Fortinet: Advanced Analytics

Código: FOR-005

Propuesta de Valor: HARDWARE - REDES - TELECOMUNICACIONES

Duración: 19 Horas

En este curso, aprenderá a usar FortiSIEM en un entorno de múltiples inquilinos. Aprenderá sobre las reglas y su arquitectura, cómo se generan los incidentes, cómo se realizan los cálculos de referencia, los diferentes métodos de remediación disponibles y cómo el marco MITRE ATT&CK se integra con FortiSIEM. También aprenderá cómo integrar FortiSOAR con FortiSIEM.

AUDIENCIA

- Profesionales de seguridad involucrados en la gestión, configuración, administración y monitoreo de dispositivos FortiSIEM y FortiSOAR en una implementación empresarial o de proveedor de servicios utilizada para monitorear y proteger las redes de las organizaciones de los clientes.

PRE REQUISITOS

Debe comprender los temas tratados en los siguientes cursos, o tener una experiencia equivalente:

- FCP - FortiGate Security
- FCP - FortiGate Infrastructure
- FCP - FortiSIEM

También se recomienda que comprenda los siguientes temas o tenga experiencia equivalente:

- Programación en Python
- Lenguaje de plantillas Jinja2 para Python
- Sistemas linux
- Tecnologías SOAR

OBJETIVOS

- Identificar varios requisitos de implementación para una implementación de FortiSIEM de múltiples inquilinos.
- Implemente FortiSIEM en un entorno híbrido con y sin recopiladores.
- Diseñe soluciones multiusuario con FortiSIEM.
- Implemente recopiladores en un entorno de múltiples inquilinos.
- Administra la asignación y restricciones de EPS en FortiSIEM.
- Administre la utilización de recursos de un clúster FortiSIEM de múltiples inquilinos.
- Mantener y solucionar problemas de una instalación de colector.
- Implemente y administre agentes de Windows y Linux.
- Cree reglas evaluando eventos de seguridad.
- Definir acciones para una regla de seguridad de patrón único.

CERTIFICACIÓN DISPONIBLE

- Certificación oficial de **COGNOS**.
- Este curso lo prepara para el examen: Fortinet NSE 7 - Advanced Analytics 6.3. Este examen se encuentra en la ruta de certificación de: **FCSS Security Operations**

CONTENIDO

1. INTRODUCCION AL ARRENDAMIENTO MULTIPLE

2. DEFINICON DE COLECTORES FortiSIEM Y CONECTORES FortiSOAR

3. COLECTORES OPERATIVOS

4. AGENTES DE WINDOWS Y LINUX

5. NORMAS

6. REGLAS DE SEGURIDAD DE SUBPATRON UNICO

7. MULTIPLES REGLAS DE SUBPATRON

8. LINEAS DE BASE

9. REGLAS DE REFERNCIA

10. FortiSIEM UEBA

11. CONSULTAS ANIDADAS Y TABLAS DE BUSQUEDA

12. CONDICIONES CLARAS

13. REMEDIACION

BENEFICIOS

- Al finalizar el curso, los participantes podrán identificar los atributos del incidente que desencadenan un incidente. Identificar múltiples reglas de seguridad de patrones y defina condiciones y acciones para ellas.