COURSE OUTLINE

TRENDS Academy
Learning | Evolving | Empowering

Certified SOC Analyst

Duration: 3 Days

Course Objectives:

- gain knowledge of soc processes, procedures, technologies, and workflows.
- gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber killchain, etc.
- able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (iocs) that can be utilized during active and future investigations.
- able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (ids/ips, end-point protection, servers, and workstations).
- gain knowledge of the centralized log management (clm) process.
- able to perform security events and log collection, monitoring, and analysis.
- gain experience and extensive knowledge of security information and event management.
- gain knowledge of administering siem solutions (splunk/alienvault/ossim/elk).
- gain hands-on experience in siem use case development process.
- able to develop threat cases (correlation rules), create reports, etc.
- learn use cases that are widely used across the siem deployment.
- plan, organize, and perform threat monitoring and analysis in the enterprise.
- able to monitor emerging threat patterns and perform security threat
- analysis.
- gain hands-on experience in the alert triaging process.
- able to escalate incidents to appropriate teams for additional assistance.
- able to use a service desk ticketing system.
- able to prepare briefings and reports of analysis methodology and results.
- gain knowledge of integrating threat intelligence into siem for enhanced incident detection and response.
- able to make use of varied, disparate, constantly changing threat information.
- gain knowledge of incident response process.
- gain understating of soc and irt collaboration for better incident response

Target Audience:

- SOC Analysts (Tier I and Tier Il)
- Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network Defense Technicians, Network Security Specialist, Network Security Operator, and any security professional handling network security operations
- Cybersecurity Analyst
- Entry-level cybersecurity professionals
- Anyone who wants to become a SOC Analyst.

Course Outline:

- ➢ Module 01: Security Operations and Management
- ➢ Module 02: Understanding Cyber Threats, loCs, and Attack Methodology
- ➢ Module 03: Incidents, Events, and Logging
- ➢ Module 04: Incident Detection with Security Information and Event Management (SIEM)
- ➢ Module 05: Enhanced Incident Detection with Threat Intelligence
- ➢ Module 06: Incident Response

REGISTER NOW!

training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph

EC-Council

Trends Academy is an EC-Council Accredited Training Center.