LRQA NETTITUDE

Case Study

SOC Services: Managed Vulnerability Scanning Penetration Testing

LRQA Nettitude provides vulnerability scanning and penetration testing for a leading investment company

Industry:
Financial

Location:
UK

Profile:
This client is a leading UK-based pension investment company

Why do organisations need vulnerability scanning?

Being able to identify vulnerabilities before they are exploited is crucial in today's connected world. Every year thousands of vulnerabilities are discovered and organisations scramble to stay on top of them.

This client had previously experienced a high number of vulnerabilities, with a significant delay between reporting and remediation.

The rising cyber threat

28%

A quarter of all UK cyber-attacks target companies within the financial sector. This accounted for 28% of all reported breaches within the past 12 months.

83%

In 2022 over 49,000 fraudulent incidents across UK businesses were recorded as a result of cybercrime. Around 83% of these were the result of a targeted phishing attack.

Time period

Three year managed vulnerability scanning
Six-monthly penetration testing

Vulnerability scanning and penetration testing

VULNERABILITY SCANNING

Vulnerability scanning identifies vulnerabilities within an environment and is much wider in scope than penetration testing. It is used to estimate how susceptible the environment is to different vulnerabilities. Vulnerability scanning uses automated tools that scan an environment on a regular and repeatable basis to generate a report based on risk exposure. Vulnerability scanning does not try to exploit the vulnerabilities and is normally non-intrusive.

PENETRATION TESTING

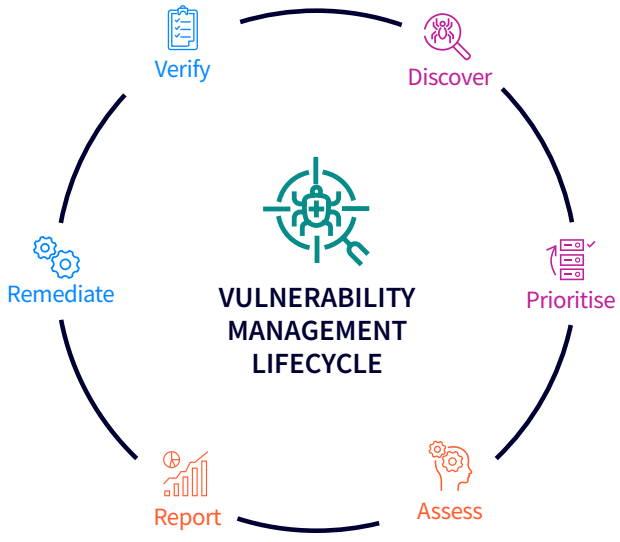
Penetration testing goes beyond vulnerability scanning. It attempts to identify and then actively exploit previously unknown weaknesses or vulnerabilities within an environment and is much more rigorous than vulnerability scanning. Penetration testing is not normally an automated process and involves human interaction to a targeted scope. Penetration testing is normally performed infrequently, a few times a year, to a set schedule.

Both vulnerability scanning and pen testing are critical to ensure a comprehensive view of threats and vulnerabilities an organisation could be facing.

On-boarding the client

Setting up the client for managed vulnerability scanning was smooth and simple, done via a scoping document and kick-off call. This process is then repeated ahead of six-monthly penetration tests:

- **Steps** - Ensuring LRQA Nettitude has the correct authorisation to perform the test.
- **Dates** - Confirm the dates of engagement.
- **Point of contact** - Verified who the point of contact is, and how we want to communicate during the test and all subsequent reports.
- **Environment** – Determine which environments are included e.g. servers or workstations.
- **Firewalls** - Assess whether anything is blocking connections or could prevent testing.
- **Credentials** - Request low-privilege user accounts for testing purposes.



LRQA NETTITUDE

Key results:

- Improved security and control
- Rapid identification of vulnerability
- Elimination of blindspots
- Improvement of operation efficiencies

LRQA Nettitude services deployed

- Managed Vulnerability Scanning
- Penetration Testing

Results

LRQA Nettitude's Managed Vulnerability Scanning provided our client with highly accredited expertise, combined with Gartner magic quadrant leading security technology to deliver industry-leading protection.

The services implemented provided the client with a proactive and threat-led approach; informed by our offensive and threat intelligence teams to protect against the latest industry threats.

Regular penetration testing also provides the client with a real-world view of where and how attackers can exploit weaknesses in their infrastructure, networks, people, and processes.

A test isn't just a test at LRQA Nettitude.
The client also benefitted from:

- A high-level management report
- An in-depth technical review document
- Actionable insights prioritised by impact
- Support to fix what needs to be fixed in a timescale that suits them
- An end-of-engagement debrief via the delivering consultant

Findings summary

LRQA Nettitude identified six vulnerabilities during the engagement. The following table shows the categorisation by severity:

Critical	High	Medium	Low	Info
0	1	3	1	1

What our client said

"From scoping through to conclusion, our experience with LRQA Nettitude has been excellent. The scoping documentation is clear and detailed enough to minimise the time required to agree scope/cost and to focus on the testing we need.

The remote testing procedure is straightforward and allows us to execute a test without having to bring a tester physically to site, reducing the work required from our side. The tester was approachable and communicative throughout and did not require us to be constantly available in order for them to execute the test.

Post-test documentation is comprehensive, well laid out, and provides excellent detail and evidence of findings and further reading. Follow-up questions on remediation are also dealt with quickly and concisely."

Get in touch
Visit **www.nettitude.com** for more information
or email enquiries to **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES

Americas
810 Seventh Avenue
Suite 1110
New York
NY 10019

Asia Pacific
460 Alexandra Road
#15-01
mTower
Singapore 119963

Europe
Fidiou 9
Athina
106 78
Greece