VULNERABILITY MANAGEMENT AND PENETRATION TESTING

UNDERSTANDING AND MEDIATING VULNERABILITIES WITHIN YOUR ORGANISATION'S ENVIRONMENTS.

KEY BENEFITS

24/7*365
Continuous monitoring with reporting scheduled as required, for a comparable cost of an annual penetration test.

DEMONSTRATES COMPLIANCE
A report that can be referenced by auditors for compliance, including Cyber Essentials.

THREE COMPLEMETARY SOLUTIONS
Complementary solutions provide clients with flexibility to ensure they have the service that meets their needs

AS THE THREAT LANDSCAPE CONTINUES TO EXPAND, IT'S VITAL THAT ORGANISATIONS ADOPT A STRATEGY OF CONTINUOUS ENUMERATION. GIVEN THE POTENTIAL EXPOSURE TO THREATS CAUSED BY WEAKNESSES AND MISCONFIGURATIONS IN THEIR CLOUD ENVIRONMENT AND WIDER IT ESTATE, THERE IS AN INCREASED RISK OF DATA BREACHES AND PRIVACY NONCOMPLIANCE.

Node4 has three offerings to meet this need. They are:

- **Vulnerability Scanning**
- **Web Application Pen Testing**
- **External Penetration Testing**

These are standalone options, but also act as a complementary solutions.

VULNERABILITY SCANNING VS PENETRATION TESTING

People have different understandings of the terms vulnerability scanning and penetration testing. They are closely related services, but it's not uncommon for organisations to believe they need one service, when in fact, it's the other. That's why we work with our clients to understand their needs and advise on the best approach.

Node4's definition of the differences are as follows:

VULNERABILITY MANAGEMENT

This scans an organisation's estate and focuses on providing security details on active network components and services – internal and external - and the risks and vulnerabilities of those components and services.

These include open network ports, missing software patches and command line vulnerabilities, such as SQL injection and buffer overflow. Vulnerability Management can be likened to checking if the doors and windows on a house are all locked.

PENETRATION TESTING

This combines the use of scanning tools with cyber-security specialists to inspect internet-facing applications or websites for security flaws and loopholes which can be exploited by attackers.

Pen testing uses the vulnerabilities identified as part of vulnerability management and tries to leverage them to successfully 'hack' into an organisation. It's more akin to actively trying to break into a house.

VULNERABILITY SCANNING

We believe that every organisation should know their vulnerabilities. That's why Node4 offers an automated service that allows clients to schedule and receive reports on tests carried out by automated systems that use AI to fulfil the roll of an attacker.

Once completed, a report is created to inform remediation. That report can be referenced by auditors for compliance purposes, such as Cyber Essentials, and also used to inform a more detailed penetration test.

WEB APPLICATION PENETRATION TESTING

Web Service Scanning is designed to understand the code and format of the web service being utilised. This can be any web endpoint, including API's, websites and/or other web applications.

This service uses the latest tools to find weaknesses in the code or format of your service to confirm if it can be exploited.

We also provide a detailed report of our findings with recommendations, which we will discuss in detail.

EXTERNAL PENETRATION TESTING

Node4's CREST-certified pen testing team utilise human intelligence to enhance manual and automated scans. This will help you identify how an actor might attempt to get into your network via external IPs.

We provide a detailed report of our findings, using our knowledge and expertise to advise how to strengthen weak points in the network or service being scanned, which we talk take you through.

DISCOVER MORE ABOUT NODE4'S VULNERABILITY MANAGEMENT AND PENETRATION TESTING SERVICES BY CONTACTING US ON THE DETAILS BELOW.