

NCFE Level 3 Certificate in Cyber Security Practices

Level 3 cyber security: principles, threat intelligence, testing and controls, incident response, legislation and ethics, and professional skills. 150 guided learning hours, ...

**Study it online.
Finish with a qualification
that is on your record for life.**

WHERE IT SITS

- Entry
- Level 1
- Level 2
- **Level 3**
- Level 4
- Level 5

Level 3

REGULATED LEVEL

150

LEARNING HOURS

6

UNITS

100%

ONLINE

**Delivered online**

Tutor support. Start when you are ready.

**Assessed on your work**

A portfolio of your own work. No written exam.

**Awarded by NCFE**

Ofqual-recognised. We are approved centre 11001657.

**Ask us**

For the fee and the next start date.

**Start when you are ready**

150 guided learning hours, 220 total hours, self-paced online

**Tutor support throughout**

Questions answered within 2 working days, feedback within 10.

**Nothing paid at application**

Payment only after you accept an offer.

WHAT YOU WILL STUDY

6 units, 150 guided learning hours



Understand cyber security principles	30 h · 20%
Threat intelligence in cyber security	30 h · 20%
Cyber security testing, vulnerabilities and controls	30 h · 20%
Cyber security incident response	30 h · 20%
Understand legislation and ethical conduct within cyber security	20 h · 13%
Professional skills and behaviours for cyber security	10 h · 7%

UNIT BY UNIT

What each unit covers

01. Understand cyber security principles

30 hours

- ✓ Understand cyber security
- ✓ Understand security by design principles
- ✓ Understand core terminology and key aspects of cyber security

02. Threat intelligence in cyber security

30 hours

- ✓ Understand cyber threat intelligence
- ✓ Understand malicious software
- ✓ Understand threat models
- ✓ Know about social engineering

03. Cyber security testing, vulnerabilities and controls

30 hours

- ✓ Understand common types of testing in cyber security
- ✓ Understand controls in cyber security
- ✓ Be able to reduce or remove potential cyber security vulnerabilities
- ✓ Be able to apply a cyber security control

04. Cyber security incident response

30 hours

- ✓ Understand what is meant by a cyber security incident response
- ✓ Be able to develop a cyber security incident response plan
- ✓ Be able to develop an incident post mortem report

05. Understand legislation and ethical conduct within cyber security

20 hours

- ✓ Understand legislation relating to cyber security
- ✓ Understand ethical conduct within cyber security
- ✓ Understand information security standards

06. Professional skills and behaviours for cyber security

10 hours

- ✓ Understand behaviours required for a career in cyber security
- ✓ Be able to identify skills required for a career in cyber security
- ✓ Understand the importance of continuous professional development

The learning outcomes NCFE publishes for each unit. The assessment criteria beneath them are on the qualification page.

6

UNITS TO COMPLETE

20

LEARNING OUTCOMES

150

GUIDED LEARNING HOURS

Guided learning hours are the taught time NCFE specifies. Your own study time is on top, and how long you take is up to you.

HOW IT WORKS

From your first unit to your certificate

01

You produce evidence

A portfolio of your own work, against the published criteria.

02

An assessor marks it

Qualified, and required to show current competence in the sector they assess.

03

The marking is checked

Sampled internally each term, and quality assured by NCFE from outside the school.

04

NCFE certificates you

Claimed through the NCFE portal. Recognised independently of us.

WHAT WE COMMIT TO

Answers, in working days



Within 2 working days

General questions



Within 10 working days of submission

Assessment feedback



Within 1 working day

Technical problems



Within 1 working day

Urgent welfare concerns

Published in DAIS-POL-024 Online Learning and Digital Delivery, and on every qualification page.

GETTING ON

Entry requirements



There is no specific prior knowledge a learner must have for this qualification.



This qualification is suitable for learners aged 16 and above.

✓ Learners may find it helpful if they have already achieved a Level 2 Digital Skills or Information Technology qualification.

✓ You will need a digital device and internet access, as Units 03 and 04 include practical tasks such as implementing a basic security control.

✓ Registration is at the discretion of the centre, in accordance with equality legislation.

THE COST

How paying works

TWO WAYS

Pay in full, which costs less than the published fee, or pay monthly. No interest and no credit agreement, and the payments stop on their own.

THE CURRENT FEE

On the qualification page at dataaischool.com, or ask us and we will tell you. It is not printed here, so nothing in this guide can quote you a price we are no longer charging.

Nothing is paid when you apply. Payment is taken only after you accept an offer, and we confirm the amounts with you first.



How long it takes. 150 guided learning hours, 220 total hours, self-paced online

BEFORE YOU START

What you need to take part



Device

Laptop or desktop computer



Operating system

Windows 10 or macOS 10.15 or later



Browser

Google Chrome or Mozilla Firefox, latest version



Internet speed

10 Mbps download and 5 Mbps upload



Webcam

Required for live sessions and identity verification



Microphone

Required for live sessions

Published in DAIS-POL-024, and told to every learner before enrolment.

IN MORE DETAIL

About this qualification

This is a regulated Level 3 qualification (NCFE qualification number 603/5762/9). It gives learners the chance to develop knowledge and skills relating to cyber security practices, with a view to seeking employment or proceeding to further study in this area. You study six mandatory units totalling 150 guided learning hours. Unit 01 covers the concepts of cyber security including confidentiality, integrity and availability, the consequences of inadequate cyber

security, core terminology, good and bad actors and their motivations, the sectors most vulnerable to attack, and the principles of security by design. Unit 02 covers cyber ...

ASKED BEFORE

Questions people ask

Who awards NCFE Level 3 Certificate in Cyber Security Practices, and how do I get my certificate?

NCFE Level 3 Certificate in Cyber Security Practices is awarded by NCFE, an Ofqual-approved awarding organisation, and sits on the Regulated Qualifications Framework (RQF). The qualification number is 603/5762/9. The Data and AI School of London is an NCFE approved centre (Account No. 11001657). We ...

How long does NCFE Level 3 Certificate in Cyber Security Practices take?

This qualification carries 150 guided learning hours and a total qualification time of 220 hours. It is studied online at your own pace, so how long it takes in calendar time depends on how much you can commit each week.

What do I need before I can start?

There is no specific prior knowledge a learner must have for this qualification. We assess every applicant individually and will tell you if a different level would suit you better.

Can I study this entirely online?

Yes. Teaching, materials and assessment are all delivered through our Moodle-based virtual learning environment, so you can study from anywhere in the UK. You need a laptop or desktop computer, a current version of Chrome or Firefox, and a broadband connection of at least 10 ...

The same answers as the qualification page, built from the same record.

NEXT STEP

Apply, or ask us first

Applying costs nothing and commits you to nothing. Eight short steps, no card details and no deposit. We check the qualification suits you and say so if another fits better, and payment is taken only after you accept an offer.

+44 207 0990 956

info@dataaischool.com

We reply within 2 working days



Scan for the full details

The Data and AI School of London. NCFE approved centre, account 11001657. Office LG06, 1 Quality Court, Chancery Lane, London WC2A 1HR. Company 16953235. ICO ZC086597.

