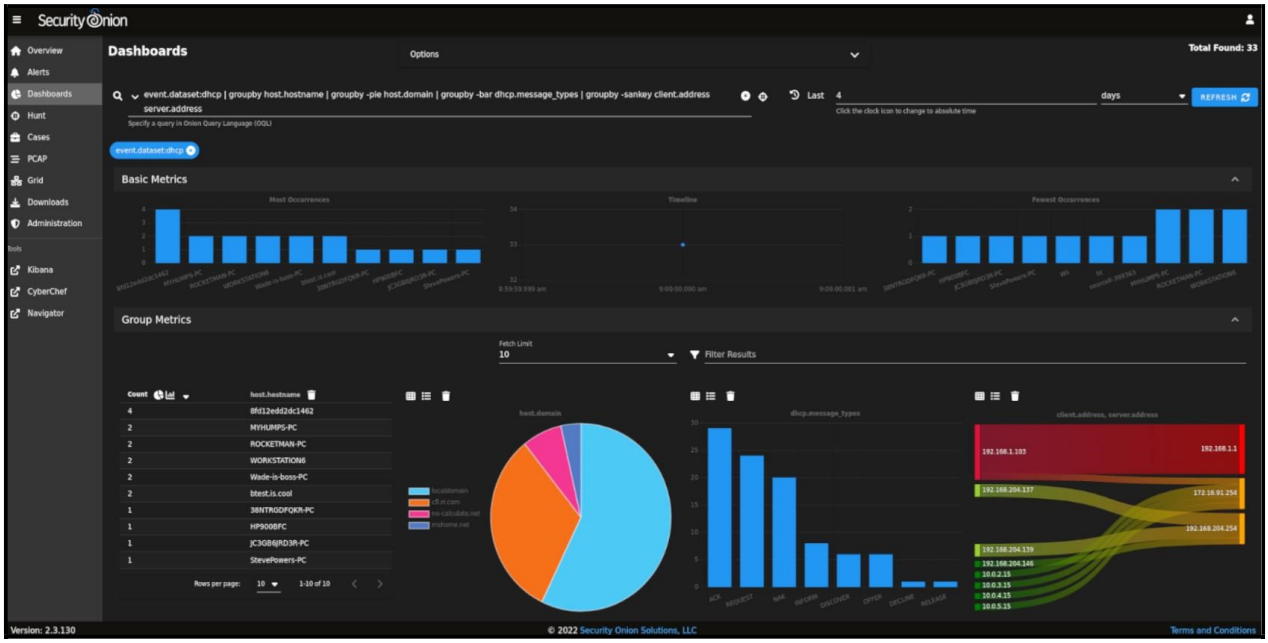
## Cursos de Especialización Profesional

**CURSO : Ciberseguridad con Security Onion**
**Duración : 20 horas**




# SYLLABUS

## I. DESCRIPCIÓN

Este curso tiene un nivel intermedio y está dirigido para profesionales y administradores de red que quieran especializarse en Seguridad Defensiva para blueteam implementando soluciones modernas para detectar y proteger la infraestructura de las organizaciones de ataques externos e internos.

Durante el desarrollo de los diferentes temas del curso desarrollaremos los conceptos de Identificación y detección de Ataques e incidentes de seguridad que se presentan en los diferentes puntos de nuestra red, empezaremos revisando como detectar los ataques de la Red LAN, para luego analizar la detección en los Servidores y Equipos de Perímetro y como Implementar la Solución de Security Onion para una Correcta detección y Gestión de Amenazas dentro de la Organización.

## II. METODOLOGÍA

El curso contará con sesiones teórico-prácticas. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios y discusión en clase. Se trabaja con equipos reales y maquinas virtuales.

## III. REQUISITOS

- Conocimientos de Redes de Datos y Protocolos TCP/IP.
- Conocimientos básicos de Redes LAN

## IV. MATERIALES

- Manual y Guía de Laboratorios del curso.
- Los Laboratorios se realizarán con máquinas virtuales.

## V. PLAN DE TEMAS

El programa incluye los siguientes módulos

### Detalle de cada Módulo:

## Tema 1 : Implementación Security Onion

- Plataforma Security Onion
- Instalación de Security Onion en StandAlone
- Instalación Distribuida del Nodo Manager
- Instalación distribuida del Nodo Search
- Instalación distribuida del Nodo Forward
- Gestión de Usuarios
- Troubleshooting y Gestión de Políticas
- Updates de Security Onion
- Consideraciones de Hardening
- Monitoreando la Salud de SO
- Endpoint en SO
- Elastic Fleet
- Deployment de Agentes
- Performance de Zeek y Suricata
- Performance y Script de Zeek
- Alertas de Suricata
- Alertas de Playbook

## Tema 2 : Detección de Amenazas con Security Onion

- Plataforma Security Onion
- Caso de estudio – Alert Triage y Creación de Casos