

FortiSOAR Analyst (SOAR-ANL)

ID SOAR-ANL Preis auf Anfrage Dauer 3 Tage

Zielgruppe

SOC-Analysten, die für die Entwicklung von Playbooks, die Erstellung von Modulen, Vorlagen, Dashboards und Widgets sowie die Bearbeitung von Vorfällen mit FortiSOAR zuständig sind, sollten an diesem Kurs teilnehmen.

Empfohlenes Training für die Zertifizierung zum

NSE 6 Certified: Security Operations (NSE6SO)

Voraussetzungen

Sie müssen über Kenntnisse der im FortiOS-Administrator-Kurs behandelten Themen verfügen (oder über gleichwertige Erfahrungen).

Es wird ausserdem empfohlen, dass Sie über Kenntnisse der in den folgenden Kursen behandelten Themen verfügen oder über gleichwertige Erfahrungen verfügen:

- [FortiManager Administrator \(FMG\)](#)
- !FortiSOAR Administrator (FORT-SOARADMIN)
- Grundlegende Kenntnisse in der Programmierung mit Python
- Grundlegende Kenntnisse der Jinja2-Template-Sprache
- Grundlegende Kenntnisse im Bereich E-Mail-Sicherheit und SIEM-Technologie

Kursziele

Nach Abschluss dieses Kurses sollten Sie in der Lage sein:

- Beschreiben Sie SOAR, SIEM, Automatisierung und Orchestrierung
- Beschreiben Sie Module, Bereitstellungsmodelle und FortiSOAR-Gerätetypen
- Navigieren in der FortiSOAR-Benutzeroberfläche
- Anpassen der Navigation mit dem Navigationseditor
- Beschreiben Sie das SOAR-Framework-Lösungspaket
- Beschreiben Sie Vorlagen, Dashboards und Berichte
- Beschreiben Sie das Sicherheitsmanagement, den rollenbasierten Zugriff und die Teams

- Beschreiben Sie die Auslöser für FortiSOAR-Playbooks
- Beschreiben Sie die Schritte des FortiSOAR-Playbooks
- Ein Playbook erstellen
- Daten aus FortiSIEM einlesen
- Vorverarbeitungsregeln erstellen
- Beschreiben Sie Jinja und JSON und erläutern Sie, wie FortiSOAR diese nutzt
- Beschreiben Sie dynamische Variablen und Werte
- Beschreiben Sie die integrierten Funktionen
- Ein Modul entwerfen und veröffentlichen
- FortiSOAR-Entitäten exportieren und importieren
- Dashboards konfigurieren
- Widgets in Vorlagen konfigurieren
- Operatoren anwenden, um Bedingungen auszuwerten
- Demonstrieren Sie die JSON- und YAQL-Abfragefilter
- Beschreiben Sie FortiSOAR-Vorfälle
- Kampagnen beschreiben
- Beschreiben Sie die MITRE ATT&CK-Matrix für Unternehmen
- Beschreiben Sie die Phasen eines Vorfalls in FortiSOAR
- Beschreiben Sie den Workflow zur Vorfallobarbeitung in FortiSOAR
- Schicht- und Warteschlangenverwaltung konfigurieren
- Kriegeräume einrichten
- Behebung häufiger Probleme mit Playbooks
- Behebung häufiger Probleme mit Steckverbindern
- Protokollierungsstufen und Protokolldateien für die Analyse konfigurieren
- Beschreiben Sie die Grundlagen von APIs
- FortiSOAR-API konfigurieren
- FortiManager-API-Integration mit FortiSOAR konfigurieren
- Beschreiben Sie FortiAI auf FortiSOAR

Hinweis: Dieser Kurs bietet eine Einführung in die grundlegenden Ordner- und Dateistrukturen von Widgets und Konnektoren. Die für die Entwicklung benutzerdefinierter Widgets und Konnektoren erforderliche Programmierung wird dabei nicht behandelt.

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>