Incident Response Testing - Simulation

Ensuring organisational resilience against cyber threats requires a robust and well-practised incident response capability.

NCC Group's Incident Simulation Exercise is designed to enhance cyber readiness by providing tailored, hands-on scenarios that test and strengthen your team's ability to detect, respond to, and recover from significant cyber incidents.

Improves maturity of incident response capability

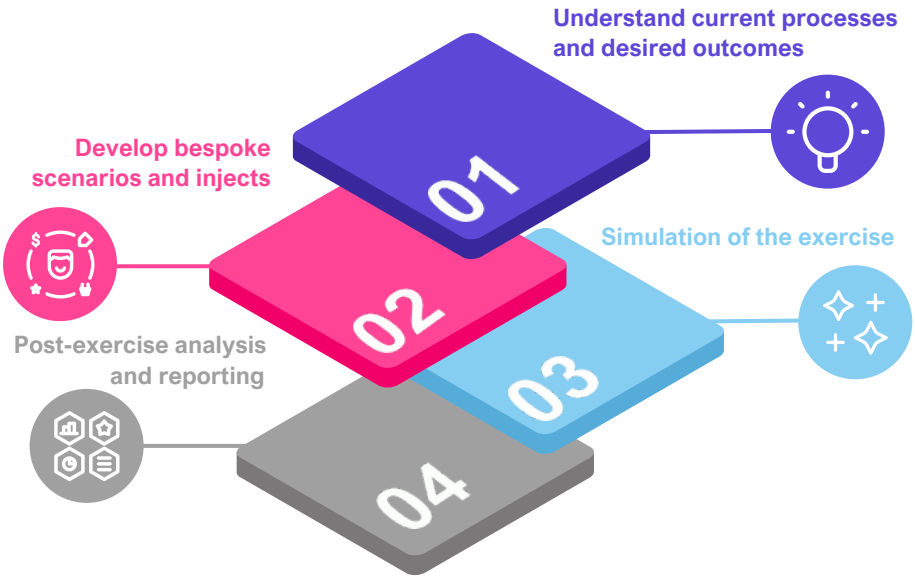
NCC Group's Incident Simulation has been specifically designed to assess incident management controls and provide assurance of their effectiveness. Its holistic approach will look at controls from the identification of an incident all the way to implementing lessons learnt.

Provides alignment to industry incident response models

Changes to organisational objectives or structure may sometimes render incident management controls ineffective. NCC Group's Incident Simulation, therefore, is aligned to your organisational objectives whilst considering industry best practice standards. NCC Group will combine this with experience from cyber threats in your sector, to ensure the exercise identifies key areas for improvement and is actionable and understandable to wide audience of stakeholders.

Improves awareness of incident management within the organization

The Incident Simulation process will include reviews of all relevant parts of the business, not just the IT team. The review will consider other functions of the business that maybe involved in areas such as data protection, legal and marketing. Creation of incident response plans will include plans for all these business functions so they are actively involved in the event of an incident.



Benefits

- Improves maturity of incident response capability
- Provides alignment to industry incident response models.
- Improves awareness of incident management within the organisation
- Provides repeatable processes for incident response handling
- Ensures cyber incident and breaches are correctly reported.

Diagnose & Scope

Develop a scenario for you specific to your Business

Discovery to align the simulation with your environment and objectives.

We begin with a structured discovery to understand your current processes, stakeholders, maturity, and desired outcomes. This ensures the exercise is relevant, risk-aligned, and designed to test real decision paths across technical, operational, and strategic levels.

Develop Master Events List

Design Scenarios & Master Events List

Bespoke scenarios with realistic injects and clear outcomes.

We co-create tailored scenarios and injects that reflect your threat landscape (including AI-enabled adversary behaviours), then map them to a Master Events List with expected events, decision points, and outcomes. A sample scenario may involve privileged-account compromise leading to firewall changes and control-bypass, crafted to test detection, escalation, containment, and recovery.

Develop Exercise Protocols

Briefings & Protocols

Prepare participants; clarify aims, roles, and control measures.

Participants receive notes and briefings so everyone understands the exercise aims, objectives, command structure, and control measures. We tailor protocols across Technical (IT/Cyber), Operational (Silver/Gold), and Strategic (Exec, Legal, Comms, Regulatory) audiences to promote realistic, cross-functional engagement

Develop Exercise Injects

Run the Simulation Exercise

Facilitated tabletop delivery with dynamic and realistic scenarios and injects.

A theory-based or practical tabletop exercise (typically up to six hours) guides teams through interactive scenarios and decision making. Consultants introduce realistic scenarios and injects (e.g., phishing, malware, ransomware) and an AI-driven threat module to help participants "think like an attacker," challenging detection and response capabilities under pressure.

Report

Debrief & Report

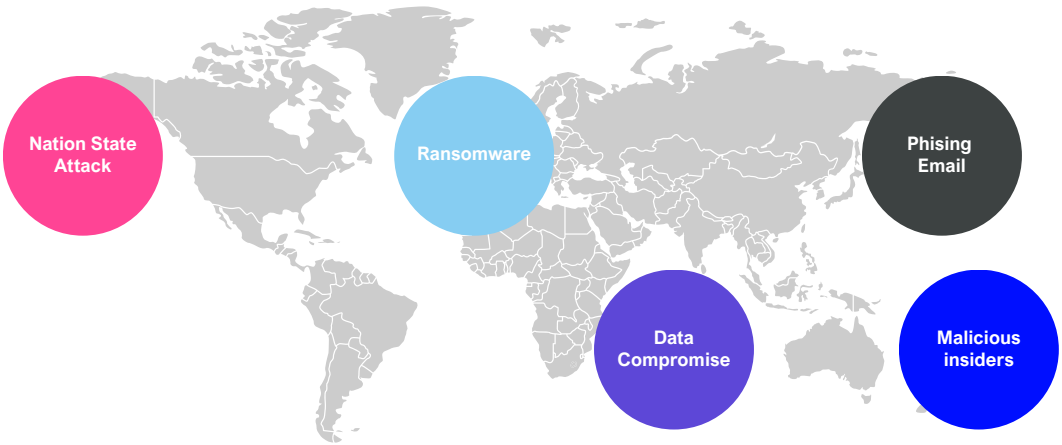
Actionable insights, performance observations, and recommendations.

We conduct an immediate debrief, then deliver a comprehensive report that captures performance, observations, and actionable recommendations. Where appropriate, we recommend follow-on activities (e.g., vulnerability scanning, threat modelling, penetration testing) to strengthen resilience end-to-end.

NCC Group's Incident Simulation service has been purposefully designed to help an organisation understand strengths and weaknesses in responding to a security Incident. NCC Group has developed scenario-based exercises with the aim of:

- Validating an organisation's ability to identify the critical information requirements in a fast-moving incident scenario.
- Validating an organisation's ability to manage a cyber-security incident that originates from multiple attack routes as part of a coordinated campaign;
- Validating an organisation's ability to generate appropriate data to support the identification of an incident's point of origin for subsequent analysis;
- Confirming the process for notifying relevant parties within an organisation that a targeted security incident has occurred and identifying the interactions with the organisation unit to invoke an effective response;
- Confirming the process for deploying appropriate resources required to manage a targeted cyber-security incident; and,
- Confirming the means by which critical information is logged and reported during a cyber-security incident.

The scenario is tailored to an organisation's specific infrastructure and critical systems, and systems and can be based on subjects and scenarios, which the organisation has been receiving through normal operations. The scenarios can also be aimed at various levels –such as technically focused, aimed at testing the IT team response, or exploring wider issues such as data protection, breach reporting so as to include wider parts of the organisation such as DPO an[illegible] legal all the way to exercising the Executive (Gold Team).



Summary

- The NCC Group Incident Simulation allows organisations to gain a view of their Incident Response (IR) maturity and identify improvements in their incident response plans.
- The Incident Simulation also allows organisations to provide training awareness for relevant organisational functions and staff, through the form of a real-life scenario.
- NCC Group works extensively in the cyber security industry delivering over 20,000 cyber consultancy days every year from our various business units.
- NCC Group's clients include Tier One banks, global technology providers, global manufacturers and FTSE 100 organisations to the industry. Our client base is truly global across North America, Europe, the Middle East and Asia and Australasia.
- Each element of an organisation is involved including Cyber Incident Response Services, Threat intelligence, Penetration Testing and Red Teaming, Cyber Security Reviews, PCI, Security Improvement Programmes, Strategy work, Vulnerability scanning Managed Security services such as SOC's and SIEM solutions.
- NCC Group's IR capability and experience is unparalleled with a fully global Cyber Incident Response Team and specialist IR consultants.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with organisations to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are well placed to help organisations identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com