Networking to Security Operations Centre [SOC] Operations Course

Introduction

Cybersecurity capability depends on more than awareness alone. Organisations need personnel who understand how networks operate, how security controls fit together, how threats are detected, and how incidents are escalated within a Security Operations Centre (SOC) environment.

The 10-Day Networking to SOC Pathway provides a structured development route for individuals entering the cybersecurity field or strengthening their technical foundations. Delivered by Mercury EW in collaboration with SudoCyber, the course uses SudoCyber's technical course material to provide a practical and progressive learning experience aligned to recognised cybersecurity pathways.

The programme bridges the gap between networking fundamentals, security operations, incident response thinking, and the realities of working in or alongside a SOC. It is designed to support learners as they develop the confidence, vocabulary, and technical understanding required to contribute more effectively within cyber security environments.

A key feature of this course is its progression towards CompTIA accreditation, giving learners a recognised development pathway while ensuring the training remains practical, relevant, and grounded in real-world cyber operations.

Throughout the course, learners will explore how networks function, how threats move through systems, how logs and alerts support detection, and how analysts investigate, escalate, and communicate cyber incidents. The course is particularly valuable for organisations seeking to grow internal cyber capability, reduce reliance on external recruitment, and create a clearer pathway into SOC and cybersecurity roles.

What you will learn:

- Core networking principles, including OSI model, TCP/IP, ports, protocols, DNS, DHCP, routing, and segmentation
- How common network services and infrastructure support business operations
- Security fundamentals, including authentication, access control, endpoint protection, email security, and secure configuration
- How cyber threats exploit networks, users, systems, and misconfigured environments
- The purpose and function of a SOC
- How alerts, logs, and indicators of compromise are used to support investigation
- Introduction to incident response, escalation, containment, and recovery thinking
- How frameworks such as the cyber kill chain and MITRE ATT&CK support analyst understanding
- The role of communication, prioritisation, and decision-making within SOC operations
- How technical knowledge supports progression towards recognised CompTIA accreditation
- Practical approaches to building confidence for entry-level cyber and SOC roles

Who should attend?

This course is designed for individuals moving into cybersecurity, technical support, SOC operations, or cyber-adjacent roles who require a structured foundation in networking, security concepts, and operational cyber awareness. It is particularly relevant for:

- **Junior cyber security analysts**
- **IT support and service desk personnel**
- **Network technicians and administrators**
- **Personnel transitioning into cyber roles**
- **Graduates, apprentices, and early-career cyber professionals**
- **Organisations developing internal cyber talent pipelines**

The course is suitable for learners with limited cybersecurity experience, although a basic familiarity with IT systems would be beneficial. The programme is designed to build confidence progressively, moving from core networking principles through to practical SOC awareness and incident response thinking.

Key Organisations

Ministry of Defence

Government Departments and Agencies

Defence and Security Organisations

Critical National Infrastructure (CNI) Providers

Managed Service Providers and SOC Teams

Commercial Organisations developing internal cyber capability

Any organisation seeking to build technical cyber skills and support progression towards recognised accreditation

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility