EC-Council Certified Network Defender (CND)

ID CND **Preis** CHF 4'790.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Netzwerk-Administratoren
- Administratoren für Netzwerksicherheit
- Netzwerktechniker
- Analyst für Datensicherheit
- Ingenieur für Netzwerksicherheit
- Netzwerk-Verteidigungstechniker
- Sicherheitsanalytiker
- Sicherheitspersonal
- Sicherheit im Netz
- Cybersecurity-Ingenieur

Voraussetzungen

Grundkenntnisse in Netzwerkkonzepten

Kursziele

- Planen, Implementieren und Verwalten des Netzwerksicherheitsmanagements in einem Unternehmen.
- Erwerb von Kenntnissen über verschiedene Sicherheitsrisiken, Bedrohungen und Schwachstellen.
- Unterstützung bei der Erlangung und Aufrechterhaltung der Konformität einer Organisation mit den erforderlichen regulatorischen Standards und Rahmenwerken.
- Entwurf und Umsetzung von Netzsicherheitsstrategien und -verfahren .
- Anwendung von Sicherheitsprinzipien, -protokollen und -kontrollen, die für die heutige verteilte und mobile Computerumgebung geeignet sind.
- Anwendung einer starken Identitäts- und Zugriffsverwaltung (IAM), Netzwerksegmentierung und Verschlüsselungstechniken zur Stärkung des Unternehmensnetzwerks.
- Verwaltung und Pflege der Windows-Sicherheitsverwaltung.
- Verwaltung und Pflege der Linux-Sicherheitsverwaltung.
- Verwalten und mindern Sie die Sicherheitsrisiken und Herausforderungen, die mit den Richtlinien des Unternehmens zur Nutzung mobiler Geräte verbunden sind.
- Verwaltung und Abschwächung der Sicherheitsrisiken und -herausforderungen im Zusammenhang mit IoT-Geräten in Unternehmen.
- Implementierung starker Datensicherheitstechniken zum Schutz der Daten eines Unternehmens.
- Implementierung und Verwaltung der Sicherheit von Virtualisierungstechnologien, d.h. Netzwerkvirtualisierung (NV), Software Defined Network (SDN),
- Network Function Virtualization (NFV), OS-Virtualisierung, Container, Docker und Kubernetes, die in modernen Netzwerken eingesetzt werden.
- Implementierung und Verwaltung von Cloud-Sicherheit auf verschiedenen Cloud-Plattformen wie AWS, Azure, Google Cloud Platform usw.
- Implementierung und Verwaltung der Sicherheit drahtloser Netzwerke.
- Durchführung von Risikobewertungen und Schwachstellenbeurteilungen/Scans mit verschiedenen Scanning-Tools und Erstellung detaillierter Berichte.
- Identifizieren Sie die kritischen Daten und wählen Sie eine geeignete Sicherungsmethode, ein geeignetes Medium und eine geeignete Technik, um regelmässig eine erfolgreiche Sicherung der Unternehmensdaten durchzuführen.
- Bereitstellung einer ersten Reaktion auf einen Netzsicherheitsvorfall und Unterstützung des IRT und der forensischen Untersuchungsteams bei der Bewältigung eines Vorfalls.
- Identifizierung der Indikatoren für die Gefährdung (Indicators of Compromise, IoC) und der Indikatoren für Angriffe (Indicators of Attack, IoA) in Netzwerken .
- Integration von Bedrohungsdatenfunktionen, um Bedrohungsdaten für die proaktive Verteidigung zu nutzen/zu verarbeiten.
- Führen Sie eine Analyse der Angriffsoberfläche durch, indem Sie Indikatoren für Sicherheitsrisiken (Indicators of Exposures, IoE) identifizieren.
- Unterstützung bei der Planung von Business Continuity (BC) und Disaster Recovery (DR).
- Überwachung des Netzverkehrs und Gewährleistung seiner Sicherheit .
- Protokollverwaltung durchführen.
- Überwachung der Netzwerkprotokolle auf Anomalien.
- Verwalten von Proxy und Inhaltsfilterung .
- Fehlerbehebung im Netzwerk bei verschiedenen Netzwerkproblemen.
- Identifizierung verschiedener Bedrohungen für das Netzwerk einer Organisation .
- Härtet die Sicherheit der verschiedenen Endpunkte im

Netzwerk des Unternehmens individuell.
- Wählen Sie die geeignete Firewall-Lösung, Topologie und Konfigurationen, um die Sicherheit durch die Firewall zu erhöhen.
- Bestimmen eines geeigneten Standorts für IDS/IPS-Sensoren, Abstimmen von IDS auf falsch-positive und falsch-negative Ergebnisse und Konfigurationen zur Erhöhung der Sicherheit durch IDPS-Technologien
- Pflege des Bestands an Computern, Servern, Terminals, Modems und anderen Zugangsgeräten.
- Bereitstellung von Anleitungen und Schulungen zum Sicherheitsbewusstsein.
- Hinzufügen, Entfernen oder Aktualisieren von Benutzerkontoinformationen.
- Einspielen von Betriebssystem-Updates und Patches sowie Vornahme von Konfigurationsänderungen.
- Aktualisierung der Systemkonfigurationen zur Aufrechterhaltung einer aktuellen Sicherheitslage unter Verwendung aktueller Patches, Härtungstechniken für Geräte und Betriebssysteme sowie Zugriffskontrolllisten.
- Verwalten Sie die Netzwerk-Authentifizierung, -Autorisierung und -Abrechnung (AAA) für Netzwerkgeräte.
- Überprüfen Sie Audit-Protokolle von Firewall, IDS/IPS, Servern und Hosts im internen, geschützten Netzwerk.
- Analyse, Fehlerbehebung und Untersuchung von Anomalien in sicherheitsrelevanten Informationssystemen auf der Grundlage der Sicherheitsplattform.
- Wartung, Konfiguration und Analyse von netz- und hostbasierten Sicherheitsplattformen.
- Bewertung von Sicherheitsprodukten sowie von Verfahren und Prozessen im Bereich der Sicherheit.
- Identifizierung und Klassifizierung von Unternehmensressourcen, einschliesslich Hardware, Software, Daten und kritischer Infrastruktur.
- Implementierung von Tools und Techniken zur Überwachung der Systemintegrität, um Änderungen in kritischen Dateien, Konfigurationen oder Systemzuständen zu erkennen.
- Verstehen der Rolle und Funktionalität von EDR/XDR-Lösungen, die zur Eindämmung und Beseitigung von Bedrohungen eingesetzt werden.
- Verstehen der Rolle und Funktionalität von UEBA-Lösungen, die zur Überwachung und Analyse von Benutzer- und Entitätsaktivitäten auf anomale Verhaltensmuster implementiert wurden.
- Durchführung von PIA-Prozessen zur Evaluierung und Bewertung der potenziellen Auswirkungen neuer Systeme, Prozesse oder Initiativen auf den Datenschutz.
- Zusammenarbeit mit den Sicherheitsteams zur Verbesserung der Strategien zur Bedrohungsjagd und der Reaktionsfähigkeit bei Zwischenfällen.
- die Rolle von SOAR-Plattformen (Security Orchestration, Automation, and Response) bei Cybersicherheitsoperationen zu verstehen.
- Planung und Durchführung der Integration von Zero-Trust-Prinzipien in bestehende Sicherheitsarchitekturen und -infrastrukturen.
- Bleiben Sie auf dem Laufenden über die neu aufkommenden Cyber-Bedrohungen mit Hilfe der neuesten Cyber-Sicherheitsnachrichten, Branchenpublikationen und seriösen Informationsquellen, einschliesslich Sicherheitsblogs, Forschungsberichten und Whitepapers.
- die Rolle von KI/ML bei der Verbesserung der Cyberabwehr, der Erkennung von Bedrohungen und der Reaktion darauf zu verstehen.

Kursinhalt

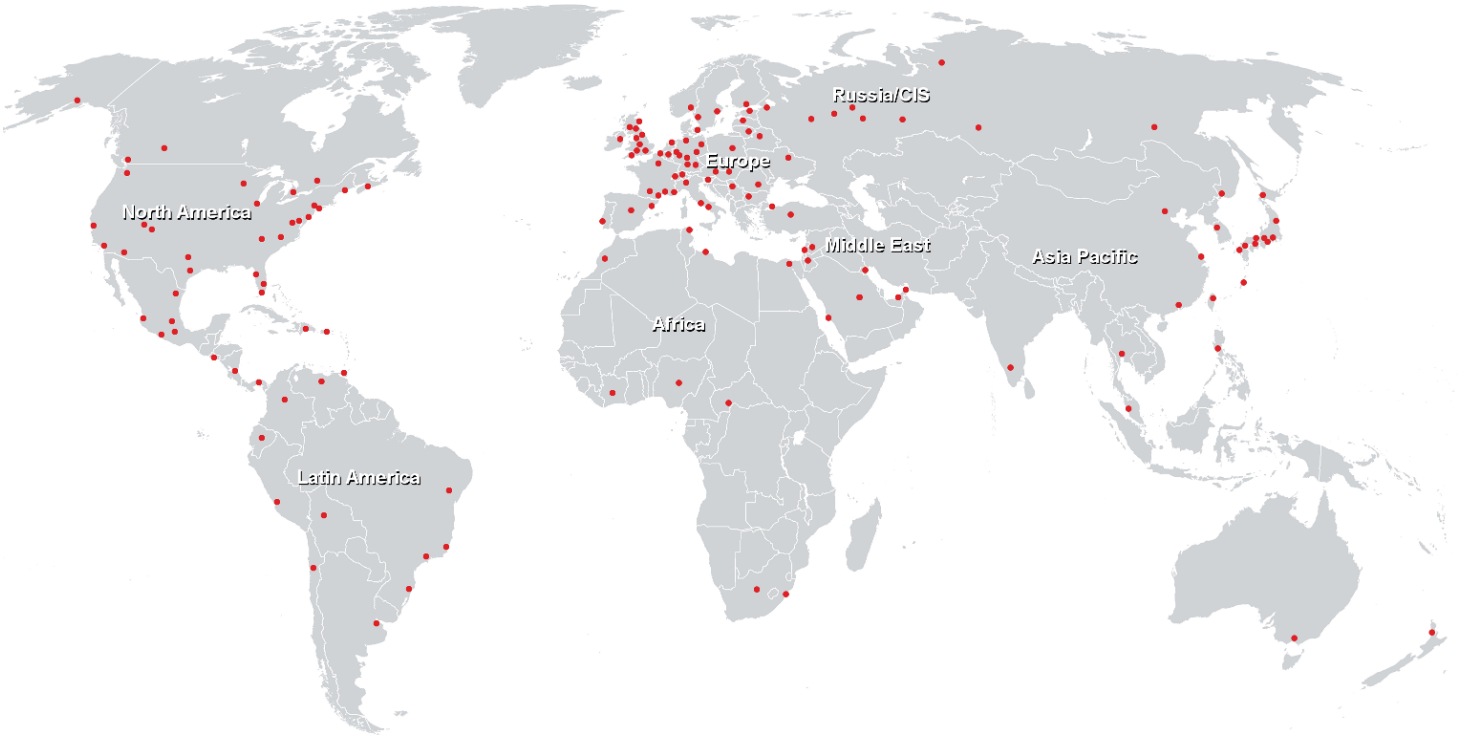
- Netzwerkangriffe und Verteidigungsstrategien
- Administrative Netzsicherheit
- Technische Netzsicherheit
- Sicherheit am Netzwerkrand
- Endpunktsicherheit - Windows-Systeme
- Endpunktsicherheit-Linux-Systeme
- Endpunktsicherheit - Mobile Geräte
- Endpunktsicherheit - IoT-Geräte
- Sicherheit von Verwaltungsanwendungen
- Datensicherheit
- Sicherheit virtueller Unternehmensnetzwerke
- Sicherheit von Unternehmens-Cloud-Netzwerken
- Sicherheit von drahtlosen Unternehmensnetzwerken
- Überwachung und Analyse des Netzwerkverkehrs
- Überwachung und Analyse von Netzwerkprotokollen
- Reaktion auf Zwischenfälle und forensische Untersuchungen
- Geschäftskontinuität und Disaster Recovery
- Risikovorwegnahme mit Risikomanagement
- Bewertung der Bedrohung mit Angriffsflächenanalyse
- Bedrohungsvorhersage mit Cyber Threat Intelligence

APPENDIX (Selbststudie)

- APPENDIX A: Grundlagen des Computernetzwerks
- APPENDIX B: Physische Netzwerksicherheit
- APPENDIX C: Sicherheit von virtuellen privaten Netzwerken (VPN)
- APPENDIX D: Endpunktsicherheit - MAC-Systeme

EC-Council Certified Network Defender (CND)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch