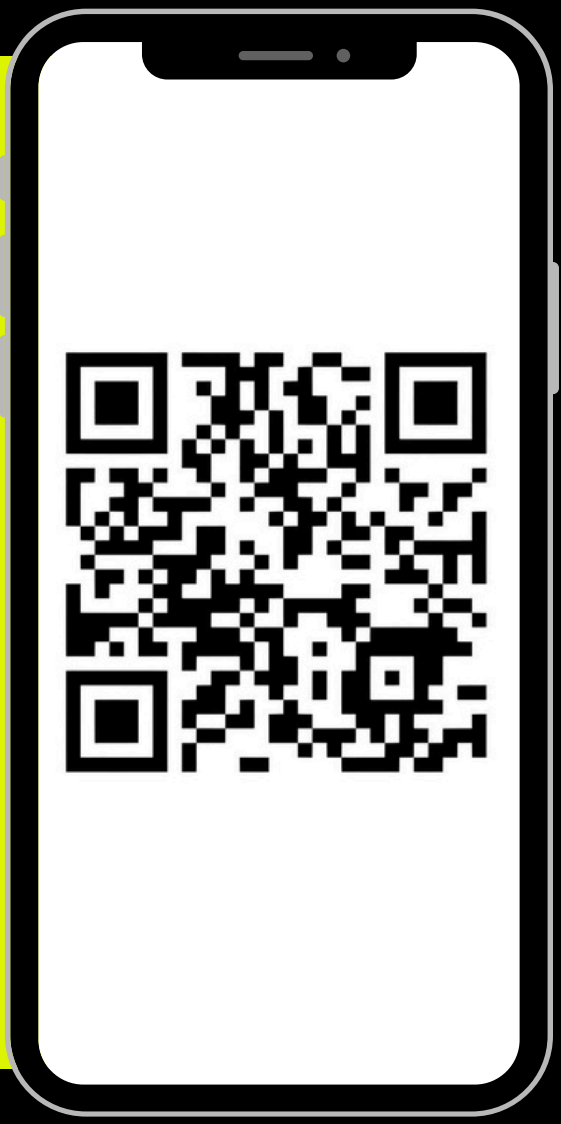
Grünwalder Weg 32
82041 Oberhaching München

+49-(0)174-47-47-338

office@gc-group.io

https://www.global-cybersecurity-academy.com

https://web.arbeitsagentur.de/weiterbildungssuche/suche?sty=0&anbieter=302047



AZAV zertifiziert

CompTIA Authorized Partner DELIVERY PARTNER

KURSNET