

Cyber Operations Engineer

Dublin, Co. Dublin, Ireland

Job Description

Career Level: 5 | Career Family: Digital and Technology | Career Sub-Family: IT Security

The role also supports cyber security projects, security reviews, SOC activities, incident response and the secure adoption of emerging technologies including Artificial Intelligence.

Responsibilities

1. Act as a champion for vulnerability management, cloud security and cyber security best practices across daa, helping to improve security awareness and reduce organisational risk.
2. Monitor, assess and prioritise vulnerabilities across daa infrastructure, cloud platforms, applications and Operational Technology environments, ensuring risks are understood and addressed in line with business priorities.
3. Communicate remediation priorities to technical and business stakeholders and coordinate remediation activities with IT owners, service providers and vendors to reduce cyber risk.
4. Manage the outsourced vulnerability management service provider, ensuring effective delivery of agreed services, governance, reporting, continuous improvement and adherence to daa security standards and processes.
5. Develop and maintain vulnerability management standards, procedures, metrics, dashboards and governance processes to support operational and management decision making.
6. Monitor emerging vulnerabilities, zero-day threats, threat intelligence and attack techniques, assessing relevance to daa and supporting appropriate response and mitigation activity.
7. Support the delivery of cyber security reviews, assessments, projects, strategic initiatives and continuous improvement activities across new and existing technologies.
8. Support Security Operations Centre activities including cyber security monitoring, investigations, incident response, cyber exercises, tabletop simulations and lessons learned reviews.
9. Support initiatives relating to Artificial Intelligence, automation and emerging technologies, helping ensure associated cyber security risks are appropriately managed.

Note: The successful candidate may be required to participate in an on-call rota to support cyber operations and incident response activities outside normal business hours. This may

include supporting the investigation, management and recovery of cyber security incidents, major service-impacting security events and other urgent cyber response activities.

Qualifications

Experience

At least 5 years' experience in IT and/or Cyber Security, including strong experience in Vulnerability Management, Cyber Security Engineering, Security Operations, Cloud Security or a related discipline. Experience working in complex operational environments supporting critical infrastructure, internal stakeholders, technology vendors, managed service providers and outsourced security service providers is required. Experience supporting governance, audit, compliance or cyber security improvement initiatives is also desirable.

Skills

Suitable candidates should have experience of vulnerability management processes, technologies and remediation practices; cloud security principles, governance and cloud vulnerability management; OT or industrial control system security concepts; cyber security technologies including incident response, threat assessment, malware analysis and investigation of Indicators of Compromise; SOC, SIEM, EDR/XDR and threat intelligence technologies; security frameworks including ISO27001, NIST Cyber Security Framework, MITRE ATT&CK and Cyber Essentials; risk management, remediation planning, reporting, metrics, stakeholder communication, project delivery, vendor management, Artificial Intelligence security considerations and emerging cyber threat trends. Strong communication and presentation skills are required, with the ability to engage both technical and non-technical audiences.

Education & Qualifications

Suitable candidates should have an Honours Bachelor's Degree and/or Master's Degree, or equivalent, in Cyber Security, Information Technology, Computer Science, Engineering or a related discipline.

Mandatory Practicing/Training/Compliance Certification

Relevant cyber security certifications such as CISSP, CISM, CySA+, Microsoft security certifications, cloud security certifications, vulnerability management certifications or incident response certifications are desirable.

Professional Memberships

Professional membership of a recognised cyber security, information security, technology or risk management body is desirable but not mandatory.