Solution Brief

Retail Compromise Assessment

Optimise Peak Trading with confidence by exposing hidden threats and ensure your network is secure.

The golden quarter represent immense opportunity but also heightened risk. With increased digital transactions, customer data flow, and operational pressure, cyber threats can silently infiltrate your environment, jeopardising revenue, reputation, and customer trust.

NCC Group's Compromise Assessment helps you uncover hidden threats, validate the effectiveness of existing defences, and ensure your networks are secure, so you can trade with confidence when it matters most.

Why Retailers Need This Now

Threat actors are increasingly targeting retail environments with sophisticated techniques that bypass traditional security controls. These attacks often go unnoticed until damage is done, especially during high-traffic periods.

Our Retail Compromise Assessment is designed to:

- Detect active compromises and historic attacker activity
- Validate your security posture ahead of peak trading
- Provide actionable insights to reduce risk before it impacts operations

Our targeted assessment

Our targeted Retail Compromise Assessment will identify any malicious behaviours indicative of a host being compromised across your estate.

We utilise **SentinelOne** to efficiently triage hosts, combining industry-leading tools with expert consultant analysis.

Included in the service:

- Deployment of SentinelOne agent for 30 days
- Analysis of detections using NCC Group's Threat Intelligence
- Identity and vulnerability assessment reports via SentinelOne EDR platform
- Industry leading tool combined with consultant-led analysis

The Process

1. Provision SentinelOne platform and provide agent for deployment
2. Deployment period of 1 week following
3. Analysis takes place over 2-3 weeks following deployment
4. Evidence of active compromise will be raised immediately should such activity be identified
5. Report provided 1 week after completion of analysis
6. Incident Response: If a compromise is detected, the service can be swiftly pivoted into an incident response engagement to provide you with actionable recommendations to begin taking containment actions

Optional Add-Ons

Enhance your assessment with additional modules

Security Tool Review:
Ingest data from an existing deployed security tool to provide further evidence to review

SIEM Log Review:
Review logs that are ingested into an existing SIEM tool to provide further evidence to review

External Attack Surface Mapping One-off Scan:
Provides a point in time view of your external attack surface and appetite for risk

Customisation:
Should there be another NCC Group service or additional requirement you wish to action, we can tailor modules to meet your specific retail needs

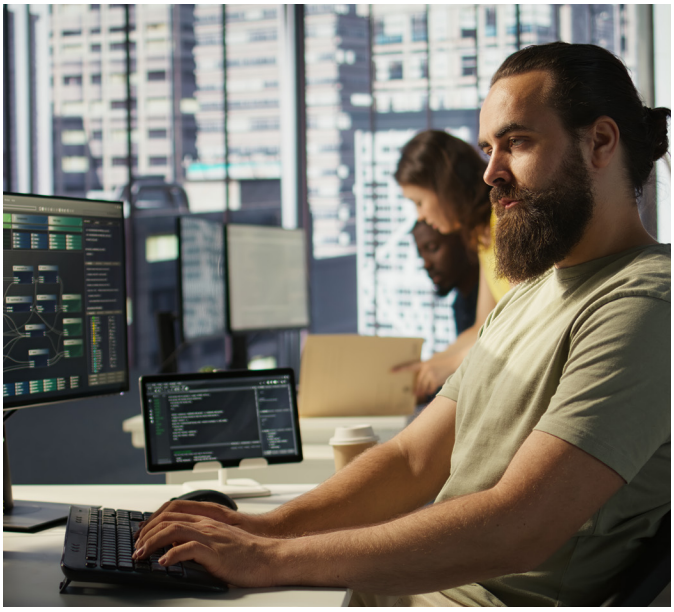
Why NCC Group

Our Digital Forensics and Incident Response (DFIR) team brings global expertise in investigating complex incidents across retail environments.

Whether you're gearing up for Black Friday, Christmas, or any high-volume trading period, NCC Group ensures you're not just ready—but resilient

NCSC-Certified Response
Cyber Incident Response Team accredited to NCSC CIR Scheme Standard and Enhanced Level.

BSI-certified Advanced Persistent Threat Response Provider



Detect signs of compromise and protect your estate from cyber threats

Get in touch to speak to member of our team about options which suit your needs.

0161 209 5111

Get in touch

We're a people powered, tech-enabled global cyber security and resilience company with over 2000 colleagues around the world.

For over 25 years we've been trusted by the world's leading companies and Governments to manage and deliver cyber resilience, working together to create a more secure digital future.

We are proud to deliver important and groundbreaking projects for our clients.