EC-Council Certified Threat Intelligence Analyst (CTIA)

ID CTIA **Preis** auf Anfrage **Dauer** 3 Tage

Zielgruppe

- Analyst für Cyber-Bedrohungsanalysen
- Cyber-Bedrohungsjäger
- Cyber Threat Intelligence-Mitarbeiter/Forscher/Berater
- Analyst für Cybersicherheit/Informationssicherheitsbedrohungen
- Cyber Threat Intelligence Ingenieur/Spezialist/Leiter/Manager
- SOC-Analyst für Bedrohungsanalysen
- Leitender Analyst für Bedrohungsanalysen zur Cyberkriminalität
- Ausserordentlicher Direktor für Bedrohungsmanagement
- Projektleiter/Direktor für Bedrohungsanalyse

Voraussetzungen

- Alle Cybersicherheitsexperten der mittleren bis oberen Ebene mit mindestens 3 Jahren Erfahrung.
- Personen mit den von EC-Council anerkannten Zertifizierungen C|EH und C|ND können sich für diesen Kurs anmelden.

Kursziele

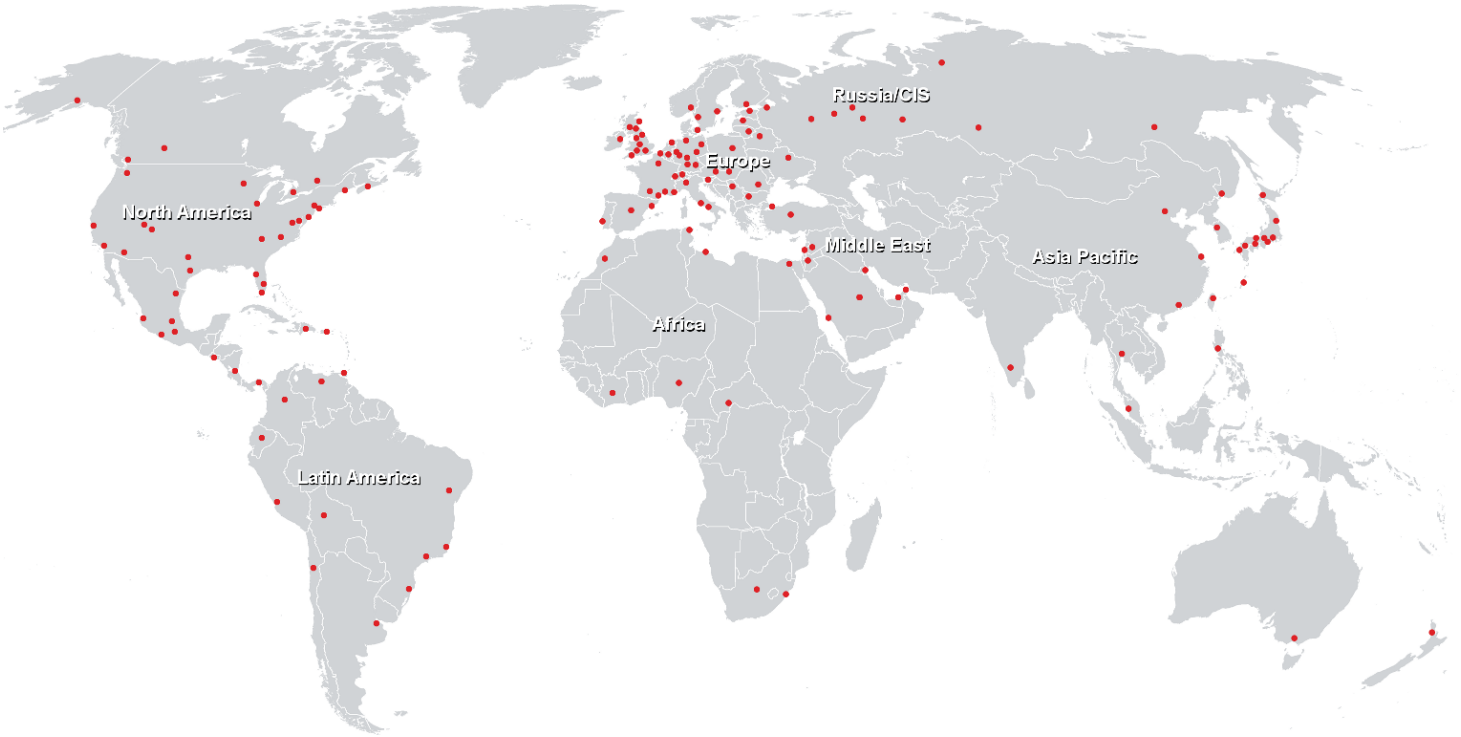
- Grundlagen der Bedrohungsaufklärung (Arten von Bedrohungsaufklärung, Lebenszyklus, Strategie, Fähigkeiten, Reifegradmodell, Rahmenwerke, Plattformen, usw.)
- Verschiedene Cybersicherheitsbedrohungen und Angriffsrahmen (Advanced Persistent Threats, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis usw.)
- Verschiedene Schritte bei der Planung eines Bedrohungsanalyseprogramms (Anforderungen, Planung, Leitung und Überprüfung)
- Verschiedene Arten von Bedrohungsdaten, Quellen und Methoden der Datenerfassung
- Sammlung und Beschaffung von Bedrohungsdaten durch Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), Malware Analysis und Python Scripting
- Verarbeitung und Nutzung von Bedrohungsdaten
- Techniken zur Analyse von Bedrohungsdaten (statistische Datenanalyse, Analyse konkurrierender Hypothesen (ACH), strukturierte Analyse konkurrierender Hypothesen (SACH), usw.)
- Vollständiger Prozess der Bedrohungsanalyse, der die Modellierung von Bedrohungen, die Feinabstimmung, die Bewertung sowie die Erstellung von Runbooks und Wissensdatenbanken umfasst
- Erstellen und Weitergeben von Berichten über Bedrohungsdaten
- Austausch von Bedrohungsdaten und Zusammenarbeit mit Python-Skripten
- Verschiedene Plattformen, Gesetze und Vorschriften für den Austausch von Informationen
- Wie man Bedrohungsanalysen in einer Cloud-Umgebung durchführt
- Grundlagen der Bedrohungsjagd (Arten der Bedrohungsjagd, Prozess, Schleife, Methodik usw.)
- Automatisierung der Bedrohungsjagd mit Python-Skripten
- Bedrohungsdaten im SOC-Betrieb, bei der Reaktion auf Zwischenfälle und im Risikomanagement

Kursinhalt

- Modul 01: Einführung in Threat Intelligence
- Modul 02: Cyber-Bedrohungen und Angriffsstrukturen
- Modul 03: Anforderungen, Planung, Lenkung und Überprüfung
- Modul 04: Datenerhebung und -verarbeitung
- Modul 05: Datenanalyse
- Modul 06: Nachrichtenübermittlung und -verbreitung
- Modul 07: Bedrohungsjagd und Erkennung
- Modul 08: Bedrohungsdaten im SOC-Betrieb, bei der Reaktion auf Zwischenfälle und im Risikomanagement

EC-Council Certified Threat Intelligence Analyst (CTIA)

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