Higher National Unit Specification

General information

Unit title: Network Security Monitoring (SCQF level 8)

Unit code: J27N 35

Superclass: CC

Publication date: August 2019

Source: Scottish Qualifications Authority

Version: 02

Unit purpose

The purpose of this unit is to enhance learners existing knowledge and skills in networking and cyber security using a range of technologies to monitor threats to networks and report on areas of vulnerability.

This is a specialist unit, intended for learners with a vocational interest in computing or STEM. It is particularly suitable for learners who are undertaking, or have recently completed an HNC in Cyber Security or Computing.

The focus of the unit is on the generic application of these concepts and does not necessarily require any specific hardware or software for delivery.

On completion of this unit, learners will be prepared to progress onto other units in the HNC/D Cyber Security, for example, *Computer Networks: Administering Network Systems*, *Wireless Device Security* and *Working in Cyber Security*.

Outcomes

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

1 Describe common threats, attackers and their tools.
2 Explain network attacks.
3 Describe network monitoring tools.
4 Explain defence and threat intelligence.

Credit points and level

1 Higher National Unit credit at SCQF level 8: (8 SCQF credit points at SCQF level 8)

Higher National Unit Specification: General information (cont)

Unit title: Network Security Monitoring (SCQF level 8)

Recommended entry to the unit

No previous knowledge or experience is required. However, it would be beneficial if learners had some prior knowledge and skills in networking or cyber security. This may be evidenced by possession of relevant units such as *Computer Networking: Concepts, Practice and Introduction to Security*, or the NPAs in Cyber Security or Professional Computer Fundamentals.

Core Skills

Core Skills Component – more than one

Achievement of this Unit gives automatic certification of the following Core Skills component:

Core Skill component	Critical Thinking at SCQF level 6 Accessing Information at SCQF level 6

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of this Unit specification.

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.

It is suggested that this unit is delivered as part of the HND Cyber Security. It is also advisable that the unit is taught along with other relevant units. For example, *Computer Networks: Administering Network Systems*, *Wireless Device Security* and/or *Working in Cyber Security*.

The Assessment Support Pack (ASP) for this unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

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: Network Security Monitoring (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

Describe common threats, attackers and their tools.

Knowledge and/or skills

- Social engineering
- Hackers and cyber criminals
- Attack tools
- Security tools
- Common threats and attacks
- Malware
- Viruses
- Trojans
- Worms
- Ransomware
- Identifying malware behaviour

Outcome 2

Explain network attacks.

Knowledge and/or skills

- Reconnaissance
- Access
- Phishing
- Denial of service
- Distributed Denial Of Service (DDOS)
- Buffer overflow
- Evasion methods

Higher National Unit Specification: Statement of standards (cont)

Unit title: Network Security Monitoring (SCQF level 8)

Outcome 3

Describe network monitoring tools.

Knowledge and/or skills

- Network protocol analysers (Wireshark and tcpdump)
- Netflow
- Flow stitching
- Flow deduplication
- NAT stitching
- Security Information and Event Management (SIEM) systems
- Current popular SIEM systems
- Forensic analysis
- Correlation
- Aggregation
- Reporting

Outcome 4

Explain defence and threat intelligence.

Knowledge and/or skills

- Assets
- Vulnerabilities
- Threats
- Security onion
- Security artichoke
- Security policies
- Access control Confidentiality, Integrity, Availability (CIA)
- Authentication, Authorization, and Accounting (AAA)
- Information sources
- Network intelligence communities
- Security blogs and podcasts
- Threat intelligence services

Higher National Unit Specification: Statement of standards (cont)

Unit title: Network Security Monitoring (SCQF level 8)

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence
2 Product evidence

The **knowledge evidence** will relate to all outcomes. Knowledge evidence is required for all knowledge and/or skills statements except those explicitly relating to skills. The evidence may be produced over an extended period in lightly controlled conditions. The amount of evidence may be the minimum required to infer competence. The knowledge evidence may be sampled when testing is used. In this case, the evidence must be produced under controlled conditions in terms of location (supervised), timing (limited) and access to reference materials (not permitted). The sampling frame must cover all outcomes but not all knowledge/skills statements; however, the majority of the knowledge/skills should be sampled in every test. The sampling frame must always include the following:

- Social engineering
- Hackers and cyber criminals
- Attack and security tools
- Common threats and attacks
- Identifying malware behaviour
- Reconnaissance
- Access
- Evasion methods
- Network protocol analysers (Wireshark and tcpdump)
- Security Information and Event Management (SIEM) systems
- Forensic analysis
- Asset vulnerabilities
- Threats
- Security onion
- Security artichoke
- Security policies
- Access control Confidentiality, Integrity, Availability (CIA)
- Authentication, Authorization, and Accounting (AAA)
- Information sources
- Network intelligence communities
- Security blogs and podcasts
- Threat intelligence services

The 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).

The **product evidence** will relate to Outcomes 3 and 4. It will demonstrate that the learner can analyse network logs, work with and investigate network security data and then make judgements and recommendations. This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary (see below).

Higher National Unit Specification: Statement of standards (cont)

Unit title: Network Security Monitoring (SCQF level 8)

The SCQF level of this unit (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.
- Awareness and understanding of some major current issues and specialisms.
- 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.
- To adapt routine practices within accepted standards.
- Undertake critical analysis, evaluation and/or synthesis of ideas, concepts, information and issues that are within the common understandings in a subject/discipline/sector.
- Use a range of approaches to formulate and critically evaluate evidence-based solutions/responses to defined and/or routine problems and issues.
- Exercise autonomy and initiative in some activities at a professional level in practice or in a subject/discipline/sector.
- Work, under guidance, with others to acquire an understanding of current professional practice.
- Manage, under guidance, ethical and professional issues in accordance with current professional and/or ethical codes or practices.

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: Network Security Monitoring (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

This unit is designed to give learners an opportunity to learn about network security monitoring.

Learners should learn that network security monitoring is a vital part of working in computing. Awareness of threats and current protection, physical security, and business processes must be constantly monitored in order to ensure security and minimise risk to the business and the end service user. Leaners may well be aware of recent attacks due to coverage in news reports; these can be used as examples to explain the underlying theory and concepts involved in this unit.

Due to the constantly changing nature of this subject area, awareness of the constant requirement for continual professional development should be emphasised.

Learners should learn how to analyse the data collected and the importance of raising security awareness and the need to communicate at levels appropriate to colleagues, employers and clients.

It is recommended that centres facilitate hands-on experience for learners as far as possible. Learners should be encouraged to contact IT support managers in their own work environment to assist in research in that organisation and/or information topics appropriate to each of the outcomes. It is anticipated that this unit may be delivered to learners with a variety of backgrounds and, wherever possible, teaching should be slanted towards their individual areas of interest.

The listed knowledge/skills in each outcome indicate areas of study and discussion. The list is not exhaustive and may be adjusted in line with industry and updates to legislation. It is envisaged that all the bullet points would be covered during the delivery of this unit.

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 teacher. It seeks 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.

Higher National Unit Support Notes (cont)

Unit title: Network Security Monitoring (SCQF level 8)

Outcomes 1 and 2 relate to the underpinning knowledge required for the unit. It should be made clear to the learner the professionalism and ethics required when working in this field. To be effective working in this area an awareness of historical, current and future threats and trends in this area is required. Many instances of these threats are available through news reports and relevant social media sites. It is likely the learner may be familiar with these many of these.

Outcome 1

- Social engineering — Manipulation of people to gain confidential information. Types of attacks include phishing through emails, social networks, IM client, chat forums, phone calls, and baiting scenarios to encourage clicking links or downloads with embedded malicious code/software
- Hackers and cyber criminals — Exploration of the mind of a hacker; a criminal's imagination to exploit; psychology of a criminal and reasons why they do what they do eg, financial gain; threat actors (amateurs, hacktivists)
- Attack tools — Kali Linux suite (Metasploit, NMAP, Wireshark, air cracking, password cracking, John the Ripper)
- Security tools — Nessus, Snort, elements of a security operations centre (process, people, technology) — firewall types, IDS/IPS, ACL's Social Engineering Toolkit (SET)
- Common threats and attacks — reference to recent hijacked people, companies, nations
- Malware — Designed to disrupt, damage, steal. Common malware includes: viruses, trojans, worms, ransomware, rootkit, spyware, adware, scareware

Outcome 2

Scenarios, recent events, case studies, guest speakers, and industrial visits provide opportunities for learners to understand the level and detail of work involved. Classroom discussion is actively encouraged to voice student opinion and thoughts in an interactive setting.

- Reconnaissance — Discovery (unauthorised) of systems, services exposing vulnerabilities, these can be passive or active. Examples could include the target of end point device, precedes access attacks/DoS. Exploring: Information queries using tools such as whois, nslookup, dig, ping sweeps, port scans, vulnerability scans
- Access — Exploitation of discovered or known vulnerabilities. Exploring: password attacks, pass-the-hash, port redirection, MITM, spoofing
- Manipulation — May include exploring using willingness to help. Exploring: pretexting, spam, phishing, gift exchange, tailgating, baiting, visual observation, spear, whaling, pharming, website compromise, vishing, smishing
- Denial of Service — Interrupting service may include exploring: overwhelming/or volume of traffic, error packets through buffer overflow (ping of death). Exploring: Distributed Denial Of Service (DDOS) and components (zombies, bots, botnets, handlers, botmaster)
- Evasion methods — Hidden/undetected attacks. Explore: encryption, tunnelling, host distraction, packet fragmentation, checksum manipulation, traffic encoding, and/or pivoting

Higher National Unit Support Notes (cont)

Unit title: Network Security Monitoring (SCQF level 8)

Outcome 3

This outcome covers the information and skills required to effectively utilise network monitoring tools and work in a professional, accurate and efficient manner. It should be made clear to the learner the professionalism and ethics required when working in in this field. Where possible real-life examples of logs to analyse would be beneficial to learners.

Compare and contrast:

- Network protocol analysers (Wireshark and tcpdump, inline traffic interrogation, network TAPs, SNMP) traffic mirroring/switch port analyser, netflow (flow stitching, flow deduplication, NAT stitching), packet filtering, deep packet inspection)
- Security Information and Event Management (SIEM) systems — Explore real-time analysis of security alerts by network hardware and application; explore log collections of servers, switches, routers, storage arrays, operating systems, firewalls captured for further analysis; SIEM components (HIDS, syslog, alerts and reports, compliance, asset management, threat feeds, endpoint data)
- Current popular SIEM systems paid vs open source (Splunk vs ELK — Elasticsearch, Logstash, Kibana)
- Forensic analysis (collection — identification of potential sources of data; examination — assessing and extracting information, analysis correlation of data to draw conclusions; reporting — preparing and presenting information)

Outcome 4

This outcome covers the resources available to enable learners to successfully access and utilise sources of information and work in a professional, accurate and efficient manner. The learner will be aware of the national, international standards and a range of frameworks available to support and protect organisations to prevent network threats. As in previous outcomes it should be made clear to the learner the professionalism and ethics required when working in this field.

Compare and contrast:

- Risks to assets — Probability of occurrence and consequences
- Vulnerabilities — Weaknesses including system susceptibility or flaw, attacker access to flaw, attacker capability to flaw
- Threats and exploits — Possible dangers of breach in security through pieces of software or sequence of commands to take advantage of a bug or vulnerability to gain control of a computer system
- Security onion for intrusion prevention and detection. Prevention through: device hardening, Authentication, Authorization, and Accounting (AAA), content filtering, Intrusion Prevention Systems (IPS), firewall including NextGen. Detection methods using tools such as Logstash, Snort, Bro, Squil, Squert, NetworkMiner
- Business and security policies (password, Acceptable Use Policy (AUP), remote access, network, BYOD)
- Access control models (mandatory, discretionary/non-discretionary, attribute-based)
- Communications security — Confidentiality, Integrity, Availability (CIA)

- Security community — (Network intelligence communities, discretionary, threat intelligence services)
- Assets
- Vulnerabilities
- Threats
- Security onion
- Security artichoke
- Security policies
- Access control Confidentiality, Integrity, Availability (CIA)
- Authentication, Authorization, and Accounting (AAA)
- Information sources
- Network intelligence communities
- Security blogs and podcasts
- Threat intelligence services

Guidance on approaches to delivery of this unit

Due to the constant changes with cyber threats to company networks it is advised that reputable online resources are used to ensure the updating of content delivered. Learner research, both individual and group along with discussions and presentations, is an effective way to ensure content is current and relevant. Guest speakers, industry visits, and attending events wherever possible should be considered. As network security monitoring is a combination of practical skills, experience and specialist system knowledge, it is vital that learners are given as many opportunities as possible to learn from practical experiences, and real-life examples.

A suggested distribution of time, across the outcomes, is:

- Outcome 1: 6 hours
- Outcome 2: 8 hours
- Outcome 3: 13 hours
- Outcome 4: 13 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements) 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 (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

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.

Higher National Unit Support Notes (cont)

Unit title: Network Security Monitoring (SCQF level 8)

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 to 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.

The knowledge evidence required comprises the underpinning knowledge required in Outcomes 1, 2, 3 and 4. Learners may be assessed using different methods, for example:

1 A constructed response test comprising several short answer questions, marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response of no more than one or two paragraphs. Questions would be selected across all four outcomes and would each be worth five marks. Learner responses would be marked out of 50 with a pass mark of 30. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken, sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration would be 60 minutes.
2 Case study where a brief/scenario can be provided.
3 Report/presentation (individual or group).

For Outcomes 3 and 4, it would be ideal for learners to carry out a practical investigation on network security data using appropriate network monitoring tools. If the resources required to carry out the practical assignment are not available, sample logs could be investigated or the topics highlighted could be researched and presented in a format accepted by the centre.

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary. The evidence should be generated under supervised conditions and work can be authenticated by continual observation or by individual questioning to ensure that it is the learner's own work.

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate).

If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

Higher National Unit Support Notes (cont)

Unit title: Network Security Monitoring (SCQF level 8)

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

Opportunities to develop aspects of Core Skills occur across all outcomes of this unit, these are:

- *Information and Communication Technology (ICT)* at SCQF level 6
- *Communication* at SCQF level 6
- *Problem Solving* at SCQF level 6

In terms of *Information and Communication Technology*, there are opportunities in the use of software to read and analyse data logs, entering and editing data, locating and extracting information and evaluating and presenting information.

In this unit learners will naturally use and develop aspects of the Core Skill of *Problem Solving* at SCQF level 6 as they analyse network logs and assess vulnerabilities. Additional opportunities could be realised depending on how the unit is delivered with the possibility of integrated learner activities.

In this unit learners will naturally use and develop aspects of the Core Skill of *Communication* at SCQF level 6 as they work through the assessment requirements and presenting their results. Additional opportunities could be realised depending on how the unit is delivered with the possibility of integrated learner activities.

The Critical Thinking component of Problem Solving at SCQF level 6 and Accessing Information component of Information and Communication Technology at SCQF level 6 are embedded in this unit. When a learner achieves these units, their Core Skills profile will also be updated to include these components

History of changes to unit

Version	Description of change	Date
02	Core Skills Components Critical Thinking and Accessing Information at SCQF level 6 embedded.	16/08/19

General information for learners

Unit title: Network Security Monitoring (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 will provide you with an introduction to working in an IT support environment using network monitoring tools. You will gain an understanding of the threats, factors and tools that can be used by malicious hackers to target individuals and organisations. The aim of the unit is, that by knowing the tools that malicious hackers use, you will then learn the techniques and technologies used to monitor and defend systems from attack.

On completion of this unit, you will be able to discuss and explain current trends in cyber threats. You will be able to use and analyse network monitoring software and make recommendations based on your judgements. You will also be able to access international threat intelligence sources to identify, explain and implement remediation for common vulnerabilities.

On successful completion of the unit, you will be able to:

- Describe common threats, attackers and their tools
- Explain network attacks
- Describe network monitoring tools
- Explain defence and threat intelligence

You will be assessed using several methods, which will test your knowledge and practical skills. This could be by questioning or by producing a report or keeping an online journal of continuous research and group discussions.

Opportunities to develop aspects of Core Skills occur across all outcomes of this unit, these are:

- *Information and Communication Technology (ICT)* at SCQF level 6
- *Communication* at SCQF level 6
- *Problem Solving* at SCQF level 6

You will have the opportunity to develop the Core Skill of *Information and Communication Technology*, there are opportunities in the use of capturing and analysing security, logs and evaluating data, making recommendations based on your judgements.

You will have the opportunity to naturally use and develop aspects of the Core Skill of *Problem Solving* at SCQF level 6 as you work through the assessment requirements, analysing network logs, and assessing vulnerabilities. There will be additional opportunities to develop your problem-solving skills through analysis of practical logs and tasks.

You will have the opportunity to naturally use and develop aspects of the Core Skill of *Communication* at SCQF level 6 as you work through the assessment requirements. You will have the opportunity to research current threats and trends and other related topics, and comment and present your findings.

General information for learners

Unit title: Network Security Monitoring (SCQF level 8)

The Critical Thinking component of Problem Solving at SCQF level 6 and Accessing Information component of Information and Communication Technology at SCQF level 6 are embedded in this unit. When a learner achieves these units, their Core Skills profile will also be updated to include these components.