WEITERBILDUNG | BILDUNGSINSTITUT GROS

Cyber Security Analyst

IT-Sicherheit & Netzwerkabwehr | Maßnahmenbeschreibung

AZAV-ZERTIFIZIERT

Maßnahme-Art	Dauer	Unterrichtsform	Einstieg	Abschluss	Förderung
Weiterbildung	**Flexibel**	**Präsenz & Online**	**Laufend möglich**	**Trägerzertifikat**	**100 % möglich**

1. Beschreibung der Maßnahme

Die Weiterbildung zum **Cyber Security Analyst** qualifiziert Teilnehmende zu gefragten Sicherheitsexpertinnen und -experten, die kritische IT-Infrastrukturen vor Cyberangriffen schützen. Die Maßnahme vermittelt praxisnahes Fachwissen zu Bedrohungsanalyse, Netzwerkabwehr, Ethical Hacking sowie Security Operations – und bereitet auf den sofortigen Einsatz im Security Operations Center (SOC) oder als IT-Sicherheitsbeauftragter vor. Der Unterricht erfolgt im hybriden Lernmodell mit virtuellen Cyber-Ranges sowie Live-Unterricht via Microsoft Teams oder in Präsenz.

2. Kursinhalte und Fachmodule

Modul 1 – Bedrohungsanalyse

- **Schwachstellen-Scans:** Systeme auf Sicherheitslücken prüfen (Vulnerability Scanning mit einschlägigen Tools)
- **Malware-Analyse:** Schadsoftware (Ransomware, Trojaner) sicher erkennen, isolieren und neutralisieren
- **Social Engineering:** Phishing-Attacken und psychologische Manipulationsmethoden erkennen und abwehren

Modul 2 – Netzwerksicherheit

- **Firewalls & VPNs:** Sichere Konfiguration von Netzwerkgrenzen, Zugriffskontrollen und verschlüsselten Tunneln
- **Intrusion Detection:** Implementierung und Betrieb von IDS/IPS-Systemen zur automatisierten Angriffserkennung
- **Traffic-Analyse:** Auswertung und Interpretation von Netzwerkpaketen (z. B. mit Wireshark)

Modul 3 – Ethical Hacking (Red Teaming)

- **Penetration Testing:** Kontrollierte, autorisierte Hackerangriffe auf die eigene Infrastruktur methodisch durchführen
- **Exploiting:** Gefundene Sicherheitslücken demonstrieren, dokumentieren und gezielt schließen

Modul 4 – Security Operations (Blue Teaming)

- **Incident Response:** Strukturiertes, dokumentiertes Vorgehen bei einem erfolgreichen Cyberangriff
- **SIEM-Systeme:** Security Information and Event Management Tools konfigurieren, überwachen und auswerten

Modul 5 – Security Compliance & Recht (BIG Plus)

- Grundlagen der ISO 27001 Zertifizierung und Informationssicherheits-Managementsysteme (ISMS)
- BSI-Grundschutz – Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik

- DSGVO und Datenschutz im IT-Security-Umfeld
- NIS-2-Richtlinie der Europäischen Union und ihre Anforderungen an Unternehmen

3. Lernziele und Abschluss

Nach erfolgreichem Abschluss sind Teilnehmende unmittelbar einsatzbereit im Security Operations Center (SOC) oder als interne IT-Sicherheitsbeauftragte.

- **Trägerzertifikat:** Anerkanntes, detailliertes Abschlusszertifikat des Bildungsinstitut Gros als Nachweis für Arbeitgeber
- **Angewandte Praxis:** Cyberangriffe in Echtzeit erkennen, isolieren und professionell abwehren
- **Prävention & Hardening:** IT-Architekturen so absichern, dass Angreifer von vornherein scheitern
- **Compliance-Kompetenz:** Unternehmen zu ISO 27001, BSI-Grundschutz und NIS-2 fachkundig beraten

4. Zielgruppe

Diese hochspezialisierte Weiterbildung richtet sich an Personen mit solider IT-Grundlage, die gezielt in den Bereich der Cybersicherheit aufsteigen möchten:

- IT-Administratoren, die Netzwerke und Server verwalten und sich auf IT-Sicherheit spezialisieren möchten
- Fachinformatiker/-innen (FISI / FIAE) als exzellente Zusatzqualifikation für Expertenpositionen
- IT-Consultants, die Unternehmen zu Hacking-Prävention und Compliance (ISO 27001) beraten
- Ambitionierte Autodidakten mit fundierten Linux- und Netzwerkkenntnissen, die sich professionalisieren
- IT-Fachkräfte aus verwandten Bereichen mit analytischem Denkvermögen und hohem Verantwortungsbewusstsein

5. Zugangsvoraussetzungen

- Solide IT-Grundkenntnisse in Netzwerktechnik und Betriebssystemen (Windows & Linux)
- Ausgeprägtes logisches und analytisches Denkvermögen
- Gute Englischkenntnisse (Fachvokabular, Tools und Dokumentationen sind überwiegend englischsprachig)
- Hohes Verantwortungsbewusstsein und Integrität im Umgang mit sensiblen Daten und Sicherheitswissen
- Persönliches Eignungsgespräch beim Bildungsinstitut Gros (kostenfrei)

6. Unterrichtsform und Lehrmethoden

Virtuelle Cyber-Ranges	Live-Unterricht von Security-Experten	Vollzeit oder Berufsbegleitend
Training in abgeriegelten virtuellen Sandbox-Umgebungen: Exploits sicher testen, Angriffe simulieren und abwehren – ohne realen Schaden.	IT-Security-Experten aus der Wirtschaft führen live durch Red- und Blue-Teaming, Incident Response und Compliance-Themen.	Flexibel wählbar: Vollzeit oder berufsbegleitend – vor Ort oder 100 % online via Microsoft Teams.

7. Berufliche Perspektiven und Einsatzgebiete

Cyberangriffe und Ransomware nehmen jährlich exponentiell zu. Zertifizierte Security-Analysten genießen quasi eine Jobgarantie und erzielen absolute Spitzengehälter – branchenübergreifend und weltweit.

Typische Einsatzgebiete	Gehaltsaussichten
• Security Operations Center (SOC) und IT-Sicherheitsfirmen • Kritische Infrastrukturen (KRITIS): Energieversorger, Banken, Kliniken • Interne IT-Sicherheitsabteilungen im Mittelstand und bei Konzernen • IT-Forensik und staatliche Ermittlungsbehörden (z. B. BKA, LKA) • Aufstieg zum CISO (Chief Information Security Officer)	Einstiegsgehalt (Junior Analyst) **3.800 – 4.500 € / Monat** Mit Seniorität / als CISO **bis 8.000 € / Monat** Nachweisbare Fähigkeiten (Zertifikate, Bug-Bounties) treiben das Gehalt schnell in die Höhe.

8. Förderungsmöglichkeiten

Die Maßnahme ist AZAV-zertifiziert und kann zu **100 % über einen Bildungsgutschein (Agentur für Arbeit / Jobcenter)** oder andere Förderinstrumente finanziert werden.

Förderinstrument	Ansprechpartner	Leistung
Bildungsgutschein (BGS)	Agentur für Arbeit / Jobcenter	100 % Kurskosten + ggf. Lebensunterhalt
Qualifizierungschancengesetz	Agentur für Arbeit / Arbeitgeber	Weiterbildungsförderung für Beschäftigte
AVGS (Aktivierungs-Gutschein)	Agentur für Arbeit	Kurzmaßnahmen und Eignungsfeststellung
Anerkennungsberatung	IQ Netzwerk / Migrationsberatung	Anerkennung ausländischer IT-Abschlüsse

Höchste	**100 %**	**Trägerzertifikat**	**SOC-Ready**
Nachfrage am Markt	**Förderung möglich**	**Anerkannter Nachweis**	**Sofort einsatzbereit**

Bildungsinstitut Gros
Zukunft. Bildung. Karriere.
info@bildungsinstitut-gros.de

Telefon: 0170 2846888
Website: www.bildungsinstitut-gros.de
Unterricht: Microsoft Teams & Präsenz

Dieses Dokument dient als Maßnahmenbeschreibung zur Vorlage bei der Agentur für Arbeit oder dem Jobcenter.