

Cybersecurity Weiterbildung



12 months of live classes



2-month internship



Full-time



Flexible & remote

4.9 ★★★★★
Student reviews



“

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, Cybersteps' program doesn't just go over theory, it delivers real hands-on experience.

Marc Nöthen



“

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



“

The program is intensive and well-structured, perfect for building a career in cybersecurity. The instructors explain complex topics clearly and give practical examples, not just theory. The hands-on labs are very helpful to understand real-world scenarios, and the daily schedule keeps you disciplined and consistent.

Soroush Shariatmadari



Your Path to a Cybersecurity Career

Led by cybersecurity experts from elite military units and top cybersecurity firms, Cybersteps' industry-leading training is designed to make you job-ready. We've trained experts now defending the world's most critical systems. **Now it's your turn.**



Cybersecurity Focused

The highest quality of training, always-updated curriculum, and strong connections to the industry.



Advanced AI Tools and Skills

We place AI at the center of our curriculum and learning experience to help you learn effectively and stay ahead of the evolving job market.



Hands-On, Military-Tested Training

Our innovative learning platform gives you practical, real-world experience through simulations and interactive labs built by elite military instructors.



Designed for Germany's Job Market

Tailored to in-demand roles like SOC Analyst, Cyber Consultant, Cloud Engineer, GRC Analyst, and IT Admin.



1-on-1 Expert Mentorship

Our teachers, mentors, and career advisors will provide all the support and coaching you need to help you achieve your goals.



Industry Credentials

We will prepare you for leading industry-recognized certifications. Exam vouchers and full preparation are included.

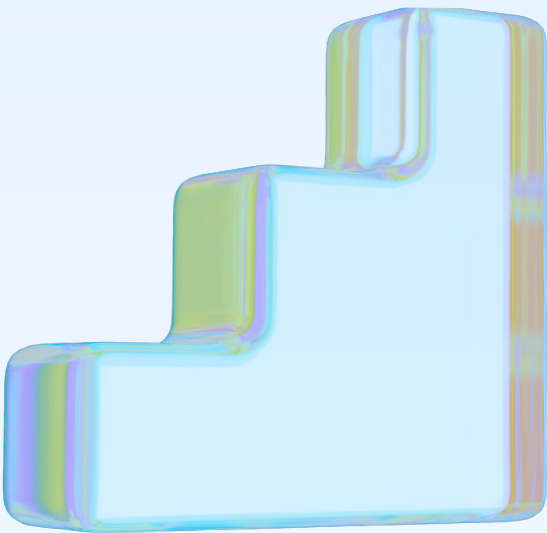
Hardware provided: powerful laptop

To support your success from day one, we'll provide you with a brand-new Lenovo ThinkPad laptop (or similar) to use throughout your training — and yours to keep once you graduate.



From Theory To Practice: How We Teach

At Cybersteps, we use the *Reverse Classroom* methodology, a proven approach adopted by leading universities and STEM programs, designed to enhance learning outcomes and help each student meet their full potential.



Three-Stage Learning Process

- **Before Class:** Review videos and reading materials and complete introductory exercises to prepare at your own pace before the instructor-led sessions so you can 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 with increasing difficulty, so you are always challenged according to your current skills and knowledge.

Personalized Development Tracking

To help you reach your full potential, you will always be challenged at a level that matches your background and progress – never bored, and never too frustrated.

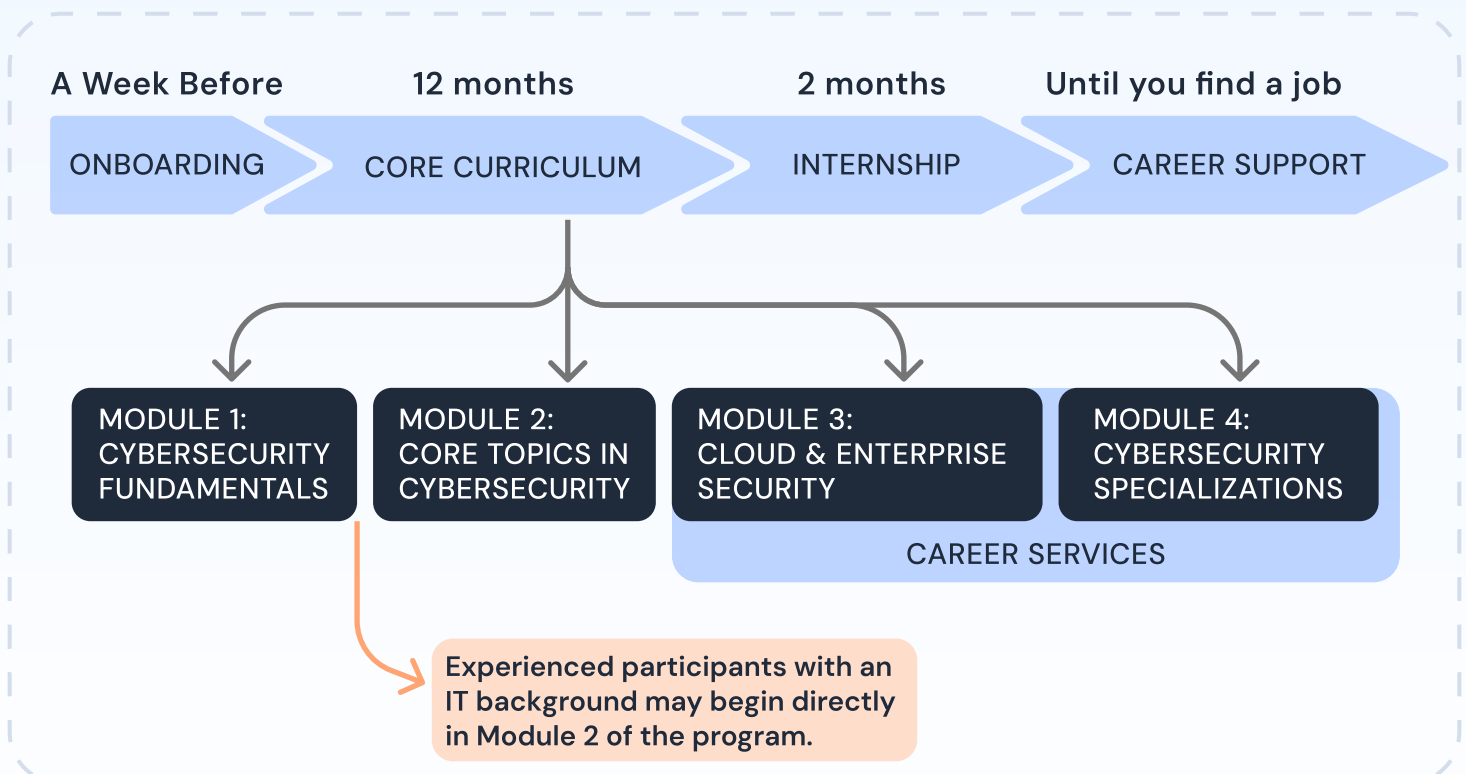
We track your progress through exercises, projects, and mentorship sessions, to identify the right cybersecurity career path for you based on your strengths and goals. We also provide detailed feedback throughout the program, ensuring you stay on track to meet your career goals.

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					

Program Structure And Timeline

09:00–10:00	13:00–14:00
Live class and demo	Lunch Break
10:00–10:10	14:00–15:00
Short break	Review Session
10:10–11:00	15:00–17:00
Live class and demo	Guided hands-on practice
11:00–13:00	17:00–18:00
Guided hands-on practice	Pre-class for the next day

Program Timeline



Hands-on Skills

During our exercises, simulations, and labs, you will gain hands-on skills with industry-leading tools, equipping you with the knowledge and practical experience to excel in today's cybersecurity job market.



Networking

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



Operating Systems

- Windows
- Linux
- Android



Scripting & Automation

- Python
- PowerShell
- Bash
- SQL
- Git



Cloud & IT Administration

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



Virtualization

- VMware
- Docker
- Kubernetes



AI & LLMs

- AI Assistants (ChatGPT, Claude, Gemini)
- AI Agents (Claude Code, Gemini CLI)
- Hugging Face
- LangChain



Cybersecurity Tools

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



Hands-On Projects

- Real attack simulations
- SIEM investigations
- Cloud security labs
- Build & defend your own systems



splunk>



vmware



AI For Cybersecurity

In addition to our core curriculum, we place a strong emphasis on learning how to use AI tools in cybersecurity. Throughout the program, you will be using AI for tasks like coding and data analytics, but also for writing reports, and conducting research. You will also learn how AI systems can be hacked – or secured – and how AI is being used in Cybersecurity for both defenders and attackers.

AI Tools in Practice

Hands-on use of leading tools for research, writing, coding, and data analysis.

Prompting & Workflows

Simple patterns to get reliable results using clear instructions, constraints, and iteration.

AI Agents & Skills

Automation of multi-step tasks using tools, memory, and structured workflows.

AI Security

Risks like prompt injection and data leakage, and how to use AI safely in real environments.

AI for Defensive Cybersecurity

AI-assisted threat analysis, investigations, automation, and defensive workflows.

AI for Offensive Cybersecurity

Using AI for reconnaissance, vulnerability discovery, and red-team workflows within penetration testing.

 **Claude** **Gemini****ChatGPT**

Expert Support. Real-World Practice.

An academic team of experts, always there to support you

Be part of a small cohort with personal attention and an open, welcoming community.

Instructors: Experienced cybersecurity professionals who will lead your live daily sessions, demos, and workshops.

Teaching Assistants: Enthusiastic junior cybersecurity professionals who will support you around the clock, every time you run into problems or have a question.

Career Advisors: HR specialists who help you prepare strong applications, improve your interview skills, and navigate your job search.

Guest Industry Experts: Senior managers from leading companies sharing unique perspectives.

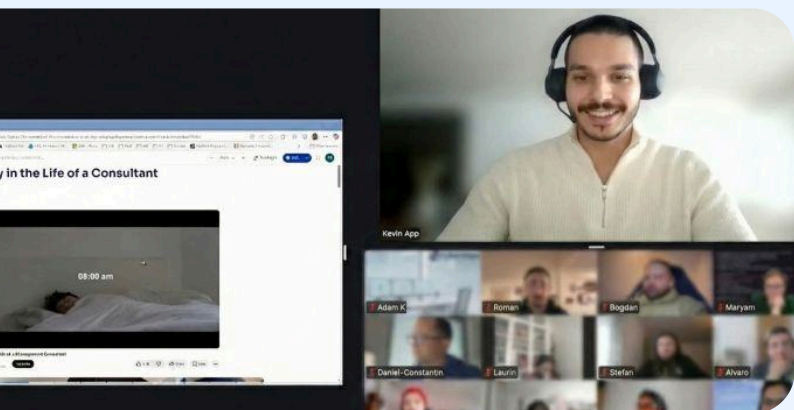


Practical curriculum built around hands-on projects

Apply what you learn through real-world projects, group challenges, and capstones that simulate cybersecurity work.

Example Projects

- **Bait n' Switch:** Deploy a public honeypot and analyze real attack attempts.
- **Chat with Entra:** Develop an AI cloud security auditor that connects to real-time data.
- **Secure Learningsteps :** Deploy a cloud application and protect it from malicious actors.
- **Game of Active Directory:** Multi-day purple-team drill: attack and defend an Active Directory environment.



Module 1: Cybersecurity Fundamentals

Starting from zero, we build strong foundations in computer systems, networking, and applications. You'll learn how operating systems work, how systems communicate, and how modern applications and data are structured.

You'll also work with basic security tools and develop learning habits for the rest of the program.



Key Topics

Computer Fundamentals

Understand how computers work, including hardware, software, and core system concepts.

Operating Systems

Work with Windows and Linux, develop CLI skills, manage files and processes, and understand system security basics.

Networking

Learn how systems communicate using TCP/IP, IP addressing, and routing, and analyze traffic using tools like Wireshark.

Web Applications

Understand how web applications work (HTTP/HTTPS, APIs), how data is stored and queried using databases, and build basic applications.

AI Essentials

Use AI tools effectively, understand their capabilities and limits, and apply them to real cybersecurity tasks.

Cryptography

Learn how encryption, hashing, and key management protect data and systems.

Core Certification

CompTIA Tech+



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

Optional

CompTIA Network+



Highlights

- Run your first real commands in the terminal
- Build your own website using AI
- Explore how AI systems can be attacked
- Launch your first network attack

Module 2: Core Topics in Cybersecurity

In the second module, you will move into real-world cybersecurity using a purple team approach. You'll learn how attacks happen and how to detect and respond to them, while exploring different roles to shape your path, such as SOC analyst, penetration tester, security engineer, and GRC analyst.

By the end of this module, you'll be prepared for the CompTIA Security+ certification.



Key Topics

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.

Initial Access & Social Engineering

Learn how attackers gain entry through reconnaissance and phishing, and how to detect and prevent these attacks.

Web Hacking

Identify and exploit common web vulnerabilities, and understand how to secure applications against them.

Vulnerabilities & Exploitation

Analyze and exploit systems across Windows, Linux, and Active Directory, and apply hardening and mitigation techniques.

Security Monitoring & Forensics

Detect attacks using SIEM tools, analyze logs, and investigate incidents to understand what happened and how to respond.

Governance, Risk & Compliance (GRC)

Understand frameworks, risk management, and how organizations design controls to prevent and reduce real-world risks.

Core Certification

CompTIA Security+



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

Highlights

- Hack websites and understand how attacks work
- Exploit vulnerabilities across systems and applications
- Investigate real security incidents and analyze what happened
- Complete a capstone purple team project: attack and defend an Active Directory environment

Module 3: Cloud & Enterprise Security

In this module, you move into enterprise cloud security, focusing on how modern organizations build and protect cloud environments. You'll work hands-on with core cloud systems, automate infrastructure, monitor real activity, and manage identity and access at scale.

By the end of this module, you'll prepare to certify for the Microsoft Azure Fundamentals (AZ-900) and an additional optional Microsoft Azure certification – AZ-104 or SC-200.

Key Topics

Cloud Foundations

Work with core cloud building blocks: virtual machines, networking, storage, and identity basics. Understand how cloud environments are structured and operated

DevSecOps & Infrastructure as Code

Deploy and secure workloads using automation and Infrastructure as Code (Terraform). Work with containers and orchestration, and integrate security into build and deployment pipelines.

Cloud Monitoring & Detection

Enable logging across cloud resources and use tools like Microsoft Sentinel to detect threats, analyze alerts, and investigate incidents in real-world scenarios.

Cloud Identity & Access (Entra ID)

Manage identities and access using RBAC, Conditional Access, and Privileged Identity Management (PIM). Understand authentication flows (OAuth) and how identity becomes the main security boundary.

Microsoft 365 & Enterprise Security

Secure enterprise environments by managing users, devices, & policies. Analyze activity and logs across cloud and hybrid environments to detect and prevent threats.

Career Training

Optimize your CV and LinkedIn profile to showcase your 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)



Foundations of Azure cloud computing and cloud security.

Choose One

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



OR

Azure Administrator Associate (AZ-104)



OR

Azure Security Operations Analyst Associate (SC-200)



Highlights

- Get your own Azure subscription to practice
- Deploy and secure a production-level application
- Run a public honeypot and analyze real attacks

Module 4: Cybersecurity Specializations

In this final module, you'll earn a highly valued IHK (or PECB, if you prefer) certification and choose your cybersecurity specialization with guidance from your mentor.

Specializing helps you build deeper expertise and strengthens your profile for employers. You'll gain hands-on experience with the tools and frameworks most relevant to your specialization, along with an additional specialized certification, personalized career mentoring, and interview coaching to help you enter the job market with confidence.



Key Topics

Realistic Company Environment: Attack & Defence

Work with a realistic corporate environment that mirrors modern organizations. Explore attack vectors, investigate attacker behaviour, analyse weaknesses, and improve defences.

Advanced Governance, Risk & Compliance

Go deeper into cybersecurity governance, risk management, and compliance. Work with frameworks and regulations such as ISO/IEC 27001 and NIS2 through audits, risk assessments, evidence collection, and compliance reporting.

AI Security & AI for Cybersecurity

Learn how AI is changing cybersecurity from both attacker and defender perspectives. Explore attacks on AI systems, defensive approaches, AI-powered security workflows, and apply your knowledge in a final hands-on project.

Specialized Career Training

Strengthen your application strategy and interview skills for cybersecurity roles. Practice presenting your experience, projects, and certifications through mock interviews, role-specific simulations, and expert-led career coaching.

Highlights

- Official IHK Certification: Cyber Security Advisor
- Practical AI: Get a Claude Pro (or Equivalent) Subscription and Learn How to Truly Master AI
- Compliance With The ISO/IEC 27001 Standard
- ISMS Implementation
- Audit and Report Preparation

Core Certification

IHK Cyber
Security Advisor



The official IHK Cyber Security certification: identify, mitigate, and respond to cyber threats.

OR

PECB ISO/IEC 27001
Lead Implementer



Implement and manage ISO/IEC 27001 compliance across an organization.

OR

ISO/IEC 27001
Foundation



Understand the fundamentals of ISO/IEC 27001 compliance and information security.

Specialize

One additional certification – see next page for details.

Module 4: Cybersecurity Specializations

Based on the specialization path you choose, you'll focus on the tools, frameworks, and skills that matter most for that specific role and gain in-depth knowledge in that area.

You can choose from six in-demand areas, with each path built around a real career outcome and pairing hands-on experience with one additional specialized certification from a leading provider.



Security Operations (SOC)

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



CompTIA
CySa+

OR



Hack The
Box CDSA



Penetration Testing (Ethical Hacking)

Think like an attacker to find weaknesses before criminals do, simulating real-world attacks and helping organizations close the gaps you uncover.



CompTIA
PenTest+

OR



Hack The
Box CPTS



Security Engineering

Secure cloud environments by designing secure architectures, managing access, implementing safeguards, and reducing security risks.



Cloud and AI Security
Engineer Associate (SC-500)



Governance, Risk & Compliance (GRC)

Shape the rules that keep organizations safe, translating regulations and risk into clear policies that align security with business goals.



BSI IT-Grundschutz
Practitioner



Cybersecurity Project Management

Drive cybersecurity initiatives from start to finish, coordinating teams, budgets, and deadlines to deliver complex security projects successfully.



CompTIA Project+



Application Security

Secure software from the inside out, spotting vulnerabilities in code and helping development teams build applications that are safe by design.



HTB Certified Offensive AI
Expert (COAE)

8-Week Industry Internship: Real-World Cybersecurity Experience

Hands-on work experience in a real company

Through our network of partnerships, we have access to over 400 companies in Germany and Europe. We'll match you with employers from our partner network for interviews to find the right position for you. Internship placement is guaranteed for students who meet basic performance requirements – and we work hard to get every motivated student there, with the vast majority successfully placed.

8 Weeks, Full-Time

Duration can be adjusted on request

Online or On-site

Depending on availability

Flexible Start Date

Start right after graduation, or anytime within 6 months

Optional Full-Time Employment

Many employers offer a permanent role based on performance



Internship Fields Include

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



Careersteps: Career Accelerator

Through Careersteps, we support your job hunt during and after the program, with expert coaching from HR professionals and cybersecurity interviewers, helping you stand out and secure your first cybersecurity role. We accelerate this journey through tailored 1:1 mentorship, collaborative group workshops, and the most up-to-date learning resources.



Professional LinkedIn & Resume

Create cybersecurity-focused LinkedIn profile and resume highlighting your technical capabilities and achievements. We will help you customize your CV for specific roles and how to strategically use LinkedIn to attract attention from recruiters and other industry professionals.



Advanced Job Search Strategies

Learn to leverage LinkedIn, specialized job boards, and professional networks to find cybersecurity opportunities effectively. Use advanced job search strategies to expand your options while focusing on the most relevant job opportunities.



Industry Networking Opportunities

Participate in our events and partner 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 and mock interviews. 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.



Success is giving our students the right tools to take ownership of their career story. Watching them gain new knowledge, build confidence, and proactively drive their own path forward is incredibly rewarding.

Charlotte Jäger,
Career Advisor for Cybersecurity Talent



“

It's a great program – I am learning so much and it's been such a great experience. Roman makes the lessons easy to follow and actually fun, even when the topics get complicated and tricky.

Stanislav Safaniuk



“

My experience has been very positive. I come from a non-technical background, but the instructors are very beginner-friendly. They are highly knowledgeable, experienced, and professional, and make complex topics easy to understand. The learning environment is supportive and motivating, which has helped me gain confidence. I would recommend this program to anyone looking to change careers.

Fazluddin Bawar



“

A year ago, I decided to transition into cyber security and chose Cybersteps. Looking back, I am convinced it was the right decision. What truly set the experience apart was the continuous support. From dedicated career services, 1:1 coaching, CV and LinkedIn optimization, to consistent mentorship and guidance throughout the program, the Cybersteps team was always there to ensure I stay on track and feel prepared for the industry.

Akar Sarpal





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  XIONIX

Reach Out To Us

Learn More About Our Program

<https://cybersteps.de>

info@cybersteps.de

+49 30 585823080

