Cyber Attack Simulation

Assessing individual applications and systems in isolation is no longer sufficient to protect your organisation. Instead, it is imperative that real-world adversarial behaviours and techniques are emulated to determine your ability to detect and respond to a cyber attack. Organisations must use more complex and skilled attack primitives to better defend and protect their business.

The Solution

A Cyber Attack Simulation assessment is a covert engagement designed to identify weaknesses in your cyber preventive controls, staff security awareness and to challenge your internal security team's detection and response capabilities.

The ultimate objective of the engagement is to gain access to your critical assets. NCC Group will assess your organisation through the emulation of adversarial behaviours and techniques that are used by real-world threat actors, including hacktivists, cyber criminals, cyber spies, state-sponsored actors as well as the ever-present insider threat.

Throughout the simulated attack, a number of different attack scenarios will be planned and attempted in order of likely success.

Features

Cyber Attack Simulation engagements follow dynamic attack paths that attempt to reach the agreed goals and objectives. These may include:

- Targeting your publicly accessible services such as email and web servers, VPNs, Virtual Desktop Environments, and Office 365 instances.
- Targeting your staff via their web and email clients to assess their level of cyber security awareness and the effectiveness of your security controls around communications.
- Attempts to discover and execute privilege escalation and credential access techniques.
- Attempts to achieve objectives, whether that's the ability to cause an impact or gain access to critical data sets or systems.
- Assessing whether your workstation and server lockdowns are effectively restricting access to sensitive data as well as preventing unauthorised applications and custom payloads, that may allow privilege escalation.
- Establishing covert egress channels to enable command and control, persistent access, and a means of collecting and exfiltrating data.
- Determining to what extent lateral movement is possible within your network.

Benefits

Expert:
Delivered by NCC Group's experienced Cyber Attack Simulation consultants who have a wealth of knowledge and experience conducting Advanced Persistent Threat (APT) attacks.

Intelligence-led:
All attack scenarios are derived from the threat intelligence gathered on your organisation, mimicking the most realistic threats your organisation faces.

Comprehensive reporting:
Executive-level summary of the business risks you face along with appropriate mitigation strategies, supported with thorough technical appendices.

Thorough:
A methodology that assesses your ability to protect yourself against all stages of the cyber kill chain.

Safe:
All activities are performed to pre-agreed rules of engagement, minimising the risk of any adverse operational impact.

Simulated Attack Phases

NCC Group will assess your defensive capability against the key phases of the attack methodology. Each phase is mapped to the MITRE ATT&CK framework and further analysed against your ability to detect or respond to the threat actors' activities.

In Phase

The "In" phase focuses on the methods used by threat actors to gain their initial foothold on the system and the activities utilised on the target devices. This includes the initial access, command executions, setting up persistence, and local privilege escalation.

Through Phase

The "Through" phase mimics the tactics, techniques and procedures used by threat actors to evade detection, move laterally to other hosts, identify how the target systems are accessed, and achieve the privileges to do so.

Out Phase

The "Out" phase is where the specific objectives for the target system are performed, what the impact is on the Confidentiality, Integrity, or Availability aspects relevant to that system. The most common option is how any data is moved out of the target organisation.

Metrics

By measuring the detection capabilities within these three phases and cross- referencing them with the MITRE ATT&CK framework it is possible to identify common areas of weakness and prioritise remediation. The metrics recorded can be used for comparison to show year-on-year improvements.

Cyber Attack Simulation Services

A full Cyber Attack Simulation can be provided in its entirety or as two separate services, covering the "In," "Through," and "Out" phases.

External Attack Simulation

The External Attack Simulation focuses on the "In" phase of a comprehensive Cyber Attack Simulation. It emulates a real-world threat actor attempting to gain an initial foothold on the system and the activities utilised on the target devices.

These simulations aim to understand the threats posed by remote attackers. They identify how threat actors might breach an environment. The engagement focuses on gaining initial access to the environment by attempting to exploiting vulnerabilities in exposed services, compromising web applications, password attacks, attempting to bypass multi-factor authentication and by employing social engineering tactics like targeted phishing and vishing campaigns.

Assumed Breach Simulation

The Assumed Breach Simulation targets the "Through" and "Out" phases of a comprehensive Cyber Attack Simulation. It emulates a real-world threat actor operating from a position of assumed compromise, aiming to achieve specific goals.

These simulations focus on understanding the threats posed by attackers who already have a presence on the network. This can include mimicking both insider threats and successful remote attacks along with more tailored scenarios such as supply chain attacks, exploiting an organisation's people, processes, and technology to gain sufficient access to achieve their objectives.

What to Expect

We will provide your organisation with a detailed report that provides an attacker's eye view of your organisation and its operations. NCC Group will highlight weaknesses in your systems, processes, and security architecture. This will be tailored to different audiences to provide technical signatures and heuristics to Blue Teamers and threat hunters, making strategic recommendations for the board and improving the state of security in both the short and long term.

NCC Group will provide a report that contains:

- Executive-level summary of your business risk and means of addressing it.
- Details of the deficiencies in your cyber controls, general staff awareness, and your Blue Team's detection and response capabilities.
- Likely threat actors, attack scenarios and the potential outcomes of a cyber breach for your organisation.
- A prioritised remediation roadmap addressing both strategic and tactical issues.
- Thorough technical appendices detailing all identified deficiencies and suggested remedial actions.

A post-assessment briefing will also be provided to give you an opportunity to discuss the engagement's findings and recommended next steps.

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

+44 (0)161 209 5200

bidteam@nccgroup.com