CYBERQUIZZER CHEAT SHEET

Kill Chain vs ATT&CK vs D3FEND

Three frameworks that are constantly confused because they overlap. They answer different questions — and exam items hinge on knowing which question is being asked.

Scan to drill this sheet

	Cyber Kill Chain Lockheed Martin, 2011	MITRE ATT&CK MITRE, 2013	D3FEND MITRE / NSA-funded, 2021
Answers	How does an intrusion **unfold**?	What exactly do adversaries **do**?	What can defenders **deploy** against it?
Point of view	Offensive, strategic	Offensive behaviour, observed	Defensive countermeasures
Shape	Linear chain — 7 phases, in order	Matrix — 14 tactics × ~200 techniques	Knowledge graph — countermeasures tied to techniques
Top level	Recon → Weaponize → Deliver → Exploit → Install → C2 → Actions	14 tactics, Reconnaissance through Impact	Model, Harden, Detect, Isolate, Deceive, Evict, Restore
ID format	None — phases are named, not numbered	`TA0001` · `T1566.001`	`D3-NTA` — mnemonic, not numeric
Reach for it when	Briefing non-specialists, or arguing for defence in depth	Threat hunting, detection coverage, red-team planning, IR reports	Choosing controls, and proving a detection gap is closed
Main limit	Assumes a tidy order; weak on insiders and cloud	Huge; no sequence and no prioritisation of its own	Youngest and least complete; thinner adoption

They stack, they don't compete

One row of the same intrusion, read through all three.

KILL CHAIN SAYS

Delivery — the weapon reached the target.

Useful for the exec summary: "we were breached at the delivery stage."

ATT&CK SAYS

`T1566.001` Spearphishing Attachment

Precise enough to hunt for, write a detection against, and compare with threat intel.

D3FEND SAYS

`D3-MA` Message Analysis

The countermeasure that answers it — plus what it does and does not cover.

Where people lose the mark

Three distinctions that decide most framework questions.

Sequence vs catalogue

If the question implies a **fixed order** of stages, it wants the Kill Chain. If it names a specific behaviour or an ID, it wants ATT&CK.

D3FEND is not "ATT&CK for defence"

ATT&CK already contains mitigations. D3FEND is a **vocabulary for countermeasures** — what a control actually does, expressed precisely enough to compare products.

Not a maturity model

None of the three scores you. They describe attacker and defender behaviour — **NIST CSF, CIS Controls and CMMC** are the frameworks that rate maturity.

Reading a comparison won't stick — turn it into instinct.

Drill which-framework questions until you spot the tell in the wording. Ten minutes a day, free forever, no card.

`cyberquizzer.com/go/frameworks-sheet`