Collaborative Attack Simulation

Organisations are increasingly finding that vulnerability mitigation strategies alone are no longer sufficient to defend their business.

The need to understand the attacker mindset, interpret ongoing malicious activities and actively defend are becoming increasingly important components of an appropriate defence in depth strategy.

Organisations must ensure their security operations teams are appropriately skilled to detect and respond to the real-world adversarial behaviours they face.

The Solution

A Collaborative Attack Simulation combines the Red and Blue Team activity and sees NCC Group attack simulation experts embedded within your internal security operations (Blue Team) during the simulation of a real-world attack.

The assessment aims to collaboratively replicate attacks to identify opportunities for improvement within your Blue Team's detection capabilities, remediation processes, and removal procedures.

This service can be delivered in a number of modes with either a focus on education or benchmarking. In all cases, full details of attack timelines, techniques used and an analysis of any detection and response capabilities will be provided.

The key differences between the differing approaches are at what point elements of this analysis are presented and to what degree we assist your Blue Team in their response to the attack.

Benefits

Immediate Uplift:
Both the education of your staff and configuration of your systems will be noticeably improved by the conclusion of the engagement.

Bespoke:
Every engagement is tailored to your organisation's specific concerns, team composition, and desired outcomes.

Expert:
Delivered by NCC Group's experienced Red Team, supported where appropriate by Incident Response consultants who have a wealth of knowledge and experience conducting and defending against Advanced Persistent Threat (APT) attacks.

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

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.

Defensive Maturity Model

NCC Group will assess your defensive capability against the key phases of the attack methodology:

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Furthermore, each phase will be mapped to the MITRE ATT&CK framework and further analysed against your ability to perform the following actions against threat actor activities:

- Detect
- Deny
- Disrupt
- Degrade
- Deceive

What to Expect

The assessment will be performed from three perspectives:

Tool coverage:
Details of current defensive tooling and the level of coverage

Blue Team process:
Evaluation of capability and effective response to varying threat actor techniques for each part of the Kill Chain

Maturity rating:
A modified version of the Capability Maturity Model (CMM)

Following the completion of the assessment, our team of experts will provide a detailed report with a number of recommended prioritised actions to both the Blue Team and the wider IT team.

The results of which will be used to strengthen the detection mechanisms deployed in your environment.

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

+44 (0)161 209 5200

bidteam@nccgroup.com