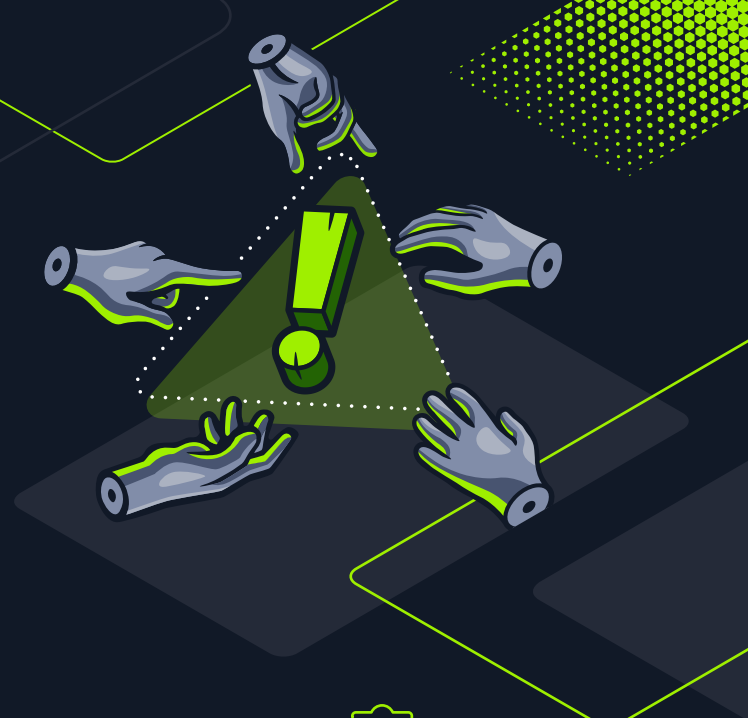


HTB Crisis Control

Realistic AI-enhanced on-premises cyber crisis simulations for executives and technical teams.



The cyber readiness gap



Lack of realism in drills

40% of CISOs feel unprepared with today's threat landscape, while 60% of directors report insufficient cyber resilience training.



Disjointed crisis response

Security, IT, legal, HR, and PR rarely rehearse together, leading to missteps and chaos under pressure.



New regulatory mandates

EU NIS2, DORA, and SEC rules demand swift documented incident response and 4-day disclosures for material incidents, forcing organizations to prove they can act and report quickly.

HTB Crisis Control drops organizations in **live-fire cyber incident simulations** that combine AI-enhanced injects in real-time adversary attacks. Teams from the SOC to the executive suite collaborate under pressure, exposing gaps in playbooks, improving coordination, and exiting with **board-ready evidence of resilience**.

- **Experience simulation** AI-enhanced crisis drills with real threat data and live red team attacks.
- **Strengthen cross-team coordination** – SOC, IR, and executives train together, breaking silos and improving response.
- **Ensure compliance & readiness** – Exercises mapped to NIST CSF, NIS2, DORA, and SEC requirements with board-ready reporting.

Hyper-realistic scenarios, delivered on-site by HTB experts

Each scenario mirrors nation-state attacks, cybercrime campaigns, or emerging threats that push teams to rehearse under real-world pressure.

Operation Thunderstrike



Volt Typhoon

Simulate a state-grade Volt Typhoon strike to test executive recovery playbooks under realistic pressure.

Anglerfish Anomaly



Cuttlefish Malware

Uncover stealthy router compromises threatening remote employees and clients.

Operation Silk Road Serpent



Mustang Panda

Face an espionage campaign designed to steal sensitive information.

Operation Ghost in the Machine



APT33

Rehearse an IT/OT cyberattack on national energy infrastructure.

Scattered Wealth



Scattered Spider

Confront a fast-moving cybercrime group using social engineering and extortion.

Operation Snowfall



Snowflake Breach

Stress-test cloud defenses against a major data breach and decision-making during a high-stakes crisis.

Turn simulation into strategy



Each exercise concludes with a comprehensive, board-ready report that validates playbooks, highlights strengths and areas for improvement, and reinforces existing procedures.

Expose gaps in response and communication.

Utilize recommendations tailored to targeted training and continuous improvement.

Access technical annexes detailing the attack chain and system compromises.

Harness actionable insights to satisfy auditors and regulators. Justify resource allocation.



Where organizations see impact

Cross-functional breach and crisis simulation

Build trust and eliminate silos across IT, security, and business units.



Governance, risk and compliance testing

Rehearse NIS2, DORA, and SEC obligations by simulating strict reporting timelines and third-party breach impacts.

NIS 2

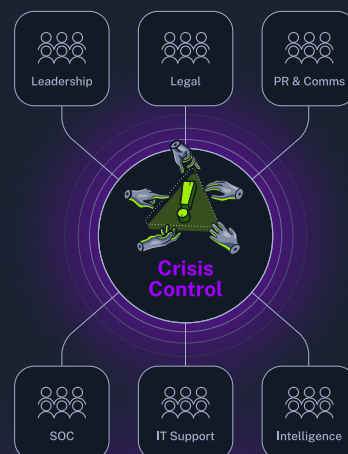
DORA

SEC

Technical threat hunting and incident response

Engage attackers and defenders in real-time while executives experience decision-making under pressure.

Live Fire Team TTX



“

Crisis Control is a realistic approach to simulating a cyber incident. The tabletop was expertly scoped, planned, and delivered, touching on the key areas that matter during crisis management. Having the team on site for briefings not only makes this more real but also improves the feedback cycle during such an exercise. The technical environment does a great job at emulating benign noise, enabling a truly realistic experience.

Michael Lamb
Head of SOC