Overview of the role

Enabling organisations to protect, defend, and respond to cyber threats.

Contents

Hide menu

1. Key information
2. Occupational summary
3. Typical job titles
4. Occupation duties
5. Knowledge
6. Skills
7. Behaviours
8. Qualifications
9. Professional recognition
10. Consultation
11. Progression routes
12. Supporting uploads
13. Involved employers

Standard in development
L6: Cyber security technical professional (integrated degree)
Version 2.0

Title of occupation

Cyber security technical professional (integrated degree)

UOS reference number

ST0409

Core and options

No

Level of occupation

Level 6

Occupational maps data

Route: Digital
Pathway: Digital Support and Services
Cluster: Cyber security professional

Typical duration of apprenticeship

48 months

Degree apprenticeship

integrated degree

Resubmission

No

Would your proposed apprenticeship standard replace and existing framework?

No

Does professional recognition exist for the occupation?

Yes

Regulated occupation

Is this a statutory regulated occupation?

No

Occupational summary

This occupation is found in all sectors and organisations that employ technology, for example Digital, Telecoms, Technology, Business Services, Defence, Government, Finance, Health, Retail, Hospitality, Critical Infrastructure, Transport, Automotive sectors; and in all types and sizes of organisation including large corporates, public sector bodies, academic institutions, charities, and small and medium enterprise (SME).

The broad purpose of the occupation is to enable organisations to protect, defend, and respond to cyber threats.

In their daily work, an employee in this occupation interacts with a broad range of people from their own organisation and externally including suppliers and customers, technical specialists, non-specialists, peers and senior representatives. The roles are typically office or computer room/lab based. Some employers will also have security clearance requirements, which may impose residency or nationality restrictions.

An employee in this occupation will be responsible for understanding cyber threats and how to mitigate risks and consequences arising from them, and applying practical cyber security knowledge within legal, regulatory and ethical frameworks. All roles apply cyber security expertise in a business or organisational context. Cyber security requires analytical and creative problem solving, taking account of technical and sociotechnical (human) factors.

Typical job titles

Applied cryptosecurity specialist Cyber essentials auditor Cyber risk consultant Cyber security operations centre (csoc) analyst Governance, risk, and compliance (grc) analyst Incident response specialist Information assurance consultant Information security consultant Offensive security analyst/specialist Penetration tester ("ethical hacker") Security analyst Security architect Security engineer Security tester Threat hunter Threat intelligence analyst Vulnerability analyst

Are there any statutory / regulatory or other typical entry requirements?

No

Occupation duties

DUTY	KSBS
Duty 1 Conduct technical research on attack techniques and malware.	K1 K2 K3 K4 K5 K6 K7 K8 K11 K12 K13 K17 K20 K22 K24 S1 S2 S6 S7 S8 S9 S12 S14 S15 S20 S21 S22 S26 S27 B1 B6 B7 B9 B15 B16 B18
Duty 2 Conduct cyber security audit processes to assess security posture against regulations and standards.	K1 K10 K14 K15 K16 K19 K22 K24 S5 S11 S13 S16 S19 S20 S21 S26 B1 B2 B3 B6 B7 B9 B16 B17
Duty 3 Conduct business continuity and disaster recovery planning and incident response operations.	K1 K10 K12 K13 K21 K22 K23 K24 S1 S17 S21 S23 S26 S27 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B12 B14 B17
Duty 4 Conduct threat research and identify vulnerabilities in systems and organisations	K1 K2 K3 K4 K5 K6 K7 K8 K11 K12 K13 K15 K17 K20 K22 K24 S1 S2 S3 S6 S7 S8 S9 S12 S13 S14 S15 S20 S21 S22 S26 S27 B1 B6 B7 B9 B10 B13 B14 B15 B16 B18

DUTY	KSBS
and assess significance.	
Duty 5 Conduct cyber risk assessments.	K1 K7 K10 K11 K12 K14 K15 K16 K17 K18 K22 K23 K24 S1 S8 S12 S13 S15 S16 S20 S21 S26 B1 B2 B6 B7 B9 B10 B11 B14 B15 B16 B17
Duty 6 Apply cyber security to engineering design, development, (deploy, configure, operate) support and maintenance.	K1 K2 K3 K4 K5 K6 K7 K9 K10 K11 K12 K17 K18 K22 K23 K24 S1 S2 S4 S5 S6 S7 S8 S10 S11 S18 S19 S20 S21 S24 S26 S27 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15 B16 B17 B18
Duty 7 Detecting and responding to cyber security incidents and conducting technical investigations to determine the attack method and wider implications.	K1 K2 K3 K4 K5 K6 K7 K8 K11 K12 K15 K20 K21 K22 K24 S1 S2 S3 S6 S7 S8 S9 S12 S22 S23 S24 S26 S27 B1 B2 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15 B16 B17 B18
Duty 8 Understand and uphold legal, regulatory, cyber security professional codes of practice and ethical principles.	K1 K8 K13 K15 K16 K22 K24 S1 S3 S13 S20 S21 S22 S23 S24 S25 S26 S27 B3 B5 B6 B7 B9 B17
Duty 9 Maintain and improve a security management system to ensure it is effective and	K1 K11 K12 K16 K17 K18 K19 K21 K22 K23 K24 S1 S11 S13 S15 S16 S17 S18 S19 S21 S23 S24 S25 S26 B1 B2 B4 B5 B6 B7 B9 B10 B11 B14 B15 B16 B17 B18

DUTY	KSBS
compliant to relevant standards and regulations.	
Duty 10 Plan and execute safe and secure attack simulations to test system or organisational security.	K1 K6 K7 K11 K12 K17 K19 K20 K21 K22 K24 S1 S2 S8 S9 S12 S13 S14 S15 S20 S21 S23 S24 S26 B1 B2 B3 B4 B5 B6 B7 B9 B10 B13 B14 B15 B16 B17 B18
Duty 11 Identify means to evidence to a satisfactory level that security design, controls and measures are effective to achieve intended outcomes.	K1 K9 K10 K12 K14 K16 K17 K18 K19 K23 K24 S1 S4 S5 S6 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16 S17 S18 S19 S20 S21 S23 S24 S25 S B2 B3 B6 B7 B9 B10 B11 B12 B13 B15 B16 B17 B18
Duty 12 Continuously improve resilience by considering changing threat environment, new security approaches and lessons from experience.	K1 K8 K11 K12 K13 K15 K16 K17 K18 K19 K21 K23 K24 S1 S3 S8 S9 S10 S12 S13 S14 S17 S19 S20 S21 S22 S23 S25 S26 S27 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B13 B14 B15 B16 B17 B18

KSBs

Knowledge

K1: Foundations of cyber security, its significance, concepts considering confidentiality, integrity, availability, risk, threats, vulnerabilities and assurance and how they inter-relate.
K2: Foundations of network technology considering communications, internetworking, protocols, standards, performance, and security features.
K3: Foundations of data technology considering databases, machine learning, artificial intelligence, digital representation of systems, data governance, and security features.

K4: Foundations of processing architectures considering logic, memory, physical and virtual hardware, machine level coding, operational technology, logic controllers, and security features.
K5: Foundations of operating systems considering architectures, mechanisms, virtualisation, and security features.
K6: Foundations of algorithm and program design considering concepts, compiled, interpreted, object oriented, and scripting.
K7: Attack surface that arises from the interplay between software, hardware and industrial control or critical infrastructure environment.
K8: Foundations of reverse engineering malware.
K9: Secure by design engineering practices considering lifecycle, software and hardware composition, secure coding, code analysis, testing & patching, memory safety, and malware resistance.
K10: Secure by design engineering practices considering lifecycle, system engineering and service architecture, including supply chain.
K11: Threats, vulnerabilities, impacts and mitigations applied to digital systems.
K12: Human dimensions of cyber security.
K13: Methods and techniques for structured and ethical intelligence analysis and assessment.
K14: Methods and techniques for cyber security risk analysis and assessment.
K15: Approaches to evaluate the significance of risk assessments in the threat context to advise the organisation's risk stakeholders.
K16: UK and international standards, including ISO27001, EU NIS and UK GovAssure, for security management and their application in an organisation.
K17: Function and beneficial use of the different types of security controls and components, including for access, connectivity, identity, and integrity.
K18: Form and structure of a security case for an organisation's risk stakeholders.
K19: Methods and techniques to evidence confidence in the implemented security controls, resilience measures and supply chain, through life.
K20: Methods, tools and techniques for detecting threat actor activity and attacks, including indicators of compromise, threat actor tactics, techniques and procedures.
K21: Approaches to incident response including management, escalation, investigation, 3rd party involvement, supply chain, customers and wider stakeholders.
K22: Cyber security and data protection laws and regulations and ethical standards that are applicable in the UK.
K23: Essential role of wider organisational stakeholders and supply chain in achieving desired security outcomes.
K24: Security aspects of technology foundations when applied in real and relevant solutions.

Skills

S1: Apply an attackers perspective.
S2: Design, build, configure, optimise, test and troubleshoot complex networks.
S3: Apply data collection, processing and analysis tools and methods.
S4: Build, test and troubleshoot a digital system to a specification.
S5: Configure an operating system in accordance with recognised good practice, law, regulation and local security policy.
S6: Write, test, debug programs in high and low level languages and scripts.
S7: Design, implement and analyse algorithms for solving problems.

S8: Construct solutions involving software, physical systems and people and analyse for security exploits.
S9: Analyse malware and identify its mechanisms.
S10: Apply secure programming principles and design patterns to address security issues.
S11: Apply engineering and software development methodologies and models.
S12: Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.
S13: Evaluate the cyber risk arising from an organisation's culture and the effectiveness of individual roles and responsibilities.
S14: Undertake ethical system reconnaissance.
S15: Conduct cyber threat and risk modelling and analysis to determine their significance in a context.
S16: Undertake cyber risk assessments to external standards and frameworks.
S17: Apply an information security management system to develop an information security management plan.
S18: Configure and operate security technology components including boundary control, access control, attack detection, system audit, cryptography management, separation and virtualisation.
S19: Architect a system in accordance with a security case.
S20: Critically analyse secure architectural solutions and security controls against defined security objectives.
S21: Apply and justify an assurance approach to give sufficient basis for confidence that a solution meets its intended security outcomes.
S22: Proactively find threat actor activities in a system using monitoring, analysis, intrusion detection and threat hunting tools and methods.
S23: Execute incident response plans and procedures collaborating with internal and external stakeholders including suppliers, clients, authorities and specialists.
S24: Define scope of security testing and forensic investigation activities in accordance with legal and ethical requirements to meet security objectives.
S25: Develop and apply an information security policy or process to address an identified risk or to meet legal or regulatory requirements.
S26: Devise and integrate automation to optimise a cyber security function.
S27: Apply an intelligence lifecycle to cyber threat data in an organisational context.

Behaviours

B1: Produces clear written reports and presentations about complex issues.
B2: Makes concise, engaging and well-structured verbal presentations, arguments and explanations.
B3: Sensitive to the preferences, motivations, strengths and limitations of other people.
B4: Works effectively with others to achieve a common goal (Demonstrates effective teamwork).
B5: Leads, influences and persuades others (Leads in the sense that by their behaviour sets the right example).
B6: Gives feedback to beneficial effect and incorporates received feedback into his/her own learning and development (Giving & receiving feedback).
B7: Demonstrates professional behaviours, ethics and courtesies, timeliness and focus when faced with distractions, and completes tasks to deadlines meeting quality expectations (Be professional).

B8: Continues to apply expected methods and works in a structured way when under the pressures inherent in a crisis (for example a cyber security incident) (Continue to be professional in a crisis).
B9: Works independently with minimal supervision.
B10: Demonstrates balanced perspective considering the technology solution, business objectives and the user experience.
B11: Wins business commitment to support technology arguments with excellent persuasion.
B12: Deals with different, competing interests within and outside the organisation with excellent negotiation.
B13: Logical thinking and creative approach to problem solving.
B14: Anticipates potential issues and takes initiative to prevent problems or propose solutions.
B15: Demonstrates a 'security mind-set': shows a deep curiosity about how systems function, how they can be compromised, and how they can be secured (how to break as well as fix).
B16: Demonstrates inherent scepticism, persistent challenge and obsessive search for independent evidence (in cyber security to mitigate propaganda, 'fake news', ('vendor claims'), group think).
B17: Demonstrates a thorough approach to cyber security, showing meticulousness, accuracy, and a focus on progress towards intended outcomes.
B18: Exhibits a strong desire and ability to continuously learn, adapt to new information, and independently seek out knowledge to stay current and effective.

Qualifications

English and maths

English and maths qualifications must be completed in line with the apprenticeship funding rules.

Does the apprenticeship need to include any mandated qualifications in addition to the above-mentioned English and maths qualifications?

Yes

Other mandatory qualifications

BSC (Hons) Cyber Security Technical Professional Degree

Level: 6 (integrated degree)

Professional recognition

This standard aligns with the following professional recognition:

- UK Cyber Security Council for Associate

This standard partially aligns with the following professional recognition:

- The Crisis Resilience Professionals Guild for Member

In order to enter the Crisis Resilience Professionals Guild at Member Level, apprentices would need to complete the Guild's bite-size course entitled "The Introduction to Resilience & Security".

Consultation

The occupational standard and degree apprenticeship assessment plan (AAP) went out for consultation on Monday 26th October with results due back on Monday 9th November. Any feedback we receive as part of this public survey consultation will be fed into the development of the occupational standard and AAP.

Progression routes

Supporting uploads

Mandatory qualification uploads
Mandated degree evidence uploads
Professional body confirmation uploads
ST0409_standard_professional-body-confirming-alignment_Professional recognition.msg

Involved employers

QinetiQ (Chair of the employer group), Accenture, BAE Systems, BT, Cabinet Office, The Chartered Institute of Information Security (CIISec), DarkTrace, Department for Science, Innovation and Technology (DSIT), Department for Works and Pensions (DWP), Fox Red Risk, Fujitsu, IBM, Keibra, Lloyds Banking Group, Ministry of Housing, Communities & Local Government (MHCLG), Multiverse, Network Rail, PA, PwC, QA, Raytheon, Siemens, Sky, Specialist Hub, TechSkills, TechUK, UK Cyber Security Council

Other involved stakeholders

Birmingham City University, Blackpool and The Fylde College, City & Guilds, Liverpool John Moores University, MK:U, Cranfield University, Open University, University of Gloucestershire, University of Staffordshire

Subject sector area

6.1 Digital technology (practitioners)