El career path **SOC Level 1** de TryHackMe.com es un «learning path». Es decir, un itinerario de aprendizaje enfocado en formar profesionales con las habilidades esenciales para desempeñarse como analista de nivel 1 en un Centro de Operaciones de Seguridad (Security Operations Center, SOC). El contenido se orienta tanto a la teoría como a la práctica, y cubre las competencias básicas que se requieren en un entorno SOC real. Es una excelente forma de aprender ciberseguridad para trabajar en entornos de SoC reales.

Os dejo los enlaces a todas las publicaciones que hemos hecho en hacks4geeks, acerca de todos los módulos que contiene. Al entrar en cada una de ellas, podréis ver a su vez, todos los enlaces a los writeups de cada una de sus salas:

- Módulo Cyber Defense Frameworks
- Módulo Cyber Threat Intelligence
- Módulo Network Security and Traffic Analysis
- Módulo Endpoint Security Monitoring
- Módulo Security Information and Event Management
- Módulo Digital Forensics and Incident Response
- Módulo Phishing
- Módulo SOC Level 1 Capstone Challenges

Si queréis acceso directo a todas las salas de la plataforma, también os las dejo aquí abajo. Haced click en la flechita de cada uno para ver los enlaces directos a sus correspondientes salas:

Cyber defense frameworks

- Junior security analyst intro
- Pyramid of pain
- Cyber kill chain
- Unified cyber kill chain
- Diamond model
- MITRE (premium)
- Summit (premium)
- Eviction (premium)

Cyber threat intelligence

- Intro to cyber threat intel
- Thread intelligence tools
- Yara (premium)
- OpenCTI (premium)
- MISP (premium)
- Friday overtime (premium)
- Trooper (premium)

Network security and traffic analysis

- Traffic analysis essentials
- Snort

- Snort challenge – The basics (premium)
- Snort challenge – Live attacks (premium)
- NetworkMiner (premium)
- Zeek (premium)
- Zeek exercies (premium)
- Brim (premium)
- Wireshark: the basics (premium)
- Wireshark: packet operations (premium)
- Wireshark: traffic analysis (premium)
- TShark: the basics (premium)
- TShark: CLI wireshark features (premium)
- TShark challenge 1: teamwork (premium)
- TShark challenge 2: directory (premium)

Endpoint security monitoring

- Intro to endpoint security
- Core Windows processes (premium)
- Sysinternals (premium)
- Windows event logs (premium)
- Sysmon (premium)
- Osquery: the basics (premium)
- Wazuh
- Monday monitor (premium)
- Retracted (premium)

Security information and event management

- Introduction to SIEM
- Investigating with ELK 101 (premium)
- ItsyBitsy (premium)
- Splunk Basics (premium)
- Incident handling with Splunk (premium)
- Investigationg with Splunk (premium)
- Benign (premium)

Digital forensics and incident response

- DFIR: an Introduction
- Windows forensics 1
- Windows forensics 2 (premium)
- Linux forensics (premium)

- Autopsy (premium)
- Redline
- KAPE
- Volatility (premium)
- Velociraptor (premium)
- TheHive project (premium)
- Intro to malware analysis (premium)
- Unattended
- Disgruntled (premium)
- Critical
- Secret recipe (premium)

Phishing

- Phishing analysis fundamentals
- Phishing emails in action
- Phishing analysis tools (premium)
- Phishing prevention (premium)
- The greenholt phish (premium)
- Snapped phish-ing line (premium)

SOC Level 1 Capstone Challenges

- Tempest (premium)
- Boogeyman 1 (premium)
- Boogeyman 2 (premium)
- Boogeyman 3 (premium)