Curriculum
Cyber Security

Full-time: 16 weeks / 4 months

English **Remote**

Start your career in the field of cybersecurity.
In this intensive bootcamp, you'll gain expertise in technical security measures, cloud and AI risks, as well as governance, risk, and compliance structures. You'll learn how to securely assess modern IT and cloud environments, identify and manage risks, threats and vulnerabilities, and enforce compliance as per security standards.

You will be specifically prepared for roles where technical understanding, regulatory compliance, and strategic thinking come together.

Future jobs for you:

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

A cybersecurity analyst earns on average between 60.000 € and 90.000 € a year.

Tech Stacks

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

AI in Cybersecurity
- AI-Assisted reconnaissance & Scan
- Analysis and Security workflows
- AI enabled SOC support
- AI attack surface, Risk Assessments
- Security Automations with AI
- AI Governance Risk and Reporting

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 (Splunk / ELK / Microsoft Sentinel)
- Endpoint Detection & Response (EDR/XDR)

Cloud & Virtualization Security
- Cloud Security Best Practices (AWS, Azure)
- Infrastructure as Code (Terraform Basics)
- Cloud Identity & Zero Trust Models

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
- Portfolio Development (Hands-on Labs)
- Capstone Security Project
- Certification Preparation:
  - CompTIA A+
  - CompTIA Security+
  - CompTIA CySA+

Governance Risk and Compliance
- Information Security Risk Management
- Risk Identification
- Risk Treatment & Acceptance
- Introduction to ISO/IEC 27001:2022 standards
- Structure of ISO Management System Standards (HLS)

Soft Skills

Click here for final projects

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

★ Zertifikat CompTIA CySA+

★ Zertifikat CompTIA A+

★ Zertifikat 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

Vollzeit: 16 Wochen / 4 Monate

Englisch **Remote**

Starten Sie Ihre Karriere im Bereich Cybersicherheit. In diesem intensiven Bootcamp erwirbst du Fachwissen über technische Sicherheitsmaßnahmen, Cloud und KI-Risiken sowie Governance-, Risiko- und Compliance-Strukturen. Du lernst, wie du moderne IT- und Cloud-Umgebungen sicher bewertest, Risiken, Bedrohungen und Schwachstellen identifizierst und verwaltest sowie die Einhaltung von Sicherheitsstandards durchsetzt.

Du wirst speziell auf Positionen vorbereitet, in denen technisches Verständnis, Einhaltung gesetzlicher Vorschriften und strategisches Denken zusammenkommen.

Zukunftsjobs für dich:

- **Informationssicherheitsprüfer:in**
- **Cybersecurity Analyst**
- **Threat Intelligence Analyst**
- **Security Operations Center (SOC) Analyst**

Ein Cybersecurity Analyst verdient im Durchschnitt zwischen 60.000 € und 90.000 € im Jahr.

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)
- Git & GitHub (Versionskontrolle & Zusammenarbeit)
- Linux- und Unix-Befehlszeile
- Grundlagen der Vernetzung (TCP/IP, DNS, HTTP, VPN)

KI in der Cybersicherheit

- KI-gestützte Aufklärung und Scan-Analyse sowie Sicherheits-Workflows
- Angriffsfläche für KI, Risikobewertungen
- KI-gestützte SOC-Unterstützung
- Sicherheitsautomatisierung mit KI
- KI-Governance, Risiko und Berichterstattung

Cybersicherheitsanalyse

- Bedrohungsinformationen und Risikobewertung
- Kryptografie und Datenschutz
- Incident Response & Digitale Forensik
- Protokollanalyse und Bedrohungssuche

Sicherheitsmaßnahmen und -technik

- Netzwerksicherheit und Firewalls
- Identitäts- und Zugriffsmanagement (IAM)
- Intrusion Detection und Prevention (IDS/IPS)
- SIEM (Splunk / ELK / Microsoft Sentinel)
- Endpunkt-Erkennung und -Reaktion (EDR/XDR)

Cloud- und Virtualisierungssicherheit

- Bewährte Verfahren für Cloud-Sicherheit (AWS, Azure)
- Infrastruktur als Code (Terraform-Grundlagen)
- Cloud-Identität und Zero-Trust-Modelle

Schwachstellenanalyse und Penetrationstests

- Schwachstellenscans und -ausnutzung
- Webanwendungssicherheit (OWASP Top 10)
- Social Engineering und Phishing-Simulation
- Methoden des Red Teams vs. Blue Teams
- Berichterstattung und Strategie zur Behebung von Mängeln

Berufsvorbereitung

- Sicherheitsfallstudien und -forschung
- Portfolioentwicklung (praktische Übungen)
- Capstone-Sicherheitsprojekt
- Vorbereitung auf die Zertifizierung:
  - CompTIA A+
  - CompTIA Security+
  - CompTIA CySA+

Governance, Risiko und Compliance

- Risikomanagement für Informationssicherheit
- Risikoidentifizierung
- Risikobehandlung und -akzeptanz
- Einführung in die Normen ISO/IEC 27001:2022
- Struktur der ISO Managementsystemnormen (HLS)

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