cybersteps

Become a Cybersecurity Analyst

- 12 months of live classes
- 2-month internship
- Full-time
- Flexible & remote

4.9

★★★★★

Student reviews

CERTQUA

Qualitätsmanagement

zugelassener Träger nach AZAV

> Anyone who really wants to build practical IT or cybersecurity skills is in the right place here. Unlike many other providers where I unfortunately wasted time, this program doesn't just go over theory, it delivers real hands-on experience.

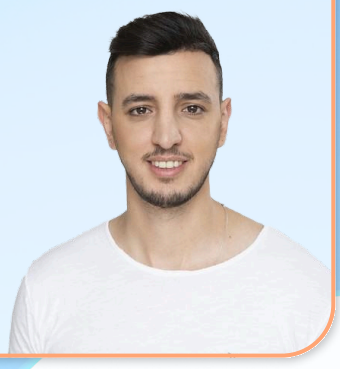
Marc Nöthen,
Cybersecurity Student

> I had no background in cybersecurity, and it felt overwhelming at first. But Roman broke things down in a way that made it click, and step by step, I felt like I belonged.

Doreen Fischel,
Cybersecurity Developer

> As an employer, finding skilled cybersecurity talent is always a challenge. Cybersteps is bridging the gap, providing companies like ours with well-prepared cybersecurity analysts who can make an immediate impact.

Shahar Vaknin,
Director of CTO Office clutch



Your Path to a Cybersecurity Career

Born from elite military and top cybersecurity firms, Cybersteps delivers battle-tested, industry-led training that makes you job-ready. We've trained experts now defending the world's most critical systems. Now is your turn.

Cybersecurity Focused
We specialize solely on cybersecurity, making us true experts with the network to get you interviews and land the job.

Designed for Germany's Job Market
A career-focused program for high-demand roles like IT Security Admin, SOC Analyst, Cybersecurity Consultant, and GRC Manager.

Advanced AI Tools and Skills
Our program places AI as a central component to help you stay ahead of the job market and the evolving cybersecurity landscape.

1-on-1 Expert Mentorship
You will get personal guidance and mentorship, technical support, and career coaching to help you achieve your professional goals.

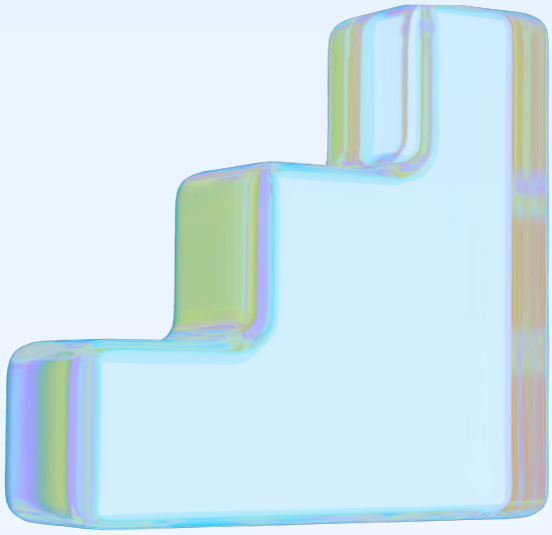
Hands-On, Military-Tested Training
Gain practical, real-world experience through a battlefield-tested curriculum taught by elite military-trained instructors.

Industry Credentials
Prepare for 8 industry-recognized certifications, fully paid, including exam vouchers and training. Test up to 6 months after the program.

New Advanced Laptop - Yours to Keep!
To support your success from day one, we'll provide you with a brand-new strong laptop at no cost. Use it throughout your training and keep it once you graduate.

Flipped Classroom & Personalized Learning

At Cybersteps, we use the Flipped Classroom methodology, a proven approach adopted by leading universities and STEM programs. This method enhances learning outcomes by helping each student meet their full potential.

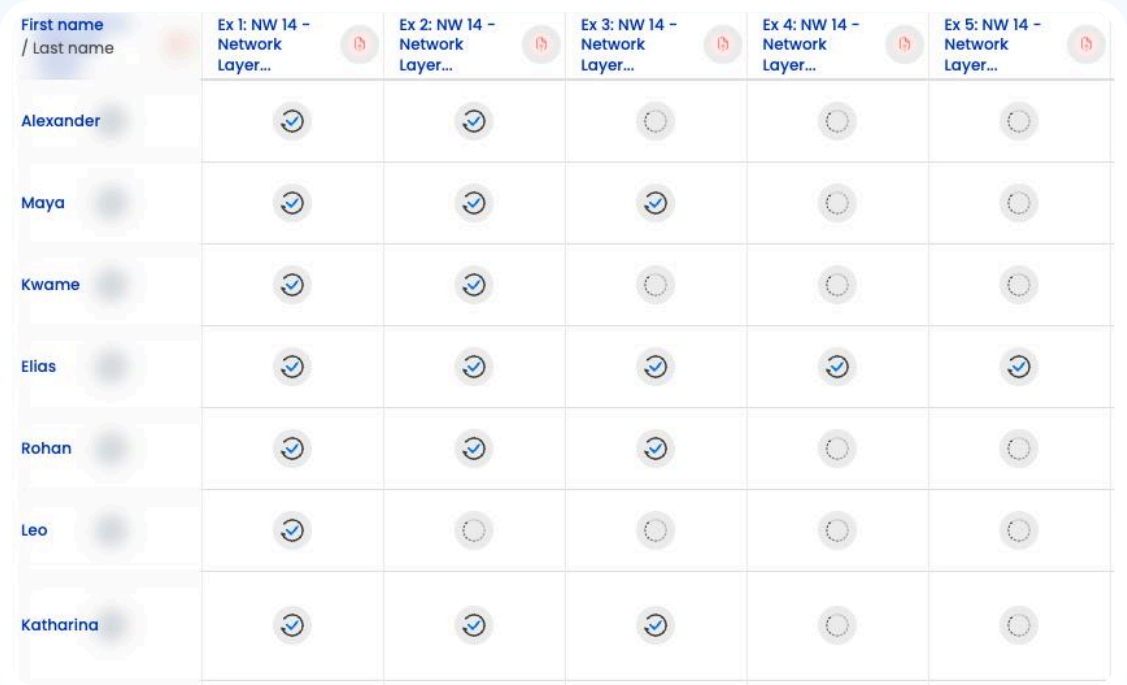


Three-Stage Learning Process

- **Before Class:** Review new material via videos and reading materials and complete exercises to prepare at your own pace for the instructor-led sessions and make the most out of them.
- **In Class:** Participate in small, engaging sessions led by industry experts featuring live demos, guided lab work, and in-depth Q&A discussions.
- **After Class:** Reinforce your skills with exercises, labs, and advanced challenges in a progressive difficultly level, so you are always challenged according to your current level.

Personalized Development Tracking

To help you reach your full potential, you will be consistently challenged at a level that matches your background and progress - never bored, and never too frustrated. We track your progress through exercises, projects, and mentorship sessions, to identify the best cybersecurity career path based on your strengths and goals. We provide detailed feedback, ensuring you stay on track to meet your career goals.



Program Structure And Timeline

09:00–10:00

Live class and demo

10:00–10:10

Short break

10:10–11:00

Live class and demo

11:00–13:00

Guided hands-on practice

13:00–14:00

Lunch Break

14:00–15:00

Review Session

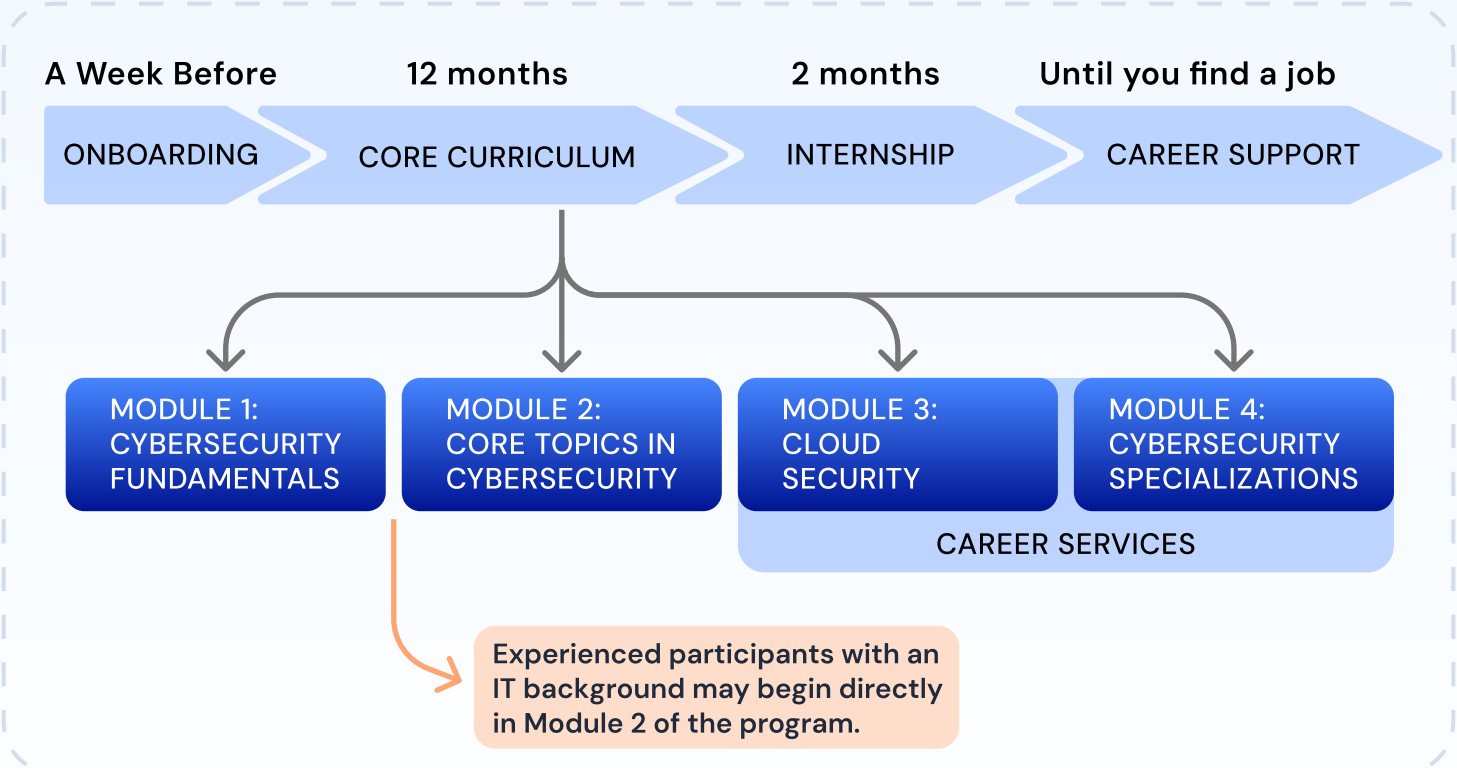
15:00–17:00

Guided hands-on practice

17:00–18:00

Pre-class for the next day

Program Timeline



Hands-on Skills

Our curriculum blends theory and hands-on experience with in-demand tools, equipping you with the skills and certifications to excel in today's cybersecurity job market. In addition to our core cybersecurity material, we place a strong emphasis on learning today's most powerful tool - AI.

Programming & Scripting

- Python
- PowerShell
- Bash

AI & LLMs

- Copilot
- Hugging Face
- LangChain
- ChatGPT

Virtualization

- VMware
- Docker
- Kubernetes

Operating Systems

- Windows
- Linux
- macOS

Networking

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

Data Analytics

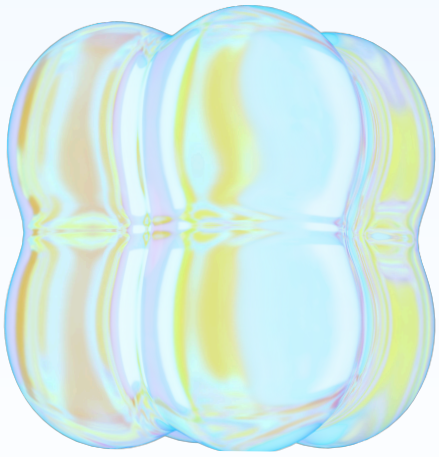
- SQL
- PostgreSQL

IT Administration & Cloud

- Microsoft 365
- Active Directory
- Azure Cloud
- Sysinternals

Cybersecurity Tools

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



AI skills

- **Intro to AI:** What AI is, key concepts, where it shows up in real jobs, and common usecases.
- **AI Tools Overview:** Hands-on work with top tools for deep technical research, business writing, coding, and data analysis.
- **Prompt Engineering:** Simple patterns for reliable results when prompting using clear instructions, constraints, verification, and iteration.
- **AI Agents:** Automating multi-step tasks with tools, memory, and guardrails to boost productivity.

Module 1: Cybersecurity Fundamentals

Starting from zero, we build strong foundations in coding, computer networks, and operating systems. In this first module, you'll work with basic security tools and develop effective learning habits that will support you throughout the course. You'll also begin cultivating the mindset of an independent and skilled cybersecurity professional. By the end of this module, you'll earn the CompTIA Tech+ certification.

Key concepts and technologies

Introduction to Computers
Understand how hardware and software work, and use the terminal to perform advanced actions.

Python for Cybersecurity Analysts
Master Python scripting to automate tasks and enhance cybersecurity operations.

Networking Basics
Explore the OSI and TCP/IP models, understand IP addressing, subnets, and routing, and use tools like Wireshark to analyze network traffic.

Operating Systems
Work with Windows and Linux, develop CLI skills, explore file systems and processes, and learn to configure and secure operating systems.

AI Tools
Explore core AI concepts and learn how tools like ChatGPT and GitHub Copilot can be leveraged for cybersecurity.

Data Analytics Fundamentals
Learn to work with data using SQL, manage database storage, and perform basic data analysis.

Web Fundamentals
Understand how websites work with HTML, CSS, and JavaScript, explore client-server communication (HTTP/HTTPS), and deploy basic web applications.

Core Certification

CompTIA Tech+

An entry-level certification that validates foundational IT and cybersecurity knowledge.

Optional

CompTIA Network+

Skills:

- **Applications and Software**
- **Infrastructure**
- **IT Concepts and Terminology**
- **Security**
- **Database Fundamentals**
- **Software Development Concepts**

Module 2: Core Topics in Cybersecurity

In Module 2, we dive deeper into core cybersecurity practices and the reasoning behind them. You'll gain a comprehensive understanding of the industry landscape, helping you map out your own professional path in cybersecurity. By the end of this module, you'll be prepared to earn the CompTIA Security+ certification.

Key concepts and technologies

Security Fundamentals
Learn key security controls, the CIA triad (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Accounting), and critical concepts like Zero Trust, change management, and physical security.

Cryptography
Understand symmetric & asymmetric encryption, apply hashing, obfuscation, and digital signatures, and explore blockchain fundamentals through hands-on exercises.

Threats & Vulnerabilities
Identify threat actors and attack methods, analyze network, system, and application vulnerabilities, and develop mitigation strategies for malware, social engineering, and supply chain attacks.

Security Architecture
Design secure networks and systems, focusing on application, OS, mobile device, and communication security (email & web).

Governance, Risk & Compliance (GRC)
Study compliance frameworks, risk management, and third-party risk assessments, and understand the role of audits and assessments in security.

Cybersecurity Roles
Explore key roles like incident responder, penetration tester, SOC analyst, and security engineer, gaining insight into their responsibilities and required skills.

Core Certification

CompTIA Security+

A leading certification for junior cybersecurity professionals. It validates core cybersecurity skills, industry-standard security tools, and cybersecurity best practices.

Skills:

- **General Security Concepts**
- **Threats, Vulnerabilities & Mitigations**
- **Security Architecture**
- **Security Operations**
- **Security Program Management & Oversight**

Module 3: Cloud Security

In this module, we scale up to enterprise-level cybersecurity, focusing on securing large-scale Cloud and on-premise IT environments. You'll gain hands-on experience with essential tools used to protect organizations from cyber threats, including Azure Cloud Administration, Microsoft 365, and Windows Active Directory.

Key concepts and technologies

Azure Cloud Administration
Configure and manage Azure cloud resources (VMs, storage, networks), implement RBAC & conditional access, and secure cloud environments through labs and weekly projects.

Cloud Security
Secure Azure environments by applying least-privilege access, hardening VMs and networks with NSGs and firewalls, enabling logging and monitoring, and using Microsoft Sentinel to detect and investigate threats through hands-on labs and attack/defense projects.

Microsoft 365 Management & Active Directory (Entra)
Manage users, groups, and GPOs, secure Windows environments, and analyze event logs for system security. Gain hands-on experience in server setup and security through daily exercises and projects.

Career Training
Optimize your CV and LinkedIn profile to showcase your cybersecurity skills and experience. Work with your mentor to define your ideal career path, identify high-demand roles, and develop the skills needed to stand out in the job market.

Core Certification

Microsoft Azure Fundamentals (AZ-900)

Foundational knowledge of cloud computing, Azure services, and cloud security principles.

Optional

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

Microsoft Azure AI Fundamentals (AI-900)

Microsoft Azure Administrator (AZ-104)

Skills:

- General cloud concepts
- Azure architecture and services
- Azure management and governance

Module 4: Cybersecurity Specializations

In this final module, you'll refine your cybersecurity skills for roles such as SOC Analyst, IT Security Consultant, IT Security Admin, and Compliance & Risk Specialist. You'll gain hands-on experience with SIEM, compliance, and advanced security tools, coupled with personalized career mentoring, and interview coaching to confidently enter the job market.

Key concepts and technologies

SOC, Incident Response & Penetration Testing
Work with SIEM platforms, analyze forensic artifacts, and master the incident response lifecycle. Develop log analysis, alert triage, and threat mitigation skills, and engage in purple-team exercises to apply penetration testing and red-team tactics.

Cloud & Advanced IT Security
Build a home lab to practice cloud and on-premises security. Identify and remediate security flaws, explore advanced attack techniques, and develop defensive strategies against evolving threats.

Compliance & Risk Management
Help companies achieve compliance with key regulations like ISO/IEC 27001 and GDPR. Conduct risk assessments, security audits, and compliance reporting, integrating incident management with regulatory standards.

Specialized Career Training
Enhance your job search, LinkedIn networking, and interview skills with structured methods like STAR. Prepare for both technical and behavioral cybersecurity interviews through expert-led HR coaching and mock interviews, ensuring you're ready to impress employers.

Core Certification

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:

- SMS Principles & Framework
- ISO/IEC 27001 Compliance
- ISMS Implementation
- Audit Preparation

Beyond The Classroom: Projects And Interactive Learning

Project-Based Learning
Apply technical concepts in real-world individual and collaborative projects to build a strong professional portfolio.

Capstone Projects
Complete comprehensive, multi-day projects that simulate real cybersecurity challenges, showcasing your expertise, teamwork, and problem-solving skills to employers.

Example projects

- **Python:** Log analysis using InsightLog
- **Networking:** Extracting files from Windows VM
- **Windows & Python:** Build a process-monitoring antivirus
- **AI:** deploy cloud LLM application and protect it from malicious actors
- **Capstone:** Multi-day Purple team Active Directory hacking & defending drill

Cyber Games
Engage in competitions, hackathons, and challenges that transform cybersecurity learning into an exciting and rewarding experience.

Student Presentations
Research, develop, and deliver presentations on cybersecurity topics to enhance your professional communication abilities.

Mentor Consultations
Schedule one-on-one sessions with your assigned mentor to review progress, address questions, and receive personalized career guidance.

CyberTalks
Gain insights from industry managers as they analyze actual cyber attacks, from historic cases like Stuxnet to todays most sophisticated cyber operations.

Industry Internship: Your Path to Real-World Cybersecurity Experience

Gain hands-on experience with an optional internship in one of these environments:

Student-Sourced: Find a role of your choice with our guidance

Partner Organizations: Work in a corporate setting with one of our industry partners

Non-profits: Apply your skills to meaningful projects

Cybersteps' Internal Internship: Solve real-world challenges under our expert mentorship

Internship Fields

- **Cybersecurity Analyst**
- **Security Operations Center (SOC) Analysis**
- **IT Security Administration**
- **Network Security Technician**
- **Cybersecurity Consultant**
- **GRC Analyst**

Professional Opportunities Following Program Completion

Cybersecurity Consultant

Assess security risks, conduct audits, and recommend defense strategies in a role that blends technical problem-solving with client interaction.

Typical salary range: €52,000–€78,000*

Cloud Security Engineer

Secure data and applications in cloud environments by designing secure architectures, implementing safeguards, and monitoring for vulnerabilities.

Typical salary range: €64,000–€117,000*

SOC Analyst

Be the frontline defender of an organization—monitor threats, analyze incidents, and coordinate responses to ensure 24/7 security.

Typical salary range: €51,000–€74,000*

IT Security Administrator

Manage security operations, including policies, firewalls, and user access, to protect networks and build a secure organizational IT environment.

Typical salary range: €69,000–€93,000*

**Source: Glassdoor*

Career Development Support

Cybersteps supports your job hunt during and after the program with expert career coaching designed by HR and cybersecurity interviewers, so you stand out and secure your first cybersecurity job.

Professional LinkedIn & Resume:
Create cybersecurity-focused LinkedIn profile and resume highlighting your technical capabilities and achievements. Learn to customize your CV for specific roles and strategically use LinkedIn to connect with recruiters and industry professionals.

Advanced Job Search Strategies:
Learn to leverage LinkedIn, specialized job boards, and professional networking to find the best cybersecurity opportunities. Use job search strategies to increase your visibility and stand out in a competitive field.

Industry Networking Opportunities:
Participate in our events to establish valuable industry connections, and leverage our professional network to build your own.

Technical & behavioral interview preparation:
Perfect your technical and behavioral cybersecurity interviews with expert-designed simulations. Receive personalized feedback to refine your responses, boost confidence, and effectively showcase your technical expertise to employers.

Business Communication Skills:
Enhance your email writing, technical reporting, and presentation skills, essential for success in cybersecurity and tech. Master industry best practices in workplace communication, giving you a competitive edge in both job applications and professional settings.

> Cybersecurity felt like the perfect career choice—it lets me turn my passion for gaming and technology into real-world problem-solving and a high-paying job. I highly recommend Cybersteps for anyone looking for a career in cybersecurity.

Avi Kozokin,
Cybersecurity researcher at IONIX

We're Here to Help

Contact Us to Learn More

https://cybersteps.de

info@cybersteps.de

+49 30 585823080

Cybersteps GmbH • Schloßstr. 50 in 12165 Berlin, Germany