GTC Transforming Emerging Economies

GTC International Consulting Limited
Riverbank House
1 Putney Bridge Approach
Fulham, London, SW6 3BQ
T: +44(0)2037055710
E:enquiries@thegtcgroup.com
W: www.thegtcgroup.com

Security Operations & SOC Management

COURSE OVERVIEW

This course provides a detailed explanation of how organizations establish, operate, and mature Security Operations Centers (SOCs) to effectively detect, prevent, and respond to cybersecurity threats. It covers the structure and functions of SOCs, core security operations processes, monitoring and analysis tools (SIEM, SOAR, IDS/IPS, threat intelligence platforms), and the integration of automation to enhance efficiency. Participants will learn about incident triage, escalation workflows, log analysis, and continuous monitoring, as well as key frameworks such as MITRE ATTACK and NIST CSF. The course also emphasizes governance, staffing models, performance metrics, and compliance considerations.

WHO SHOULD ATTEND?

This course is designed for SOC analysts, cybersecurity engineers, IT security professionals, incident responders, network administrators, and managers seeking to enhance their operational expertise. It is equally valuable for business leaders, and auditors aspiring to enter cybersecurity roles, and who want a strong understanding of SOC structures, workflows, and technologies.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Operate core SOC tools and technologies for monitoring, detection, and response.
- Apply incident detection and triage processes using industry frameworks.
- Integrate threat intelligence into daily SOC operations.
- Manage escalation procedures and cross-team communication during incidents.
- Implement SOC governance models, staffing approaches, and performance metrics.
- Align SOC practices with international standards and compliance requirements.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- Comprehensive coverage of SOC structures, roles, and workflows.
- Practical learning with SIEM, SOAR, IDS/IPS, and threat intelligence tools.
- Application of MITRE ATT&CK framework for threat detection and response.
- Best practices in incident triage, escalation, and response management.
- Exploration of automation and AI in SOC operations.
- Guidance on SOC maturity models and performance measurement.
- Alignment with global frameworks such as NIST, ISO 27001, and CIS controls.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.
1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded.