IT-Sicherheitsanalyse

IT-Sicherheit / Cybersecurity · Anbieter: Distart Education GmbH

FÖRDERUNG & KOSTEN

Kurspreis: auf Anfrage

Förderfähig über: Bildungsgutschein, Zuschuss bei der Qualifizierung Beschäftigter, Qualifizierungsgeld zur Förderung der beruflichen Weiterbildung Beschäftigter, Arbeitslosengeld bei beruflicher Weiterbildung, KOMPASS - Förderung der beruflichen Weiterbildung von Solo-Selbstständigen

AZAV-zertifizierter Bildungsträger — Förderung durch die Agentur für Arbeit möglich

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Zeitgebunden
Dauer	9 Wochen in Vollzeit oder 18 Wochen in Teilzeit
Umfang	430 Unterrichtseinheiten
Unterrichtssprache	Deutsch
Kursstart	Startet jeden Tag
Vorkenntnisse	Keine Vorerfahrung
Inklusive	Notebook / Tablet (geliehen)

Bildungsträger & Kontakt

Distart Education GmbH
Petersstraße 35, 04109 Leipzig
Telefon: 0341 9288039
E-Mail: hallo@distart.de
Web: https://www.distart.de

Kurs online ansehen

01 Kursbeschreibung

Zielsetzung des Kurses

Der Kurs "IT-Sicherheitsanalyse" behandelt Methoden zur Identifikation, Bewertung und Dokumentation von Schwachstellen in IT-Systemen. Im Mittelpunkt stehen Verfahren der Risikoanalyse, der technischen Prüfung und der Auswertung sicherheitsrelevanter Daten. Eingebettet ist der Kurs in das Fachgebiet der Informationssicherheit mit Bezügen zu Netzwerken, Betriebssystemen und Compliance-Anforderungen. Ziel ist die strukturierte Herangehensweise an Sicherheitsanalysen entlang etablierter Standards und Prozesse.

Lernziele

Identifikation typischer Schwachstellen in Netzwerken, Betriebssystemen und Anwendungen

Durchführung von strukturierten Risikoanalysen inklusive Schutzbedarfs- und Bedrohungsmodellierung

Anwendung von Scan- und Monitoring-Werkzeugen zur Erhebung sicherheitsrelevanter Daten

Bewertung von Findings anhand definierter Kriterien und Scoring-Modelle

Erstellung nachvollziehbarer Sicherheitsberichte mit Maßnahmenableitung und Priorisierung

Integration der Analyseergebnisse in Prozesse von Incident- und Vulnerability-Management

Berufsperspektiven

Die Kursinhalte finden Anwendung in Berufsfeldern wie IT-Sicherheitsanalyst in Security Operations mit Fokus auf Monitoring, Log-Analyse und Incident-Einordnung. Typische Tätigkeitsfelder umfassen Vulnerability-Management und Schwachstellenmanagement in IT-Abteilungen oder Dienstleistungsumgebungen. Der Kurs adressiert Inhalte für Tätigkeiten wie Netzwerk- und Systemprüfung im Umfeld von Penetration Testing Light und Compliance-getriebener Sicherheitsüberprüfung. Weitere Einsatzbereiche sind Governance-, Risk- und Compliance-Aufgaben mit Bezug zu Reporting und Auditvorbereitung.

Zusammenfassung

Der Kurs "IT-Sicherheitsanalyse" behandelt Verfahren zur Schwachstellenidentifikation, Risikobewertung, technischen Analyse und zum Berichtswesen in der Informationssicherheit. Im Rahmen dieser Weiterbildung werden Methoden, Prozesse und Werkzeuge für strukturierte Sicherheitsprüfungen vermittelt. Die Themen finden Anwendung in Tätigkeitsfeldern wie Security Operations, Vulnerability-Management und GRC-orientierter Sicherheitsüberprüfung.

02 Lehrplan & Module

Gesamtumfang	**430 Unterrichtseinheiten* in 10 Modulen**

* Eine Unterrichtseinheit entspricht 45 Minuten.

1. Grundlagen der IT-Sicherheit und Bedrohungen

25 Unterrichtseinheiten
(ca. 6% vom Gesamtumfang)

Grundlagen IT Sicherheit für Penetrationtester
Recht und Ethik
Technische Grundlagen
Häufige Angriffstypen

2. Schwachstellen in Webanwendungen und Webseiten

100 Unterrichtseinheiten
(ca. 23% vom Gesamtumfang)

Einrichtung der Laborumgebung für Webanwendungen
Reconnaissance (Informationsgewinnung)
Tools und Techniken zur Websicherheit
Scanning von Webanwendungen
OWASP Top 10: Schwachstellen in Webanwendungen

3. API Penetration Testing

30 Unterrichtseinheiten
(ca. 7% vom Gesamtumfang)

Einführung in APIs & Technische Vorbereitung
API Reconnaissance & Data Exposure
Angriffe auf API's

4. Sicherheitslücken in IT-Infrastruktur und Netzwerken

100 Unterrichtseinheiten
(ca. 23% vom Gesamtumfang)

Grundlagen von IT Netzwerken
Einführung in Netzwerkprotokolle, Ports & Erweiterung der Laborumgebung
Scanning und Enumeration von Netzwerken
Exploitation Grundlagen
Typische Schwachstellen in Netzwerken und Infrastruktur
Privilege Escalation für Linux
Privilege Escalation für Windows
Post-Exploitation

5. Active Directory Penetration Testing

35 Unterrichtseinheiten
(ca. 8% vom Gesamtumfang)

Einführung in Active Directory (AD) & Erweiterung der Laborumgebung
Angriffe auf Active Directory

6. E-Mail-Sicherheit und Phishing-Abwehr

20 Unterrichtseinheiten
(ca. 5% vom Gesamtumfang)

Social Engineering Grundlagen
Organisatorische Maßnahmen zur Abwehr von Social Engineering
Typische Schwachstellen in E-Mails

7. Organisatorische Sicherheitsmaßnahmen und präventive Maßnahmen

65 Unterrichtseinheiten
(ca. 15% vom Gesamtumfang)

Sicherheitsrichtlinien nach BSI Standards
IT Richtlinien in der Praxis
Passwort und Rechte-Managment
Firewalls und Antivirus-Software
Update- und Patch-Management
Sichere Nutzung von Netzwerken, mobilen Geräten & Richtlinien für sichere Kommunikation
Backupmanagement

8. Physical Penetration Testing

10 Unterrichtseinheiten
(ca. 2% vom Gesamtumfang)

Grundlagen des Physical Penetration Testing

9. Abschlussprojekt – Penetrationstest und Reporting

25 Unterrichtseinheiten
(ca. 6% vom Gesamtumfang)

Durchführung eines realen Penetrationstests
Erstellung eines detaillierten Penetrationstest-Berichts

10. Prüfungsvorbereitung & Abschlussprüfung

20 Unterrichtseinheiten
(ca. 5% vom Gesamtumfang)

Wiederholung und Prüfungsvorbereitung
Abschlussprüfung

03 Voraussetzungen

Vorkenntnisse

Niveau: Keine Vorerfahrung

Ein Hauptschulabschluss oder ein höherwertiger Abschluss sind wünschenswert, aber keinesfalls Pflicht.

Persönliche Eignung: Lern- und Leistungsbereitschaft sowie Kontaktbereitschaft,

Gesundheitliche Anforderungen: Nahsehvermögen sowie Sprech- und Hörvermögen,

Mindestalter 18 Jahre bei Vertragsabschluss,

Sprachkenntnisse in Deutsch: vergleichbar B2,

Grundkenntnisse in der Bedienung von Computern,

Begeisterung und vorhandene Affinität zum Themenbereich

Technische Voraussetzungen

Teilnehmende benötigen einen handelsüblichen PC oder Laptop mit Internetanschluss und einem unterstützten Browser (Edge, Firefox, Safari, Chrome). Für die Teilnahme im virtuellen Klassenzimmer wird zusätzlich ein Mikrofon oder eine Webcam mit Mikrofon benötigt. Ein mobiler PC wird bei Notwendigkeit bereitgestellt.

04 Zielgruppen & Berufsperspektiven

- Arbeitssuchende
- QuereinsteigerInnen
- WiedereinsteigerInnen
- RehabilitantInnen
- Fachkräfte
- AkademikerInnen
- Selbsständige
- BerufseinsteigerInnen
- Führungskräfte
- Berufstätige
- Ohne Berufsabschluss

Mögliche Berufsbilder: Penetration Tester, Security Operations Engineer, IT-Security Engineer

NÄCHSTER SCHRITT

Kursdetails online ansehen und Anbieter kontaktieren

Distart Education GmbH · Petersstraße 35, 04109 Leipzig
0341 9288039 · hallo@distart.de · https://www.distart.de

Online ansehen