Cyber Incident Response

Nettitude provides urgent Incident Response services to major online retailer

Industry: **Online Retailer**

Location: Global

Profile:
This client is a leading global online retailer, placed within the top 50 businesses of the e-commerce market.

The Client's Issue

The client suspected that their IT Network had been compromised. However, they possessed insufficient skills and experience to investigate and secure their environment from further attacks. The client had also observed a malware alert from their anti-virus solution within a vital server, and had been alerted to other suspicious activity in their admin accounts but were unsure how to proceed.

Possible Impact

The average cost of a breach

The cost of an average data breach is $3.86 million while the average resolution time is 280 days. Incident response management helps reduce the impact of a cyber breach by swiftly sending triage to your organisation.
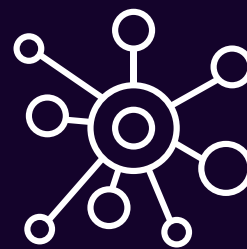
£3,860,000 | **+9 months**
The average cost of a data breach | The average resolution time following a breach
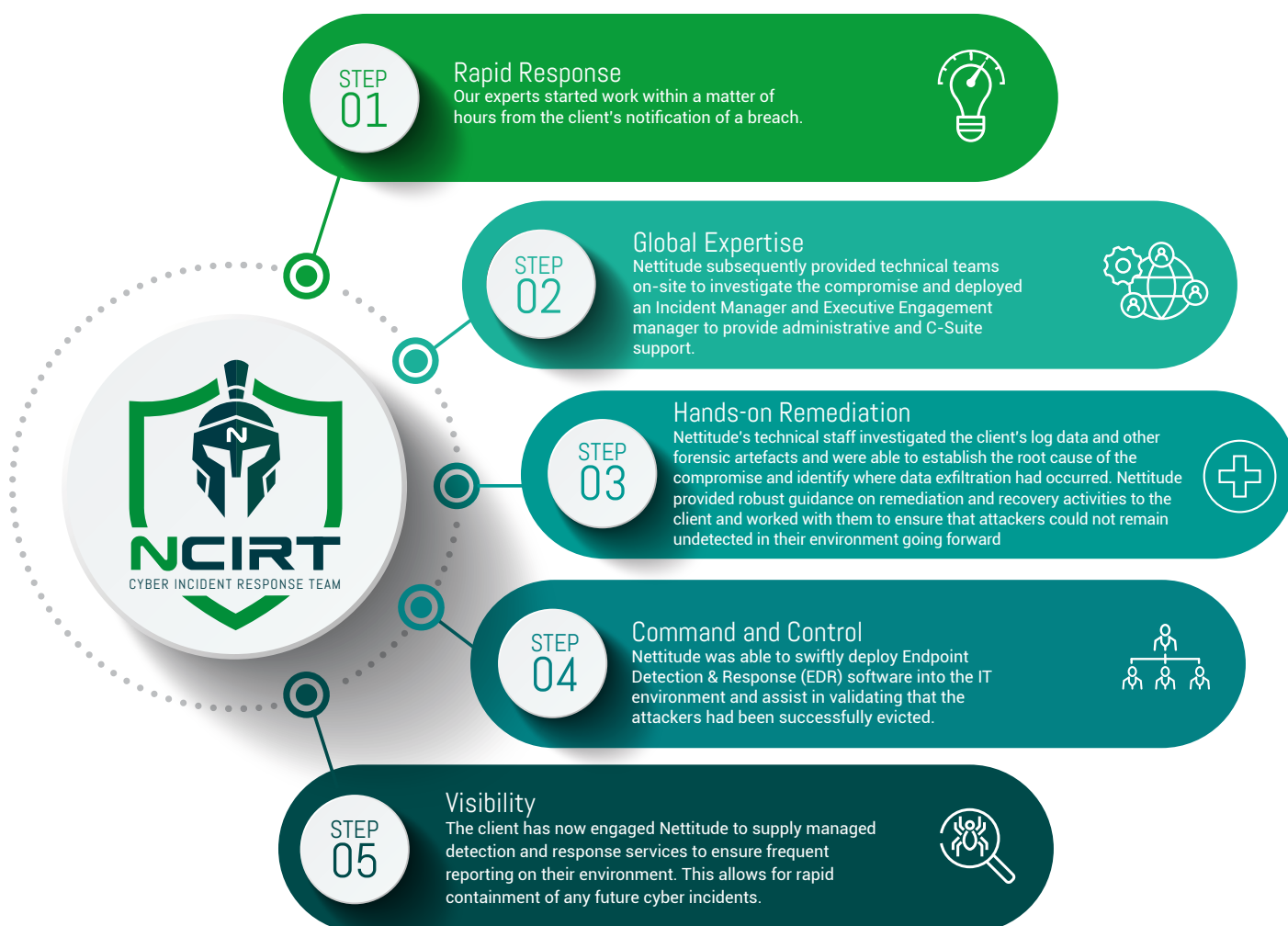
NETTITUDE
AN LRQA COMPANY

Nettitude's Solution

Nettitude's Cyber Incident Response Team (NCIRT) is committed to helping you at every stage of the incident response lifecycle. From preparation, eradication, and remediation, through to lessons learnt.

As part of our Managed Incident Response Service, we provide a full range of tactical and strategic solutions tailored to your environment and organisational needs ensuring a robust security posture when you need it the most.

Time period
2022 onward

How NCIRT Successfully Resolved The Incident

STEP 01
Rapid Response
Our experts started work within a matter of hours from the client's notification of a breach.

STEP 02
Global Expertise
Nettitude subsequently provided technical teams on-site to investigate the compromise and deployed an Incident Manager and Executive Engagement manager to provide administrative and C-Suite support.

STEP 03
Hands-on Remediation
Nettitude's technical staff investigated the client's log data and other forensic artefacts and were able to establish the root cause of the compromise and identify where data exfiltration had occurred. Nettitude provided robust guidance on remediation and recovery activities to the client and worked with them to ensure that attackers could not remain undetected in their environment going forward

STEP 04
Command and Control
Nettitude was able to swiftly deploy Endpoint Detection & Response (EDR) software into the IT environment and assist in validating that the attackers had been successfully evicted.

STEP 05
Visibility
The client has now engaged Nettitude to supply managed detection and response services to ensure frequent reporting on their environment. This allows for rapid containment of any future cyber incidents.

NCIRT
CYBER INCIDENT RESPONSE TEAM

Results

Using leading industry technology and certified experts, the NCIRT managed, contained, and assisted in remediation of the client's cyber breach, ensuring minimum impact on business.

This client now benefits from a Managed Incident Response retainer providing them with assurance when they most need it.

Client's Outcome:

Nettitude's early advice prevented a full deployment of ransomware malware across our entire IT network. Their timely response and investigation enabled the business to reduce the impact of the breach and continue operations.

The Client Now Benefits From:

24 Hour IR Hotline	Bank of retained hours aligned and ready for an incident

NCIRT guaranteed response. Four hour SLA (IR consultant contact)

Nettitude guided and assisted onboarding process for all incident response services:
- IR policy and procedure review
- IR table top planning and readiness exercise

Access to NCIRT expert technical team

Aligned Cyber Response Engement Manager and Cyber Response Incident Manager

Key Results:

- Rapid containment of security breach
- Improved security posture
- Control of network
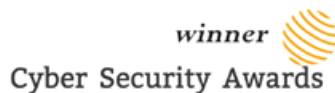- Visibility of network
- Assurance of expert assistance

Nettitude Services Deployed

- Incident Response
- Certified Incident Response Analysts & Consultants
- Cyber Response Incident Manager
- Endpoint Detection & Response Software

About Nettitude

Founded in 2003, Nettitude is an award-winning provider of cybersecurity services, bringing innovative thought leadership to the ever-evolving cybersecurity marketplace. Leveraging our tenacious curiosity, we aim to operate at the forefront of the industry.

We aim to empower our clients, imparting knowledge, advice, and assistance to help them deploy changes in behaviour, understanding, and where appropriate, culture.

CREST

VA | PEN TEST | STAR Intelligence-led PT | STAR Threat intelligence | CSIR | SOC | OVS

PCi Security Standards Council ™
QUALIFIED SECURITY ASSESSOR

PCi Security Standards Council ™
APPROVED SCANNING VENDOR

CYBER ESSENTIALS

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

Computing Security Awards
★ FINALIST ★

winner
Cyber Security Awards

CYBERSECURITY BREAKTHROUGH AWARD 2020
THREAT INTELLIGENCE COMPANY OF THE YEAR

bsi
ISO 9001 Quality Management Systems CERTIFIED
ISO/IEC 27001 Information Security Management CERTIFIED

cis
ISO 14001:2004 REGISTERED FIRM

UK Head Office
Jephson Court, 1 Tancred
Close, Leamington
Spa, CV31 3RZ
+44 345 520 0085

Americas
50 Broad Street,
Suite 403, New
York, NY 10004
+1 212 335 2238

Asia Pacific
18 Cross Street,
#02-101, Suite S2039,
Singapore,
048423

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com

NETTITUDE
AN LRQA COMPANY