Training: Fortinet
FortiAnalyzer Analyst

FORTINET Premier Authorized Training Center

TRAINING GOALS:

In diesem Kurs lernen Sie die Grundlagen der Verwendung von FortiAnalyzer für die zentralisierte Protokollierung kennen. Zentralisierte Protokollierung. Außerdem lernen Sie, wie Sie aktuelle und potenzielle Bedrohungen identifizieren können. Bedrohungen durch Log-Analyse. Schließlich erfahren Sie etwas über die Ereignisverwaltung, Vorfälle, Berichte und Aufgabenautomatisierung mit Playbooks. Diese Fähigkeiten bieten eine solide Grundlage für die Arbeit eines SOC-Analysten in einer Umgebung mit Fortinet-Produkten.

Ziele

Nach Abschluss dieses Kurses werden Sie in der Lage sein:

- Verstehen grundlegender Konzepte und Funktionen
- Beschreiben des Zwecks des Sammelns und Speicherns von Protokollen
- Anzeigen und Durchsuchen von Protokollen in Log View und FortiView
- Verstehen der FortiSoC-Funktionen
- Verwalten von Ereignissen und Event-Handlern
- Konfigurieren und Analysieren von Vorfällen
- Ausführen von Threat Hunting-Aufgaben. Verstehen von Ausbruchswarnungen
- Beschreiben der Funktionsweise von Berichten innerhalb von ADOMs
- Anpassen und Erstellen von Diagrammen und Datensätzen
- Anpassen und Ausführen von Berichten
- Konfigurieren von externem Speicher für Berichte
- Anhängen von Berichten an Vorfälle
- Fehlerbehebung bei Berichten
- Verstehen von Playbook-Konzepten
- Erstellen und Überwachen von Playbooks

Zielgruppe

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Dieser Kurs dient der Vorbereitung auf die Zertifizierungsprüfung NSE 5 FortiAnalyzer Analyst.

CONSPECT:

- SOC-Konzepte und Sicherheitsinfrastruktur
- Protokolldatenfluss und Navigation
- Ereignisse, Indikatoren und Vorfälle
- FortiAI, Bedrohungsanalyse und Fehlerbehebung
- Berichte
- Playbooks

REQUIREMENTS:

Vertrautheit mit allen Themen, die in den Kurs FortiOS Administrator behandelt werden. Kenntnisse der SQL SELECT-Syntax sind hilfreich

Difficulty level

CERTIFICATE:

Die Teilnehmer erhalten Zertifikate, die von Fortinet (Kursabschluss) unterzeichnet sind.

Dieser Kurs dient dazu, Sie auf die Fortinet *NSE5 FortiAnalyzer Analyst* Prüfung vorzubereiten.

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 6
- CPE lab hours: 5
- CISSP domains: Security Operations

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007