Higher National Unit Specification

General information

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)
Unit code: J4BC 35

Superclass: CB
Publication date: June 2020
Source: Scottish Qualifications Authority
Version: 01

Unit purpose

The purpose of this unit is to introduce learners to cyber security intrusion detection, analysis and response. It covers the role of intrusion detection and prevention systems in monitoring network and system activity to identify potential intrusion or other anomalous behaviour.

The unit is suitable for learners with no previous experience or those who already have some basic knowledge of cyber security and want to further develop their knowledge and skills. Learners will gain an understanding of the main methods of cyber security intrusion detection, and the roles they perform. Learners will understand that intrusion detection systems (IDS) are designed to identify if intrusion has been attempted, is occurring, or has occurred. This also includes validating issues reported by IDS alarms and user generated notifications as well as tuning intrusion detection systems to provide valid alarm signals. Learners will appreciate how intrusion responses are the initial actions taken to mitigate or resolve a cyber security incident and restore normal operation of an information system and the information stored in it.

This unit is a specialist unit intended for learners with a vocational interest in cyber security defence. On completion of this unit, learners will appreciate that effective intrusion detection involves the comprehensive and continuous monitoring of networks and systems to identify anomalous behaviours, validate them and respond accordingly.

Outcomes

On successful completion of the unit the learner will be able to:

1. Explain the need for and role of intrusion detection systems.
2. Describe the different techniques for intrusion detection.
3. Explain the role of intrusion prevention.
Higher National Unit Specification: General information (cont)

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Credit points and level

1 Higher National Unit credit at Scottish Credit and Qualifications Framework (SCQF) level 8:
(8 SCQF credit points at SCQF level 8)

Recommended entry to the unit

The unit is suitable for learners with no previous experience or those who already have some basic knowledge of cyber security and want to further develop their knowledge and skills. However, it would be beneficial if learners have a basic understanding of networked computer systems/internet and an appreciation of information systems. This unit is particularly suitable for those working in vocational and professional areas who wish to enhance their knowledge and skills in cyber security.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

This unit is one of several units that make up the Professional Development Award (PDA) in Cyber Resilience at SCQF level 8. This unit, ideally, should be delivered as part of the award. The unit can be delivered on a stand-alone basis.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website www.sqa.org.uk/assessmentarrangements.
Higher National Unit Specification: Statement of standards

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed, and different items should be sampled on each assessment occasion.

Outcome 1

Explain the need for and role of intrusion detection systems.

Knowledge and/or skills

- Intrusion detection function and principles
- Protective monitoring
- Intrusion detection as part of the overall security system
- Detection of potential anomalous system behaviour
- Reporting direct misuse of access to systems/network data

Outcome 2

Describe the different techniques for intrusion detection.

Knowledge and/or skills

- Host based intrusion detection systems
- Network based intrusion detection systems
- Signature based detection
- Anomaly based detection
- Typical components in an IDS solution
- Tuning and customisation capabilities for IDS

Outcome 3

Explain the role of intrusion prevention.

Knowledge and/or skills

- Intrusion prevention operation
- Types of prevention
- Network intrusion prevention system
- Host intrusion prevention system
- Actions in response to/escalation of an intrusion event
Higher National Unit Specification: Statement of standards (cont)

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Evidence requirements for this unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used. Evidence is required to demonstrate that learners have satisfied the required knowledge and/or skills across all outcomes.

The evidence requirements for this unit are:

- Knowledge evidence — outcomes 1, 2 and 3

The evidence of cognitive competence must cover all outcomes. Knowledge evidence may be written or oral, or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). All evidence must be produced by the learner. Authentication must be used where this is uncertain.

This evidence should be produced over the life of the unit under loosely controlled conditions (including access to resources and reference materials). The knowledge evidence may be sampled when testing is used. When testing is used, it must be controlled in terms of location, timing and access to reference materials. Learners are expected to demonstrate a breadth of understanding across all the knowledge statements: as a result, sampling need not be of a detailed nature.

The level of this unit (SCQF level 8) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence:

- A knowledge of the scope, defining features, and main areas of the subject/discipline/sector
- A discerning understanding of a defined range of core theories, concepts, principles and terminology
- Using a range of professional skills, techniques, practices and/or materials associated with the subject/discipline/sector, a few of which are advanced and/or complex
- Convey complex information to a range of audiences and for a range of purposes
- Exercise autonomy and initiative in some activities at a professional level in practice or in a subject/discipline/sector

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The ‘guide to assessment’ provides further advice on methods of authentication.

The ‘guidelines on approaches to assessment’ (see the support notes section of this specification) provides specific examples of instruments of assessment.
Higher National Unit Support Notes

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

The context for this unit is the recognition at national level of the importance of embedding cyber security intrusion detection knowledge and skills across the workforce in every sector. In order to improve an organisation’s cyber resilience, there needs to be an increased awareness of cyber security intrusion detection across the wider workforce. This will help to increase organisational capabilities to better understand the nature of cyber security intrusion detection and be able to better refine the organisation’s controls to defend its information systems and assets as a result of anomalies and breaches that may occur.

The main purpose of this unit is to provide learners with the knowledge and skills to understand cyber security incident detection methods and the rationale used to select these methods.

Cyber security is an emerging and wide-ranging area of study, and learners undertaking this unit do not need to cover all topics in excessive detail. However, it is important that good coverage is given to each of the knowledge statements in order to provide the learner with a broad view of the outcomes and the steps taken throughout each of the processes. The assessor must ensure that learners understand the key roles of cyber intrusion detection and intrusion prevention systems, and how these are applied. Learners should develop an overall appreciation of cyber security intrusion detection. A holistic awareness of cyber security incident detection can be applied on both a personal and organisational level. Any sector of society can be vulnerable to current, evolving and new types of cyber threats. This unit encourages the learner to become knowledgeable about the roles of cyber security intrusion detection, how these can alert the potential of a cyber security attack and provide fast response.

The unit is useful for those wanting to better understand cyber security in relation to intrusion detection and those who may intend to work in either a technical or non-technical business role, educational role or service role.

All outcomes are knowledge based, where the learner learns about the different roles of cyber security intrusion detection and intrusion prevention. Outcome 2 is about the main types of cyber security intrusion detection systems and outcome 3 focuses on the approach to intrusion prevention.
Higher National Unit Support Notes

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Learners are provided with the opportunity to develop skills in research and analysis as, for example, they investigate systematic step-by-step security intrusion response systems.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the assessor but to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1

This learning outcome covers the need for cyber security intrusion detection systems in order to alert when an attack, or misuse of systems, is occurring. Learners will understand that the main roles of intrusion detection are to monitor network and system activity to identify potential intrusion or other anomalous behaviour, to analyse the information in order to initiate an appropriate response and escalating as necessary. Learners will:

- Understand that intrusion detection aims to search for and detect potential breaches or identify recognised indicators and alerts
- Be made aware that an IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyse network traffic for abnormal activities
- Learn that protective monitoring includes efficient, automatic monitoring, alerting and reporting of system changes, significant system events and file integrity monitoring

Useful resources include:

_Intrusion detection and intrusion prevention:_
https://www.imperva.com/learn/application-security/intrusion-detection-prevention/

_Survey of intrusion detection systems: techniques, datasets and challenges:_

Outcome 2

This outcome focuses on the main types of cyber security intrusion response techniques used including:

- system file comparisons against malware signatures
- scanning processes that detect signs of harmful patterns
- monitoring user behaviour to detect malicious intent and monitoring system settings and configurations
Higher National Unit Support Notes

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Learners will understand the two main variants of IDS that are used to identify unauthorised, illicit, and anomalous behaviour:

♦ Network Intrusion Detection System (NIDS) — is based on observing network traffic as it traverses a NIDS sensor
♦ Host Intrusion Detection System (HIDS) — HIDS products are aimed at specific devices, such as servers, PCs or workstations, where an agent is installed on each system to monitor and alert local operating system and application activity

Learners will appreciate that these use a combination of signatures, rules, and heuristics to identify unauthorised activity and will learn that placement of sensors is important in producing meaningful alerts. Learners will explore how IDS systems respond to signatures and anomalies. They will learn that signature-based detection is the process of comparing signatures against observed events to identify possible attacks and that anomaly-based detection is the process of comparing normal activity models against observed events to identify significant deviations concerning users, hosts, network connections, or applications. Learners will understand the need to tune and customise IDS to maintain performance and reduce false positive alerts.

Useful resources include:

The Ultimate Cheat Sheet on IDS, IPS and HIDS:
https://www.uzado.com/blog/the-ultimate-cheat-sheet-on-ids-ips-and-hids

Outcome 3

Outcome 3 focusses on intrusion prevention systems (IPS). Learners will understand that this is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor networks, looking for possible malicious incidents and capturing information about them. Learners will understand how the IPS reports these events to system administrators to take preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with security policies, deterring employees and network guests from violating the rules these policies contain. Learners will appreciate that in modern workplace environments there may be many access points present on a typical business network and it is therefore essential to monitor for signs of potential violations, incidents and imminent threats. Learners will appreciate that IPS are active systems that can control access to an IT network or system and protect it from abuse and attack. These systems are designed to monitor intrusion data and take the necessary action to prevent an attack from developing. A typical IPS configuration uses web application firewalls and traffic filtering solutions to secure applications. Learners will learn that IPS work by scanning all network traffic and performing real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out appropriate actions.

Useful resources include:

Published by: 5STARCooks, ISBN: 9780655569350
Higher National Unit Support Notes (cont)

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

Guidance on approaches to delivery of this unit

A practical, hands-on approach to learning should be adopted in order to engage learners and exemplify key concepts. Active, project-based and collaborative learning is encouraged, underpinned with appropriate knowledge before learners commence practical activities.

At this level, learning should be mainly led by the learners themselves, with some assessor intervention. It is anticipated that an initial introduction and explanation will be required for each outcome. However, there is significant scope for learners to research and explore the topics once this initial seeding has taken place. Assessors should expect a significant amount of independent learning to take place and support learners with this where appropriate.

The outcomes should be undertaken in order with outcome 1 attempted first, then outcome 2 and outcome 3 last.

A suggested distribution of time across the outcomes is:

Outcome 1: 10 hours
Outcome 2: 20 hours
Outcome 3: 10 hours

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable for learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Assessment for outcomes 1, 2 and 3 could take the form of a knowledge based written exam containing short and long answer questions; an assignment, presentation/interview, or a combination of these. Learner responses should be marked against a guide or solution provided by the assessor. Centres should also take steps to ensure that the work of learners is their own, for example, by asking them to sign a declaration.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions and intervene to remedy them before progressing to the next outcome.

Summative assessment may be carried out at any time. However, when testing is used it is recommended that this is carried out towards the end of the unit (but with enough time for remediation and re-assessment). When continuous assessment is used, this could commence early in the life of the unit and be carried out throughout the duration of the unit.
Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA’s qualifications is available at www.sqa.org.uk/e-assessment.

Opportunities for developing Core and other essential skills

Although this unit does not embed any Core Skills, there are opportunities to develop Core Skills in Communication, Information Communication Technology (ICT) and Problem Solving.

All outcomes involve investigation-led problem solving and use of ICT systems to identify techniques for monitoring networks and systems, and the presence and types of security incident.

In addition, all outcomes should provide opportunities to practise writing clearly and simply, which will contribute to the Core Skill component of Written Communication.

The unit will also provide opportunities to develop broader skills, such as analytical thinking, which will be required when learners functionally decompose learning objectives, and citizenship in the context of cyber security resilience (safe working practices; protecting self and others, etc).
## History of changes to unit

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of change</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Scottish Qualifications Authority 2020

This publication may be reproduced in whole or in part for educational purposes provided that no profit is derived from reproduction and that, if reproduced in part, the source is acknowledged.

Additional copies of this unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.
General information for learners

Unit title: Intrusion Detection, Analysis and Response (SCQF level 8)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit is suitable for you whether you have no previous experience or some basic knowledge of cyber security and want to further develop your knowledge and practical skills in this increasingly important field. It would be advantageous to have a basic understanding of computer systems and networks. The unit is particularly suitable for those already working in vocational and professional roles.

The unit will explain why organisations need to implement a range of intrusion detection techniques in order to identify possible cyber security attacks and compromises to information, and the different roles intrusion detection methods perform. You will explore the different types of intrusion detection and protective monitoring methods used. You will also gain an understanding of the typical components in an intrusion detection solution and the need to tune and customise these to maintain optimum performance.

The unit covers the theoretical and practical aspects of the overall process that encompass cyber security intrusion detection and broadly covers the following topics:

- the need to perform intrusion detection to identify cyber security attacks and other breaches
- the different methods of cyber security intrusion detection
- typical components used in an intrusion detection system
- monitoring for incidents
- maintaining, fine tuning and optimising intrusion detection systems to produce valid alerts
- the role of intrusion prevention systems

Teaching methodologies for this unit may incorporate a variety of techniques, for example, active, project-based and collaborative learning. The unit may be assessed in a variety of ways; for example, answering a series of short and long answer questions covering all topics; completing a case study project or by more contemporary means, such as a blog or e-portfolio, where you can showcase your work.

There will be opportunities for you to also develop Core Skills in Communication, Information Communication Technology (ICT) and Problem Solving.

This unit is part of the PDA in Cyber Resilience at SCQF level 9. By the end of this unit, you will be able to identify the main principles and benefits of cyber security intrusion detection and prevention. You will also be able to identify the main types of intrusion detection methods and their usage and learn the importance of using cyber security intrusion detection to alert on breaches, attacks and other anomalous behaviours. On completion of this unit you may be able to progress to more advanced cyber security units.