Descripción del Curso

En este curso, aprenderá sobre las configuraciones iniciales, la arquitectura y el descubrimiento de dispositivos en la red de FortiSIEM. También aprenderá cómo recopilar información de rendimiento y agregarla con datos de syslog para enriquecer la vista general de la salud de su entorno, cómo usar la base de datos de configuración para facilitar en gran medida las auditorías de cumplimiento y cómo integrar FortiSIEM en su infraestructura de reconocimiento de red.

Quien debe asistir

Cualquier persona responsable de la gestión del día a día de FortiSIEM debe asistir a este curso.

Requisitos previos

Debe tener una comprensión de los temas tratados en los siguientes cursos, o tener una experiencia equivalente.

- NSE 4 *FortiGate Security*
- NSE 4 *FortiGate Infrastructure*

Agenda

1. Introduction
2. SIEM and PAM Concepts
3. Discovery and FortiSIEM Agents
4. FortiSIEM Analytics
5. CMDB Lookups and Filters
6. Group By and Data Aggregation
7. Rules and MITRE ATT&CK
8. Incidents and Notification Policies
9. Reports and Dashboards
10. Maintaining and Tuning
11. Troubleshooting

Objetivos

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

- Identificar los impulsores comerciales para el uso de herramientas SIEM
- Describir los conceptos de SIEM y PAM
- Describir las características clave de FortiSIEM
- Comprender cómo los recolectores, trabajadores y supervisores trabajan juntos
- Configurar notificaciones
- Crear nuevos usuarios y roles personalizados
- Describir y habilitar dispositivos para el descubrimiento
- Entender cuándo usar agentes
- Realice búsquedas históricas estructuradas en tiempo real
- Agrupar y agregar resultados de búsqueda
- Examinar las métricas de rendimiento
- Crear reglas de incidentes personalizadas
- Editar informes existentes o crear nuevos
- Configurar y personalizar los tableros
- Exportar información de CMDB
- Identificar los componentes del agente de Windows
- Describir el propósito de los agentes de Windows
- Comprender cómo funciona el administrador de agentes de Windows en varios modelos de implementación
- Identificar informes relacionados con agentes de Windows
- Comprender el agente de monitoreo de archivos de FortiSIEM Linux
- Comprender el registro de agentes
- Supervise las comunicaciones de los agentes después de la implementación
- Solucionar problemas de FortiSIEM

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

Este curso lo prepara para el examen de certificación NSE 5 FortiSIEM.

- Fortinet NSE-5

Duración

3 Diás
