FortiAnalyzer Analyst

Erweitern Sie Ihre Fähigkeiten rund um den FortiAnalyzer 7.4.1

Seminar | 8 Termine verfügbar | Zertifikat

Präsenz / Virtual Classroom | 16 Unterrichtseinheiten

Seminarnummer: 31488

Stand: 19.12.2025. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31488

In diesem Kurs lernen Sie die Grundlagen der Verwendung von FortiAnalyzer für die zentralisierte Protokollierung kennen. Außerdem lernen Sie, wie Sie aktuelle und potenzielle Bedrohungen durch Protokollanalyse identifizieren können. Schließlich werden Sie die Verwaltung von Ereignissen, Vorfällen, Berichten und die Aufgabenautomatisierung mit Playbooks untersuchen. Mit diesen Kenntnissen verfügen Sie über eine solide Grundlage für die Arbeit als SOC-Analyst in einer Umgebung, die Fortinet-Produkte verwendet.

Nutzen

Nach diesem Kurs sind Sie in der Lage:

- Grundlegende FortiAnalyzer-Konzepte und -Funktionen zu verstehen
- Den Zweck des Sammelns und Speicherns von Protokollen zu beschreiben
- Protokolle in Log View und FortiView anzuzeigen und zu suchen
- SOC-Funktionen zu verstehen
- Ereignisse und Ereignis-Handler zu verwalten
- Vorfälle zu konfigurieren und zu analysieren
- Threat Hunting-Aufgaben durchzuführen
- Ausbruchswarnungen zu verstehen
- Die Funktionsweise von Berichten innerhalb von ADOMs zu beschreiben
- Diagramme und Datensätze zu erstellen und anzupassen
- Berichte auszuführen und anzupassen
- Externe Speicher für Berichte zu konfigurieren
- Berichte an Vorfälle anzuhängen
- Fehlerbehebung bei Berichten durchzuführen
- Playbook-Konzepte zu verstehen

- Playbooks zuerstellen und zu überwachen

Zielgruppe

Jeder, der für die Analyse von Fortinet Security Fabric und die Automatisierung von Aufgaben zur Erkennung von und Reaktion auf Cyberangriffe mit FortiAnalyzer verantwortlich ist, sollte diesen Kurs besuchen.

Voraussetzungen

Vertrautheit mit allen Themen, die in den Kursen FCP - FortiGate Security und FCP - FortiGate Infrastructure behandelt werden
Kenntnisse der SQL SELECT-Syntax sind hilfreich

Inhalte des Seminars

Agenda

1. SOC Concepts and Security Fabric
2. Log Data Flow and Navigation
3. Events, Indicators, and Incidents
4. FortiAI, Threat Hunting, and Troubleshooting
5. Reports
6. Playbooks

Wichtige Hinweise

Die Original-Herstellerunterlage zu diesem Kurs erhalten Sie als digitale Kursunterlage in englischer Sprache.

Das Seminar wird in Kooperation mit unserem Kooperationspartner Arrow Electronics in gewohnter TÜV-Rheinland-Qualität durchgeführt.

Sollte ein von uns beauftragter Partner zur Leistungserbringung Unterauftragnehmer einsetzen, stellen wir sicher, dass diese den erforderlichen Standards entsprechen.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31488 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.