

# Vulnerability Assessment Service

Quickly identify known security vulnerabilities



# MANAGED VULNERABILITY ASSESSMENT

---

Comtact's Managed Vulnerability Assessment Service provides regular vulnerability assessments of your IT infrastructure to identify exposure to 'known' vulnerabilities - the most frequent method used by hackers.

Forming part of a range of information security and assurance services, Comtact's Vulnerability Assessment represents a highly impactful step to reduce your security exposure, build a roadmap for further improvement and focus your security spend/resources.

- Includes a clear, in-depth report, categorised by risk, with expert recommendations/next actions.

VULNERABILITY  
ASSESSMENT SERVICES



INTERNAL  
VULNERABILITY  
SCANS

EXTERNAL  
VULNERABILITY  
SCANS

## INTERNAL VULNERABILITY SCANS

---

- Conducted on-site, from within the corporate firewall, an Internal Vulnerability Scan detects security issues such as unpatched (or unsupported) software, applications and operating systems, or incomplete roll-out of security technologies.
- Quickly identifies known security vulnerabilities (such as those exploited by WannaCry), including both Windows and non-Windows-based vulnerabilities – and will almost identify critical issues, particularly if no previous vulnerability assessment programme is in place.

## EXTERNAL VULNERABILITY SCANS

---

- An External Vulnerability Scan assesses your security from an Internet-based (external) viewpoint – the viewpoint of a hacker.
- Focuses on external-facing IP addresses, detecting vulnerabilities including open ports, application-level weaknesses and weak credentials for protocols including SMTP, POP3, HTTP and VPN.

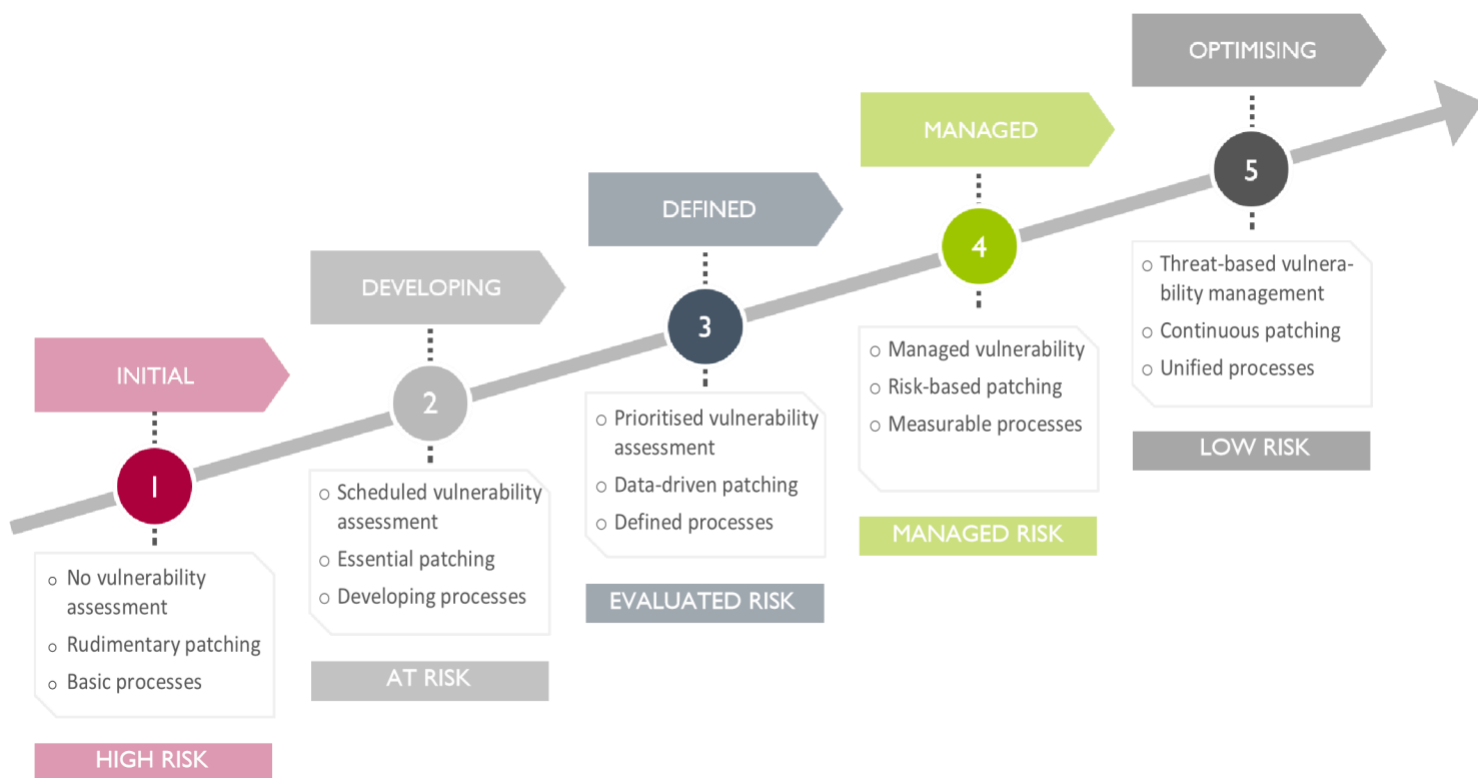
### WHY REGULARLY SCAN FOR VULNERABILITIES?

A vulnerability scan is a technical security assessment using a set of tools to scan your network for known vulnerabilities (e.g. open ports, unpatched security updates).

- A vulnerability scan (Internal and External) is a requirement for the government-backed Cyber Essentials PLUS scheme.
- Scans can be performed Internally on the network (from the inside), or Externally (from the outside looking in). It is important to remember that a vulnerability scan provides a detailed snapshot of your vulnerabilities, a point in time – so should be used as part of an on-going vulnerability & patch management programme.

### DEVELOPING A VULNERABILITY MANAGEMENT ROADMAP

By following a clear, defined roadmap, Comtact can help you assess, develop and refine your vulnerability management processes to reduce security risks.



## VULNERABILITY AS SERVICES



### ADVANCED SCANNING

Experienced testers gather data to assess the state of current security and expert controls.



### EXPERT ANALYSIS

Expert analysis to profile and rank recommendations, ranked by risk and impact.

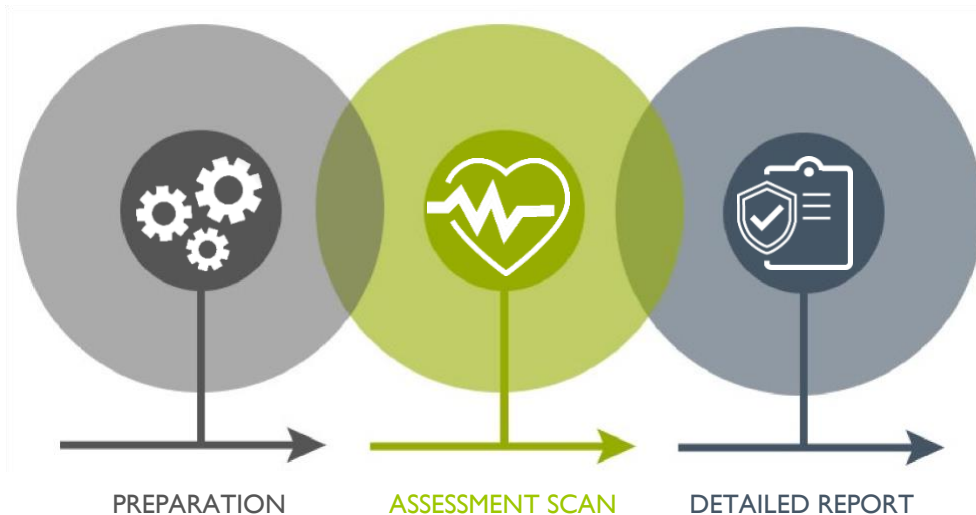


### RISK-BASED REPORT

In-depth report, with risk vulnerabilities,

## WHAT TO EXPECT

Contact's vulnerability assessment scans follow a defined methodology to identify possible points of weaknesses and compromise.



---

## PREPARATION & SCOPE

The first step is to discuss, define and agree the scope of the scanning requirements, as well as controls, methodology, and communication processes to meet the client's infrastructure requirements.

---

## EXECUTION OF VULNERABILITY SCAN

To agreed protocols, Internal scans are conducted on-site, whereas external scans are performed remotely. Expert data analysis identifies and classifies exposure to known vulnerabilities.

---

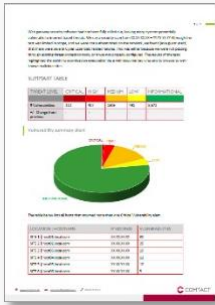
## REPORT, RECOMMENDATIONS & NEXT ACTIONS

Following analysis of the data, an easy to digest, in-depth report documents the discovered vulnerabilities, based on risk – suitable for both technical personnel and senior management. The remediations and recommended next actions provide an essential roadmap to identify the next steps which will have the greatest impact, by severity, volume and task.

---

## THE DETAILED RISK-BASED REPORT ON THE FINDINGS INCLUDE:

- ✓ Summary: Overview of key threats and business risks, in a high-level format suitable for non-technical Directors.
- ✓ Technical: Detailed technical report, highlighting organisation's exposure to known internal and external vulnerabilities
- ✓ Risk scoring: Report includes a vulnerability scoring system to rate issues discovered, based on severity and remediation impact.
- ✓ Priority plan & next actions: A prioritised action plan based on potential risk to emphasise the most effective course of action.



## VIEW SAMPLE REPORT

Take a look at a sample report to understand the approach, critical security intelligence and actionable steps with our vulnerability assessments.

[www.comtact.co.uk/vulnerability-scans](http://www.comtact.co.uk/vulnerability-scans)

## FAQs

### INTERNAL vs. EXTERNAL SCANS



74% OF ORGANISATIONS  
FIND KNOWN CRITICAL VULNERABILITIES

#### INTERNAL VULNERABILITY SCAN

Performed from within the firewall, Internal vulnerability scans identify network vulnerabilities locally, such as required software patches, or incomplete deployment of security technologies.

#### EXTERNAL VULNERABILITY SCAN

Performed external to the network (from the outside looking in – the viewpoint of a hacker), External vulnerability scans look for vulnerabilities at your network perimeter, such as open ports, or unprotected connections.

### VULNERABILITY SCAN vs. PEN TEST

Is a Vulnerability Scan the same as a Pen Test?

No. A vulnerability scan is sometimes labelled as a “Pen Test”, but the two are very different. But both play an important role in reducing security vulnerabilities and represent an important part in assessing and improving your security defences.

## VULNERABILITY SCAN

A Vulnerability Scan is a technical assessment, which simply identifies and reports on known vulnerabilities, using software tools to scan your IT estate to identify unpatched software, open ports, or incomplete security software deployment (for example).

## PENETRATION TEST

A Penetration Test (Pen Test) is a manual test – and attempts to exploit these vulnerabilities to determine whether unauthorised access or other malicious activity is possible – an ethical hack.

## ABOUT COMCONTACT LTD

---

Operating 24/7, Comcontact Ltd. is a specialist Cyber Security and IT Managed Service Provider, supporting clients day and night from our ISO27001-accredited UK Security Operations Centre (SOC).

As part of a multi-layer security defence, Comcontact's Cyber Defence Team identifies, protects and secures some of the UK's leading organisations, as part of a multi-layer security defence to target and disrupt hacker behaviour.

