SOC Level 2

Category: Networking & Security | **Vendor:** TCM Security

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Related Exam:	SOC Level 2; SOC

Course Overview

Security Operations (SOC) 201 is an advanced course designed to elevate your ability to detect, investigate, and respond to complex cyber threats at scale. Building on the foundational skills from SOC 101, this course focuses on developing an effective investigative methodology and mastering the responsibilities of an Incident Responder or Threat Hunter. Through hands-on labs and realistic scenarios, you'll investigate sophisticated threats across enterprise environments, applying advanced techniques aligned with the MITRE ATT&CK framework. The curriculum emphasizes proactive threat hunting as part of a continuous detection and response cycle, helping analysts identify active threats, uncover security gaps, and improve future investigations. By the end of the course, you'll be equipped with the mindset, tools, and methodologies needed to confidently investigate incidents, trace root causes, and respond effectively to advanced adversaries. This course includes an Exam Vouchers for TCM Security's Practical SOC Analyst Professional (PSAP) certification – Launching September 2025. Each exam voucher includes 1 exam attempt and is valid for 12-months from the course completion date or certification release date.

About This Course

Security Operations (SOC) 201 is an advanced course designed to elevate your ability to detect, investigate, and respond to complex cyber threats at scale. Building on the foundational skills from SOC 101, this course focuses on developing an effective investigative methodology and mastering the responsibilities of an Incident Responder or Threat Hunter. Through hands-on labs and realistic scenarios, you’ll investigate sophisticated threats across enterprise environments, applying advanced techniques aligned with the MITRE ATT&CK framework. The curriculum emphasizes proactive threat hunting as part of a continuous detection and response cycle, helping analysts identify active threats, uncover security gaps, and improve future investigations. By the end of the course, you'll be equipped with the mindset, tools, and methodologies needed to confidently investigate incidents, trace root causes, and respond effectively to advanced adversaries. This course includes an Exam Vouchers for TCM Security’s Practical SOC Analyst Professional (PSAP) certification – Launching September 2025. Each exam voucher includes 1 exam attempt and is valid for 12-months from the course completion date or certification release date.

Who Should Attend

SOC 201 is designed for individuals seeking to advance their defensive security skills beyond foundational knowledge. Ideal candidates include those already familiar with core SOC concepts who are ready to develop expertise in investigating and responding to sophisticated cyber threats. This course is suited for Tier 2 Security/SOC Analysts, Tier 3 Security/SOC Analysts, Incident Responders, Threat Hunters, Digital Forensic Examiners.

Prerequisites & Entry Requirements

General Prerequisites:

This course relies heavily on working with IR investigations and forensic artifacts, but does not cover learning basic analysis tools. It is strongly recommended to have taken or be familiar with the Security Operations (SOC) 101 material and its prerequisites, which includes experience with:

- Networking Fundamentals: Practical Help Desk (PHD) or equivalent
- Operating System Fundamentals: Practical Help Desk (PHD) or equivalent
- Security Operations Fundamentals
- Network Traffic Analysis
- Endpoint Security Monitoring
- Log Analysis and Management
- Security Information and Event Management (SIEM)
- Basic Digital Forensics Exposure

Learning Outcomes

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

Develop a robust and reliable investigator's mindset to approach incidents methodically Learn industry-standard methodologies and tools for detecting, hunting, and responding to cyber threats across enterprise environments Gain experience performing incident response and threat hunting at scale Learn to investigate and identify advanced adversary tactics following the MITRE ATT&CK framework, including execution artifacts, lateral movement, credential theft, living off the land techniques, persistence, defense evasion, command and control, and many more Learn to perform effective attack timeline analysis, and guide effective incident response and remediation efforts Investigate the root cause of security incidents by uncovering the entry point

Detailed Course Outline

Day 1:

- Understanding the modern adversary
- Introduction to incident response
- Incident decision making
- Introduction to threat hunting
- Threat hunting teams, data sources, and maturity models
- Cyber threat intelligence
- Exploring the MITRE ATT&CK Navigator
- Structured and unstructured threat hunting
- Data transformation techniques
- Data transformation in the command-line, PowerShell, and Splunk
- Searching, aggregations, statistics, and visualizations

Day 2:

- Understanding and categorizing anomalies
- Masquerading
- Ambiguous identifiers
- Frequency and volume anomalies
- Temporal anomalies
- Location and environmental anomalies
- Structure and format anomalies
- Absence and suppression anomalies
- Entropy analysis
- Dissecting threat reports
- Threat hunting lab
- Tracing an attack chain
- Hunting execution
- Hunting malicious process trees
- Hunting persistence
- Hunting defense evasion
- Hunting command and control
- Hunting lateral movement

Day 3:

- Collection at scale
- Collection with WMI
- PowerShell 101
- PowerShell remoting
- Remote collection frameworks
- Triage artifact collection with KAPE
- Incident response with Velociraptor
- Windows memory structures
- The Volatility framework
- Process analysis
- Command line analysis
- Network analysis
- Registry analysis

Upcoming Schedule

Available training dates for SOC Level 2:

Start Date	End Date	Location	Delivery	Price
21 Sep 2026	23 Sep 2026	Online	Virtual	€1,999.00
07 Dec 2026	09 Dec 2026	Online	Virtual	€1,999.00

Frequently Asked Questions

Q: What delivery options are available for SOC Level 2?

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: Which exam does this course prepare me for?

This course prepares you for the SOC Level 2; SOC official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day SOC Level 2 course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the SOC Level 2 training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for SOC Level 2?

Yes, we provide corporate training, dedicated training, and closed classes for SOC Level 2. 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 SOC Level 2?

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 SOC Level 2 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)