COMPUSAFE
Agile Solutions

Cyber Security Engineer

Ihr individuelles Talentprogramm

*Wir bieten eine praxisnahe, marktbezogene Ausbildung zum Cyber Security-Engineer - **modular und rollenorientiert** aufgebaut. Speziell auf Ihren Unternehmensbedarf entwickelt: Ein einzigartiges Trainingskonzept statt Standardlösung.*

Workforce Transformation als strategischer Hebel für Cyber-Exzellenz

Kompetenzen stärken und zukünftige Spezialisten aufbauen

Praxisnahe, marktbezogene Ausbildung zum Cyber Security-Engineer

Messbare Sicherheit durch strategische Kompetenzentwicklung

Ihr strategischer Mehrwert

- ✓ Potenziale Ihrer Belegschaft gezielt entwickeln
- ✓ Neue Sicherheitskompetenzen systematisch aufbauen
- ✓ Aufbau von Cyber Security Nachwuchstalenten
- ✓ Digitale Souveränität
- ✓ Beschleunigung der Transformation
- ✓ Gezielte Kompetenzentwicklung

Ein Unternehmen der audius

Worum es geht

Workforce Transformation als strategischer Hebel für Cyber-Exzellenz

Projekte und Infrastrukturen sind heute mehr denn je durch komplexe Bedrohungsszenarien gefährdet. Doch Sicherheit entsteht nicht allein durch Technologie, sondern durch die Menschen, die sie bedienen. **Workforce Transformation** ist unser ganzheitlicher, menschenzentrierter Ansatz, der Organisation, Technologie und Kultur verbindet.
Wir entwickeln eine flexible, sicherheitsbewusste und handlungsfähige IT-Belegschaft, die (pro)aktiv auf aktuelle Geschäftsanforderungen und wachsende Cyber-Bedrohungen reagieren kann.

Wir bieten keine Standard-Schulungen, sondern **strategische Kompetenzentwicklung zum Cyber Security-Engineer**.

Kernpunkte unseres Ansatzes

Potenziale aktivieren statt nur Personal suchen

Workforce Transformation
Ganzheitlicher, menschenzentrierter Ansatz, der Organisation, Technologie und Kultur verbindet

Reskilling
Strategischer Rollenwechsel von klassischen IT- oder administrativen Aufgaben in spezialisierte Cyber Security-Funktionen

Upskilling
Vertiefung bestehender IT-Skills in den Bereichen Sicherheitsmanagement, Monitoring und Incident-Response. Abgestimmt auf aktuelle Standards wie NIS2

Modularer Aufbau
Rollenorientiertes Programm, individuell auf Ihren spezifischen Kundenbedarf und sicherheitskritische Einsatzszenarien abgestimmt

Praxisnahe Ausbildung
Marktbezogene Ausbildung zum Cyber Security-Engineer mit direkter Anwendungsorientierung im operativen Betrieb

Strategische Kompetenzentwicklung
Keine Standard-Schulungen, sondern gezielte Entwicklung relevanter Sicherheitskompetenzen entlang Ihrer Cyber-Sicherheitsstrategie

Der Weg zum Cyber Security-Engineer

Modular. Praxisnah. Zertifiziert.

Modul 1:
Foundation & Digital Awareness 2026

- **Cyber-Awareness 2.0:** Fokus auf Identitätsschutz und Erkennung von KI-gestützten Angriffen (Deepfakes, Social Engineering).
- Grundlagen der CIA-Triade und Einführung in moderne Angriffsvektoren.
- Netzwerkgrundlagen als Basis für sichere Infrastrukturen.

Modul 2:
Secure Infrastructure & Zero Trust

- **Hardening in der Praxis:** Absicherung von Windows/Linux-Systemen und hybriden Cloud-Umgebungen.
- Implementierung von **Zero Trust Frameworks** – Vertrauen wird kontinuierlich geprüft, nie vorausgesetzt.
- Betriebliche Praxisphase zur Etablierung einer Routine im Umgang mit Schwachstellen.

Modul 3:
Advanced Defense & Compliance-Management

- **NIS2-Expertise:** Praktische Umsetzung regulatorischer Anforderungen und Meldeprozesse gemäß dem NIS2-Umsetzungsgesetz.
- Incident-Response und **digitale Forensik:** Schnelles Handeln bei Sicherheitsvorfällen zur Minimierung von Ausfallzeiten.
- **Aufbau von Resilienz:** Notfallpläne und Wiederherstellungsstrategien für geschäftskritische Prozesse.

Modul 4: AI-Security & Professional Certification

- **AI-Powered Defense:** Einsatz von KI-Tools für automatisiertes Threat-Hunting und Anomalie-Erkennung.
- Security-Automatisierung durch Scripting und SIEM-basierte Analysen.
- **Abschluss:** Vorbereitung auf anerkannte Zertifikate (z. B. CompTIA Security+, CySA+), um die Marktrelevanz Ihrer Experten zu sichern.

Erkennen Sie sich hier wieder?

- Sicherheitskritisches Umfeld mit Defence-Bezug oder hohem Schutzbedarf
- Defence-nahe Industrie, Streitkräfte oder wehrtechnische Projekte
- Führungs- oder Schlüsselrolle in IT, OT oder sicherheitsrelevanten Prozessen
- Hoher Zeitdruck, komplexe Compliance-Anforderungen (z.B. NIS2, KRITIS) und wachsende Cyber-Bedrohungen

Lassen Sie uns in Kontakt treten, das Workforce Transformation-Team berät Sie gerne!

„Mit Workforce Transformation entwickeln wir für Sie handlungsfähige Cyber Security-Engineers, die (pro)aktiv auf aktuelle Anforderungen und wachsende Cyber-Bedrohungen reagieren können."

Anke Schnitzer
Head of Workforce Transformation
+49 170 28 64 481
Anke.Schnitzer@compusafe.de

CompuSafe Data Systems AG
Oetztaler Straße 18
D-81373 München
www.compusafe.de