SC250 ISACA Certified Cybersecurity Operations Analyst (CCOA) Vorbereitung

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Vorbereitung auf die ISACA-Zertifizierung zum Certified Cybersecurity Operations Analyst. Vermittelt werden Kenntnisse zur Erkennung von Bedrohungen, Identifikation von Schwachstellen und Ableitung von Gegenmaßnahmen. Behandelt wird zudem die technische Analyse und Reaktion auf Sicherheitsvorfälle. Das Training bereitet gezielt auf die offizielle Prüfung vor.

Zielgruppe:

Der Workshop **SC250 ISACA Certified Cybersecurity Operations Analyst (CCOA) Vorbereitung** richtet sich an IT-Sicherheitsfachkräfte und Cybersecurity-Analysten, die ihre technischen Fähigkeiten im Bereich Cyber Defense ausbauen und durch eine anerkannte Zertifizierung nachweisen möchten. Empfohlen wird der Kurs vor allem für Fachleute mit ca. 2–3 Jahren Berufserfahrung in der IT-Sicherheit.

Typische Rollen aus der Zielgruppe sind unter anderem:

- Cybersecurity-Analysten
- Informationssicherheits-Analysten (Information Security Analysts)
- SOC-Analysten (Security Operations Center Analysts)
- Schwachstellen-Analysten (Vulnerability Analysts)
- Analysten für Incident Response (Incident-Response-Analysten)

Voraussetzungen:

Um die Zertifizierung eines **CCOA** erhalten zu können, müssen folgende Anforderungen erfüllt sein:

- Erfolgreiche Abschluss der CCOA Prüfung
- Beachtung des Codes of Professional Ethics von ISACA
- Nachweis von mindestens zwei bis drei Jahren Berufserfahrung im Bereich Cybersecurity-Analyst

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

Der Workshop **SC250 ISACA Certified Cybersecurity Operations Analyst (CCOA) Vorbereitung** bereitet Sie intensive auf die ISACA-Prüfung zur Erlangung der CCOA-Zertifizierung vor.

Inhalte/Agenda:

- **Domain 1 – Technologie-Grundlagen (25%)** – Vermittlung der wesentlichen technischen Grundlagen in der IT
- ♦ Networking (Netzwerke)
- ♦ System & Endpoint (Systeme & Endgeräte)
- ♦ Anwendungen
- ♦ **Domain 2 – Cybersecurity-Prinzipien und Risiken (20%)** – Überblick über Sicherheitsgrundsätze und das Management von Risiken
- ♦ Cybersecurity Principles (Grundlagen der IT-Sicherheit)
- ♦ Cybersecurity Risk (IT-Risiken)
- ♦ **Domain 3 – Taktiken, Techniken und Verfahren von Angreifern (10%)** – Verständnis der Vorgehensweisen von Cyber-Angreifern (Adversarial Tactics, Techniques & Procedures)
- ♦ Threat Landscape (Bedrohungslandschaft)
- ♦ Means and Methods (Mittel und Methoden)
- ♦ **Domain 4 – Erkennung und Reaktion auf Sicherheitsvorfälle (34%)** – Detaillierte Behandlung des Incident Managements von der Erkennung bis zur Reaktion
- ♦ Incident Detection (Erkennung von Vorfällen)
- ♦ Incident Response (Reaktion auf Vorfälle)
- ♦ **Domain 5 – Absicherung von Assets (11%)** – Maßnahmen zum Schutz von Unternehmenswerten (Systeme, Daten und Infrastruktur)
- ♦ Controls (Kontrollen)
- ♦ Vulnerability Management (Schwachstellenmanagement)
- ♦