cybersteps

Werde Cybersecurity Analyst

- 12 Monate Live-Unterricht
- 2-monatiges Praktikum
- Vollzeit
- Flexibel & remote

4.9

★★★★★

Studentenbewertungen

CERTQUA

Qualitätsmanagement

zugelassener Träger nach AZAV

> Wer wirklich praktische IT- oder Cybersicherheitskenntnisse aufbauen möchte, ist hier genau richtig. Im Gegensatz zu vielen anderen Anbietern, bei denen ich leider Zeit verschwendet habe, geht dieses Programm nicht nur über Theorie, es vermittelt echte praktische Erfahrung.

Marc Nöthen,
Cybersecurity Student

> Ich hatte keinerlei Vorkenntnisse in Cybersicherheit, und anfangs war es ziemlich überwältigend. Aber Roman hat alles so aufgeschlüsselt, dass es Klick gemacht hat, und Schritt für Schritt hatte ich das Gefühl, dazuzugehören.

Doreen Fischel,
Cybersecurity Developer

> Als Arbeitgeber ist es immer eine Herausforderung, qualifizierte Cybersicherheitstalente zu finden. Cybersteps schließt diese Lücke, indem es Unternehmen wie unserem gut vorbereitete Cybersecurity-Analysten vermittelt, die sofort einen Beitrag leisten können.

Shahar Vaknin,
Director of CTO Office clutch

Dein Weg In Die Cybersecurity-Karriere

Entstanden aus Eliteeinheiten des Militärs und führenden Cybersicherheitsunternehmen bietet Cybersteps praxisbewährtes, branchenorientiertes Training, das dich optimal auf den Beruf vorbereitet. Wir haben bereits Expertinnen und Experten ausgebildet, die heute die kritischsten Systeme der Welt schützen. Jetzt bist du an der Reihe.

100% Cybersecurity Fokus
Wir sind ausschließlich auf Cyber-sicherheit spezialisiert und machen dich zu einer echten Fachkraft mit einem starken Netzwerk, das dir Türen zu Interviews und Jobs öffnet.

Auf den deutschen Markt zugeschnitten
Ein karriereorientiertes Programm, das auf gefragte Rollen wie IT-Sicherheits-administrator, SOC-Analyst, Cybersecurity Consultant und GRC-Manager zugeschnitten ist.

Zukunftssicher im Zeitalter der KI
Unser Programm integriert Künstliche Intelligenz als zentrales Element, damit du den Entwicklungen auf dem Arbeits-markt und in der Cybersicherheits-branche immer einen Schritt voraus bist.

Branchenzertifizierungen
Bereite dich auf acht international anerkannte Zertifizierungen vor. Vollständig finanziert, inklusive Prüfungsgutscheinen, einlösbar bis sechs Monate nach dem Programm.

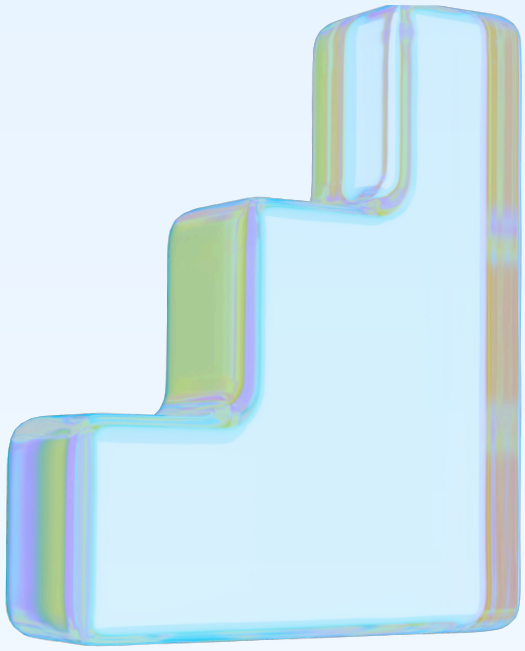
Praxisnah & militärisch erprobt
Sammle echte Praxiserfahrung mit einem bewährten Ausbildungskonzept, das von Elite-Instruktoren mit militärischem Hintergrund geleitet wird.

Individuelles Mentoring mit Experten
Du erhältst persönliche Betreuung und Mentoring, technische Unterstützung sowie Karrierecoaching, um deine beruflichen Ziele zu erreichen.

Neuer hochwertiger Laptop – und er gehört dir!
Um deinen Erfolg von Anfang an zu unterstützen, stellen wir dir kostenlos einen leistungsstarken Laptop zur Verfügung. Du nutzt ihn während deiner gesamten Ausbildung - und darfst ihn nach dem Abschluss behalten.

Flipped Classroom & Personalisiertes Lernen

Bei Cybersteps nutzen wir die Flipped-Classroom-Methode, einen bewährten Ansatz, der von führenden Universitäten und MINT-Programmen angewendet wird. Diese Methode verbessert die Lernergebnisse, indem sie jedem Studierenden hilft, sein volles Potenzial zu entfalten.

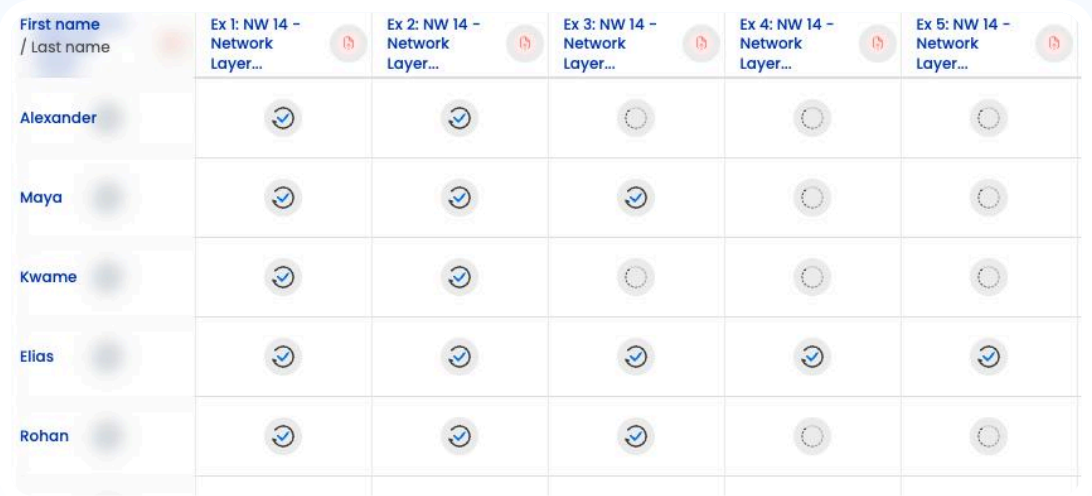


Dreistufiger Lernprozess

- **Vor dem Unterricht:** Bearbeite neue Lerninhalte über Videos und Lesematerialien und absolviere Übungen in deinem eigenen Tempo, um dich optimal auf die von Dozierenden geleiteten Sitzungen vorzubereiten und das Beste daraus zu machen.
- **Im Unterricht:** Nimm an kleinen, interaktiven Sitzungen mit Branchenexpertinnen und -experten teil, inklusive Live-Demonstrationen, angeleiteter Laborarbeit und vertiefender Q&A-Diskussionen.
- **Nach dem Unterricht:** Festige deine Kenntnisse durch Übungen, Laboraufgaben und fortgeschrittene Herausforderungen mit ansteigendem Schwierigkeitsgrad, sodass du stets entsprechend deines aktuellen Niveaus gefordert wirst.

Personalisiertes Entwicklungs-Tracking

Um dir zu helfen, dein volles Potenzial zu entfalten, wirst du kontinuierlich auf einem Niveau gefördert, das zu deinem Hintergrund und Fortschritt passt, nie gelangweilt, nie überfordert. Wir verfolgen deinen Fortschritt durch Übungen, Projekte und Mentoring-Sitzungen, um den besten Karrierepfad im Bereich Cybersicherheit auf Basis deiner Stärken und Ziele zu identifizieren. Du erhältst detailliertes Feedback, damit du stets auf Kurs bleibst, um deine beruflichen Ziele zu erreichen.

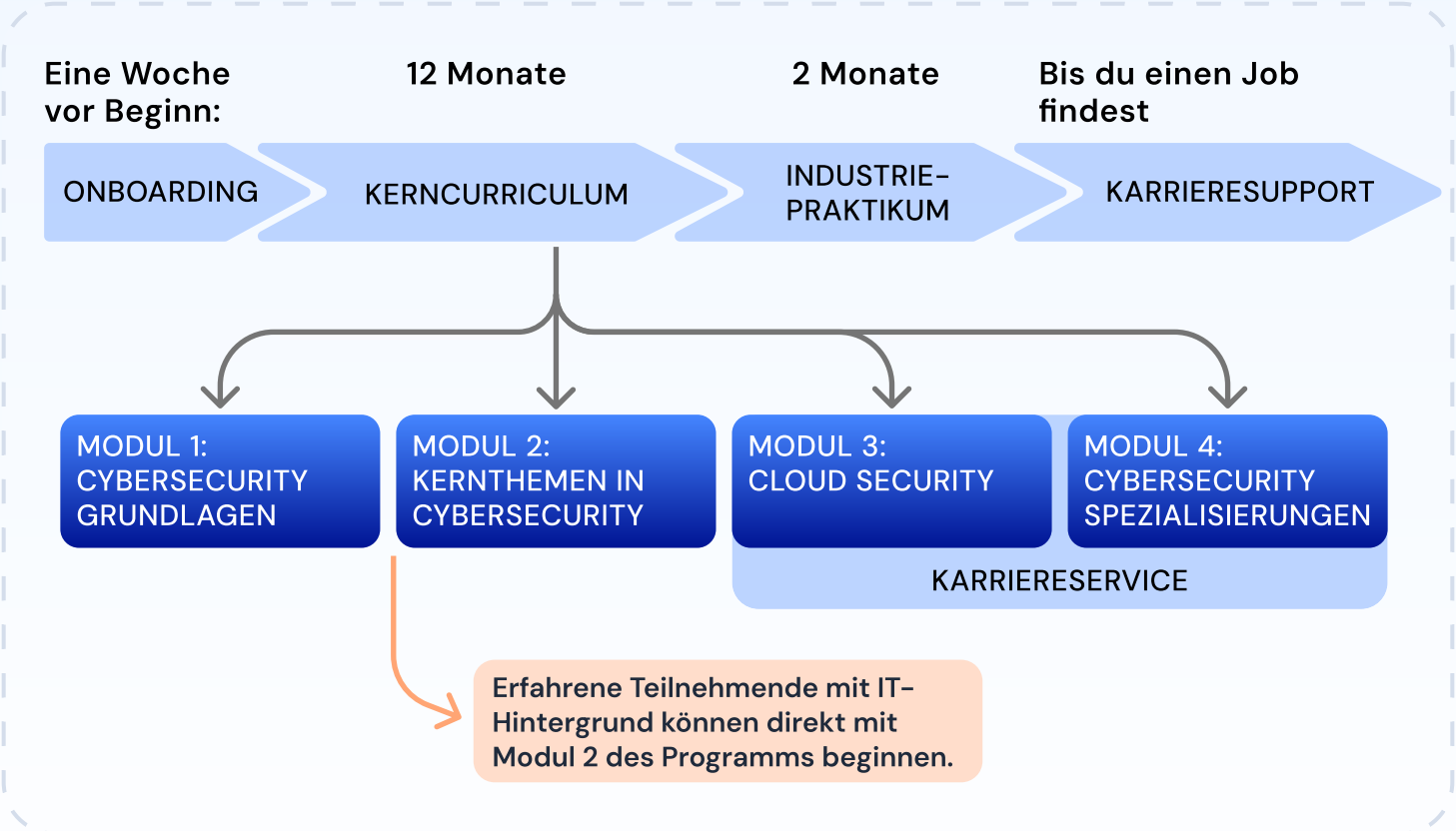


First name / Last name	Ex 1: NW 14 - Network Layer...	Ex 2: NW 14 - Network Layer...	Ex 3: NW 14 - Network Layer...	Ex 4: NW 14 - Network Layer...	Ex 5: NW 14 - Network Layer...
Alexander	✓	✓			
Maya	✓	✓	✓		
Kwame	✓	✓			
Elias	✓	✓	✓	✓	✓
Rohan	✓	✓	✓		

Programmstruktur & Zeitplan

09:00–10:00	13:00–14:00
Live-Unterricht und Demo	Mittagspause
10:00–10:10	14:00–15:00
Kurze Pause	Wiederholungssitzung
10:10–11:00	15:00–17:00
Live-Unterricht und Demo	Angeleitetes praktisches Training
11:00–13:00	17:00–18:00
Angeleitetes praktisches Training	Vorbereitung auf den nächsten Tag

Programmablauf



Praxisnahe Fähigkeiten

Unser Lehrplan kombiniert Theorie mit praxisorientierter Arbeit an gefragten Tools, sodass du die Kenntnisse und Zertifikate erhältst, die du brauchst, um auf dem heutigen Arbeitsmarkt der Cybersicherheit erfolgreich zu sein. Neben den Kerninhalten der Cybersicherheit legen wir besonderen Wert auf den Umgang mit dem aktuell mächtigsten Werkzeug, der Künstliche Intelligenz (KI).

Programmierung & Scripting

- Python
- PowerShell
- Bash

KI & LLMs

- Copilot
- Hugging Face
- LangChain
- ChatGPT

Virtualisierung

- VMware
- Docker
- Kubernetes

Betriebssysteme

- Windows
- Linux
- macOS

Netzwerktechnik

- Wireshark
- Cisco Packet Tracer
- TCPDump
- Snort
- Nmap

Datenanalyse

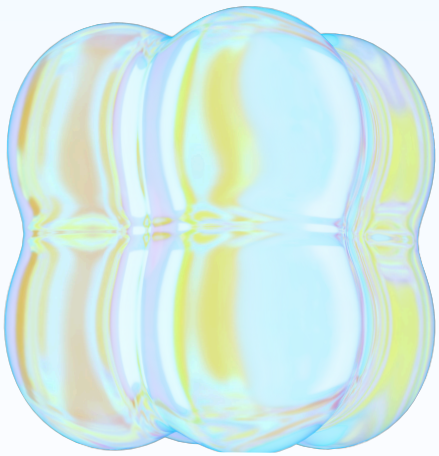
- SQL
- PostgreSQL

IT-Administration & Cloud

- Microsoft 365
- Active Directory
- Azure Cloud
- Sysinternals

Cybersecurity Tools

- SIEM (Microsoft Sentinel, Splunk, Wazuh)
- Kali
- Metasploit
- Mimikatz
- Burp Suite



KI-Kompetenzen

- **Einführung in KI:** Was Künstliche Intelligenz ist, zentrale Konzepte, wo sie im Berufsalltag vorkommt und typische Anwendungsfälle.
- **Überblick über KI-Tools:** Praktische Arbeit mit führenden Tools für technische Recherche, Business Writing, Programmierung und Datenanalyse.
- **Prompt Engineering:** Einfache Muster für zuverlässige Ergebnisse beim Erstellen von Prompts, durch klare Anweisungen, Einschränkungen, Überprüfung und Wiederholung.
- **KI-Agenten:** Automatisierung mehrstufiger Aufgaben mithilfe von Tools, Speicherfunktionen und Sicherheits-mechanismen zur Steigerung der Produktivität.

Module 1: Cybersecurity Grundlagen

Wir beginnen bei null und bauen starke Grundlagen in Programm-ierung, Computernetzwerken und Betriebssystemen auf. In diesem ersten Modul arbeitest du mit grundlegenden Cybertools und entwickelst Lerngewohnheiten, die dich während des gesamten Kurses unterstützen. Außerdem beginnst du, die Denkweise einer kompetenten Cybersicherheitsfachkraft zu entwickeln. Am Ende dieses Moduls erhältst du die CompTIA Tech+ Zertifizierung.

Wichtige Konzepte und Technologien

Einführung in Computer
Verstehe, wie Hardware und Software funktionieren, und nutze das Terminal, um erweiterte Aktionen auszuführen.

Python für Cybersecurity-Analysten
Lerne, Aufgaben mit Python zu automatisieren und Cybersicherheitsprozesse zu optimieren.

Grundlagen der Netzwerktechnik
Erkunde die OSI- und TCP/IP-Modelle, verstehe IP-Adressierung, Subnetze und Routing, und nutze Tools wie Wireshark zur Analyse des Netzwerkverkehrs.

Betriebssysteme
Arbeite mit Windows und Linux, entwickle CLI-Kenntnisse, erkunde Dateisysteme und Prozesse und lerne, Betriebssysteme zu konfigurieren und abzusichern.

KI-Tools
Lerne grundlegende Konzepte der Künstlichen Intelligenz kennen und wie Tools wie ChatGPT und GitHub Copilot in der Cybersicherheit eingesetzt werden können.

Grundlagen der Datenanalyse
Arbeite mit Daten unter Verwendung von SQL, verwalte Datenbankspeicher und führe einfache Datenanalysen durch.

Grundlagen des Webs
Verstehe, wie Websites mit HTML, CSS und JavaScript funktionieren, wie Client-Server-Kommunikation (HTTP/HTTPS) abläuft und wie man einfache Webanwendungen bereitstellt.

Kernzertifizierung

CompTIA Tech+

Eine Einstiegszertifizierung, die grundlegende IT- und Cybersicherheitskenntnisse bestätigt.

Optional

CompTIA Network+

Skills:

- **Anwendungen und Software**
- **Infrastruktur**
- **IT-Konzepte und Terminologie**
- **Sicherheit**
- **Grundlagen der Datenbanken**
- **Grundlagen der Softwareentwicklung**

Module 2: Kernthemen in Cybersecurity

In Modul 2 tauchen wir tiefer in die zentralen Praktiken der Cybersicherheit und deren Hintergründe ein. Du erlangst ein umfassendes Verständnis der Branchenlandschaft und kannst dadurch deinen eigenen beruflichen Weg in der Cybersicherheit planen. Am Ende dieses Moduls bist du darauf vorbereitet, die CompTIA Security+ Zertifizierung zu erwerben.

Wichtige Konzepte und Technologien

Grundlagen der Sicherheit
Lerne zentrale Sicherheitskontrollen kennen, das CIA-Dreieck (Vertraulichkeit, Integrität, Verfügbarkeit), AAA (Authentifizierung, Autorisierung, Abrechnung) sowie wichtige Konzepte wie Zero Trust, Änderungsmanagement und physische Sicherheit.

Kryptografie
Verstehe symmetrische und asymmetrische Verschlüsselung, Hashing, Verschleierung und digitale Signaturen. Erkunde die Grundlagen der Blockchain-Technologie durch praktische Übungen.

Bedrohungen & Schwachstellen
Identifiziere Bedrohungsakteure und Angriffsarten, analysiere Schwachstellen in Netzwerken, Systemen und Anwendungen, und entwickle Strategien zur Abwehr von Malware, Social Engineering und Supply-Chain-Angriffen.

Sicherheitsarchitektur
Entwirf sichere Netzwerke und Systeme mit Fokus auf Anwendungssicherheit, Betriebssysteme, mobile Geräte sowie E-Mail- und Web-Kommunikation.

Governance, Risk & Compliance (GRC)
Erlerne Compliance-Frameworks, Risikomanagement und Drittanbieter-Risikobewertungen. Verstehe die Rolle von Audits und Assessments innerhalb der Sicherheitsstrategie.

Rollen in der Cybersicherheit
Erkunde Schlüsselrollen wie Incident Responder, Penetration Tester, SOC-Analyst und Security Engineer und gewinne Einblicke in deren Aufgaben und erforderliche Kompetenzen.

Kernzertifizierung

CompTIA Security+

Eine führende Zertifizierung für Berufseinsteiger*innen im Bereich Cybersicherheit.
Sie bestätigt grundlegende Sicherheitskompetenzen, Branchenstandards bei Tools sowie bewährte Sicherheitspraktiken.

Skills:

- **Allgemeine Sicherheitskonzepte**
- **Bedrohungen, Schwachstellen & Gegenmaßnahmen**
- **Sicherheitsarchitektur**
- **Sicherheitsoperationen**
- **Sicherheitsmanagement & -überwachung**

Module 3: Cloud Security

In diesem Modul steigen wir in die Cybersicherheit auf Unternehmensebene ein, mit dem Fokus auf den Schutz groß angelegter Cloud- und On-Premise-IT-Umgebungen. Du sammelst praxisnahe Erfahrung mit den wichtigsten Tools zum Schutz von Organisationen vor Cyberbedrohungen, darunter Azure Cloud Administration, Microsoft 365 und Windows Active Directory.

Wichtige Konzepte und Technologien

Azure Cloud Administration
Konfiguriere und verwalte Azure-Cloud-Ressourcen (VMs, Speicher, Netzwerke), implementiere RBAC und bedingten Zugriff, und sichere Cloud-Umgebungen durch Laborübungen und wöchentliche Projekte ab.

Cloud Security
Schütze Azure-Umgebungen durch die Anwendung des Least-Privilege-Prinzips, das Absichern von VMs und Netzwerken mit NSGs und Firewalls, das Aktivieren von Protokollierung und Monitoring sowie den Einsatz von Microsoft Sentinel zur Erkennung und Untersuchung von Bedrohungen, durch praxisorientierte Laborübungen und Angriffs-/Verteidigungsprojekte.

Microsoft 365 Management & Active Directory (Entra)
Verwalte Benutzer, Gruppen und GPOs, sichere Windows-Umgebungen und analysiere Ereignisprotokolle für Systemsicherheit. Sammle praktische Erfahrung in der Servereinrichtung und -sicherheit durch tägliche Übungen und Projekte.

Karrierevorbereitung
Optimiere deinen Lebenslauf und dein LinkedIn-Profil, um deine Kenntnisse und Erfahrungen im Bereich Cyber-sicherheit optimal zu präsentieren. Arbeite mit deinem Mentor daran, deinen idealen Karriereweg zu definieren, gefragte Rollen zu identifizieren und die Fähigkeiten zu entwickeln, um dich auf dem Arbeitsmarkt abzuheben.

Kernzertifizierung

Microsoft Azure Fundamentals (AZ-900)

Grundlegendes Wissen über Cloud Computing, Azure-Dienste und Cloud-Sicherheitsprinzipien.

Optional

Security, Compliance, and Identity Fundamentals (SC-900)

Microsoft Azure AI Fundamentals (AI-900)

Microsoft Azure Administrator (AZ-104)

Skills:

- **Allgemeine Cloud-Konzepte**
- **Azure-Architektur und -Dienste**
- **Azure-Management und -Governance**

Module 4: Cybersecurity Spezialisierung

In diesem letzten Modul verfeinerst du deine Cybersicherheits-kenntnisse für Rollen wie SOC-Analyst, IT-Sicherheitsberater, IT-Sicherheitsadministrator oder Compliance- & Risikospezialist. Du sammelst praxisnahe Erfahrung mit SIEM, Compliance und fortgeschrittenen Sicherheitstools, kombiniert mit individuellem Karriere-Mentoring und Interview-Coaching, damit du selbstbewusst in den Arbeitsmarkt einsteigen kannst.

Wichtige Konzepte und Technologien

SOC, Incident Response & Penetration Testing
Arbeite mit SIEM-Plattformen, analysiere forensische Artefakte und beherrsche den Incident-Response-Zyklus. Entwickle Fähigkeiten in Log-Analyse, Alarm-Triage und Bedrohungsabwehr. Nimm an Purple-Team-Übungen teil, um Penetrationstests und Red-Team-Taktiken praktisch anzuwenden.

Cloud & Erweiterte IT-Sicherheit
Richte ein eigenes Labor ein, um Cloud- und On-Premise-Sicherheit zu üben. Identifiziere und behebe Sicherheitslücken, untersuche fortgeschrittene Angriffstechniken und entwickle Verteidigungsstrategien gegen neue Bedrohungen.

Compliance & Risikomanagement
Hilf Unternehmen, die Einhaltung wichtiger Vorschriften wie ISO/IEC 27001 und DSGVO zu gewährleisten. Führe Risikoanalysen, Sicherheitsaudits und Compliance-Berichte durch und integriere Incident-Management in regulatorische Standards.

Spezialisierte Karrierevorbereitung
Verbessere deine Jobsuch-, LinkedIn- und Interviewfähigkeiten mithilfe strukturierter Methoden wie STAR. Bereite dich durch praxisnahe HR-Coachings und Probeinterviews gezielt auf technische und verhaltensorientierte Vorstellungsgespräche vor, um Arbeitgeber zu überzeugen.

Kernzertifizierung

PECB ISO/IEC 27001 Lead Implementer

Establish, implement, manage, and maintain an Information Security Management System in accordance with ISO/IEC 27001 - the most recognized security framework.

Optional

BSI IT-Grundschutz Practitioner

IHK: Data Protection Officer

Hack The Box: Certified Defensive Security Analyst

eJPT Junior Penetration Tester

Skills:

- **ISMS-Prinzipien und -Framework**
- **ISO/IEC 27001-Compliance**
- **ISMS-Implementierung**
- **Audit-Vorbereitung**

Über Den Unterricht Hinaus: Projekte Und Interaktives Lernen

Projektbasiertes Lernen
Wende technische Konzepte in realen, individuellen und gemeinschaftlichen Projekten an, um ein starkes berufliches Portfolio aufzubauen.

Abschlussprojekte
Bearbeite umfassende, mehrtägige Projekte, die reale Cybersicherheitsherausforderungen simulieren und zeige dein Fachwissen, deine Teamfähigkeit und deine Problemlösungs-kompetenz gegenüber Arbeitgebern.

Beispielprojekte

- **Python:** Log-Analyse mit InsightLog
- **Netzwerke:** Extrahieren von Dateien aus einer Windows-VM
- **Windows & Python:** Entwicklung eines Prozessüberwachungs-Antivirus
- **KI:** Einsatz einer Cloud-LLM-Anwendung und Schutz vor böswilligen Akteuren
- **Abschlussprojekt:** Mehrtägige Purple-Team-Übung zu Active-Directory-Hacking und Verteidigung

Cyber Games
Nimm an Wettbewerben, Hackathons und Challenges teil, die das Erlernen von Cybersicher-heit in ein spannendes und lohnendes Erlebnis verwandeln.

Studierenden-Präsentationen
Recherchiere, entwickle und halte Präsentationen zu Cybersicherheitsthemen, um deine professionellen Kommunikationsfähigkeiten zu stärken.

Mentorengespräche
Vereinbare persönliche 1:1-Sitzungen mit deinem Mentor, um deinen Fortschritt zu besprechen, Fragen zu klären und individuelle Karriereberatung zu erhalten.

CyberTalks
Erhalte Einblicke von Branchenexpertinnen und -experten, die reale Cyberangriffe analysieren, von historischen Fällen wie Stuxnet bis hin zu den modernsten Cyberoperationen der Gegenwart.

Industriepraktikum: Dein Weg zu echter Cybersicherheitserfahrung

Sammle praxisnahe Erfahrungen mit einem optionalen Praktikum in einer dieser Umgebungen:

Eigenständig organisiert: Finde mit unserer Unterstützung eine Rolle deiner Wahl.

Partnerunternehmen: Arbeite in einem Unternehmensumfeld bei einem unserer Branchenpartner.

Gemeinnützige Organisationen: Setze deine Fähigkeiten in sinnvollen Projekten ein.

Internes Cybersteps-Praktikum: Löse reale Herausforderungen unter Anleitung unserer Expertinnen und Experten.

Praktikumsbereiche

- **Cybersecurity Analyst**
- **Security Operations Center (SOC) Analysis**
- **IT-Sicherheits-administration**
- **Netzwerk-Sicherheitstechniker**
- **Cybersecurity Consultant**
- **GRC Analyst**

Berufliche Möglichkeiten nach Abschluss des Programms

Cybersecurity Consultant

Bewerte Sicherheitsrisiken, führe Audits durch und entwickle Verteidigungs-strategien in einer Rolle, die technisches Problemlösen mit direktem Kunden-kontakt verbindet.

Typisches Gehalt: €52,000–€78,000*

Cloud Security Engineer

Schütze Daten und Anwendungen in Cloud-Umgebungen durch die Ent-wicklung sicherer Architekturen, die Implementierung von Schutzmaßnahmen und die Überwachung auf Schwachstellen.

Typisches Gehalt: €64,000–€117,000*

SOC Analyst

Sei die erste Verteidigungslinie eines Unternehmens: Überwache Bedrohungen, analysiere Vorfälle und koordiniere Reaktionen, um rund um die Uhr Sicherheit zu gewährleisten.

Typisches Gehalt: €51,000–€74,000*

IT Security Administrator

Verwalte Sicherheitsoperationen wie Richtlinien, Firewalls und Benutzerzugriffe, um Netzwerke zu schützen und eine sichere IT-Umgebung im Unternehmen aufzubauen.

Typisches Gehalt: €69,000–€93,000*

**Quelle: Glassdoor*

Unterstützung Bei Der Karriereentwicklung

Cybersteps unterstützt dich während und nach dem Programm bei deiner Jobsuche, mit professionellem Karrierecoaching, entwickelt von HR-Expert*innen und Cybersicherheits-Fachleuten. So stichst du hervor und sicherst dir deinen ersten Job im Bereich Cybersicherheit.

Professionelles LinkedIn-Profil & Lebenslauf:
Erstelle ein auf Cybersicherheit fokussiertes LinkedIn-Profil und einen Lebenslauf, die deine technischen Fähigkeiten und Erfolge hervorheben. Lerne, deinen Lebenslauf gezielt für bestimmte Rollen anzupassen und LinkedIn strategisch zu nutzen, um mit Recruiterinnen und Branchenexpertinnen in Kontakt zu treten.

Fortgeschrittene Strategien für die Jobsuche:
Lerne, LinkedIn, spezialisierte Jobbörsen und berufliche Netzwerke effektiv zu nutzen, um die besten Cybersicherheitschancen zu finden. Setze gezielte Suchstrategien ein, um deine Sichtbarkeit zu erhöhen und dich in einem wettbewerbsintensiven Markt hervorzuheben.

Branchennetzwerk-Möglichkeiten:
Nimm an unseren Veranstaltungen teil, um wertvolle Kontakte in der Branche zu knüpfen, und nutze unser professionelles Netzwerk, um dein eigenes aufzubauen.

Vorbereitung auf technische und verhaltensbezogene Interviews:
Perfektioniere deine technischen und verhaltensbezogenen Cybersicherheits-Interviews durch praxisnahe Simulationen, die von Expert*innen entwickelt wurden. Erhalte persönliches Feedback, verbessere deine Antworten, stärke dein Selbstvertrauen und präsentiere deine technischen Fähigkeiten überzeugend.

Business-Kommunikationsfähigkeiten:
Verbessere deine Fähigkeiten im Schreiben von E-Mails, technischen Berichten und Präsentationen, entscheidend für Erfolg in der Cybersicherheits- und Tech-Branche. Lerne bewährte Branchenstandards für professionelle Kommunikation, um dir sowohl bei Bewerbungen als auch im Arbeitsalltag einen Wettbewerbsvorteil zu verschaffen.

> Cybersicherheit fühlte sich wie die perfekte Berufswahl an, sie ermöglicht es mir, meine Leidenschaft für Gaming und Technologie in reale Problemlösungen und einen gut bezahlten Job zu verwandeln. Ich kann Cybersteps jedem empfehlen, der eine Karriere in der Cybersicherheit anstrebt.

Avi Kozokin,
Cybersecurity researcher at IONIX

Sprich Mit Uns

Wir Beraten Dich Gerne

https://cybersteps.de

info@cybersteps.de

+49 30 585823080

Cybersteps GmbH • Schloßstr. 50 in 12165 Berlin, Germany