CYBER SECURITY TECHNICIAN

GK Apprenticeships™
formerly Partnership Development Solutions (PDS) Ltd.

Details of standard

Occupation summary

This occupation is found in all sectors where information is held digitally and where that information is an asset that needs to be protected including but not limited to finance, retail, telecoms, health, media, manufacturing and local authorities.

The broad purpose of the occupation is to provide first line cyber security support. This requires individuals to monitor and detect potential security threats and escalate as necessary and to support secure and uninterrupted business operations of an organisation through the implementation of cyber security mechanisms and the application of cyber security procedures and controls. To contribute to the delivery of a security culture across an organisation, understanding vulnerabilities and threats and supporting the development of an organisation's cyber security maturity. To apply procedures and controls to maintain security and control of an organisation, and process security requests ensuring confidentiality, integrity and availability of information stored digitally.

In their daily work, an employee in this occupation interacts with a wide range of stakeholders including colleagues, managers, customers and internal and external suppliers. They would typically work as a member of a team; this may be office based or virtual. The employee will interact with, and influence colleagues and will have working level contact with customers, suppliers and partners in their capacity as an individual contributor.

An employee in this occupation will be responsible for supporting a cyber security function (frequently a Security Operations Centre or Network Operations Centre) working under supervision. The employee will be conducting specific cyber security tasks to defined procedures and standards. Specific cyber security mechanisms and controls that an individual would be required to implement would include: patching software, installing software updates, implementing access control, configuring firewalls, security incident and event management tools (SIEM) tools and protection tools (Anti-virus, Anti-malware, Anti-spam). They will be responsible for their own activities with other resources made available to them as required. As directed, the employee will engage with specific cyber security events. The employee will be expected to work with internal and external stakeholders under general direction. They will use discretion in identifying and responding to complex issues and assignments and will usually receive specific instructions and will have work reviewed at frequent milestones. They will be expected to determine when issues should be escalated to a higher level.

Typical job titles include:

Cyber Security Administrator, Access Control Administrator, Incident Response Technician, Junior Security Operations Centre (SOC) Analyst, Junior Information Security Analyst, Junior Threat and Risk Analyst, Junior Penetration Tester, Junior Security Analyst

---

Occupation duties

Duty	KSBs
Duty 1 Apply procedures and controls to maintain security and control of an organisation.	K1 K2 K3 K4 K7 K29

	S1 S2 S21 S22 B2 B4
Duty 2 Contribute to the production and development of security culture across an organisation including assisting with the promotion of cyber security awareness programmes, monitoring the effectiveness of cyber security awareness programmes, promoting an effective cyber security culture	K4 K5 K6 K7 K25 K29 K30 S3 S4 S21 S22 B5 B6
Duty 3 Process cyber security helpdesk requests ensuring confidentiality, integrity and availability of digital information, meeting relevant legal and regulatory requirements for example access control requests.	K4 K7 K8 K22 K26 S1 S5 S21 S22 B1 B2 B3 B4 B5 B6
Duty 4 Conduct the installation and maintenance of technical security controls in accordance with relevant procedures and standards.	K1 K3 K8 K9 S1 S2 S6 S21 S22 B1 B2 B4
Duty 5 Monitor, identify, report and escalate information security incidents and events in accordance with relevant procedures and standards.	K1 K2 K7 K10 K17 K19 S1 S7 S8 S21 S22 B1 B2 B3 B4 B5 B6
Duty 6 Administer cryptographic and certificate management activities in accordance with relevant procedures and standards.	K3 K9 S1 S2 S6 B1 B2 B4
Duty 7 Conduct regular review of access rights to digital information assets in accordance with relevant procedures and standards.	K1 K2 K3 K11 K12 S1 S2 S9 B1 B2 B4
Duty 8 Maintain an asset register of controlled environments in accordance with relevant policies, procedures and standards.	K1 K2 K3 K12 S1 S10 B1 B2 B4
Duty 9 Assist with backup and recovery processes in accordance with relevant policies, procedures and standards.	K1 K2 K3 K13 K15 S1 S6 B1 B2 B4
Duty 10 Contribute to documenting the scope and	K1 K2 K14 K15 K16 K17 K18

evaluating the results of vulnerability assessments in accordance with management requirements.	S1 S11 S12 B1 B2 B4 B5 B6
Duty 11 Contribute to risk assessments and escalate where appropriate in accordance with relevant procedures and standards.	K1 K2 K4 K19 K20 K27 S1 S14 S15 S21 S22 B1 B2 B4 B5
Duty 12 Contribute to routine threat intelligence gathering tasks.	K1 K2 K4 K16 S1 S13 B1 B2 B4 B5
Duty 13 Document incident and event information and incident, exception and management reports in accordance with relevant policies, procedures and standards.	K1 K2 K10 K17 K18 K19 K20 K21 S7 S8 S16 S17 S19 B1 B2 B4
Duty 14 Contribute towards the production and review of cyber security policies, procedures, standards and guidelines drawing on their experience of applying policies for example - acceptable use, incident management, patching, anti-virus, bring your own device (BYOD), access control, social media, password, data handling and data classification, information technology asset disposal	K1 K2 K4 K7 K20 K23 S18 S21 S22 B1 B2 B4 B5 B6
Duty 15 Monitor cyber security compliance and provide relevant data to auditors if required by the auditor.	K1 K2 K4 K6 K21 K24 K25 S19 S20 B1 B4 B5 B6
Duty 16 Collaborate with people both internally and externally to support secure and uninterrupted business operations of an organisation.	K1 K2 K4 K23 K25 K26 K28 K30 S1 S2 S4 S21 B1 B3 B4 B5 B6
Duty 17 Practice continuous self-learning to keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.	K4 K23 K24 K27 S22 B2 B3 B4 B7
Duty 18 Monitor and detect potential security threats and escalate in accordance with relevant procedures and standards.	K1 K16 K19 K26 S8 S13 S15 S22 B1 B2 B4

KSBs

Knowledge

K1: Principles of organisational information security governance and the components of an organisation's cyber security technical infrastructure including hardware, operating systems, networks, software and cloud

K2: Cyber security policies and standards based on an Information Security Management System (ISMS)

K3: Types of physical, procedural and technical controls

K4: Awareness of how current legislation relates to or impacts upon the occupation including Data Protection Act, Regulation of Investigatory Powers Act, Human Rights Act, Computer Misuse Act, Freedom of Information Act, Official Secrets Act, Payment Card Industry Data Security Standard (PCI-DSS), Wireless and Telegraphy Act, professional body codes of conduct, ethical use of information assets

K5: Cyber security awareness and components of an effective security culture, different organisational structures and cultures, the importance of maintaining privacy and confidentiality of an organisation's information and the impact of a poor security culture

K6: Principles of cyber security compliance and compliance monitoring techniques

K7: Core terminology of cyber security – confidentiality, integrity, availability (the CIA triad), assurance, authenticity, identification, authentication, authorization, accountability, reliability, non-repudiation, access control

K8: Common security administrative operational tasks e.g. patching, software updates, access control, configuring a range of firewalls, security incident and event management tools (SIEM) and protection tools (Anti-virus, Anti-malware, Anti-spam)

K9: Cryptography, certificates and use of certificate management tools

K10: Processes for detecting, reporting, assessing, responding to, dealing with and learning from information security events

K11: Principles of identity and access management - authentication, authorisation and federation - and the inter-relationship between privacy and access rights and access control, and the types of access control, access control mechanisms and application control

K12: Types of digital information assets used in a controlled environment and the need to maintain an inventory of information assets used in a controlled environment and the need for and practice of secure information asset disposal

K13: Disaster prevention and recovery methods and the need for continuity of service planning and how an organisation might implement basic disaster prevention and recovery practices using conventional and incremental secure backup and recovery techniques and tools both onsite and offsite including geographic considerations

K14: Categories of cyber security vulnerabilities and common vulnerability exposures –software misconfiguration, sensitive data exposure, injection vulnerabilities, using components with known vulnerabilities, insufficient logging and monitoring, broken access control and authentication, security misconfiguration, incorrect cross-site validation

K15: Components of a vulnerability assessment scope and techniques to evaluate the results of a vulnerability assessment and provide recommendations based upon the evidence provided by the vulnerability assessment tools. The impact that vulnerabilities might have on an organisation and common vulnerability assessment tools and their strengths and weaknesses

K16: Threat sources and threat identification and network reconnaissance techniques and the impact that threats might have on an organisation

K17: Types of information security events – brute force attack, malware activity, suspicious user behaviour, suspicious device behaviour, unauthorized system changes

K18: Computer forensic principles – the importance of ensuring that evidence is not contaminated and maintaining the continuity of evidence without compromising it

K19: Standard information security event incident, exception and management reporting requirements and how to document incident and event information as part of a chain or evidence

K20: Common information security policies – acceptable use, incident management, patching, anti-virus, BYOD, access control, social media, password, data handling and data classification, IT asset disposal

K21: Cyber security audit requirements, procedures and plans, need to obtain and document evidence in an appropriate form for an internal or external auditor to review

K22: The significance of customer issues, problems, business value, brand awareness, cultural awareness/ diversity, accessibility, internal/ external audience, level of technical knowledge and profile in a business context

K23: Evolving cyber security issues in the digital world including the application to critical national infrastructure, communications technologies, the need for information assurance and governance, control systems and internet of things (IoT) devises

K24: Different learning techniques and the breadth and sources of knowledge and sources of verified information and data

K25: Importance of maintaining privacy and confidentiality of an organisations information and the impact of a poor security culture

K26: Concepts of service desk delivery and how to respond to requests for assistance received by a service desk and be able to describe different methods of escalation, when to escalate to a higher level where necessary and the need to communicate accurately and appropriately during an escalation

K27: Risk assessment, risk management and business impact analysis principles

K28: How their occupation fits into the wider digital landscape and any current or future regulatory requirements

K29: How to use data ethically and the implications for wider society, with respect to the use of data

K30: Roles within a multidisciplinary team and the interfaces with other areas of an organisation

Skills

S1: Follow information security procedures

S2: Maintain information security controls

S3: Develop information security training and awareness resources

S4: Monitor the effectiveness of information security training and awareness

S5: Handle and assess the validity of security requests from a range of internal and external stakeholders

S6: Follow technical procedures to install and maintain technical security controls

S7: Monitor and report information security events

S8: Recognise when and how to escalate information security events in accordance with relevant procedures and standards

S9: Review and modify access rights to digital information systems, services, devices or data

S10: Maintain an inventory of digital information systems, services, devices and data storage

S11: Scopes cyber security vulnerability assessments

S12: Evaluate the results of a cyber security vulnerability assessment

S13: Perform routine threat intelligence gathering tasks through consulting external sources

S14: Undertake digital information risk assessments

S15: Identify and categorise threats, vulnerabilities and risks in preparation for response or escalation

S16: Document cyber security event information whilst preserving evidence

S17: Draft information management reports using standard formats appropriate to the recipients

S18: Review and comment upon cyber security policies, procedures, standards and guidelines

S19: Perform cyber security compliance checks

S20: Translate audit requirements and collate relevant information from log files, incident reports and other data sources

S21: Communication skills to co-operate as part of a multi-functional, multi-disciplinary team using a range of technical and non-technical language to provide an effective interface between internal or external users and suppliers

S22: Keep up-to-date with legislation and industry standards related to the implementation of cyber security in an organisation

Behaviours

B1: Manage own time to meet deadlines and manage stakeholder expectations

B2: Work independently and take responsibility for own actions within the occupation

B3: Use own initiative

B4: A structured approach to the prioritisation of tasks

B5: Treat colleagues and external stakeholders fairly and with respect without bias or discrimination

B6: Act in accordance with occupation specific laws, regulations and professional standards and not accept instruction that is incompatible with any of these

B7: Review own development needs in order to keep up to date with evolution in technologies, trends and innovation using a range of sources

Qualifications

English & Maths

Apprentices without level 2 English and maths will need to achieve this level prior to taking the End-Point Assessment. For those with an education, health and care plan or a legacy statement, the apprenticeship's English and maths minimum requirement is Entry Level 3. A British Sign Language (BSL) qualification is an alternative to the English qualification for those whose primary language is BSL.

Professional Recognition

This standard has professional recognition.

Body	Level
BCS - The Chartered Institute for IT	Associate BCS membership (AMBCS) and Professional
Registration for IT Technicians (RITTech)	
Chartered Institute for Information Security	/ Accredited Affiliate

Additional details

Occupational Level:

3

Duration (months):

18

Review

This apprenticeship standard will be reviewed after three years

Find an apprenticeship

Postcode (optional)