SCE – SOC Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 10h

Sobre o curso

The **SOC Essentials (SCE)** is designed for aspiring security professionals, freshers, and career switchers to provide insights into security operations frameworks and related technologies. With 8 modules covering robust topics from the computer network and security fundamentals to SOC components and architecture, SCE prepares you to identify

various aspects of cyber threats and secure digital environments. No IT/Cybersecurity experience required for this course. Test your skills with CTF-based Capstone Project and validate these newly acquired skills in proctored exams. Further, it provides 10+ hours of premium self-paced video training with 6 hands-on labs to simulate real-world scenarios

Key Features:

- 6 lab practical exercises
- 10+ hours of premium self-paced video training
- 900+ pages of ecourseware
- Capstone Project
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with 1-year validity
- Earn a globally recognized EC-Council certification.
- Increase your value in the job market

Destinatários

Who is S|CE for?

- High School/College/University students
- Teams and organizations
- Career starters

- Working professional

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Training Details: Self-paced in-demand lecture videos led by world-class instructors and hands-on labs.

Exam Details:

- Exam Code: 112-56
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Computer Network and Security Fundamentals
- Fundamentals of Cyber Threats
- Introduction to Security Operations Center
- SOC Components and Architecture
- Introduction to Log Management
- Incident Detection and Analysis
- Threat Intelligence and Hunting
- Incident Response and Handling

Computer Network and Security Fundamentals

- TCP/IP Model
- OSI Model
- Types of a Network
- Network Topologies
- Network Hardware Components
- TCP/IP Protocol Suite
- Network Security Controls
- Network Security Devices
- Windows Security
- Unix/Linux Security
- Web Application Fundamentals
- Information Security Standards, Laws, and Acts

Fundamentals of Cyber Threats

- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures
- Opportunity-Vulnerability-Weakness
- Vulnerability
- Threats & Attacks
- Example of Attacks
- Network-Based Attacks
- Application-Based Attacks
- Host-Based Attacks
- Insider Attacks
- Malware
- Phishing and Social Engineering

Introduction to Security Operations Center

- What is a Security Operations Center (SOC)
- Importance of SOC
- SOC Team Roles and Responsibilities
- SOC KPI
- SOC Metrics
- SOC Maturity Models
- SOC Workflow and Processes
- Challenges in Operating a SOC

SOC Components and Architecture

- Key Components of a SOC
- People in SOC
- Process in SOC
- Technologies in SOC
- SOC Architecture and Infrastructure
- Different Types of SOCs and Their Purposes
- Introduction to SIEM
- SIEM Architecture
- SIEM Deployment Models
- Data Sources in SIEM
- SIEM Logs
- Network in SIEM
- Endpoint Data in SIEM

Introduction to Log Management

- Incident
- Event

- Log
- Typical Log Sources
- Need of Log
- Typical Log Format
- Local Log Management
- Centralized Log Management
- Logging Best Practices
- Logging/Log Management Tools

Incident Detection and Analysis

- SIEM Use Case Development
- Security Monitoring and Analysis
- Correlation Rules
- Dashboards
- Reports
- Alerting
- Triaging Alerts
- Dealing with False Positives Alerts
- Incident Escalation
- Communication Paths
- Ticketing Systems

Threat Intelligence and Hunting

- Introduction to Threat Intelligence
- Threat Intelligence Sources
- Threat Intelligence Types
- Threat Intelligence Lifecycle
- Role of Threat Intelligence in SOC Operations
- Threat Intelligence Feeds
- Threat Intelligence Sharing and Collaboration
- Threat Intelligence Tools/Platforms
- Introduction to Threat Hunting
- Threat Hunting Techniques
- Threat Hunting Methodologies
- Role of Threat Hunting in SOC Operations
- Leveraging Threat Intelligence for Hunting
- Threat Hunting Tools

Incident Response and Handling

- Incident Handling Process
- Incident Classification and Prioritization
- Incident Response Lifecycle
- Preparation

- Identification
- Containment
- Eradication
- Recovery
- Post-incident Analysis and Reporting