Descripción del Curso

En esta clase, aprenderá a usar FortiEDR para proteger sus terminales contra ataques avanzados con la funcionalidad de respuesta a incidentes orquestada en tiempo real. También explorará las características de FortiEDR y cómo protegen sus terminales automáticamente en tiempo real.

Quien debe asistir

Los profesionales de TI y seguridad involucrados en la administración y el soporte de FortiEDR deben asistir a este curso.

Requisitos previos

Una comprensión básica de los conceptos de ciberseguridad

Agenda

1. Product Overview and Installation
2. Administration
3. Security Policies
4. Fortinet Cloud Security and Playbooks
5. Communication Control
6. Events and Alerting
7. Threat Hunting and Forensics
8. RESTful API
9. Troubleshooting

Objetivos

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

- Explicar el enfoque de FortiEDR y cómo funciona
- Identificar los componentes de comunicación y cómo están configurados
- Realice tareas administrativas importantes, que incluyen: administrar usuarios de la consola, actualizar recopiladores, eliminar datos personales para cumplir con GDPR, implementar un entorno de múltiples inquilinos y ver eventos del sistema

- Lleve a cabo los pasos básicos de solución de problemas, que incluyen: verificar que FortiEDR esté instalado y bloquear activamente el malware, identificar si FortiEDR ha bloqueado un proceso o una conexión, buscar registros y ponerse en contacto con el soporte de FortiEDR
- Realice tareas administrativas importantes, que incluyen: administrar usuarios de la consola, actualizar recopiladores, eliminar datos personales para cumplir con GDPR y ver eventos del sistema
- Reconocer qué es Fortinet Cloud Service y cómo funciona
- Complete tareas básicas en cada área de la consola de administración: el Panel, el Visor de eventos, la pestaña
- Análisis forense, el módulo Caza de amenazas, Control de comunicación, Políticas de seguridad, Playbooks, Inventario y la pestaña
- Administración Administrar eventos de seguridad y su estado
- Bloquee la comunicación de aplicaciones que son riesgosas o no deseadas, pero que no son inherentemente maliciosas
- Encuentre y elimine ejecutables maliciosos de todos los dispositivos en su entorno
- Comprenda cómo FortiEDR se integra con Fortinet Security Fabric y cómo funciona FortiXDR
- Use la API RESTful para administrar su entorno FortiEDR Priorizar, investigar y analizar eventos de seguridad
- Corrija eventos maliciosos y cree excepciones para permitir procesos seguros
- Realice tareas básicas de solución de problemas en todos los componentes de FortiEDR
- Obtener registros del recopilador y volcados de memoria

Requisitos del Sistema

Si toma una versión en línea de esta clase, debe tener una computadora con:

- Una conexión a Internet de alta velocidad
- Un navegador web actualizado
- Un visor de PDF
- Altavoces / auriculares
- Uno de los siguientes:
  - Soporte HTML5
  - Un Java Runtime Environment (JRE) actualizado con el complemento de Java 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 Especialista en FortiEDR.

La certificación NSE 5 Network Security Analyst requiere aprobar al menos dos exámenes de Especialista NSE 5. Conozca más sobre la Certificación NSE 5.

- Fortinet NSE-5

Duración

2 Dias