EC-Council SOC Essentials (SCE)

Category: Networking & Security | **Vendor:** EC-Council

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

The SOC Essentials (S|CE) Series is designed for security professionals and freshers to enhance their skills and knowledge about essential security technologies. Focused on honing candidates with in-demand skills, the S|CE course will provide insights into security operations frameworks and related technologies that are required to master the foundational concepts of SOC. In this program students will learn the basics of computer networks, TCP/IP model, OSI model, Windows/Linux/Unix security concepts, threats, vulnerabilities, and attack concepts in terms of cyber threats. Further, students will go through the complete SOC architecture: its importance, workflow, and processes of SOC. Students will learn more advanced architectural concepts like SIEM architecture and deployment models, and data sources that are commonly used. Learn everything about Log Management like; dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts. This course will also teach you sources, types, and lifecycle of threat intelligence and give an introduction to threat hunting as well while diving deep into incident response lifecycle processes. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

About This Course

The SOC Essentials (S|CE) Series is designed for security professionals and freshers to enhance their skills and knowledge about essential security technologies. Focused on honing candidates with in-demand skills, the S|CE course will provide insights into security operations frameworks and related technologies that are required to master the foundational concepts of SOC. In this program students will learn the basics of computer networks, TCP/IP model, OSI model, Windows/Linux/Unix security concepts, threats, vulnerabilities, and attack concepts in terms of cyber threats. Further, students will go through the complete SOC architecture: its importance, workflow, and processes of SOC. Students will learn more advanced architectural concepts like SIEM architecture and deployment models, and data sources that are commonly used. Learn everything about Log Management like; dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts. This course will also teach you sources, types, and lifecycle of threat intelligence and give an introduction to threat hunting as well while diving deep into incident response lifecycle processes. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

Who Should Attend

- School students, graduates, professionals, career starters and changers, IT/Technology/Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity and is interested in SOC.
- This course is also helpful for IT professionals, SOC analysts, system security professionals, security engineers, threat management professionals, incident response teams, security administrators, vulnerability management professionals, and any cybersecurity professional.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Learn the basics of computer networks Dive deep into the cyber threat concepts like threats, vulnerabilities, and attacks. Gain insights into the Security Operations Center (SOC) architecture and learn the importance, workflow, and processes of SOC. Understand advanced architectural concepts like SIEM architecture and deployment models. Learn what log management is and its key parts, like events, logs, and incidents. Learn how you can perform centralized management of logs. Gain knowledge on dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts. Discover the sources, types, and lifecycle of threat intelligence and get introduced to threat hunting. Deep dive into the Incident response lifecycle.

Detailed Course Outline

Module 1: Computer Network and Security Fundamentals

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

Module 2: Fundamentals of Cyber Threats

- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Vulnerability
- Threats & Attacks
- Example of Attacks
- Network-based Attacks
- Application-based
- Host Based Attacks
- Insider Attacks
- Malware (Viruses, Worms, Ransomware, etc.)
- Phishing and Social Engineering

Module 3: 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

Module 4: SOC Components and Architecture

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

Module 5: 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

Module 6: Incident Detection and Analysis

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

Module 7: 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

Module 8: Incident Response and Handling

- Incident Handling Process
- Incident Classification and Prioritization
- Incident Response Lifecycle
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Post-Incident Analysis and Reporting

Frequently Asked Questions

Q: What delivery options are available for EC-Council SOC Essentials (SCE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day EC-Council SOC Essentials (SCE) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council SOC Essentials (SCE) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council SOC Essentials (SCE)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council SOC Essentials (SCE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for EC-Council SOC Essentials (SCE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council SOC Essentials (SCE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)