EC-Council Certified SOC Analyst (CSA)

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

Zielgruppe

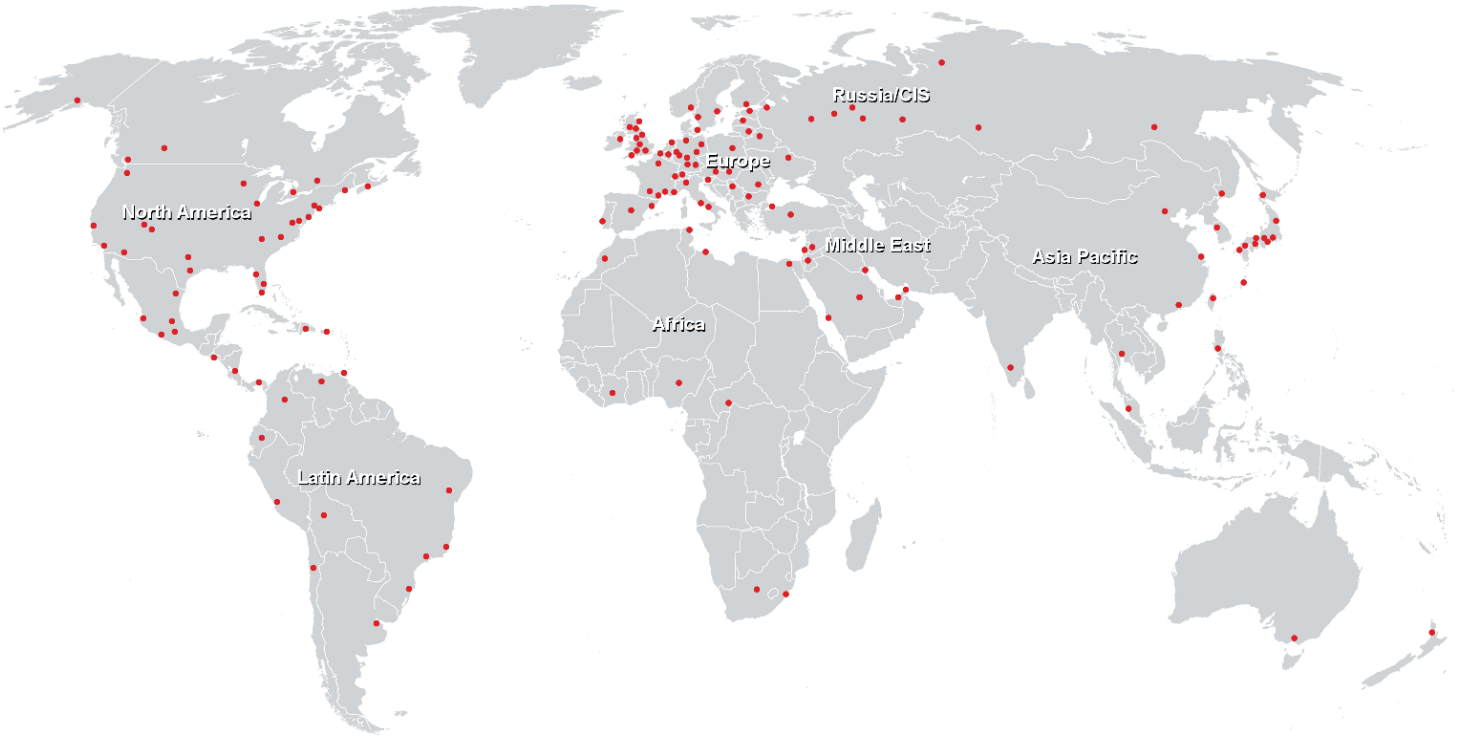
- SOC-Analysten (Tier I und Tier II)
- Netzwerk- und Sicherheitsadministratoren, Netzwerk- und Sicherheitsingenieure, Netzwerkverteidigungsanalytiker, Netzwerkverteidigungstechniker, Netzwerksicherheitsspezialisten, Netzwerksicherheitsoperatoren und alle Sicherheitsexperten, die mit Netzwerksicherheitsoperationen befasst sind
- Cybersecurity-Analyst
- Einsteiger im Bereich Cybersicherheit
- Jeder, der SOC-Analyst werden möchte.

Kursziele

- Erwerb von Kenntnissen über SOC-Prozesse, -Verfahren, -Technologien und -Workflows.
- Erwerb eines grundlegenden Verständnisses und eingehender Kenntnisse über Sicherheitsbedrohungen, Angriffe, Schwachstellen, Verhaltensweisen von Angreifern, Cyber-Kill-Chain usw.
- Sie sind in der Lage, Tools, Taktiken und Verfahren von Angreifern zu erkennen, um Indikatoren für eine Kompromittierung (IOCs) zu identifizieren, die während aktiver und zukünftiger Untersuchungen verwendet werden können.
- Fähigkeit zur Überwachung und Analyse von Protokollen und Warnmeldungen aus einer Vielzahl unterschiedlicher Technologien auf mehreren Plattformen (IDS/IPS, Endpunktschutz, Server und Workstations).
- Erwerb von Kenntnissen über den Prozess der zentralisierten Protokollverwaltung (CLM).
- Fähigkeit, Sicherheitsereignisse und Protokollerfassung, -überwachung und -analyse durchzuführen.
- Sammeln Sie Erfahrungen und umfassende Kenntnisse im Bereich Sicherheitsinformations- und Ereignisverwaltung.
- Erwerb von Kenntnissen über die Verwaltung von SIEM-Lösungen (Splunk/AlienVault/OSSIM/ELK).
- Verständnis für die Architektur, Implementierung und Feinabstimmung von SIEM-Lösungen (Splunk/AlienVault/OSSIM/ELK).
- Sammeln Sie praktische Erfahrungen bei der Entwicklung von SIEM-Anwendungsfällen.
- Fähigkeit zur Entwicklung von Bedrohungsfällen (Korrelationsregeln), Erstellung von Berichten usw.
- Lernen Sie Anwendungsfälle kennen, die bei der SIEM-Bereitstellung weit verbreitet sind
- Planung, Organisation und Durchführung von Bedrohungsüberwachung und -analyse im Unternehmen.
- Fähigkeit zur Überwachung neu auftretender Bedrohungsmuster und zur Durchführung von Analysen von Sicherheitsbedrohungen.
- Sammeln Sie praktische Erfahrungen im Prozess der Alarmtriage.
- Fähigkeit zur Weiterleitung von Vorfällen an die entsprechenden Teams für zusätzliche Unterstützung
- Fähigkeit, ein Service-Desk-Ticketing-System zu nutzen.
- Fähigkeit, Briefings und Berichte über Analysemethoden und -ergebnisse zu erstellen.
- Erwerb von Kenntnissen über die Integration von Bedrohungsdaten in SIEM zur verbesserten Erkennung von und Reaktion auf Vorfälle
- Fähigkeit zur Nutzung vielfältiger, unterschiedlicher und sich ständig ändernder Bedrohungsinformationen.
- Erwerb von Kenntnissen über den Incident Response Prozess
- Gewinnen Sie ein Verständnis für die Zusammenarbeit von SOC und IRT, um besser auf Vorfälle reagieren zu können.

EC-Council Certified SOC Analyst (CSA)

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