Compromise Assessments

NCC Group's Compromise Assessment aims to identify any malicious behaviours indicative of a host being compromised across an organisation's estate. The scope and resulting price of an assessment can be tailored to your requirements and is designed to answer the questions "Has my network estate been compromised?", "Are attackers currently in my estate?"

Threat actors are increasingly employing sophisticated attack methods that can bypass traditional protection mechanisms, including Anti-Virus software and even advanced Managed Security Services. NCC Group offer a comprehensive range of Compromise Assessment services, to help you determine the effectiveness of your defenses,
identify any active compromises and detect historic attacker activity within your environment.

The Compromise Assessment service is extremely flexible. It can provide an independent, technical, assessment of the current security posture.

- **Post Incident or suspect activity** – looking for attacker footholds or new attacker activity.
- **Supplier due diligence** – plays a crucial role when connecting networks. This helps to demonstrate, and evidence due diligence
- **Good Security practice** – to support network health checks and penetration testing.

Our Compromise Assessment aims to identify any malicious behaviours indicative of a host being compromised across an organisation's estate. The service includes

- Access to a dedicated DFIR consultant who will deliver your Compromise Assessment end to end.
- Identification of prevalent attack methods and mot common threat vectors
- Use of automated tools to hunt for threats and identify sophisticated attack methods
- Detection of configuration errors that could be exploited.
- Identification of breaches in corporate security policies.
- Investigations enriched with our leading global threat intelligence to enhance detection and improve readiness.

NCC Group are able to deliver the Compromise Assessment service utilizing your pre-deployed tooling upon request,
but we also have partnerships with industry-leading vendors such as CrowdStrike, Sentinel One and Nextron Thor that can be deployed when required.

Benefits

- Compromise Assessments performed by individuals with Incident Response (IR) and Threat Intelligence (TI) experience
- Utilises bespoke research from NCC Group's global Threat Intelligence team
- Identifies gaps in best practice and the presence of sophisticated attackers
- Uses a comprehensive approach including both network and host investigation
- Delivered by a team accredited by both NCSC and CREST

Assessment Steps

The lifecycle of a Compromise Assessment includes:

1. Deployment of industry-leading tooling from our EDR partners to detect indicators of compromise across compatible endpoints.
2. Review of security control logs to identify gaps in detection.
3. Utilise tools to improve visibility across your corporate IT estate.
4. Data is ingested into NCC Group's analysis platform or our industry-leading EDR partners for anomaly detection.
5. Data is augmented and enriched with threat intelligence from our dedicated global team.
6. DFIR consultants analyse data for potential compromises.
7. A report is provided with an explanation of findings and remediation suggestions within ten days of analysis completion.
8. If a compromise is detected, the service can be swiftly pivoted into an incident response engagement to provide you actionable recommendations to begin taking containment actions.

More in-depth Compromise Assessments may also include the following:

Bespoke Threat Intelligence: Customized threat intelligence tailored to specific needs.
Bespoke Log Review: Detailed review of logs for signs of compromise.
Password Audit: Examination of password policies and practices.
Privileged Credential Assessment: Review of privileged access and credentials.
Vulnerability Scanning: Identification of vulnerabilities within the network.
Configuration Review: Assessment of system configurations for security weaknesses.
Dedicated Malware Analysis: Examination of malware to understand its impact.
Targeted Forensics: In-depth forensic analysis to uncover detailed evidence of compromise.

Each Compromise Assessment is customised to the environment, tailoring the deployed technologies, blending them to the needs of the client. Therefore, it is crucial to capture and understand the technical layout and business context of the assurance required.

Summary

Modern networks are extremely complex, often with a mix of legacy systems alongside modern platforms. They inherently represent a mixture of risks as they provide the services to a mixture of users and technologies.

The compromise assessment looks to capture these risks, rationally analyse them and provide a view to the level of risk associated with the network, which can later inform security decisions.

Understanding these risks allows for better decision making in today's every changing agile IT environments.

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