APPRENTICESHIP STANDARD FOR CYBER INTRUSION ANALYST

Role Profile

The primary role of a Cyber Intrusion Analyst is to detect breaches in network security for escalation to incident response or other determined function. An Intrusion Analyst will typically use a range of automated tools to monitor networks in real time, will understand and interpret the alerts that are automatically generated by those tools, including integrating and correlating information from a variety of sources and in different forms and where necessary seek additional information to inform the Analyst's judgement on whether or not the alert represents a security breach. When an Analyst has decided that a security breach has been detected, he or she will escalate to an incident response team, or other determined action, providing both notification of the breach and evidence with reasoning that supports the judgement that a breach has occurred. An Analyst will typically work as part of a team (or may lead a team) and will interact with external stakeholders, including customers and third party sources of threat and vulnerability intelligence and advice.

Typical Rob Roles: Secure Operations Centre (SOC) Analyst, Intrusion Analyst, Network Intrusion Analyst, Incident Response Centre (IRC) Analyst, Network Operations Centre (NOC) Security Analyst

Entry Requirements

Individual employers will set the selection criteria, but this is likely to include A' Levels, level 3 apprenticeship or other relevant qualification relevant experience and/or an aptitude test with a focus on functional maths.

Technical Competencies

- Integrates and correlates information from various sources (including log files from different sources, network monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a network security breach.
- Recognises anomalies in observed network data structures (including. by inspection of network packet data structures) and network behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.
- Accurately, impartially and concisely records and reports the appropriate information, including the ability to write reports (within a structure or template provided).
- Recognises and identifies all the main normal features of log files generated by typical network appliances, including servers and virtual servers, firewalls, routers.
- Recognises and identifies all the main features of a normally operating network layer (including TCP/IP, transport and session control or ISO OSI layers 2-5), including data structures and protocol behaviour, as presented by network analysis and visualisation tools.
- Uses and effects basic configuration of the required automated tools, including network monitoring and analysis tools, SIEM tools, correlation tools, threat & vulnerability databases.
- Undertakes root cause analysis of events and make recommendations to reduce false positives and false negatives.
- Interprets and follows alerts and advisories supplied by sources of threat and vulnerability (including OWASP, CISP, open source) and relate these to normal and observed network behaviour.
- Undertakes own research to find information on threat and vulnerability (including using the internet).
- Manages local response to non-major incidents in accordance with a defined procedure.
- Interacts and communicates effectively with the incident response team/process and/or customer incident response team/process for incidents.
- Operates according to service level agreements or employer defined performance targets.

Technical Knowledge and Understanding

- Understands IT network features and functions, including virtual networking, principles and common practice in network security and the OSI and TCP/IP models, and the function and features of the main network appliances
- Understands and can utilise at least three Operating System (OS) security functions and associated features.
- Understands and can apply the foundations of information and cyber security including: explaining the importance of cyber security and basic concepts including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat' as well as explaining how the concepts relate to each other and the significance of risk to a business.
- Understands and can propose appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands and can propose how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understands lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.

- Understands and can advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.
- Understands the main features and applicability of law, regulations and standards (including Data Protection Act/Directive, Computer Misuse Act, ISO 27001) relevant to cyber network defence and follows these appropriately.
- Understands, can adhere to and can advise on the ethical responsibilities of a cyber security professional.

Underpinning Skills, Attitudes and behaviours

- Logical and creative thinking skills
- Analytical and problem solving skills
- Ability to work independently and to take responsibility
- Can use own initiative
- A thorough and organised approach
- Ability to work with a range of internal and external people
- Ability to communicate effectively in a variety of situations
- Maintain productive, professional and secure working environment
- Ability to interpret written requirements and technical specification documents
- Effective telephone and e mail skills, including ability to communicate effectively with strangers under pressure, including reporting a security breach

Qualifications

Apprentices must achieve each of the Ofqual-regulated Knowledge Modules, as summarised below. Further details are available in the occupational brief available from the Tech Partnership at www.thetechpartnership.com/apprenticeship/cyberintrusionanalyst

Knowledge Modules
Knowledge Module 1: Networks (for level 4 Cyber Intrusion Analyst Apprenticeship)
Knowledge Module 2: Operating Systems (for level 4 Cyber Intrusion Analyst Apprenticeship)
Knowledge Module 3: Information and Cyber Security Foundations (for level 4 Cyber Intrusion Analyst Apprenticeship)
Knowledge Module 4: Business Processes (for level 4 Cyber Intrusion Analyst Apprenticeship)
Knowledge Module 5: Law, Regulation and Ethics (for level 4 Cyber Intrusion Analyst Apprenticeship)

English and Maths

Level 2 English and maths will need to be achieved, if not already, prior to taking the end point assessment.

Professional Recognition: This apprenticeship is recognised for entry to IISP Associate Membership and for entry onto the Register of IT Technicians confirming SFIA level 3 professional competence. Those completing the apprenticeship are eligible to apply for registration.

Duration: The duration of this apprenticeship is typically 24 months.

Level: This is a level 4 apprenticeship.

Review date: This standard will be reviewed in December 2017.