
www.eysglobal.com

# CURSO DE INFORMÁTICA FORENSE

# MÓDULO 3
# El centro de operaciones de seguridad moderno

# Elementos del SOC

# INFORMÁTICA FORENSE

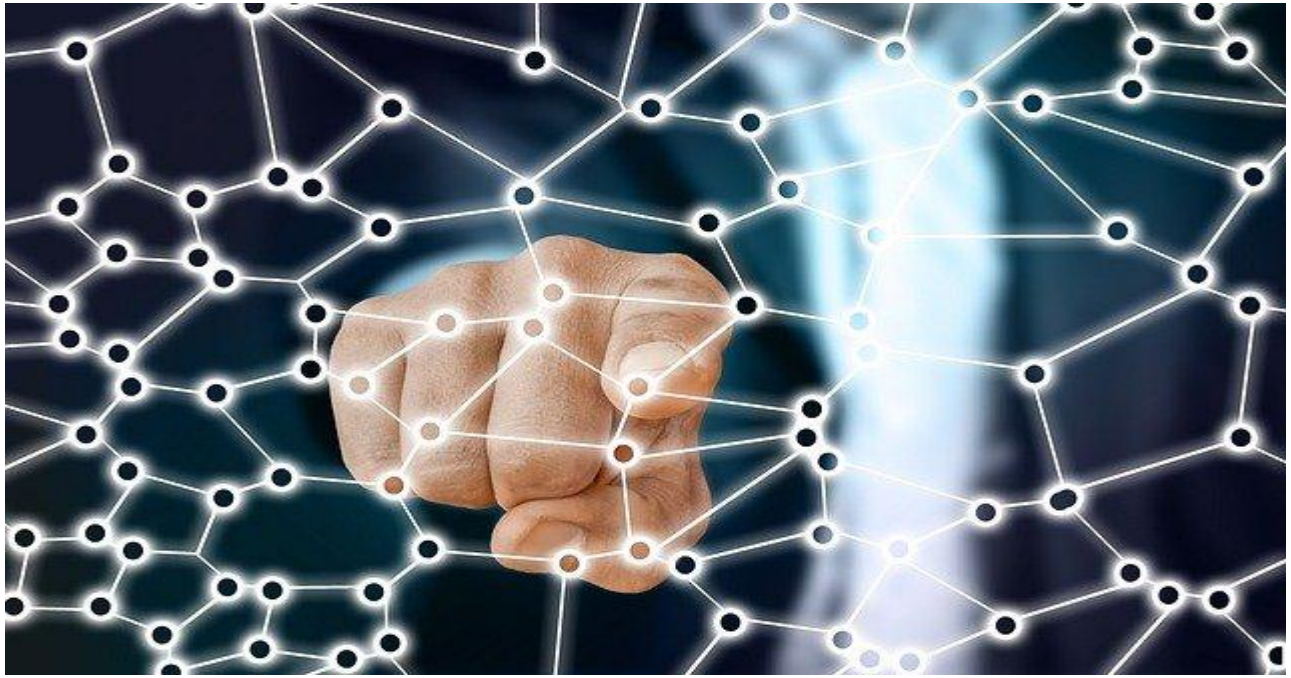
## Proceso en el SOC

El analista de seguridad de la red debe monitorear la cola de alertas de seguridad e investigar las alertas asignadas. El sistema de tickets se utiliza para asignar estas alertas a una cola de analistas

# INFORMÁTICA FORENSE

## Tecnologías en el  SOC SIEM

- Un SOC necesita un sistema de gestión de información de seguridad y eventos



# INFORMÁTICA FORENSE

## Tecnologías en el  SOC SOAR

Los equipos de grandes operaciones de seguridad (SecOps) utilizan ambas tecnologías para optimizar su SOC

# INFORMÁTICA FORENSE

## Tecnología en el SOC : SOAR


Recopila datos de alarma de todos los componentes del sistema..

# INFORMÁTICA FORENSE

## Seguridad empresarial  y gestionada

Las organizaciones más grandes pueden subcontratar al menos una parte de las operaciones de SOC a un proveedor de soluciones de seguridad

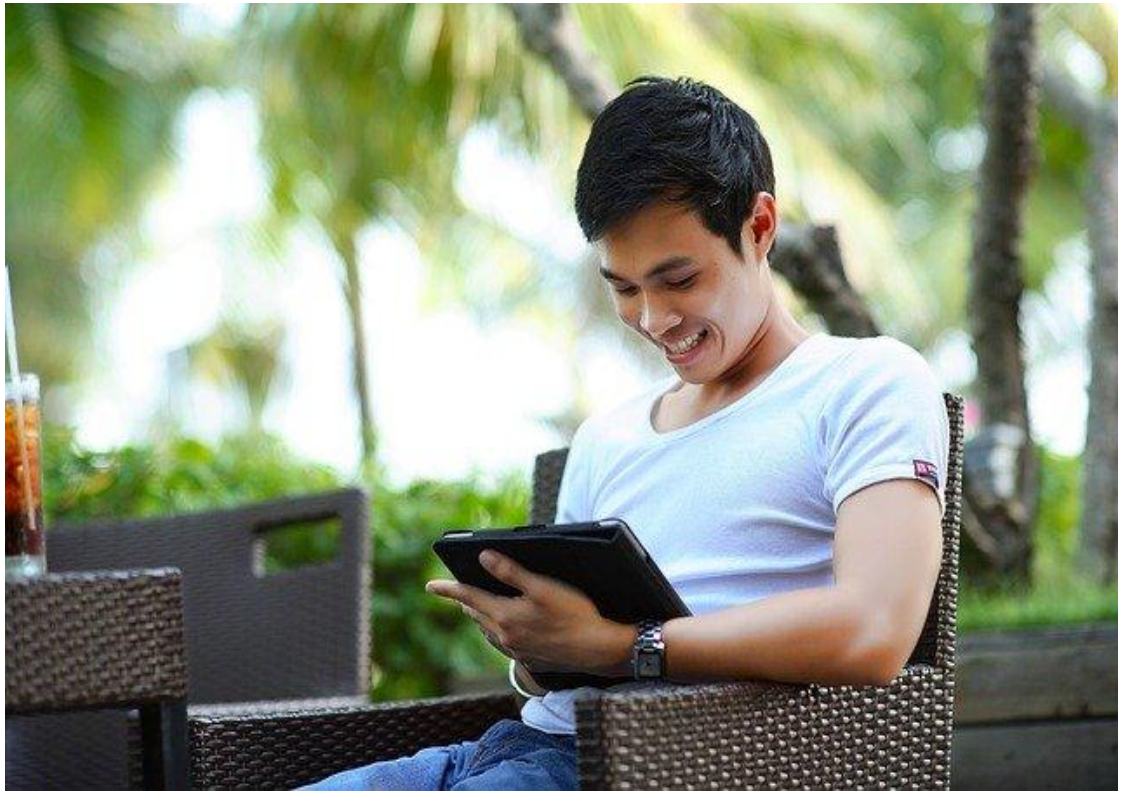
# INFORMÁTICA FORENSE

**Seguridad VS Disponibilidad**

Mantenerse la disponibilidad de la red.

# INFORMÁTICA FORENSE

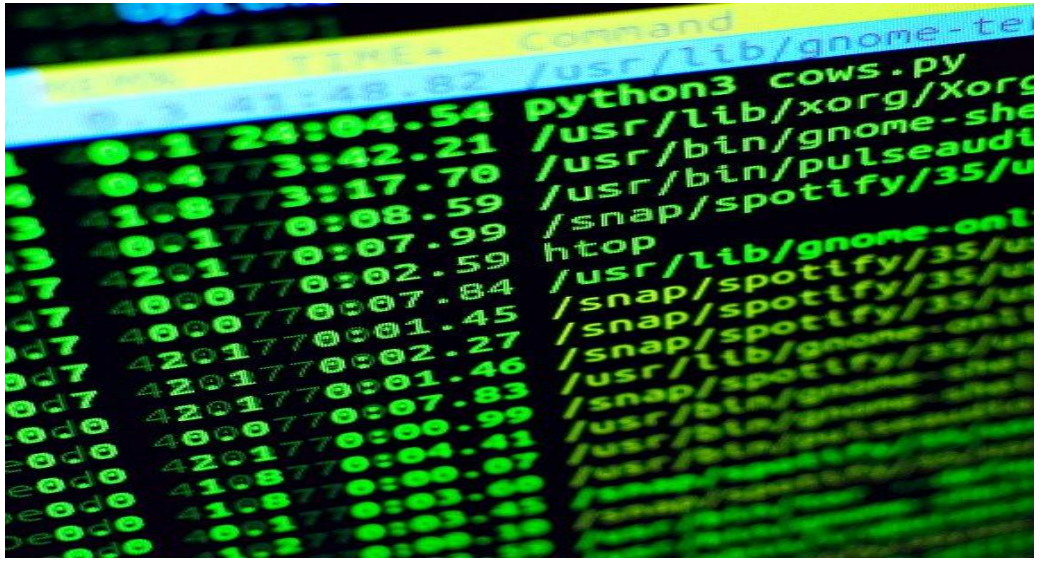
## Conviértase en defensor



Una variedad de las certificaciones de ciberseguridad que son relevantes para carreras en SOCs disponibles

# INFORMÁTICA FORENSE

**Conviértase en defensor**




***Grados***

***Programación en Python***

***Habilidades en Linux***