CyberSec First Responder (CFR): Threat Detection & Response (CFR)

ID CFR **Preis** 3.290,– € (exkl. MwSt.) **Dauer** 5 Tage

Inklusive Examensvoucher!

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Dieser Kurs deckt Methoden, Taktiken und Verfahren zur Netzwerkverteidigung und Reaktion auf Vorfälle ab, die mit den Rahmenwerken der Branche wie NIST 800-61r2 (Computer Security Incident Handling Guide), dem National Cyber Incident Response Plan (NCIRP) des US-CERT und der Presidential Policy Directive (PPD)-41 on Cyber Incident Coordination, NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) übereinstimmen. Er ist ideal für Kandidaten, die mit der Überwachung und Erkennung von Sicherheitsvorfällen in Informationssystemen und Netzwerken sowie mit der Durchführung von standardisierten Reaktionen auf solche Vorfälle betraut sind. Der Kurs stellt Werkzeuge, Taktiken und Verfahren vor, um Cybersicherheitsrisiken zu verwalten, Cybersicherheitsressourcen zu verteidigen, verschiedene Arten von allgemeinen Bedrohungen zu identifizieren, die Sicherheit der Organisation zu bewerten, Cybersicherheitsinformationen zu sammeln und zu analysieren und Vorfälle zu beheben und zu melden, sobald sie auftreten. Dieser Kurs bietet einen umfassenden Methodik für Personen, die für den Schutz der Cybersicherheit ihrer Organisation verantwortlich sind.

Dieser Kurs soll die Teilnehmer bei der Vorbereitung auf die CertNexus CyberSec First Responder (Exam CFR-410) Zertifizierungsprüfung unterstützen. Was Sie in diesem Kurs lernen und üben, kann ein wichtiger Teil Ihrer Vorbereitung sein.

Darüber hinaus erfüllen dieser Kurs und die anschließende Zertifizierung (CFR-410) alle Anforderungen für Personal, das die DoD-Direktive 8570.01-M Positionszertifizierungsgrundlagen benötigt:

- CSSP-Analyst
- Unterstützung der CSSP-Infrastruktur
- CSSP Störfallbeauftragter
- CSSP-Prüfer

Zielgruppe

Dieser Kurs richtet sich in erster Linie an Fachleute für Cybersicherheit, die sich auf eine Tätigkeit zum Schutz von Informationssystemen vorbereiten oder diese derzeit ausüben, indem sie deren Verfügbarkeit, Integrität, Authentifizierung, Vertraulichkeit und Nichtabstreitbarkeit sicherstellen. Er eignet sich ideal für jene Funktionen innerhalb von bundesstaatlichen Vertragsunternehmen und Firmen des privaten Sektors, deren Auftrag oder strategische Ziele die Durchführung von Defensive Cyber Operations (DCO) oder DoD Information Network (DoDIN) und die Bearbeitung von Vorfällen erfordern. Dieser Kurs konzentriert sich auf das Wissen, die Fähigkeiten und die Fertigkeiten, die für die Verteidigung dieser Informationssysteme in einem Cybersicherheitskontext erforderlich sind, einschließlich Schutz, Erkennung, Analyse, Untersuchung und Reaktionsprozesse.

Darüber hinaus stellt der Kurs sicher, dass alle Mitglieder eines IT-Teams - unabhängig von Größe, Rang oder Budget - ihre Rolle bei der Cyberabwehr, der Reaktion auf Vorfälle und der Bearbeitung von Vorfällen verstehen.

Voraussetzungen

Damit Sie diesen Kurs erfolgreich absolvieren können, sollten Sie die folgenden Voraussetzungen erfüllen:

- Mindestens zwei Jahre (empfohlen) Erfahrung oder Ausbildung in der Computer-Netzwerksicherheitstechnologie oder einem verwandten Bereich.
- Die Fähigkeit oder Neugierde, Schwachstellen und Bedrohungen der Informationssicherheit im Rahmen des

Risikomanagements zu erkennen.
- Grundlegende Kenntnisse der Konzepte und des betrieblichen Rahmens allgemeiner Sicherheitsvorkehrungen in Netzumgebungen. Zu den Schutzmaßnahmen gehören unter anderem Firewalls, Intrusion Prevention Systeme und VPNs.
- Allgemeine Kenntnis der Konzepte und des operativen Rahmens allgemeiner Sicherheitsvorkehrungen in Computerumgebungen. Zu den Schutzmaßnahmen gehören u. a. die grundlegende Authentifizierung und Autorisierung, Ressourcenberechtigungen und Anti-Malware-Mechanismen.
- Grundlegende Kenntnisse über einige der gängigen Betriebssysteme für Computerumgebungen.
- Grundlegende Kenntnisse einiger gängiger Konzepte für Netzwerkumgebungen, z. B. Routing und Switching.
- Allgemeine oder praktische Kenntnisse der wichtigsten TCP/IP-Netzwerkprotokolle, einschließlich, aber nicht beschränkt auf TCP, IP, UDP, DNS, HTTP, ARP, ICMP und DHCP.

Kursziele

In diesem Kurs werden Sie Sicherheitsbedrohungen erkennen, bewerten, auf sie reagieren und sich vor ihnen schützen und eine System- und Netzwerksicherheitsanalyseplattform betreiben. Sie werden:

- Bewertung der Cybersicherheitsrisiken für das Unternehmen.
- Analysieren Sie die Bedrohungslandschaft.
- Analyse der verschiedenen Aufklärungsbedrohungen für Computer- und Netzwerkumgebungen.
- Analysieren verschiedener Angriffe auf Computer- und Netzumgebungen.
- Analysieren Sie verschiedene Techniken zur Nachbereitung von Angriffen.
- Bewertung der Sicherheitslage des Unternehmens durch Audits, Schwachstellenmanagement und Penetrationstests.
- Sammeln von Informationen zur Cybersicherheit aus verschiedenen netz- und hostbasierten Quellen.
- Analysieren Sie Protokolldaten, um Hinweise auf Bedrohungen und Vorfälle zu finden.
- Aktive Bestands- und Netzwerkanalyse zur Erkennung von Vorfällen.
- Reagieren Sie auf Cybersicherheitsvorfälle mit Eindämmungs-, Abschwächungs- und Wiederherstellungstaktiken.
- Untersuchung von Cybersicherheitsvorfällen mithilfe forensischer Analysetechniken.

Kursinhalt

- Bewertung des Cybersecurity-Risikos
- Analysieren der Bedrohungslandschaft
- Analyse von Aufklärungsbedrohungen für Computer- und Netzwerkumgebungen
- Analyse von Angriffen auf Computer- und Netzwerkumgebungen
- Analyse von Techniken nach Angriffen
- Bewertung der Sicherheitsposition der Organisation
- Sammeln von Cybersecurity Intelligence
- Analysieren von Protokolldaten
- Aktive Bestands- und Netzwerkanalyse durchführen
- Reaktion auf Cybersecurity-Vorfälle
- Untersuchung von Cybersecurity-Vorfällen

Detaillierter Kursinhalt

Lektion 1: Bewertung des Cybersecurity-Risikos

- Thema A: Erkennen der Bedeutung des Risikomanagements
- Thema B: Risikobewertung
- Thema C: Risikominderung
- Thema D: Integration der Dokumentation in das Risikomanagement

Lektion 2: Analysieren der Bedrohungslandschaft

- Thema A: Bedrohungen klassifizieren
- Thema B: Analysieren von Trends, die sich auf die Sicherheitslage auswirken

Lektion 3: Analyse von Aufklärungsbedrohungen für Computer- und Netzwerkumgebungen

- Thema A: Implementierung von Bedrohungsmodellen
- Thema B: Bewertung der Auswirkungen der Aufklärung
- Thema C: Bewertung der Auswirkungen von Social Engineering

Lektion 4: Analyse von Angriffen auf Computer- und Netzwerkumgebungen

- Thema A: Bewertung der Auswirkungen von Hackerangriffen auf das System
- Thema B: Bewertung der Auswirkungen von webbasierten Angriffen
- Thema C: Bewertung der Auswirkungen von Malware
- Thema D: Bewertung der Auswirkungen von Hijacking- und Impersonation-Angriffen
- Thema E: Bewertung der Auswirkungen von DoS-Vorfällen
- Thema F: Bewertung der Auswirkungen von Bedrohungen

der mobilen Sicherheit
- Thema G: Bewertung der Auswirkungen von Bedrohungen der Cloud-Sicherheit

Lektion 5: Analyse von Techniken nach einem Angriff

- Thema A: Bewertung von Führungs- und Kontrolltechniken
- Thema B: Bewertung von Persistenztechniken
- Thema C: Bewertung der seitlichen Bewegung und der Pivot-Techniken
- Thema D: Bewertung von Datenexfiltrationstechniken
- Thema E: Bewertung von Anti-Forensik-Techniken

Lektion 6: Bewertung der Sicherheitslage der Organisation

- Thema A: Implementierung von Cybersecurity Auditing
- Thema B: Umsetzung eines Plans zum Management von Schwachstellen
- Thema C: Bewertung von Schwachstellen
- Thema D: Durchführen von Penetrationstests

Lektion 7: Sammeln von Informationen zur Cybersicherheit

- Thema A: Einsatz einer Plattform zur Sammlung und Analyse von Sicherheitsinformationen
- Thema B: Sammeln von Daten aus netzgestützten Informationsquellen
- Thema C: Sammeln von Daten aus hostbasierten Informationsquellen

Lektion 8: Analysieren von Protokolldaten

- Thema A: Verwendung gängiger Tools zur Analyse von Protokollen
- Thema B: Verwendung von SIEM-Tools für die Analyse

Lektion 9: Aktive Bestands- und Netzwerkanalyse durchführen

- Thema A: Analysieren von Vorfällen mit Windows-basierten Tools
- Thema B: Analysieren von Vorfällen mit Linux-basierten Tools
- Thema C: Analyse von Indikatoren für Kompromisse

Lektion 10: Reaktion auf Cybersecurity-Vorfälle

- Thema A: Bereitstellung einer Architektur für die Behandlung von und Reaktion auf Zwischenfälle
- Thema B: Entschärfung von Zwischenfällen
- Thema C: Übergabe von Informationen zu einem Vorfall an eine forensische Untersuchung

Lektion 11: Untersuchung von Cybersecurity-Vorfällen

- Thema A: Anwendung eines forensischen Ermittlungsplans
- Thema B: Sicheres Sammeln und Analysieren von elektronischen Beweisen
- Thema C: Nachbereitung der Ergebnisse einer Untersuchung

Anhang A: Zuordnung der Kursinhalte zum CyberSec First Responder® (Prüfung CFR-410)

Anhang B: Reguläre Ausdrücke

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch