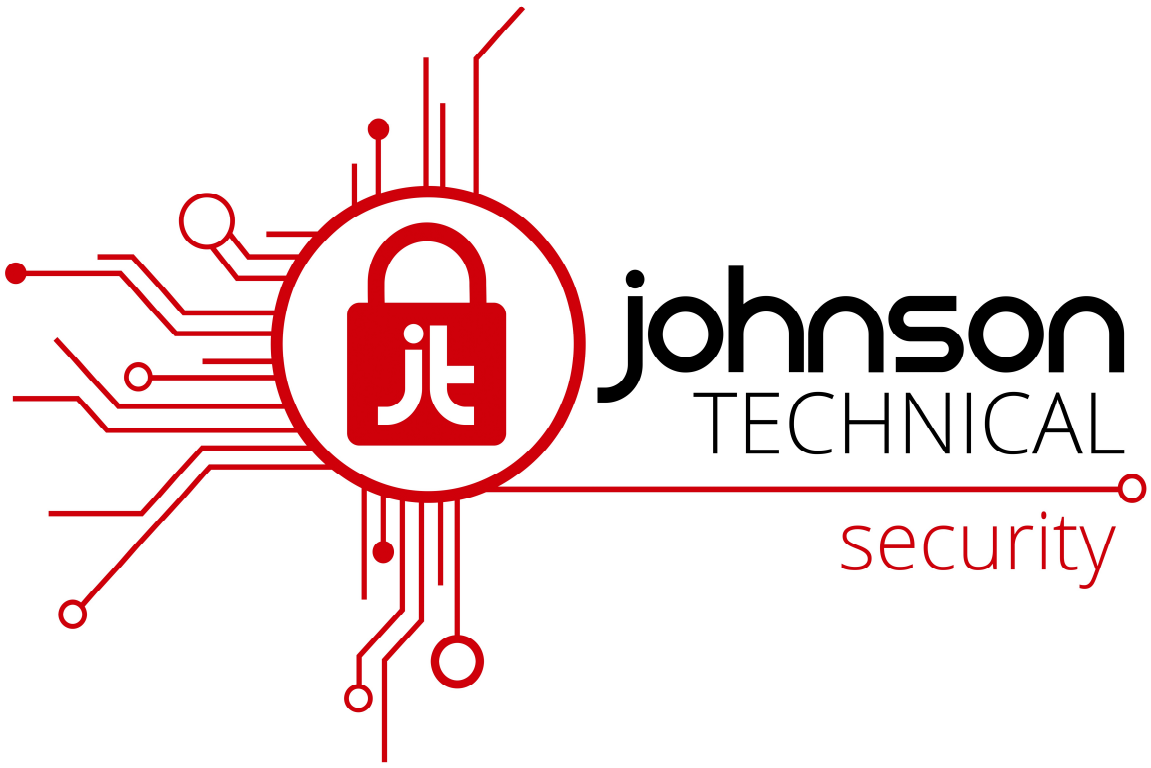
Vulnerability Assessment

Scope of Work



T: 01277 888799 E: hello@jtechnical.net W: www.jtsecurity.net

What is a Vulnerability Assessment?

A vulnerability assessment, also known as vulnerability analysis, is a process used to locate and identify any security-level defects (vulnerabilities) in a network or infrastructure. Vulnerability assessments help businesses pinpoint any vulnerabilities (such as coding bugs, security holes, etc.) before they have the chance to be compromised.

The primary goals of a vulnerability assessment are to identify these vulnerabilities, document them, report them to the organization, and provide details on how to resolve the issues.

How can a Vulnerability Assessment help your business?

A vulnerability assessment provides an organization with information on the security weaknesses in its environment and provides direction on how to assess the risks associated with those weaknesses and evolving threats. This process offers the organisation a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard.

Scope of Work:
- Planning and Defining Scope
- Gathering Information on the Infrastructure
- Internal Network Scan
- External Network Perimeter Scan
- Report Findings

Vulnerability Assessment:

Step 1: The cyber security team identify the way business processes are carried out in the organisation and agreed with the business on the assessment scope.

Step 2: The security team will gather information about hardware and software present in the network environment. More specifically, the team define whether the network has open ports or services that shouldn't be open and get an understanding of the software and driver configurations. They will also identify virtual and physical servers, as well as the security measures that were already in place, such as firewalls and intrusion detection and prevention systems (IPS/IDS).

Step 3: The security team will use a variety of scanning tools which will be configured upon gaining the necessary information on the network. The internal and External scans will then be carried out to accomplish the desired results.

Step 4: The security team will provide the organisation with a report containing the list of vulnerabilities, mentioning their severity level (low, medium or high) and defining corrective measures to reduce risks.