An NCC Group case study

Cyber Incident Response, Containment and Remediation for a FTSE 100

At a glance

Organisation:
FTSE 100 company

Challenge:
Perform breach containment following a large scale security incident

Solution:
NCC Group brought in senior advisors to liaise with the client and contain and secure the wider security estate to prevent the attackers returning

Results:
The incident was dealt with, and areas of improvement were identified, enhancing the security posture of the organisation and helping to ensure similar attacks can be handled in the future

Short Summary

NCC Group were enlisted by a FTSE 100 company to perform breach containment following a major security incident. NCC Group's Cyber Incident Response Team (CIRT) were brought in to handle and respond to the incident initially. Meanwhile, NCC Group's Security Improvement and Remediation team (SIR), were enlisted to bolster the organisation's cyber knowledge and expertise to ensure that recommended changes could be implemented rapidly and successfully. This improved the overall security posture of the organisation, and helped to ensure that similar attacks could be appropriately handled going forward.

About NCC Group

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

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

Summary

NCC Group were enlisted by a leading FTSE 100 company to perform breach containment following a large-scale security incident from advanced attackers. The incident investigation highlighted some resource challenges for the IT Security team to be able to keep pace with the increasing demand of cyber threats. These challenges required attention by the senior decision makers of the organisation.

NCC Group successfully identified the threats, managed the response to the breach, and implemented measures to contain the threat during the course of the investigation. Security Improvements were implemented as part of an agile bespoke programme which significantly reduced the risk of a future incident occurring.

Challenge

The incident demonstrated to the organisation that it needed to prioritise its IT security systems to mitigate potential vulnerabilities going forward.

The complexity of the estate and the requirement to maintain business as usual operations made improvements slow and unwieldy. NCC Group successfully prioritised, implemented and managed the response and longer term improvements to dramatically reduce the risk exposure.

Solution

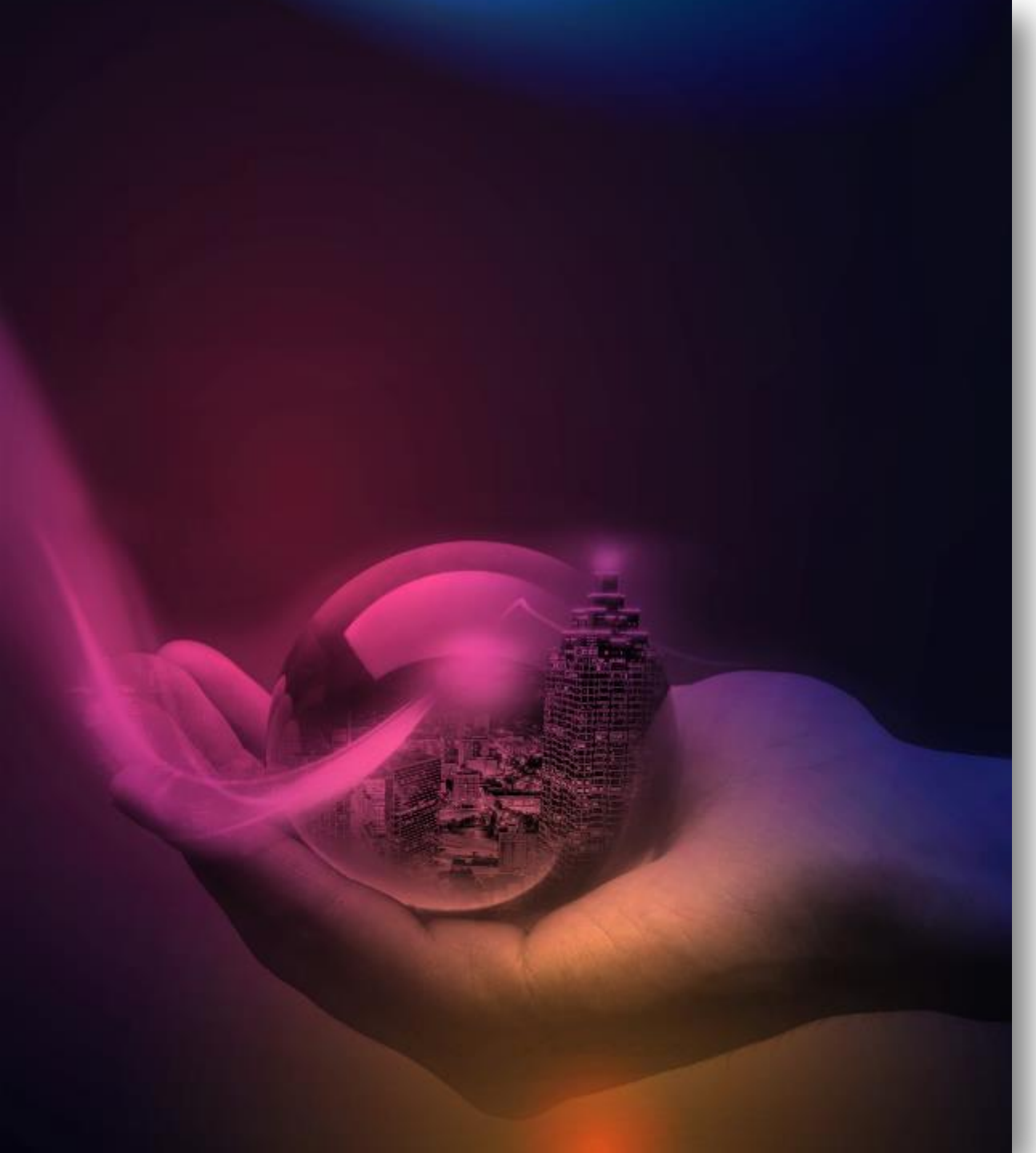
The organisation enlisted the support of NCC Group's Cyber Incident Response Team (CIRT) service to perform DFIR and threat hunting across host, logs, and networks to fully understand the extent of the infiltration.

As the extent of the incident was revealed, NCC Group senior advisors were also drafted in to liaise with the board of the organisation and manage the incident from a technical standpoint, whilst providing valuable insight to the senior non-technical audience.

The in-house IT team were not able to act on the findings that NCC Group had presented during the course of the investigation due to resource constraints and lack of advanced security knowledge. This led the organisation to engage with NCC Group's Security Improvement and Remediation (SIR) team.

The team included a senior cyber advisor and programme manager, who were able to contextualise the broader issues to the senior board of the organisation. The team also planned out the remediation steps for the containment and eradication phase; and the critical priorities for implementing security improvement fixes.

The main priority for the SIR team was to secure the wider security estate of the organisation to prevent the attackers from returning by rapidly reducing risk exposure. This was done by tasking the in-house IT function with concise work packages, as well as putting in place floating IT security gurus who acted as trouble shooters. This ensured the recommended changes could be implemented seamlessly and rapidly.



Results

The initial incident was dealt with rapidly and comprehensively thanks to NCC Group's incident response team and the close integration with senior cyber advisors and the Security Improvement team. The attackers were fully removed from the environment and the security posture of the estate was raised to prevent and crucially detect similar activity.

The vulnerabilities and areas of improvement for the organisation's overall security environment which were identified during the course of the investigation were acted upon by the SIR team, which accounted for a third of the work that NCC Group conducted for the company.

Critically, the prioritised work packages implemented cooperatively by NCC Group's SIR team and the client In-house IT team rapidly enhanced the security posture.

This not only ensured that the implemented changes were appropriately prioritised and fit for purpose, but also that the organisation was able to put in place a more strategic direction for security improvement going forward, which included long term monitoring of a Managed Detection and Response (MDR) offering from NCC Group to ensure that it is much more difficult for similar incidents go undetected.