NetSimIT

Player Guide

How to play, step by step

Gamified Network Attack Simulation Platform

v1.0

When NetSimIT loads, the Playbook Engine is locked. This is deliberate: it forces you to make your setup decisions — topology and defensive posture — before the clock starts.

- Choose a **Network Topology** tier and configure your **Defensive Posture** toggles in the left-hand panel (see sections 2 and 3).
- Press the green **Start Simulator** button in the top-right of the header.
- A full-screen countdown plays (3 → 2 → 1 → SIMULATION LIVE). Once it finishes, the Playbook Engine unlocks and you can select a playbook.
- You can still adjust your topology and defensive posture at any time after the simulator is live — the setup is not locked in permanently, only gated behind that first press.

2. The Dashboard

The screen is divided into three areas:

Area	What it contains
Left sidebar	Network Topology selector, Defensive Posture toggles, Crisis Communications, Compliance Status, and the (collapsible) Playbook Engine.
Centre canvas	The live network topology diagram. Scrollable and zoomable for the larger tiers. Every node is clickable once the simulator is live.
Bottom bar	The SIEM / Security Operations Log — a live, timestamped feed of every event: breaches, mitigations, compliance checks, comms decisions, and asset actions.

The Playbook Engine panel can be collapsed and expanded using the small arrow next to its heading, if you want more room to study the topology.

3. Network Topology

Pick how complex a network you want to defend. All four tiers include the same six core assets that every playbook can target (Edge Gateway, DMZ Web Server, Active Directory, HR/Finance Workstations, Core Database, and Cloud Storage) — the larger tiers simply add more surrounding infrastructure, servers, and endpoints around them.

Tier	Nodes	Links	Description
Simple Network	7	11	Just the essential perimeter and core assets — a flat, minimal network.
Medium Complexity	17	~24	A segmented perimeter/core network with dedicated infrastructure services.
Complex	27	41	A full single-site enterprise network — every layer from edge to cloud.
Complex Multi-Site	39	54	Headquarters, a branch office, and a colo data centre, linked over WAN.

On the diagram, node **shape** tells you what kind of asset it is: rounded squares are network infrastructure (routers, firewalls, switches), large circles are servers or cloud services, and small circles are user endpoints. Node **colour** tells you its current status:

Colour	Status	Meaning
Slate blue	Nominal	Untouched — no attack has reached this asset yet.
Cyan (pulsing)	Under attack	An attack phase is actively resolving against this asset.
Red	Compromised	The attack succeeded against this asset.

Colour	Status	Meaning
Green	Secured	This phase was stopped — by a defensive control, Incident Response, or your own asset action.

Data flowing between two nodes during an attack pivot is shown as a moving dot along the connecting line: **red** means the attack actually spread that way, **green** means the attempted move was stopped.

4. Defensive Posture

Six toggles represent your organisation-wide security capability. They can be changed at any time, including mid-attack — the simulator always checks the live toggle state at the moment each phase resolves.

Control	Full name	What it represents
SOC	Security Operations Center	Human-led monitoring and threat hunting.
MDR	Managed Detection & Response	Automated detection and containment playbooks.
CTI	Cyber Threat Intelligence	External threat feeds and campaign attribution.
VULN MGMT	Vulnerability Management	Patching, scanning, and secure configuration.
COMPLIANCE	Compliance Guard	Policy-as-code guardrails and mandated controls.
IR	Incident Response	A cross-cutting backstop — it does not stop a phase failing, but it can catch the spread before the attack reaches the next asset in the chain.

Every playbook lists which one or two controls are relevant to it ("Mitigated by: SOC / MDR", for example) on its card in the Playbook Engine. IR is different — it never appears on a playbook card, because it is not tied to a specific attack vector. It only matters once a phase has already failed: if IR is on, it can stop the attack spreading into the *next* phase, even though the current asset is still compromised.

5. Running a Playbook

Ten playbooks are available, each modelling a distinct real-world attack pattern across three phases (for example: Initial Access, Lateral Movement, Impact). Each phase presents two choices, and each choice is tied to a specific defensive control.

#	Playbook	Attack path	Mitigated by
1	Ransomware via Phishing	HR mailbox → Active Directory → Core Database	SOC / MDR
2	Supply Chain Compromise	DMZ Web Server → Core Database → Cloud Storage	Vulnerability Management
3	Insider Threat Data Theft	Core Database → HR Workstations → Cloud Storage	SOC / CTI
4	Cloud Misconfiguration Exploitation	Cloud Storage → Active Directory → Cloud Takeover	Vulnerability Mgmt / Compliance
5	Zero-Day Exploit on Edge Firewall	Edge Gateway → DMZ → Internal Reconnaissance	CTI / MDR
6	Business Email Compromise	HR/Finance → Active Directory → Wire Transfer	SOC / Compliance

#	Playbook	Attack path	Mitigated by
7	DDoS Attack with Extortion	Edge Gateway → DMZ → Extortion Demand	MDR
8	State-Sponsored APT	DMZ → Active Directory → Edge Gateway (firmware)	CTI / SOC
9	IoT / OT Environment Breach	HR/Finance Subnet → Active Directory → Core Database	Vulnerability Mgmt / MDR
10	API Hijacking (BOLA)	DMZ → Core Database → Cloud Storage	Compliance / SOC

5.1 Making a choice

Select a playbook, read the phase description, and pick one of the two choices. Behind the scenes, the simulator checks whether the control that choice depends on is currently switched on. If it is, the phase is **mitigated**. If not, it is **breached** — the targeted node turns red.

5.2 What happens after a breach

A breached phase does not just stop and wait for you to click again. If there is a next phase, the attack automatically pivots onward — the simulator picks the first available choice for the next phase and resolves it using your live toggle state, in quick succession, so you can watch exactly how fast a single gap in your defences turns into a full breach. A short "auto-pivoting" indicator appears in the Playbook Engine panel while this is happening.

The cascade stops the moment something actually catches it: a later phase's own control being on, Incident Response being on, or one of your own asset-level actions (see section 6) succeeding.

5.3 Outcomes

Verdict	What it means
ATTACK CONTAINED	The relevant control was on for the phase that stopped it.
INCIDENT CONTAINED BY IR	A control failed, but Incident Response caught the spread before it reached the next asset.
CONTAINED — ASSET RESPONSE	A control failed, but a response action you applied to that specific asset caught it instead.
FULL BREACH ACHIEVED	Nothing stopped the chain — every phase succeeded for the attacker.

6. Responding to Individual Assets

Once the simulator is live, click any node on the topology diagram to open its **Asset Response** panel. You can apply a response to any asset at any time — before it is attacked (a proactive, hardening move) or after it is already compromised (a reactive clean-up attempt). None of the six options is universally correct; each is a genuine trade-off, and the outcome is never guaranteed.

Action	What it does	Trade-off	Cost
Emergency Patch	Closes the specific vulnerability being exploited.	Strong protection; doesn’t undo an existing compromise.	Brief planned downtime.
Isolate / Quarantine	Disconnects the asset from the network entirely.	The only option that guarantees the attacker can’t pivot onward from this asset.	Legitimate traffic is cut off too.
Reset Credentials & Sessions	Invalidates every active session and credential on the asset.	Good against stolen-credential attacks; weaker once an attacker is further in.	Forced re-authentication for users.
Enhanced Monitoring	Raises logging and detection sensitivity, untouched otherwise.	Zero disruption; the weakest odds of actually stopping anything.	None.
Restore from Clean Backup	Wipes and rebuilds the asset from a known-clean image.	The best option for cleaning an already-compromised asset.	The heaviest downtime of any option.
Take No Action	A deliberate decision not to act right now.	A legitimate call — not a mistake by default.	None — and no protection either.

Isolate / Quarantine is the one option that is guaranteed to stop the asset being used as a pivot point for the attack to spread further, even if it doesn't manage to fully clean the asset. Every other option has a chance of success rather than a certainty — that uncertainty is deliberate: it mirrors the reality that not every emergency patch, backup restore, or credential reset actually lands in time.

A small badge appears on any node you've taken action on, showing which response is currently applied. You can reopen the panel and change your response at any point.

7. Crisis Communications

Three buttons in the left sidebar let you send Internal Comms, External Comms, or notify Regulatory Bodies. They can be pressed at any time, but the simulator judges each one against exactly what stage the incident is at the moment you press it — before an attack, mid-attack, once it's contained, or after a full breach — plus whether you've already sent any other comms. Each channel is a one-shot decision per playbook run: choose carefully.

- **Send Internal Comms** — best sent early, while the incident is still unfolding, so staff can help contain it and avoid repeating the same mistake.
- **Send External Comms** — best sent once the facts are settled (after containment or full breach) and ideally after internal teams already know what's happening.
- **Notify Regulatory Bodies** — only relevant once a real compromise has actually happened; sending it promptly matters, sending it only after a full breach risks missing a mandatory disclosure window.

Each decision is logged with a plain-English verdict, and a regulatory notification's timing directly affects the Cyber Resilience Bill entry in your Compliance Status panel.

8. Compliance Status & the SIEM Log

Every meaningful event — a breach, a mitigation, a comms decision — is checked against a real-world compliance framework and logged. The Compliance Status panel shows the most recent result for each of five frameworks; green means the last relevant check passed, red means it failed.

Framework	What it represents
NCSC CAF	UK NCSC Cyber Assessment Framework — outcome-based guidance for essential-service organisations.
Cyber Essentials Plus	UK government-backed technical certification for basic cyber hygiene controls.
Cyber Resilience Bill (CRB)	Placeholder framework used in-app for mandatory incident reporting and governance obligations, styled on the EU Cyber Resilience Act.
NIST CSF 2.0	US NIST Cybersecurity Framework — Identify, Protect, Detect, Respond, Recover.
SOC 2 Type II	AICPA Trust Services Criteria — audited controls for security, availability, and confidentiality.

The SIEM log at the bottom of the screen is colour-coded: green for a successful outcome, red for a breach, amber for a compliance entry, and cyan for a comms decision. It scrolls automatically and captures the entire session until you reset.

9. Session Debrief

When you press **Reset Simulator**, if you did anything meaningful that session (ran a playbook or sent a comms decision), a Session Debrief pops up: a short, plain-spoken — and deliberately slightly sarcastic — read on how the session went. It reflects your topology choice, your final defensive posture, how many attacks you contained versus how many became full breaches, how you used Incident Response and asset-level actions, and how well timed your comms decisions were.

It has a Close button and is **not saved anywhere** — once you close it, it is gone for good. Reset again and run a different setup to get a different debrief.

10. Tips for Getting the Most Out of It

- Try the same playbook twice with different toggles switched on to see exactly how much difference a single control makes.
- Turn every toggle off at least once and watch a full cascade play out — it's the fastest way to see how quickly a gap in your defences turns into a full breach.
- Use asset actions deliberately, not everywhere — hardening every node "just in case" is a valid strategy, but so is holding your response for the asset that actually matters most.
- Pay attention to the order you send comms in — internal before external is usually the safer call, and regulators generally shouldn't be your last thought.
- Read the Session Debrief before resetting again — it's the only place that gives you a whole-session view instead of a single-playbook one.
- Move up through the topology tiers as you get comfortable — Simple Network is a good place to learn the mechanics before tackling Complex Multi-Site.