Atos

A unique Security Operations Centre skills Bootcamp provides Atos with a range of new Cyber Security capabilities.

Working closely with Atos, QA's Cyber Security skills development division built a tailored 'Boot camp' training programme that enabled existing IT staff to retrain as Security Operation Centre (SOC) Analysts, providing them with a new set of highly skilled Cyber Security professionals.

The SOC Bootcamp programme for Atos was built on the trusted Cyber Curriculum authored by QA and was designed to deliver the skills needed to help them respond to security incidents and vulnerabilities.

Through the re-skilling of existing IT Technical employees, the programme ensured maximum return on training investment and enabled the organisation to rapidly develop and deploy essential Cyber Security skills into their business.

The training and development of this specific Cyber Security role - The SOC Analyst - provides them with the platform to help improve operational security by developing specific capability in:

- Incident Response and Management
- Intrusion Analysis
- Vulnerability Management
- Penetration Testing

- Security Information Event Management (SIEM)
- Information Security and Risk Management
- Security Testing

Developing the skills to protect from within

Recognising the need to provide both theory and practical learning, the QA's Cyber Lab offered delegates the perfect learning environment.

With hands-on exercises and scenario based learning - led by QA's expert Cyber Security instructors - the opportunity to practice with security tools and techniques of Cyber Security in a safe environment meant that delegates returned to their workplace with new skills that could be immediately applied.

> "The QA SOC Programme has had a significant impact in developing our new Cyber Security staff and closing the skill gap.
>
> There is a critical shortage of Cyber Security specialists in the industry, and this programme has allowed us to meet this challenge head-on."
>
> *Phil Aitchison, Director of Cyber Security*

QA
transforming performance
through learning

Industry recognised Cyber skills

The Atos SOC Bootcamp programme was specifically designed to enable delegates to gain a set of Cyber Security skills.

Using QA instructors and content, coupled with industry recognised learning paths and certifications, the outcomes from the programme meant that attendees left with deployable Cyber Security skills that are recognised by the IISP skills framework.

Skills to protect

Information Security Management - Determining, establishing and maintaining appropriate governance for (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including policies, standards and guidelines), and cost effective solutions for (including impact of third parties) information security within the organisation (IISP Ref; A1, A2, A3).

Information Risk Management - Capable of articulating the different forms of threat to, and vulnerabilities of, information systems and assets (IISP Ref; B1).

Implement Secure Systems - Comprehends the common technical security controls available to prevent, detect and recover from security incidents and to mitigate risk (IISP Ref; C1).

Security Testing - Develops and applies standards and strategies for verifying that measures taken mitigate identified risks (IISP Ref; D2).

Operational Security Management - Capable of reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security polices, standards and procedures and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations (IISP Ref; E1, E3).

Incident Management Investigation - (IISP Ref: F1, F2) Capable of triaging and supporting the investigation of an information security incident.

If you would like more details on the SOC Academy Programme, or courses and certifications in Cyber

Please contact QA on 0345 074 7978 or visit QA.COM/SOC.