MODULE 3 · FREE COURSE

How Defenders Protect



Layers of defence, essential controls, security tools and incident response

Start Your Cybersecurity Career

In this module you will learn



Defence in depth
Why security works in layers



Essential controls
The basics that stop most attacks



Security tools
Firewall, EDR, XDR, SIEM and more



Incident response
What happens when an alert fires

03

Module 3 of 8
How Defenders Protect

About 20 minutes

Defence in depth: security in layers

- **People** Awareness training, phishing reporting
- **Identity** Strong passwords, MFA, least privilege
- **Devices** Patching, EDR, encryption
- **Network** Firewalls, segmentation, secure VPN
- **Applications** Secure coding, testing, updates
- **Data** Encryption, backups, access control



If one layer fails, the next one can still stop the attacker.

Four essentials that stop most attacks

Many breaches in Japan’s October 2026 wave used weaknesses these four controls address.

MFA

on email, VPN and admin accounts

Patch fast

internet-facing systems first

3-2-1

backups: 3 copies, 2 media, 1 offline

Least access

only the access each person needs (least privilege)

Practical baseline drawn from CIS Controls and NIST CSF guidance

Security tools, explained simply

Tool	What it does	Simple comparison
Firewall	Allows or blocks network traffic by rules	A building’s security gate
EDR	Watches each computer for suspicious behaviour	A guard in every room
XDR	Connects signals from devices, email, cloud and identity	A control room linking all guards
SIEM	Collects and analyses logs from everywhere	The building’s full CCTV archive
Email security	Filters phishing and malicious attachments	Checking every parcel at reception
Vulnerability scanner	Finds missing patches and weak settings	A regular safety inspection

How a security operations centre (SOC) works



Collect

Logs and alerts

Detect

Rules and analytics flag issues

Triage

Real threat or false alarm?

Investigate

Scope and root cause

Respond

Contain and fix

A SOC analyst role is one of the most common entry points into cybersecurity.

The incident response cycle



Prepare

Plans, tools, contacts

Detect and analyse

Confirm what happened

Contain

Stop it spreading

Eradicate and recover

Remove and restore

Learn

Improve for next time

Practise with tabletop exercises before a real incident.

Frameworks: the shared language of defence



NIST CSF 2.0

Six functions: Govern, Identify, Protect, Detect, Respond, Recover



ISO/IEC 27001

International standard for an information security management system



CIS Controls

A prioritised list of practical security actions

Quick check

1. Why does security use several layers instead of one strong tool?

2. Which tool collects and analyses logs from across an organisation?

3. In incident response, what is the goal of containment?

Answers are in the lesson article.

Key takeaways

- Defence in depth means no single failure leads to a breach.
- MFA, fast patching, isolated backups and least privilege stop most attacks.
- Incident response is a cycle: prepare, detect, contain, recover, learn.

Next: Module 4 · Careers and Roles in Cybersecurity