TECH PARTNERSHIP

Digital Industries Apprenticeship: Occupational Brief

Cyber Intrusion Analyst

March 2016

Digital Industries Apprenticeships: Occupational Brief

Level 4 Cyber Intrusion Analyst

Minimum Standards and Grading Criteria

This paper defines the minimum requirements for the knowledge, skills and behaviours defined in the standard, which are required for a pass. It also defines the criteria to be used for awarding the grade for merit or distinction. This paper should be read in conjunction with the Standard and Assessment Plan for the Level 4 Software Developer Apprenticeship

Overview of Grading

There are three sets of criteria on which the assessment and grading is made. The three criteria are

The What: what the apprentice has shown they can do,

The How: the way in which the work has been done

The With Whom: The personal and interpersonal qualities the apprentice has brought to all their work relationships

Each of these three criteria has minimum (expected) requirements, which must be satisfied for a pass.

Each of these criteria has a number of dimensions which should be considered to determine if the apprentice is significantly above the minimum (expected) level of quality

The purpose of grading is to differentiate between those apprentices whose work is at the expected level of quality against the totality of the skills, knowledge and behaviours specified in the standard and those whose work is significantly above this expected level

For a pass, each of the three sets of criteria must demonstrate at least the expected (minimum requirement) level of quality

For a merit, the What has to be significantly above the level of quality and one of either the How or the With Whom has to be significantly above the level of quality expected

For a distinction, each of the three sets of criteria must be significantly above the expected level of quality

The assessor takes a holistic judgement of whether or not their assessments demonstrate that the apprentice is "significantly above the expected level of quality" in each of these three areas and can then determine which grade should be awarded

The what – what the apprentice has shown they can do

Minimum Requirements

The following table shows what the minimum, expected requirements are for a pass on this criteria

Competency Standard	**Minimum, expected, requirements for a pass**
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.	Analyst can correlate a proxy event log entry against DHCP records in order to identify the specific client that made a web request. Analyst can identify and prioritise a number of threats raised by the SIEM tool defining priorities based on research conducted against known threat and vulnerability data using multiple sources. Analyst can understand how data is indexed. Analyst can Interrogate indexed data. Analyst can understand DOS/Linux/Unix file structures. Analyst can understand of the importance of *how* a monitoring system should be considered. At the coarsest grain this should cover the need to monitor inbound and outbound traffic and what this contributes to situational awareness.
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.	Analyst can identify (from a sample of traffic) the delivery of an injected iframe from a capture conducted of a user visiting an infected website. Analyst can spot a large number of re-directs - as can happen when malvertising is used as an attack vector – eventually being able to identify a "known malicious" site as one of the redirects. Analyst can spot data exfiltration based on extremely large amounts of traffic being sent from a local client to a cloud services site. Analyst can recognise anomalous usage of port numbering and unusual association of port numbers to services. Analyst can capture traffic to create PCAP files from an interface and to Interrogate PCAP files.
Accurately, impartially and concisely records and reports the appropriate information, including the ability to write reports (within a structure or template provided).	Analyst can produce an executive summary style report covering a malware infection. Analyst can complete an incident report to a standard for delivery to a customer.

Recognises and identifies all the main normal features of log files generated by typical network appliances, including servers and virtual servers, firewalls, routers.	Analyst can recognise, for typical network appliances, time stamp, login and logout events, source and destination IP addresses, syslog messages, privilege escalation, source and destination port numbers, and configuration changes. Analyst can recognise, for servers, time stamp, login and logout events, hostname, usernames, privilege escalation, operating system event codes and critical, warning, or error events. Analyst can recognise basic log file structure types and log file source types.
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.	Analyst can recognise normal common network protocol exchanges. Analyst can recognise common malformed packets. Analyst can spot common abnormal protocol exchanges.
Uses and effects basic configuration of the required automated tools, including network monitoring and analysis tools, SIEM tools, correlation tools, threat & vulnerability databases.	Analyst can configure a packet analysis tool (e.g. TCPDump, Wireshark) to capture packets from an interface. Analyst can create a query to filter events for specific outcome e.g. find multiple user login failure over period of time. Analyst can configure a packet filter (e.g. Berkeley Packet Filter) for a specific outcome. Analyst can create a dashboard to visualise a collection of query outcomes in order to assist anomaly detection. Analyst can create a new query based on a threat database entry.
Undertakes root cause analysis of events and make recommendations to reduce false positives and false negatives.	Analyst can identify a malware infection from a PCAP traffic capture, following through to identification of the infected host, and then identifying through the use of SIEM tool, event logging and or Enterprise Anti-virus logging that the local AV had been disabled (could also do this if they were provided with access to a forensic image of the machine – or a copy of the local anti-virus logs). Analyst can identify cause of alerts generated by automated tools.
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.	Analyst can generate a basic signature for a known threat or vulnerability – e.g. a basic regex signature or at an even more basic level a straight string search of URL's for a known bad URL. Analyst can correlate information from multiple sources enabling corrective action to be implemented.
Undertakes own research to find information on threat and vulnerability (including using the internet).	Analyst can use a variety of different sources to validate information. Analyst can access commonly used/recommend online sources such as OWASP, CISP, ISS, CVE.

Manages local response to non-major incidents in accordance with a defined procedure.	Analyst can follow a defined procedure and is able to describe the procedures followed. Analyst can determine when to escalate an incident (i.e. incident is not 'non-major'). Analyst can take responsibility for management of a local response through to conclusion. Analyst can prioritise allocation of resources during an incident, and can remain calm under pressure. Analyst can correctly record the steps taken to resolutions and report as required.
Interacts and communicates effectively with the incident response team/process and/or customer incident response team/process for incidents.	Analyst can explain what's going on and what might need to be done clearly. Analyst can interact with and use workflow system e.g. ticket management tools. Analyst can do a shift handover effectively.
Operates according to service level agreements or employer defined performance targets.	Analyst can interpret a service level agreement and apply relevant parts in practice.

The What – what the apprentice has shown they can do

Criteria for a Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for what they have done

Dimensions	**Description of what significantly above the expected level of quality looks like**
Breadth – the range of tools and methods understand and applied	Understands and applies a wide range of tools and methods Accurately and appropriately applies and effectively implements the right tools and methods in a variety of different situations
Depth – the level to which these tools and methods are understood and applied	A sophisticated user - fully exploits the functionality/capability of the tools and methods

	Extensive and deep understanding of different tools and methods and how and why they can be applied in different contexts
Complexity – the extent and prevalence of inter-related and inter-dependant factors in the work and how well the apprentice has dealt with these	Deals confidently and capably with a high level of interrelated and interdependent factors in their work

The how: the way in which the work has been done

The following table shows what the minimum, expected requirements are for a pass on this criteria

Competency Standard	**Minimum expected requirements for a pass**
Apprentices can demonstrate the full range of skills, knowledge and behaviours required to fulfil their job role	Knows what skills, knowledge and behaviours are needed to do the job well Are aware of their own strengths in the job role, and any areas for improvement Appreciate who else is important, for them to do their job and fulfil the role effectively (e.g. colleagues, managers, other stakeholders) Are aware of potential risks in the job role (e.g. security, privacy, regulatory) Use personal attributes effectively in the role, e.g. entrepreneurship Understand how the job fits into the organisation as a whole
Apprentices can demonstrate how they contribute to the wider business objectives and show an understanding of the wider business environments	Understands the goals, vision and values of the organisation Aware of the commercial objectives of the tasks/ projects they are working on Understands the importance of meeting or exceeding customers' requirements and expectations Is in tune with the organisation's culture Aware of the position and contribution of the organisation in the economy Understands the key external factors that shape the way the organisation function, e.g. regulation Knows how the organisation can gain advantage in the industry, e.g. through innovation, technology, customer service etc.
Apprentices can demonstrate the ability to use both logical and creative thinking skills	Logical thinking:

when undertaking work tasks, recognising and applying techniques from both.	- Understands initial premise(s) and preconditions - Recognises the conclusion to be reached - Proceeds by rational steps - Evaluates information, judging its relevance and value - Supports conclusions, using reasoned arguments and evidence Creative thinking: - Explores ideas and possibilities - Makes connections between different aspects - Adapts ideas and approaches as conditions or circumstances change
Apprentices can show that they recognise problems inherent in, or emerging during, work tasks, and can tackle them effectively	Problem-solving: - Analyses situations - Defines goals - Develops solutions - Prioritises actions - Deals with unexpected occurrences

The How: the way in which the work has been done

Criteria for a Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for the way in which the work has been done

Dimensions	**Description of what significantly above the expected level of quality looks like**
Responsibility – the scope of responsibility and level of accountability demonstrated in the apprentices work	Undertakes work that is more complex, more critical or more difficult Works independently and takes high level of responsibility

Initiative	Independently demonstrates an ability to extend or enhance their approach to work and the quality of outcomes Doesn’t just solve the problem but explores creative or innovative options to do it better, more efficiently, more elegantly or to better meet customer needs
Delivery focus – the extent to which the apprentice has shown they can grasp the problems, identify solutions and make them happen to meet client needs	Shows strong project management skills, in defining problem, identifying solutions and making them happen Demonstrates a disciplined approach to execution, harnessing resources effectively Drives solutions – with a strong goal focused and appropriate level of urgency

The with whom: the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Minimum Requirements

The following table shows what the minimum, expected requirements are for a pass on this criteria

	Minimum expected requirements for a pass
Apprentices can manage relationships with work colleagues, including those in more senior roles, customers/clients and other stakeholders, internal or external and as appropriate to their roles, so as to gain their confidence, keep them involved and maintain their support for the task/project in hand Apprentices can establish and maintain productive working relationships, and can use a range of different techniques for doing so.	Managing relationships: • Understands the value and importance of good relationships • Influences others by listening to and incorporating their ideas and views • Acknowledges other people's accomplishments and strengths • Manages conflict constructively • Promotes teamwork by encouraging others to participate Customer/client relationships: • Understands their requirements, including constraints and limiting factors • Sets reasonable expectations • Involves them in decisions and actions • Interacts positively with them • Provides a complete answer in response to queries ('transparency', 'full disclosure') Stakeholders: • Understands who they are and what their 'stake' is • Prioritises stakeholders in terms of their importance, power to affect the task and interest in it • Uses stakeholders' views to shape projects early on • Gains support from stakeholders, e.g. to win resources • Agrees objectives
Apprentices can communicate effectively with a range of people at work, one-to-one and in groups, in different situations and using a variety of methods.	Intention/purpose: • Understands the purpose of communicating in a particular situation or circumstance (e.g. inform, instruct, suggest, discuss, negotiate etc.) • Checks that the person/people with whom one is communicating also understand the purpose

Apprentices can demonstrate various methods of communication, with an understanding of the strengths, weaknesses and limitations of these, the factors that may disrupt it, and the importance of checking other people's understanding.	• Is sensitive to the dynamics of the situation • Is aware of anything that might disrupt the effectiveness of the communication (e.g. status, past history) a. Method: • Chooses a good, appropriate method for the situation • Aware of the limitations of the chosen method, and the possible risks of miscommunication (e.g. ambiguity) • Takes account of the affective dimensions of the method (e.g. body language, tone of voice, eye contact, facial expression etc.) b. Execution: • Expresses self clearly and succinctly, but not over-simplifying • Checks that the other person/people understand what is being expressed • Takes account of the potential barriers to understanding (e.g. filtering, selective perception, information overload) • Modifies the purpose and methods of communication during a situation in response to cues from the other person/people

The With Whom: the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Criteria for Merit or Distinction

The following table shows what the apprentices would need to demonstrate to be assessed as significantly above the expected level for the personal and interpersonal qualities the apprentice has brought to internal and external relationships

Dimensions	**Description of what significantly above the expected level of quality looks like**
Scope and appropriateness – the range of internal and external people and situations that the apprentice has engaged appropriately and effectively with	Internally – works alone, 1:1, in a team and across the company with colleagues at all levels Externally – works with customers, suppliers and partners in a variety of situations Reads situations, adapts behaviours, and communicates appropriately for the situation and the audience

Reliability – the extent to which they perform and behave professionally	Can be trusted to deliver, perform and behave professionally, manages and delivers against expectations, proactively updates colleagues and behaves in line with the highest values and business ethics
A role model and exemplar to others	Actively inspires and leads others, takes others with them, leads by example

Annex: Cyber Intrusion Analyst: Knowledge and Understanding

Knowledge Module 1: Network (for Level 4 Cyber Intrusion Analyst Apprenticeship)

The Knowledge Standards	Definition of the Minimum Requirements
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 in use.	(a) Understands the 7 layer OSI model and UDP/TCP/IP network model (b) Understands typical digital network architectures for LAN and WAN scenarios (c) Understands difference between different kinds of networking equipment (d) Understands virtual network techniques and the benefits of the different approaches (e) Aware of IEEE 802 standards (f) Understands typical approaches to implementation of VoIP (g) Aware of network issues specific to wireless LAN and mobile cellular (h) Aware of main security controls and appliances employed in digital networks.

Knowledge Module 2: Operating Systems (for Level 4 Cyber Intrusion Analyst Apprenticeship)

The Knowledge Standards	Definition of the Minimum Requirements
Understands and utilises at least three Operating System (OS) security functions and associated features.	(a) Knows how to configure an OS firewall with rationale (b) Knows how to configure user/file access control list, user groups with rationale (c) Knows how to enable/disable OS services for security reasons with rationale (d) Knows how to implement a patching policy (e) Knows how to configure OS security policies with rationale (f) Able to contrast the security features in 2 different OS (e.g. Linux, Windows, iOS) (g) Able to contrast the security features implemented in server and client

Knowledge Module 3: Information and Cyber Security Foundations (for Level 4 Cyber Intrusion Analyst Apprenticeship)

The Knowledge Standards	Definition of the Minimum Requirements
Understands and applies 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.	(a) Can describe why cyber security is important to the corporate and business context (b) Can explain what the basic concepts are and how they relate to each other (c) Can describe what a security case is and explain how it is constructed Can demonstrate knowledge/awareness of the following IISP Core Skills: 1) Governance • Can explain the term Information Governance • Can explain the potential impacts that occur where poor information governance has been observed • Can outline the governance controls used within your own organisation 2) Policy & Standards • Understands the need for Information Security policy to achieve Information Security • Is aware of information security policy and standards bodies • Is aware of local processes for consultation, review and approval 3) Information Security Awareness & Training • Understands how security awareness and training contributes to maintaining Information Security • Can describe a variety of methods for improving security awareness • Can give examples of Information Security risks caused by poor security awareness • Can describe the benefit of good security awareness 4) Legal & Regulatory Environment (see TKU8) 5) Risk Assessment • Can explain how risk assessments can benefit an organisation • Can describe the main stages of a risk assessment and the principles that support assessments • Understands the common terminology, controls and approaches used • Understands the types of risks, threats and vulnerabilities and how they can impact an organisation • Is able to identify sources of information about threats and vulnerabilities from relevant industry sources 6) Risk management • Can explain how risk management can benefit the business • Can describe the process or cycle to manage risk and common terminologies used • Can describe the different type of controls used to manage risk and the concepts of impact levels • Is aware of sources of assurance to support risk management processes • Aware of the basic components of risk management : threats, likelihood, and impact 7) Security Architecture • Can describe the concept of Information Security architecture and how it can be used to reduce information risk

	• Can explain how Information Security architecture interacts with other enterprise architectures • Understands design patterns or architecture relevant to own work • Can relate security architecture to business needs 8) Information Assurance • Can describe what an Information Security Management System (ISMS) is and the potential benefits • Is aware of the existence of methodologies, processes and standards for providing Information Assurance • Can describe and demonstrate understanding of at least one Information Assurance methodology • Is aware of industry standards bodies and services and can provide examples 9) Secure Operations Management • Can explain how poor security management can adversely impact the organisation • Can describe the common causes of security incidents • Can describe security processes and procedures used within own organisation to maintain operational security • Understands security controls that relate to people, process and technology 10) Investigation (see TKU6) 11) Audit, Assurance & Review • Can explain how audits and reviews contribute to effective security management • Is aware and can describe audit and review controls used within own organisations • Is aware of common sources of information, standards, legislation and accreditation boards that are used to drive and control audit and review processes and practitioners 12) Business Continuity Management • Can explain the benefits of Business Continuity Management (BCM) and the consequences of poor BCM • Can explain the relationship of BCM with Incident management • Can describe the steps with the BCM lifecycle and the approaches that can be used to provide business continuity Can describe the different types of tests that can be used to prepare the organisation
Understands and proposes appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.	(a) Can describe the possible indicators (signatures) of compromise (b) Can describe the difference between targeted and general and systemic attacks (c) Can describe the response options that are available (e.g. containment, eradication, exploitation, legal) and the main features to implement each (d) Understands how to scope a response given the objectives for the system under threat (e) Understands how to do, and the benefits of timeline analysis (f) Can propose possible remediation actions to reduce the risk of future attacks.
Understands and proposes how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.	(a) Good awareness of the current cyber security threat landscape (known attack techniques, hazards and vulnerabilities) (b) Can recognise an emergent attack techniques, hazard or vulnerability (c) Can describe what assets are affected by an emerging threat and the impact to the organisation (d) Understands how a signature or correlation rule is developed from knowledge of an attack technique (e) Knows how to write a signature or correlation rule.

Knowledge Module 4: Business Processes (for Level 4 Cyber Intrusion Analyst Apprenticeship)

The Knowledge Standards	Definition of the Minimum Requirements
Understands lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level.	(a) Understand what processes and roles are covered in ITIL (b) Understand how ITIL processes and roles are employed in the cyber intrusion analyst's working environment
Understands and advises others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.	(a) Understands what 'cyber incident response' is, its purpose and how it fits into the corporate or business environment (b) Understands how a cyber incident investigation is conducted in at least one organisation (c) Knows what the incidence response policies and processes are that are relevant to the cyber intrusion analyst's working environment and role (d) Knows how to interface to an incident response process and who to contact (e) Knows what information is likely to be requested/required from the Cyber Intrusion Analyst and in what form to support an investigation (f) Knows how to collect and handle data to be provided to an investigation in order to meet requirements for evidence preservation in accordance with policies and processes are that are relevant to the cyber intrusion analyst's working environment and role

Knowledge Module 5: Law, Regulation and Ethics (for Level 4 Cyber Intrusion Analyst Apprenticeship)

The Knowledge Standards	Definition of the Minimum Requirements
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.	(a) Knows of all laws, regulations and standards relevant to the cyber intrusion analyst role (b) Is aware of the main regulatory bodies for their industry sector (c) Understands why and how each is relevant (d) Understands how to apply relevant parts of each in the cyber intrusion analyst's working environment (e) Knows when to seek authoritative advice and who to contact.

Understands, adheres to and advises on the ethical responsibilities of a cyber security professional.	(a) Can describe at least one industry recognised code of ethics relevant to cyber security and relate it to own experience and behaviour, with examples (b) Can describe examples that illustrate where ethical behaviour expected from a cyber-security professional may differ from accepted norms in society (c) Can explain how they apply such codes personally and at work and how their colleagues and peers recognise this.