## Cyber Security and Digital Forensics


(Ofqual Register Link)
[2]
[3]

Please note: guidance is being added over the next few days, but is in the handbook already.

Support also available through Cisco [4] Introduction to Cybersecurity [5] and Cybersecurity Essentials [6].

## Level 2

## Level 2, Unit 1 - Understanding Cyber Security and Online Threats (3 credits)

## 1. Understand the range and variety of cyber threats

1.1 I can explain the basic nature of a cyber threat [7]
1.2 I can list some of the more common threats [10]
1.3 I can explain the main features of threats to individuals [13]
1.4 I can explain the main features of threats to companies [16]

## 2. Analyse and detail the types of threat currently in operation

2.1 I can describe the motivations of people behind threats [8]
2.2 I can analyse the main threats in terms of the mechanisms they use [11]
2.3 I can describe how the features of threats make them operate [14]
2.4 I can describe how attacks on companies are designed to work [17]

## 3. Evaluate the impact of threats on various individuals and organisations

3.1 I can describe the impact on the economy of cyber threats [9]
3.2 I can assess the level of threat to my home environment [12]
3.3 I can determine the threat to a website in a safe and controlled environment [15]
3.4 I can determine the threat to a server in a safe and controlled envieonment [18]

### 1.5 I can summarise the

### 3.5 I can produce a

variety of threats for an audience [19]
in terms of their hierarchy
of damage [20]
presentation or report on my findings [21]

## Level 2, Unit 2 - Analysing and Evaluating Cyber Threats ( 3 credits)

## 1. Understand the parts of a system that are attacked

1.1 I can understand the basics of the OSI model [23]
1.2 I can explain the main hardware features of an IT system [26]
1.3 I can explain the main software features of an IT system [29]
1.4 I can understand the different user services that run on systems, such as email [32]
1.5 I can list the main ports used for different services [35]

## 2. Analyse and detail the parts of a system that are attacked

2.1 I can analyse the commonplace threats associated with the upper layers of OSI model [24]
2.2 I can describe the hardware features that protect an IT system [27]
2.3 I can describe the software features that protect an IT system [30]
2.4 I can describe the key services offered by a server [33]
2.5 I can analyse the function of each port used on a server in relation to the key services [36]

## 3. Evaluate how and why systems are attacked

3.1 I can evaluate how the different layers of the OSI model can be attacked [25]
3.2 I can evaluate how effective the hardware protection services are for an IT system [28]
3.3 I can evaluate how effective the software protection services are for an IT system [31]
3.4 I can assess the vulnerabilities of each service offered on a server [34]
3.5 I can evaluate the vulnerabilities of each key service running on a server [37]

## Level 2, Unit 3 - Applying and Deploying Security Tools and Best Practice ( 3 credits)

## 1. Understand the tools used for cyber security

## 2. Plan, use and practice with common cyber forensic tools

## 3. Evaluate the tools used and recommend best practices

## Cyber Security and Digital Forensics

-->

1.1 I can list the main tools used in cyber security [39]

1.2 I can explain the tools used to protect personal identity [42]
1.3 I can list the range of tools used to protect data [45]
1.4 I can describe the way devices are compromised [48]
1.5 I can describe the need for policies and procedures in cyber security [51]
1.6 I can list a range of laws that apply to cyber crime [54]
2.1 I can explain the main features of valid cyber security tools [40]
2.2 I can select and use tools to protect my personal identity [43]
2.3 I can set-up a range of tools to protect data for myself or others [46]
3.1 I can evaluate commonly used cyber security tools for overall effectiveness [41]
3.2 I can evaluate the tools selected for the protection of personal identity [44]
3.3 I can assess and recommend different tools to protect personal or organisational data [47]
3.4 I can assess and recommend a range of tools to protect different devices [50]
3.5 I can evaluate and recommend policies and procedures for efficient and effective cyber security [53]
3.6 I can assess the effectiveness of current laws on cyber crime [56]

## Level 2, Unit 4 - Extended Project: Securing and Defending Online Systems (6 credits)

1. Research
a working
cyber
security
system
1.1 I can investigate a working system to determine the main components [58]
1.21 can explain the main system components
2. Plan to build a cyber safe web site or server
2.1 I can make a working skeletal plan of a system [59]

## 3. Develop a cyber safe web site or server

$$
\begin{aligned}
& \begin{array}{l}
3.1 \text { I can } \\
\text { prepare a } \\
\text { system in } \\
\text { terms of } \\
\text { specifications }
\end{array}
\end{aligned}
$$ [60]

## 4. Test the system against common threats

4.1 I can develop a basic test regime [61]
5. Evaluate the effectiv eness of the system
5.11 can analyse the results in terms of the objectives [62]
4.2 I can
explain the
purpose of the
main test
4.21 can
3.21 can explain the specification in terms of
purpose of the main test
5.21 can evaluate some of the features of the system

## Cyber Security and Digital Forensics

[63]
1.3 I can describe how the components fit together [68]
1.4 I can make detailed notes of my findings [73]
system against performance [64]
2.3 I can list the main safety features that will need to be addressed for success [69]
2.4 I can explain the main hardware requirements needed [74]
performance
needs [65]
3.3 I can describe the way a web site functions [70]
3.4 I can describe the main pieces of software required [75]
procedures [66]
4.31 can explain the expected results from tests [71]

### 4.41 can

 describe the test results and what they mean [76]1.5 I can present my notes to an audience for feedback [78]
2.5 I can explain the main software aspects of the system [79]
3.5 I can
describe the
configuration
settings for a
working system [80]

| 4.5 I can |
| :--- |
| adjust the |

system in light
of test results
[81]
4.6 I can recommend final adjustments before going live [85]
5.5 I can analyse the effectiveness of the system by viewing the different log files [82]
and their purpose [67]
5.31 can justify some design decisions in terms of objectives [72]

### 5.4 I can

analyse possible improvements to the system based on usage and end user feedback [77]
5.6 I can recommend improvements to the system for futureproofing [87]

Source URL: https://theingots.org/community/csdf

## Links

[1] https://theingots.org/community/sites/default/files/uploads/user4107/TLM\ L2\ Cyber\ Ha ndbook\%201.3_1.pdf
[2] https://register.ofqual.gov.uk/Detail/Index/39715?category=qualifications\&query=603\%2F1 452\%2F7
[3] https://theingots.org/community/RQF_Levels
[4] https://www.netacad.com
[5] https://www.netacad.com/courses/intro-cybersecurity/
[6] https://www.netacad.com/courses/cybersecurity-ess/
[7] https://theingots.org/community/csdfl2u1x\#1.1
[8] https://theingots.org/community/csdfl2u1x\#2.1
[9] https://theingots.org/community/csdfl2u1x\#3.1
[10] https://theingots.org/community/csdfl2u1x\#1.2
[11] https://theingots.org/community/csdfl2u1x\#2.2
[12] https://theingots.org/community/csdfl2u1x\#3.2

## Cyber Security and Digital Forensics

[13] https://theingots.org/community/csdfl2u1x\#1.3
[14] https://theingots.org/community/csdfl2u1x\#2.3
[15] https://theingots.org/community/csdfl2u1x\#3.3
[16] https://theingots.org/community/csdfl2u1x\#1.4
[17] https://theingots.org/community/csdfl2u1x\#2.4
[18] https://theingots.org/community/csdfl2u1x\#3.4
[19] https://theingots.org/community/csdfl2u1x\#1.5
[20] https://theingots.org/community/csdfl2u1x\#2.5
[21] https://theingots.org/community/csdfl2u1x\#3.5
[22] https://theingots.org/community/csdfl2u1i
[23] https://theingots.org/community/csdfl2u2x\#1.1
[24] https://theingots.org/community/csdfl2u2x\#2.1
[25] https://theingots.org/community/csdfl2u2x\#3.1
[26] https://theingots.org/community/csdfl2u2x\#1.2
[27] https://theingots.org/community/csdfl2u2x\#2.2
[28] https://theingots.org/community/csdfl2u2x\#3.2
[29] https://theingots.org/community/csdfl2u2x\#1.3
[30] https://theingots.org/community/csdfl2u2x\#2.3
[31] https://theingots.org/community/csdfl2u2x\#3.3
[32] https://theingots.org/community/csdfl2u2x\#1.4
[33] https://theingots.org/community/csdfl2u2x\#2.4
[34] https://theingots.org/community/csdfl2u2x\#3.4
[35] https://theingots.org/community/csdfl2u2x\#1.5
[36] https://theingots.org/community/csdfl2u2x\#2.5
[37] https://theingots.org/community/csdfl2u2x\#3.5
[38] https://theingots.org/community/csdfl2u2i
[39] https://theingots.org/community/csdfl2u3x\#1.1
[40] https://theingots.org/community/csdfl2u3x\#2.1
[41] https://theingots.org/community/csdfl2u3x\#3.1
[42] https://theingots.org/community/csdfl2u3x\#1.2
[43] https://theingots.org/community/csdfl2u3x\#2.2
[44] https://theingots.org/community/csdfl2u3x\#3.2
[45] https://theingots.org/community/csdfl2u3x\#1.3
[46] https://theingots.org/community/csdfl2u3x\#2.3
[47] https://theingots.org/community/csdfl2u3x\#3.3
[48] https://theingots.org/community/csdfl2u3x\#1.4
[49] https://theingots.org/community/csdfl2u3x\#2.4
[50] https://theingots.org/community/csdfl2u3x\#3.4
[51] https://theingots.org/community/csdfl2u3x\#1.5
[52] https://theingots.org/community/csdfl2u3x\#2.5
[53] https://theingots.org/community/csdfl2u3x\#3.5
[54] https://theingots.org/community/csdfl2u3x\#1.6
[55] https://theingots.org/community/csdfl2u3x\#2.6
[56] https://theingots.org/community/csdfl2u3x\#3.6
[57] https://theingots.org/community/csdfl2u3i
[58] https://theingots.org/community/csdfl2u4x\#1.1
[59] https://theingots.org/community/csdfl2u4x\#2.1
[60] https://theingots.org/community/csdfl2u4x\#3.1
[61] https://theingots.org/community/csdfl2u4x\#4.1
[62] https://theingots.org/community/csdfl2u4x\#5.1
[63] https://theingots.org/community/csdfl2u4x\#1.2
[64] https://theingots.org/community/csdfl2u4x\#2.2
[65] https://theingots.org/community/csdfl2u4x\#3.2
[66] https://theingots.org/community/csdfl2u4x\#4.2
[67] https://theingots.org/community/csdfl2u4x\#5.2
[68] https://theingots.org/community/csdfl2u4x\#1.3
[69] https://theingots.org/community/csdfl2u4x\#2.3
[70] https://theingots.org/community/csdfl2u4x\#3.3
[71] https://theingots.org/community/csdfl2u4x\#4.3

## Cyber Security and Digital Forensics

[72] https://theingots.org/community/csdfl2u4x\#5.3
[73] https://theingots.org/community/csdfl2u4x\#1.4
[74] https://theingots.org/community/csdfl2u4x\#2.4
[75] https://theingots.org/community/csdfl2u4x\#3.4
[76] https://theingots.org/community/csdfl2u4x\#4.4
[77] https://theingots.org/community/csdfl2u4x\#5.4
[78] https://theingots.org/community/csdfl2u4x\#1.5
[79] https://theingots.org/community/csdfl2u4x\#2.5
[80] https://theingots.org/community/csdfl2u4x\#3.5
[81] https://theingots.org/community/csdfl2u4x\#4.5
[82] https://theingots.org/community/csdfl2u4x\#5.5
[83] https://theingots.org/community/csdfl2u4x\#1.6
[84] https://theingots.org/community/csdfl2u4x\#2.6
[85] https://theingots.org/community/csdfl2u4x\#3.6
[86] https://theingots.org/community/csdfl2u4x\#4.6
[87] https://theingots.org/community/csdfl2u4x\#5.6
[88] https://theingots.org/community/csdfl2u4i

