cybersteps

Cybersecurity Weiterbildung

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

4.9 ★★★★★
Student*innenbewertungen

IHK Akademie
München und Oberbayern

CERTQUA
Qualitätsmanagement
zugelassener Träger nach AZAV

> Wer wirklich praktische IT- oder Cybersecurity-Fähigkeiten aufbauen will, ist hier genau richtig. Anders als bei vielen anderen Anbietern, bei denen ich leider Zeit verschwendet habe, geht es im Programm von Cybersteps nicht nur um Theorie – es vermittelt echte praktische Erfahrung.
>
> **Marc Nöthen**

> Ich hatte keinerlei Vorkenntnisse in Cybersecurity, und am Anfang war das alles ziemlich überwältigend. Aber Roman hat die Dinge so erklärt, dass es bei mir Klick gemacht hat – und Schritt für Schritt hatte ich das Gefühl, dazuzugehören.
>
> **Doreen Fischel**

> Das Programm ist intensiv und gut strukturiert – perfekt, um eine Karriere in der Cybersecurity aufzubauen. Die Dozent*innen erklären komplexe Themen verständlich und vermitteln praktische Beispiele, nicht nur Theorie. Die praxisnahen Labs helfen enorm, reale Szenarien zu verstehen, und der feste Tagesablauf hält einen diszipliniert und konsequent.
>
> **Soroush Shariatmadari**

Dein Weg Zur Karriere In Der Cybersicherheit

Geleitet von Cybersecurity-Expert*innen aus Elite-Militäreinheiten und führenden Cybersecurity-Unternehmen, ist die branchenführende Weiterbildung von Cybersteps darauf ausgelegt, dich fit für den Job zu machen. Wir haben Expert*innen ausgebildet, die heute einige der kritischsten Systeme der Welt schützen.

Jetzt bist du dran.

Cybersecurity im Fokus
Höchste Ausbildungsqualität, ein stets aktuelles Curriculum und starke Verbindungen zur Branche.

Auf den deutschen Arbeitsmarkt zugeschnitten
Zugeschnitten auf gefragte Rollen wie SOC-Analyst*in, Cyber Consultant, Cloud Engineer, GRC Analyst*in und IT-Admin.

Moderne KI-Tools und -Fähigkeiten
Wir stellen KI ins Zentrum unseres Curriculums und Lernerlebnisses, damit du effektiv lernst und dem sich wandelnden Arbeitsmarkt immer einen Schritt voraus bist.

1-zu-1-Mentoring durch Expert*innen
Unsere Lehrkräfte, Mentor*innen sowie Karriereberater*innen bieten dir alle Unterstützung, Begleitung und das Karriere-Coaching, damit du deine Ziele erreichst.

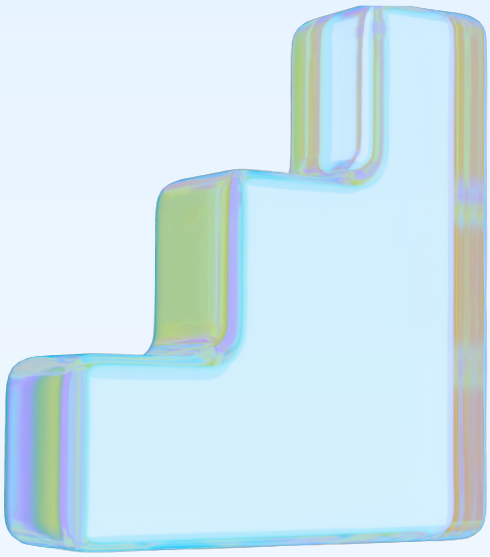
Militärisch erprobte Weiterbildung
Unsere innovative Lernplattform vermittelt dir praktische, realitätsnahe Erfahrung durch Simulationen und interaktive Labs - entwickelt von Elite-Militärausbildenden.

Branchenanerkannte Zertifizierungen
Wir bereiten dich auf führende, branchenanerkannte Zertifizierungen vor. Prüfungsgutscheine und die vollständige Vorbereitung sind inklusive.

Hardware inklusive: leistungsstarker Laptop
Damit du von Tag eins an erfolgreich bist, stellen wir dir einen brandneuen Lenovo ThinkPad-Laptop (oder ein vergleichbares Modell) für die gesamte Weiterbildung zur Verfügung – und nach dem Abschluss gehört er dir.

Von Der Theorie Zur Praxis: So Unterrichten Wir

Bei Cybersteps setzen wir auf die Reverse-Classroom-Methodik – einen bewährten Ansatz, der von führenden Universitäten und MINT-Programmen genutzt wird, um Lernergebnisse zu verbessern und alle Lernenden dabei zu unterstützen, ihr volles Potenzial auszuschöpfen.

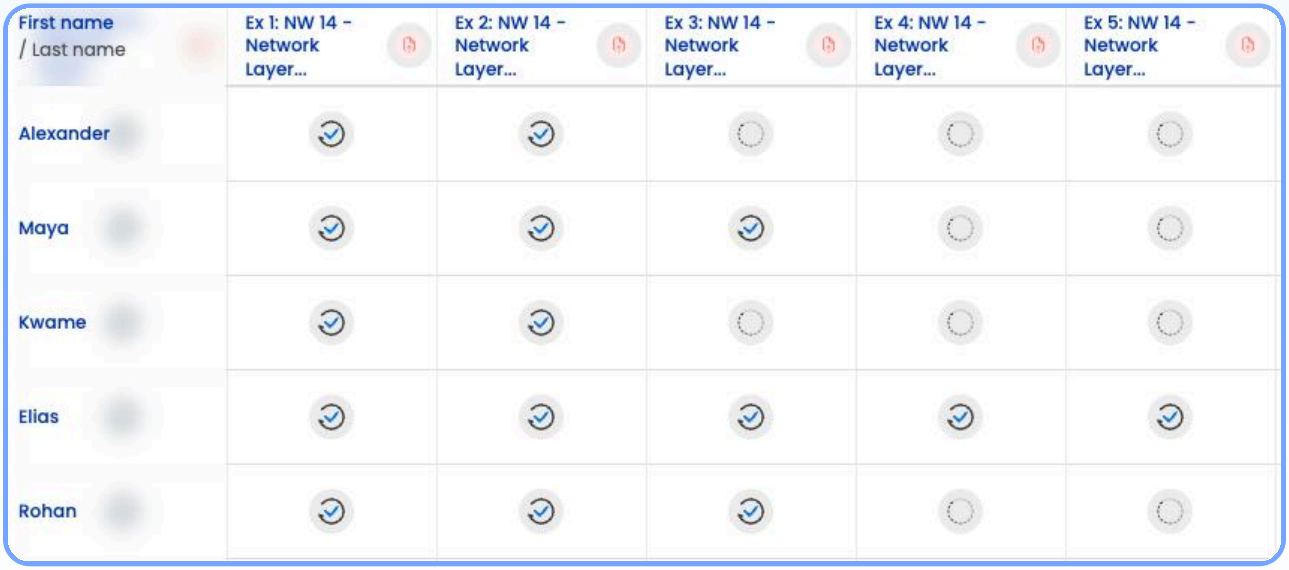


Dreistufiger Lernprozess

- **Vor dem Unterricht:** Sieh dir Videos und Lesematerialien an und absolviere Einführungsübungen, um dich in deinem eigenen Tempo auf die von Dozent*innen geleiteten Sessions vorzubereiten – so holst du das Beste aus ihnen heraus.
- **Im Unterricht:** Nimm an kleinen, lebendigen Sessions teil, die von Branchenexpert*innen geleitet werden – mit Live-Demos, angeleiteter Laborarbeit und ausführlichen Q&A-Diskussionen.
- **Nach dem Unterricht:** Vertiefe deine Fähigkeiten mit Übungen, Labs und anspruchsvollen Challenges mit ansteigendem Schwierigkeitsgrad – so wirst du immer auf deinem aktuellen Niveau gefordert.

Individuelle Fortschrittsverfolgung

Damit du dein volles Potenzial entfalten kannst, wirst du immer auf einem Niveau gefordert, das zu deinem Vorwissen und deinem Fortschritt passt – weder unterfordert noch überfordert. Wir verfolgen deinen Fortschritt anhand von Übungen, Projekten und Mentoring-Sessions, um auf Basis deiner Stärken und Ziele den passenden Karriereweg in der Cybersecurity für dich zu finden. Außerdem geben wir dir durchgehend detailliertes Feedback, damit du auf Kurs bleibst und deine Karriereziele erreichst.



Programmstruktur & Zeitplan

09:00–10:00
Live-Unterricht und Demo

10:00–10:10
Kurze Pause

10:10–11:00
Live-Unterricht und Demo

11:00–13:00
Angeleitetes praktisches Training

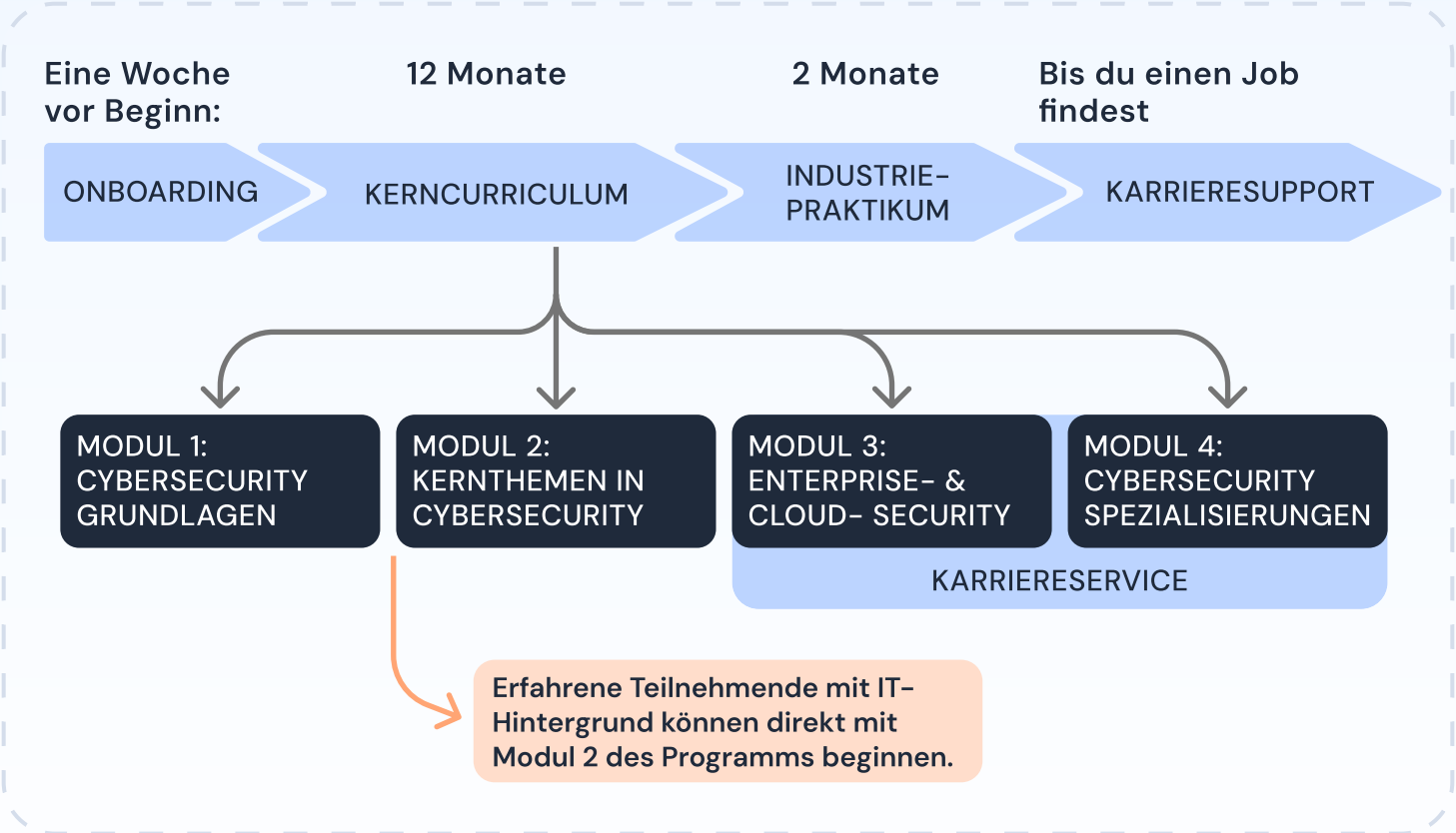
13:00–14:00
Mittagspause

14:00–15:00
Wiederholungssitzung

15:00–17:00
Angeleitetes praktisches Training

17:00–18:00
Vorbereitung auf den nächsten Tag

Programmablauf



Praktische Fähigkeiten

In unseren Übungen, Simulationen und Labs erwirbst du praktische Fähigkeiten mit branchenführenden Tools – und damit das Wissen und die praktische Erfahrung, um auf dem heutigen Cybersecurity-Arbeitsmarkt zu überzeugen.

Networking

- Wireshark
- Cisco Packet Tracer
- tcpdump
- Snort
- Nmap

Operating Systems

- Windows
- Linux
- Android

Scripting & Automatisierung

- Python
- PowerShell
- Bash
- SQL
- Git

Cloud & IT-Administration

- Microsoft 365
- Entra ID
- Azure Cloud
- Terraform
- Sysinternals

Virtualisierung

- VMware
- Docker
- Kubernetes

KI & LLMs

- KI-Assistenten (ChatGPT, Claude, Gemini)
- KI-Agenten (Claude Code, Gemini CLI)
- Hugging Face
- LangChain

Cybersecurity-Tools

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

Praxisprojekte

- Realistische Angriffs-simulationen
- SIEM-Untersuchungen
- Cloud-Security-Labs
- Eigene Systeme aufbauen und verteidigen

KI für Cybersecurity

Zusätzlich zu unserem Kern-Curriculum legen wir großen Wert darauf, den Umgang mit KI-Tools in der Cybersecurity zu lernen. Im gesamten Programm setzt du KI für Aufgaben wie Coding und Datenanalyse ein, aber auch zum Schreiben von Berichten und für Recherchen. Außerdem lernst du, wie KI-Systeme angegriffen – oder abgesichert – werden können und wie KI in der Cybersecurity sowohl von Verteidiger*innen als auch von Angreifer*innen eingesetzt wird.

KI-Tools in der Praxis
Praktischer Einsatz führender Tools für Recherche, Schreiben, Coding und Datenanalyse.

Prompting & Workflows
Einfache Muster für zuverlässige Ergebnisse durch klare Anweisungen, Vorgaben und Iteration.

KI-Agenten & Skills
Automatisierung mehrstufiger Aufgaben mit Tools, Memory und strukturierten Workflows.

KI-Sicherheit
Risiken wie Prompt Injection und Datenabfluss – und wie man KI in realen Umgebungen sicher einsetzt.

KI für defensive Cybersecurity
KI-gestützte Bedrohungsanalyse, Untersuchungen, Automatisierung und defensive Workflows.

KI für offensive Cybersecurity
Einsatz von KI für Reconnaissance, Schwachstellenerkennung und Red-Team-Workflows im Rahmen von Penetrationstests.

Claude

Gemini

ChatGPT

Expert*innen-Support. Praxisnahe Erfahrung.

Ein akademisches Expertenteam, das immer für dich da ist

Werde Teil einer kleinen Lerngruppe mit persönlicher Betreuung und einer offenen, einladenden Community.

Dozent*innen: Erfahrene Cybersecurity-Profis, die deine täglichen Live-Sessions, Demos und Workshops leiten.

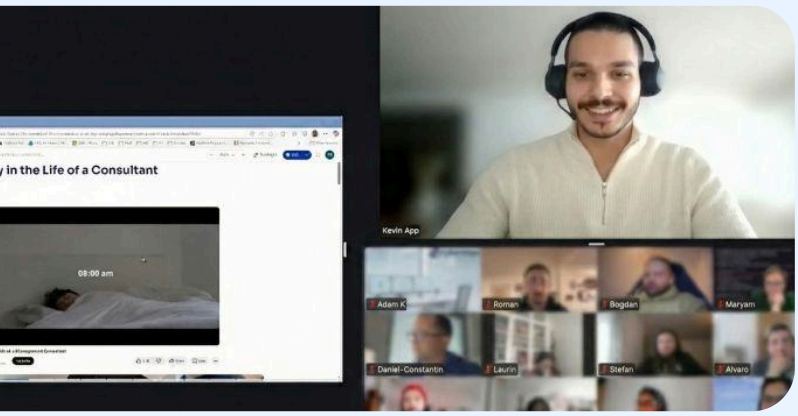
Teaching Assistants: Engagierte Junior-Cybersecurity-Profis, die dich rund um die Uhr unterstützen – immer, wenn du auf ein Problem stößt oder eine Frage hast.

Karriereberater*innen: HR-Spezialist*innen, die dir helfen, überzeugende Bewerbungen zu erstellen, deine Interview-Skills zu verbessern und deine Jobsuche zu meistern.

Gast-Branchenexpert*innen: Senior Manager*innen aus führenden Unternehmen, die einzigartige Perspektiven teilen.

Praxisnahes Curriculum rund um Hands-on-Projekte

Wende dein Wissen in realitätsnahen Projekten, Gruppen-Challenges und Capstone-Projekten an, die echte Cybersecurity-Arbeit simulieren.



Beispielprojekte

- **Bait n' Switch:** Einen öffentlichen Honeypot bereitstellen und echte Angriffsversuche analysieren.
- **Chat with Entra:** Eine*n KI-gestützten Cloud-Security-Auditor*in entwickeln, der sich mit Echtzeitdaten verbindet.
- **Secure Learningsteps:** Eine Cloud-Anwendung bereitstellen und vor böswilligen Akteuren schützen.
- **Game of Active Directory:** Mehrtägige Purple-Team-Übung – eine Active-Directory-Umgebung angreifen und verteidigen.

Modul 1: **Cybersecurity-Grundlagen**

Von Grund auf bauen wir ein solides Fundament in Computersystemen, Networking und Anwendungen auf. Du lernst, wie Betriebssysteme funktionieren, wie Systeme kommunizieren und wie moderne Anwendungen und Daten aufgebaut sind.

Außerdem arbeitest du mit grundlegenden Security-Tools und entwickelst Lerngewohnheiten für den Rest des Programms.

Kernthemen

Computer-Grundlagen
Verstehe, wie Computer funktionieren – einschließlich Hardware, Software und zentraler Systemkonzepte.

Betriebssysteme
Arbeite mit Windows und Linux, entwickle CLI-Fähigkeiten, verwalte Dateien und Prozesse und verstehe die Grundlagen der Systemsicherheit.

Networking
Lerne, wie Systeme über TCP/IP, IP-Adressierung und Routing kommunizieren, und analysiere den Datenverkehr mit Tools wie Wireshark.

Anwendungen
Verstehe, wie Webanwendungen funktionieren (HTTP/HTTPS, APIs), wie Daten in Datenbanken gespeichert und abgefragt werden, und entwickle einfache Anwendungen.

KI-Grundlagen
Setze KI-Tools effektiv ein, verstehe ihre Möglichkeiten und Grenzen und wende sie auf reale Cybersecurity-Aufgaben an.

Kryptografie
Lerne, wie Verschlüsselung, Hashing und Schlüsselmanagement Daten und Systeme schützen.

Kernzertifizierung

CompTIA Tech+

Eine Einstiegszertifizierung, die grundlegendes IT- und Cybersecurity-Wissen bestätigt.

Optional

CompTIA Network+

Highlights

- **Führe deine ersten echten Befehle im Terminal aus**
- **Baue mit KI deine eigene Website**
- **Entdecke, wie KI-Systeme angegriffen werden können**
- **Starte deinen ersten Netzwerkangriff**

Modul 2: **Kernthemen der Cybersecurity**

In Modul 2 steigst du mit einem Purple-Team-Ansatz in die reale Cybersecurity-Praxis ein. Du lernst, wie Angriffe ablaufen und wie du sie erkennst und darauf reagierst – und erkundest dabei verschiedene Rollen, die deinen Weg prägen können, etwa SOC Analyst*in, Penetration Tester*in, Security Engineer und GRC Analyst*in. Am Ende dieses Moduls bist du auf die CompTIA-Security+-Zertifizierung vorbereitet.

Kernthemen

Security-Grundlagen
Lerne wichtige Security-Controls, die CIA-Triade (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Accounting) sowie zentrale Konzepte wie Zero Trust, Change Management und physische Sicherheit.

Initial Access & Social Engineering
Lerne, wie Angreifer*innen sich über Reconnaissance und Phishing Zugang verschaffen und wie du diese Angriffe erkennst und verhinderst.

Web Hacking
Identifiziere und nutze gängige Web-Schwachstellen aus und verstehe, wie man Anwendungen dagegen absichert.

Schwachstellen & Exploitation
Analysiere Systeme unter Windows, Linux und Active Directory, nutze Schwachstellen aus und wende Hardening- und Mitigationstechniken an.

Security Monitoring & Forensik
Erkenne Angriffe mit SIEM-Tools, analysiere Logs und untersuche Incidents, um zu verstehen, was passiert ist und wie man reagiert.

Governance, Risk & Compliance (GRC)
Verstehe Frameworks, Risikomanagement und wie Organisationen Controls gestalten, um reale Risiken zu verhindern und zu reduzieren.

Kernzertifizierung

CompTIA Security+

Eine führende Zertifizierung für Junior-Cybersecurity-Profis. Sie bestätigt grundlegende Cybersecurity-Fähigkeiten, branchenübliche Security-Tools und Cybersecurity-Best-Practices.

Highlights

- **Hacke Websites und verstehe, wie Angriffe funktionieren**
- **Nutze Schwachstellen in Systemen und Anwendungen aus**
- **Untersuche reale Security-Incidents und analysiere, was passiert ist**
- **Absolviere ein Capstone-Purple-Team-Projekt: greife eine Active-Directory-Umgebung an und verteidige sie**

Modul 3: **Cloud & Enterprise Security**

In diesem Modul steigst du in die Enterprise-Cloud-Security ein und konzentrierst dich darauf, wie moderne Organisationen Cloud-Umgebungen aufbauen und schützen. Du arbeitest praktisch mit zentralen Cloud-Systemen, automatisierst Infrastruktur, überwachst reale Aktivitäten und verwaltest Identität und Zugriff im großen Maßstab.

Am Ende dieses Moduls bereitest du dich auf die Zertifizierung Microsoft Azure Fundamentals (AZ-900) sowie eine zusätzliche optionale Microsoft Azure-Zertifizierung – AZ-104 oder SC-200 – vor.

Kernthemen

Cloud Foundations
Arbeite mit zentralen Cloud-Bausteinen: virtuelle Maschinen, Networking, Storage und Identitäts-Grundlagen. Verstehe, wie Cloud-Umgebungen aufgebaut und betrieben werden.

DevSecOps & Infrastructure as Code
Stelle Workloads mit Automatisierung und Infrastructure as Code (Terraform) bereit und sichere sie ab. Arbeite mit Containern und Orchestrierung und integriere Security in Build- und Deployment-Pipelines.

Cloud Monitoring & Detection
Aktiviere Logging über Cloud-Ressourcen hinweg und nutze Tools wie Microsoft Sentinel, um Bedrohungen zu erkennen, Alerts zu analysieren und Incidents in realen Szenarien zu untersuchen.

Cloud Identity & Access (Entra ID)
Verwalte Identitäten und Zugriffe mit RBAC, Conditional Access und Privileged Identity Management (PIM). Verstehe Authentifizierungs-Flows (OAuth) und wie Identität zur zentralen Sicherheitsgrenze wird.

Microsoft 365 & Enterprise Security
Sichere Enterprise-Umgebungen, indem du Benutzer, Geräte und Richtlinien verwaltest. Analysiere Aktivitäten und Logs über Cloud- und Hybrid-Umgebungen hinweg, um Bedrohungen zu erkennen und zu verhindern.

Karrieretraining
Optimiere Lebenslauf und LinkedIn-Profil, um deine Skills und Erfahrung zu zeigen. Definiere im Mentoring deinen Karriereweg, identifiziere gefragte Rollen und entwickle die Fähigkeiten, mit denen du herausstichst.

Kernzertifizierung

Microsoft Azure Fundamentals (AZ-900)

Grundlagen von Cloud Computing, Azure-Diensten und Cloud-Security.

Wähle

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

ODER

Azure Administrator Associate (AZ-104)

ODER

Azure Security Operations Analyst Associate (SC-200)

Highlights

- **Erhalte deine eigene Azure-Subscription zum Üben**
- **Stelle eine produktionsreife App bereit und sichere sie ab**
- **Betreibe einen öffentlichen Honeypot und analysiere echte Angriffe**

Modul 4: **Cybersecurity-Spezialisierungen**

In diesem letzten Modul erwirbst du eine hoch angesehene IHK- (oder auf Wunsch PECB-) Zertifizierung und wählst im Mentoring deine Cybersecurity-Spezialisierung. Sie vertieft deine Expertise und stärkt dein Profil bei Arbeitgeber*innen. Du sammelst praktische Erfahrung mit den relevantesten Tools und Frameworks – ergänzt durch eine zusätzliche Zertifizierung, persönliches Karriere-Mentoring und Interview-Coaching, damit du selbstbewusst in den Arbeitsmarkt startest.

Kernthemen

Realistische Unternehmensumgebung: Angriff & Verteidigung
Arbeite in einer realistischen, modernen Unternehmensumgebung. Erkunde Angriffsvektoren, untersuche das Verhalten von Angreifer*innen, analysiere Schwachstellen und verbessere die Verteidigung.

Fortgeschrittene Governance, Risk & Compliance
Vertiefe dich in Governance, Risikomanagement und Compliance. Arbeite mit Frameworks wie ISO/IEC 27001 und NIS2 – durch Audits, Risikobewertungen, Nachweissammlung und Compliance-Reporting.

KI-Sicherheit & KI für Cybersecurity
Lerne, wie KI die Cybersecurity für Angreifer*innen und Verteidiger*innen verändert. Erkunde Angriffe auf KI-Systeme, defensive Ansätze und KI-gestützte Workflows und wende dein Wissen in einem abschließenden Praxisprojekt an.

Spezialisiertes Karrieretraining
Stärke deine Bewerbungsstrategie und Interview-Skills für Cybersecurity-Rollen. Präsentiere Erfahrung, Projekte und Zertifizierungen – in Mock-Interviews, rollenspezifischen Simulationen und professionellem Karriere-Coaching.

Highlights

- **Offizielle IHK-Zertifizierung: Cyber Security Advisor**
- **Praktische KI: Erhalte ein Claude-Pro-Abo (oder gleichwertig) und lerne, KI wirklich zu meistern**
- **Compliance mit dem ISO/IEC-27001-Standard**
- **ISMS-Implementierung**
- **Vorbereitung von Audits und Berichten**

Kernzertifizierung

IHK Cyber Security Advisor

Die offizielle IHK-Cyber-Security-Zertifizierung: Cyber-Bedrohungen erkennen, eindämmen und darauf reagieren.

ODER

PECB ISO/IEC 27001 Lead Implementer

ISO/IEC-27001-Compliance in einer Organisation implementieren & verwalten.

ODER

ISO/IEC 27001 Foundation

Die Grundlagen der ISO/IEC-27001-Compliance und Informationssicherheit verstehen.

Spezialisiere dich

Eine zusätzliche Zertifizierung – Details auf der nächsten Seite.

Modul 4: **Cybersecurity-Spezialisierungen**

Je nach Spezialisierungspfad konzentrierst du dich auf die Tools, Frameworks und Skills, die für die jeweilige Rolle am wichtigsten sind, und baust tiefes Fachwissen auf.

Du kannst aus sechs gefragten Bereichen wählen – jeder Pfad ist auf ein konkretes Karriereziel ausgerichtet und verbindet praktische Erfahrung mit einer zusätzlichen spezialisierten Zertifizierung eines führenden Anbietenden.

Security Operations (SOC)

Sei die erste Verteidigungslinie einer Organisation – überwache Bedrohungen, analysiere Incidents und koordiniere Reaktionen, um 24/7-Sicherheit zu gewährleisten.

CompTIA CySA+ ODER Hack The Box CDSA

Penetration Testing (Ethical Hacking)

Denke wie ein Angreifer, um Schwachstellen zu finden, bevor Kriminelle es tun – simuliere reale Angriffe und hilf Organisationen, die von dir aufgedeckten Lücken zu schließen.

CompTIA PenTest+ ODER Hack The Box CPTS

Security Engineering

Sichere Cloud-Umgebungen ab: Entwirf sichere Architekturen, verwalte Zugriffe, implementiere Schutzmaßnahmen und reduziere Risiken.

Cloud and AI Security Engineer Associate (SC-500)

Governance, Risk & Compliance (GRC)

Gestalte die Regeln, die Organisationen schützen – übersetze Vorschriften und Risiken in klare Richtlinien, die Sicherheit mit Geschäftszielen in Einklang bringen.

BSI IT-Grundschutz Practitioner

Cybersecurity Project Management

Treibe Cybersecurity-Initiativen von Anfang bis Ende voran – koordiniere Teams, Budgets und Deadlines für komplexe Security-Projekte.

CompTIA Project+

Application Security

Sichere Software von innen heraus ab – erkenne Schwachstellen im Code und hilf Entwicklungsteams, Anwendungen nach dem Secure-by-Design-Prinzip zu bauen.

HTB Certified Offensive AI Expert (COAE)

8-wöchiges Branchenpraktikum: Echte Cybersecurity-Praxiserfahrung

Praktische Berufserfahrung in einem echten Unternehmen

Über unser Partner*innennetzwerk haben wir Zugang zu über 400 Unternehmen in Deutschland und Europa. Wir vermitteln dir Interviews mit Arbeitgeber*innen aus unserem Partner*innennetzwerk, um die passende Position für dich zu finden. Wer die Grundanforderungen erfüllt, erhält einen garantierten Praktikumsplatz – und die große Mehrheit aller motivierten Lernenden wird erfolgreich vermittelt.

8 Wochen, Vollzeit
Dauer auf Anfrage anpassbar

Online oder vor Ort
Je nach Verfügbarkeit

Flexibler Starttermin
Beginne direkt nach dem Abschluss oder jederzeit innerhalb von 6 Monaten

Optionale Festanstellung
Viele Arbeitgeber*innen bieten je nach Leistung eine feste Stelle

Mögliche Praktikumsbereiche:

- Cybersecurity Analyst*in
- Security Operations Center (SOC) Analyst*in
- IT Security Administrator*in
- Netzwerksicherheitstechniker*in
- Cybersecurity Consultant
- GRC/Compliance Analyst*in

Careersteps: Career Accelerator

Mit Careersteps unterstützen wir deine Jobsuche während und nach dem Programm – mit Coaching von HR-Profis und Cybersecurity-Interviewer*innen, damit du herausstichst und deine erste Cybersecurity-Stelle bekommst. Wir beschleunigen das durch 1:1-Mentoring, gemeinsame Workshops und aktuellste Lernressourcen.

Professionelles LinkedIn-Profil & Lebenslauf
Erstelle ein cybersecurity-fokussiertes LinkedIn-Profil und einen Lebenslauf, die deine technischen Fähigkeiten hervorheben. Wir helfen dir, deinen Lebenslauf auf konkrete Rollen zuzuschneiden und LinkedIn strategisch zu nutzen, um Recruiter*innen und Branchenexpert*innen auf dich aufmerksam zu machen.

Fortgeschrittene Strategien für die Jobsuche
Lerne, LinkedIn, spezialisierte Jobbörsen und Netzwerke effektiv für die Suche nach Cybersecurity-Stellen zu nutzen. Erweitere mit fortgeschrittenen Strategien deine Optionen und konzentriere dich auf die relevantesten Stellen.

Networking-Möglichkeiten in der Branche
Nimm an unseren Events und Partner*innen-Events teil, knüpfe wertvolle Branchenkontakte und nutze unser Netzwerk, um dein eigenes aufzubauen.

Vorbereitung auf technische & Behavioral Interviews
Meistere technische Interviews und Behavioral-Interviews mit expertenkonzipierten Simulationen und Mock-Interviews. Erhalte persönliches Feedback, um deine Antworten zu verfeinern, Sicherheit zu gewinnen und dein technisches Können zu zeigen.

Business-Kommunikationsfähigkeiten
Verbessere deine E-Mail-, Reporting- und Präsentationsfähigkeiten – essenziell für den Erfolg in Cybersecurity und Tech. Beherrsche Best Practices der Arbeitsplatzkommunikation und verschaffe dir einen Vorteil bei Bewerbungen und im Berufsalltag.

> Erfolg bedeutet für mich, unseren Lernenden die richtigen Werkzeuge zu geben, um ihre eigene Karriere in die Hand zu nehmen. Zu sehen, wie sie neues Wissen gewinnen, Selbstvertrauen aufbauen und ihren eigenen Weg proaktiv gehen, ist unglaublich erfüllend.
>
> **Charlotte Jäger**,
> Karriereberaterin für Cybersecurity-Talente

CourseReport by career.io 5.0

Excellent Trustpilot

kursfinder.de POWERED BY KEYSTONE Average rating: 4.9

Google 5.0 average rating

> Es ist ein großartiges Programm – ich lerne so viel, und es ist eine richtig tolle Erfahrung. Roman macht die Lektionen leicht verständlich und sogar richtig unterhaltsam, selbst wenn die Themen kompliziert und knifflig werden.

Stanislav Safaniuk

> Meine Erfahrung war durchweg positiv. Ich komme aus einem nicht-technischen Bereich, aber die Dozent*innen sind sehr einsteigerfreundlich. Sie sind äußerst kompetent, erfahren und professionell und machen komplexe Themen leicht verständlich. Das Lernumfeld ist unterstützend und motivierend, was mir geholfen hat, Selbstvertrauen aufzubauen. Ich würde dieses Programm jedem empfehlen, der sich beruflich neu orientieren möchte.

Fazluddin Bawar

> Vor einem Jahr habe ich beschlossen, in die Cybersecurity zu wechseln, und mich für Cybersteps entschieden. Rückblickend bin ich überzeugt, dass es die richtige Entscheidung war. Was die Erfahrung wirklich besonders gemacht hat, war die kontinuierliche Unterstützung. Von engagierten Karriereservices, 1:1-Coaching sowie der Optimierung von Lebenslauf und LinkedIn bis hin zu durchgehendem Mentoring und Begleitung während des gesamten Programms – das Cybersteps-Team war immer da, um sicherzustellen, dass ich auf Kurs bleibe und mich gut auf die Branche vorbereitet fühle.

Akar Sarpal

> Cybersecurity fühlte sich wie die perfekte Berufswahl an – sie lässt mich meine Leidenschaft für Gaming und Technologie in echtes Problemlösen und einen gut bezahlten Job verwandeln. Ich kann Cybersteps jedem wärmstens empfehlen, der eine Karriere in der Cybersecurity sucht.

Avi Kozokin,
Cybersecurity Researcher bei IONIX

Kontaktiere Uns

Erfahre Mehr Über Unser Programm

https://cybersteps.de

info@cybersteps.de

+49 30 585823080

PARTNER FÜR BERLIN

MITGLIED IM bitmi Bundesverband IT-Mittelstand e.V.

Mitglied im bitkom

Mitglied im FKU FRIEDRICHSHAIN-KREUZBERGER UNTERNEHMERVEREIN E.V.

Cybersteps GmbH • Schloßstr. 50 in 12165 Berlin, Germany