



SOC Analyst

Our **five day** GCHQ certified Security Operations Centre (SOC) Analyst course puts you at the forefront of your organisation, monitoring for potential network security incidents. The course has been designed by operational SOC professionals to give you insight into the mind of an attacker, and the vendor agnostic skills and operational knowledge required to work in a fully functioning SOC.

Aim

Acquire the necessary technical skills and knowledge for an entry level analyst or practitioner to function effectively in a fully operational SOC.

Who Should Attend?

- IT professionals who wish to progress their career by working within a SOC
- Those with a keen interest in cyber security and who feel they have the necessary aptitude to succeed in a technically demanding role
- Graduates with relevant qualifications, and who are seeking to gain employment in a SOC
- Professionals newly recruited into a SOC without prior experience in security.

Learning Objectives

- Understand the principles of Security Operations and how they are applied
- Be able to discuss relevant terminology and the typical roles and responsibilities within a SOC
- Gain an understanding of the cyber threat landscape including intelligence analysis and sources, baselining and analytics
- Comprehend the requirements for compliance and reporting guidelines in areas such as PCI-DSS and ISO 27001
- Address the requirements for case management, compliance and reporting guidelines
- Understand a typical Security Operations Architecture setup
- Understand the techniques employed within a SOC to extract and analyse large quantities of data.



Certified Training

