Curriculum
Cyber Security with AI

10+Years of Building Careers

Full-time: 16 weeks / 4 months

English **Remote**

Launch your career in cybersecurity — one of Germany's most critical skills shortages.

In this intensive 16-week bootcamp, you will build expertise across all areas of cybersecurity including, technical security foundations, AI in cybersecurity, security operations, vulnerability assessment, penetration testing, and governance, risk and compliance (GRC).

The course offers 200+ hands-on labs, real Virtual Desktop Infrastructure — real tools, real diagnostic scenarios, unassisted problem-solving sessions.

Graduates will leave with a good understanding of ISO 27001, GDPR, NIS2 and BSI-Grundschutz knowledge German employers are actively hiring for. You will be prepared for roles where technical expertise, regulatory compliance, and strategic thinking come together.

Future jobs for you:

- **Information Security Auditor**
- **Cybersecurity Analyst**
- **Threat Intelligence Analyst**
- **Security Operations Center (SOC) Analyst**

Annual salary: €57,000 - €89,000

Tech Stacks

Technical Foundations
- Technical Foundations
- Security Principles (CIA Triad, Threat Models)
- Linux & Unix Command Line
- Networking Fundamentals (TCP/IP, DNS, HTTP, VPN)

Cybersecurity Analysis
- Threat Intelligence & Risk Assessment
- Cryptography & Data Protection
- Incident Response & Digital Forensics
- Log Analysis & Threat Hunting

Security Operations & Engineering
- Network Security & Firewalls
- Identity & Access Management (IAM)
- Intrusion Detection & Prevention (IDS/IPS)
- SIEM & Threat Detection (Wazuh / EDR/XDR)
- Tools: Wazuh, Kali Linux, Metasploit, Hydra, Windows Server 2022 AD, smbclient — with MITRE ATT&CK mappings across brute-force, privilege escalation and audit log tampering scenarios on real VDI

AI in Cybersecurity
- AI-Assisted reconnaissance & Scan
- Analysis and Security workflows
- AI Attack Surface & Risk Assessments
- AI Governance Risk and Reporting

Cloud & Virtualization Security
- Cloud Security Best Practices
- Cloud Identity & Zero Trust Models

Cloud & Virtualization Security
- Vulnerability Assessment & Penetration Testing
- Vulnerability Scanning & Exploitation
- Web Application Security (OWASP Top 10)
- Social Engineering & Phishing Simulation
- Red Team vs Blue Team Methodologies
- Reporting & Remediation Strategy

Career Readiness
- Security Case Studies & Research
- 200+ Hands-On Labs including Real VDI, Real Tools
- Unassisted Diagnostic Labs & Capstone Project
- Certification Preparation:
  - CompTIA Security+, CySA+ and A+

Governance Risk and Compliance
A good understanding of:
- Information Security Risk Management
- Risk Identification
- Risk Treatment & Acceptance
- ISO/IEC 27001:2022 — ISMS Design & Implementation
- Structure of ISO Management System Standards (HLS)
- BSI-Grundschutz — Germany's National Security Framework
- GDPR: Article 32 Security Requirements & Breach Notification
- NIS2 Directive / IT-SiG 3.0 — German Implementation
- Security Policy Writing & Compliance Documentation

Soft Skills

Click here for final projects

- **Communication Skills**
- **Creativity**
- **Domain Knowledge**
- **Problem Solving**
- **Collaboration**
- **Time Management**
- **Flexibility**
- **Ethical Considerations**

★ Certificate CompTIA CySA+

★ Certificate CompTIA A+

★ Certificate CompTIA Security+

Practical Project
Implementation of acquired knowledge in a real-life scenario.

Supported Job Search
We actively support job searches, offering regular networking events where participants connect with experienced tech professionals.

neue fische | SPICED

Curriculum Cyber Security mit KI

10+Years of Building Careers

Vollzeit: 16 Wochen / 4 Monate

Englisch **Remote**

Starte durch im Bereich Cybersicherheit – einem der wichtigsten Fachkräfte mangelgebiete in Deutschland.
In diesem intensiven 16-wöchigen Bootcamp erwerben Teilnehmende Fachkenntnisse in sechs Bereichen: Grundlagen der technischen Sicherheit, KI in der Cybersicherheit, Cloud-Sicherheit, Sicherheitsbetrieb und -technik, Schwachstellen Analyse und Penetrationstests sowie Governance, Risiko und Compliance (GRC).

Der Kurs bietet über 200 praktischen Übungen, mit echter virtueller Desktop-Infrastruktur – echten Tools, realen Diagnoseszenarien und selbstständigen Problemlösungs-sitzungen. Absolventen mit 4 CompTIA -Zertifizierungen sowie Kenntnissen in ISO 27001, DSGVO, NIS2 und BSI-Grundschutz sind bei deutschen Arbeitgebern sehr gefragt. Du wirst auf Positionen vorbereitet, in denen technisches Fachwissen, die Einhaltung gesetzlicher Bestimmungen und strategisches Denken zusammenkommen.

Zukunftsjobs für dich:

- **Information Security Auditor**
- **Cybersecurity Analyst**
- **Threat Intelligence Analyst**
- **Security Operations Center (SOC) Analyst**

Jahresgehalt: 57.000 - 89.000 €

Die hier vorgestellten Lehrpläne sind als beispielhafte Orientierung für die Kursinhalte gedacht. Anpassungen der Inhalte und des Zeitplans aus didaktischen und organisatorischen Gründen sowie zur Anpassung an den Stand der Technik und die aktuellen Anforderungen des Arbeitsmarktes bleiben ausdrücklich vorbehalten, ohne dadurch den Charakter des Kurses und die Gesamtqualität seiner Inhalte zu beeinträchtigen.

Tech Stacks

Technische Grundlagen
- Sicherheitsprinzipien (CIA-Triade, Bedrohungsmodelle)
- Linux- und Unix-Befehlszeile
- Netzwerk-Grundlagen (TCP/IP, DNS, HTTP, VPN)

Cybersicherheitsanalyse
- Bedrohungsanalyse und Risikobewertung
- Kryptographie und Datenschutz
- Incident Response & Digitale Forensik
- Protokollanalyse und Bedrohungsjagd

Sicherheitsbetrieb und -technik
- Netzwerksicherheit & Firewalls
- Identitäts- und Zugriffsmanagement (IAM)
- Einbruchserkennung und -prävention (IDS/IPS)
- SIEM & Bedrohungserkennung (Wazuh / EDR/XDR)
  - *Werkzeuge: Wazuh, Kali Linux, Metasploit, Hydra, Windows Server 2022 AD, smbclient – mit MITRE ATT&CK-Mappings für Brute-Force-Angriffe, Rechteausweitung und Manipulation von Audit-Logs in realen VDI-Umgebungen.*

KI in der Cybersicherheit
- KI-gestützte Aufklärung & Scan
- Analyse- und Sicherheitsworkflows
- KI-Angriffsfläche & Risikoanalysen
- KI-Governance, Risikomanagement und Berichterstattung

Cloud- und Virtualisierungssicherheit
- Bewährte Verfahren für die Cloud-Sicherheit
- Cloud-Identitäts- und Zero-Trust-Modelle

Schwachstellenanalyse & Penetrationstests
- Schwachstellenscan und -ausnutzung
- Webanwendungssicherheit (OWASP Top 10)
- Social Engineering & Phishing-Simulation
- Methodiken des roten Teams gegen das blaue Team
- Berichts- und Sanierungsstrategie

Berufsreife
- Sicherheitsfallstudien und Forschung
- Über 200 praktische Übungen, darunter echte VDI-Umgebungen und reale Tools.
- Labore für unassistierte Diagnostik & Abschlussprojekt
- Vorbereitung auf die Zertifizierung:
  - CompTIA Security+, CySA+ und A+

Governance, Risikomanagement und Compliance
Ein gutes Verständnis von:
- Informationssicherheits-Risikomanagement
- Risikoidentifizierung
- Risikobehandlung und -akzeptanz
- ISO/IEC 27001:2022 — ISMS-Design und -Implementierung
- Struktur der ISO-Managementsystemnormen (HLS)
- BSI-Grundschutz – Deutschlands Nationaler Sicherheitsrahmen
- DSGVO: Artikel 32 Sicherheitsanforderungen & Meldung von Datenschutzverletzungen
- NIS2-Richtlinie / IT-SiG 3.0 – Deutsche

Soft Skills

Hier klicken für finale Projekte

- **Kreativität**
- **Fachwissen**
- **Kommunikationsfähigkeiten**
- **Problemlösung**
- **Zusammenarbeit**
- **Zeitmanagement**
- **Flexibility**
- **Ethische Überlegungen**

★ Zertifikat CompTIA CySA+

★ Zertifikat CompTIA A+

★ Zertifikat CompTIA Security+

Praxisprojekt
Umsetzung des erworbenen Wissens in einem realen Szenario.

Unterstützte Jobsuche
Zusätzlich unterstützen wir aktiv bei der Jobsuche. Schon während des Lehrgangs können Teilnehmer:innen in regelmäßig stattfindenden Netzwerkveranstaltungen wertvolle Kontakte zu erfahrenen Fachkräften der Tech-Szene knüpfen.

neue fische | SPICED