Descripción del Curso

En este curso, aprenderá los fundamentos del uso de FortiAnalyzer para el registro y la generación de informes centralizados. Aprenderá cómo configurar e implementar FortiAnalyzer e identificar amenazas y patrones de ataque a través del registro, el análisis y la generación de informes. Finalmente, examinará la gestión de eventos, incidentes, libros de jugadas y algunas técnicas útiles de solución de problemas.

Quien debe asistir

Cualquiera que sea responsable de la administración diaria de los dispositivos FortiAnalyzer y la información de seguridad de FortiGate.

Requisitos previos

- Familiaridad con todos los temas presentados en los cursos NSE 4 FortiGate Security y NSE 4 FortiGate Infrastructure
- El conocimiento de la sintaxis SQL SELECT es útil, pero no obligatorio

---

Agenda

1. Introduction and Initial Configuration
2. Administration and Management
3. Device Registration and Communication
4. Logging
5. FortiSoC—Incidents and Events
6. FortiSoC—Playbooks
7. Reports

Objetivos

Después de completar este curso, usted debería ser capaz de:

- Describir las funciones y conceptos clave de FortiAnalyzer
- Implementar una arquitectura apropiada
- Usar controles de acceso administrativo
- Supervisar eventos y tareas administrativas
- Configurar alta disponibilidad

- Comprender la sincronización de alta disponibilidad y el equilibrio de carga
- Actualice el firmware de un clúster HA
- Verificar el funcionamiento normal de un clúster HA
- Administrar ADOM
- Administrar RAID
- Registrar dispositivos compatibles
- Solucionar problemas de comunicación
- Administrar cuota de disco
- Administrar dispositivos registrados
- Proteger la información de registro
- Ver, buscar, administrar y solucionar problemas de registros
- Supervisar y gestionar eventos
- Administre y personalice controladores de eventos
- Crear y gestionar incidentes
- Explore las herramientas utilizadas para la caza de amenazas
- Crear, ejecutar y solucionar problemas de playbooks
- Importar y exportar playbooks
- Genere y personalice informes
- Personalice gráficos y conjuntos de datos
- Administrar y solucionar problemas de informes

Requisitos del Sistema

Si toma el formato en línea de esta clase, debe usar una computadora que tenga lo siguiente:

- Una conexión a Internet de alta velocidad
- Un navegador web actualizado
- Un visor de PDF
- Altavoces o auriculares
- Uno de los siguientes:
  - Compatibilidad con HTML5
  - Un Java Runtime Environment (JRE) actualizado con Java Plugin habilitado en su navegador web

Debe usar una conexión Ethernet por cable, no una conexión WiFi. Los firewalls, incluido Windows Firewall o FortiClient, deben permitir las conexiones a los laboratorios en línea.

Certificación

This course prepares you for the NSE 5 FortiManager certification exam.

- Fortinet NSE-5

Duración

2 Dias