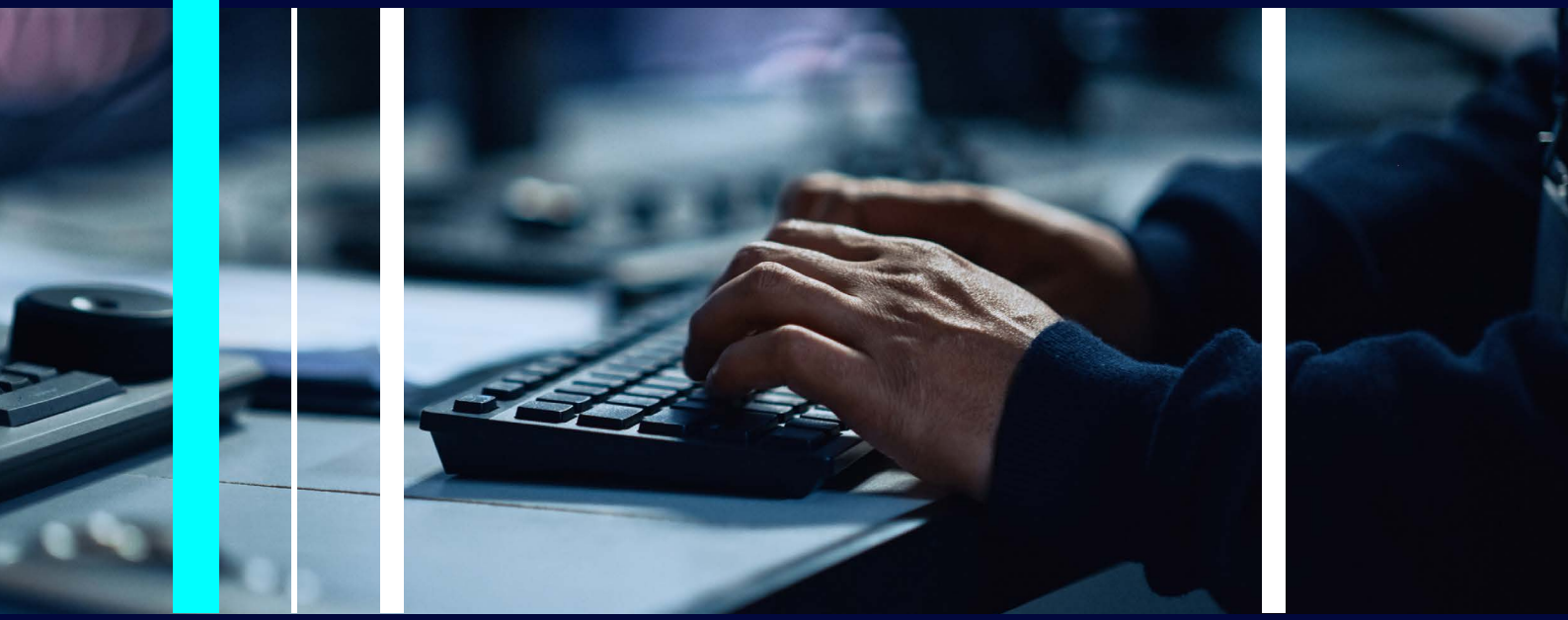
Cybersecurity vulnerability management



Overview

Vulnerability management is the process of identifying, evaluating, remediating, and reporting on security vulnerabilities in systems and the software that runs on them. It is vital that organisations have a vulnerability management programme in place to reduce the risk of an attack or data breach.

Capita's holistic vulnerability management offering is an ongoing support service that gives our clients access to a broad capability of cyber experts who monitor systems and technology for vulnerabilities and advise on the best way to deploy the relevant updates and fixes.

Spread across three main service lines: -

- Our blended vulnerability assessment focuses on external facing IPs and uses a combination of automated scanning and manual testing techniques. These assist your business in the effective ongoing management of system vulnerabilities, whether they be on web servers, database servers, firewalls, routers, or other key components of the business IT infrastructure.
- The Capita managed vulnerability assessment management service is focused on Internal networks and uses a cloud-based vulnerability tool delivered via a SaaS deployment model which leverages shared and extensible core services within a highly scalable multi-tenant cloud infrastructure. This service description covers the vulnerability management modules where customers can monitor their assets for vulnerabilities and reduce organizational risk. The system is supported by physical and virtual appliances that can be installed in minutes and require no maintenance or software updates by the user.
- And finally, the Capita PCI – ASV – This service utilizes the Qualys scanning tool to provide regular vulnerability scanning which allows your business to maintain crucial elements of PCI compliance. Capita's holistic vulnerability management offering is an ongoing support service that gives our clients access to a broad capability of cyber experts who monitor systems and technology for vulnerabilities and advise on the best way to deploy the relevant updates and fixes.

Like a support service, these offerings give peace of mind to leaders that a robust process is in place to keep on top of any potential vulnerabilities that could be exploited or attacked.

Capita

Our approach

Agree scope

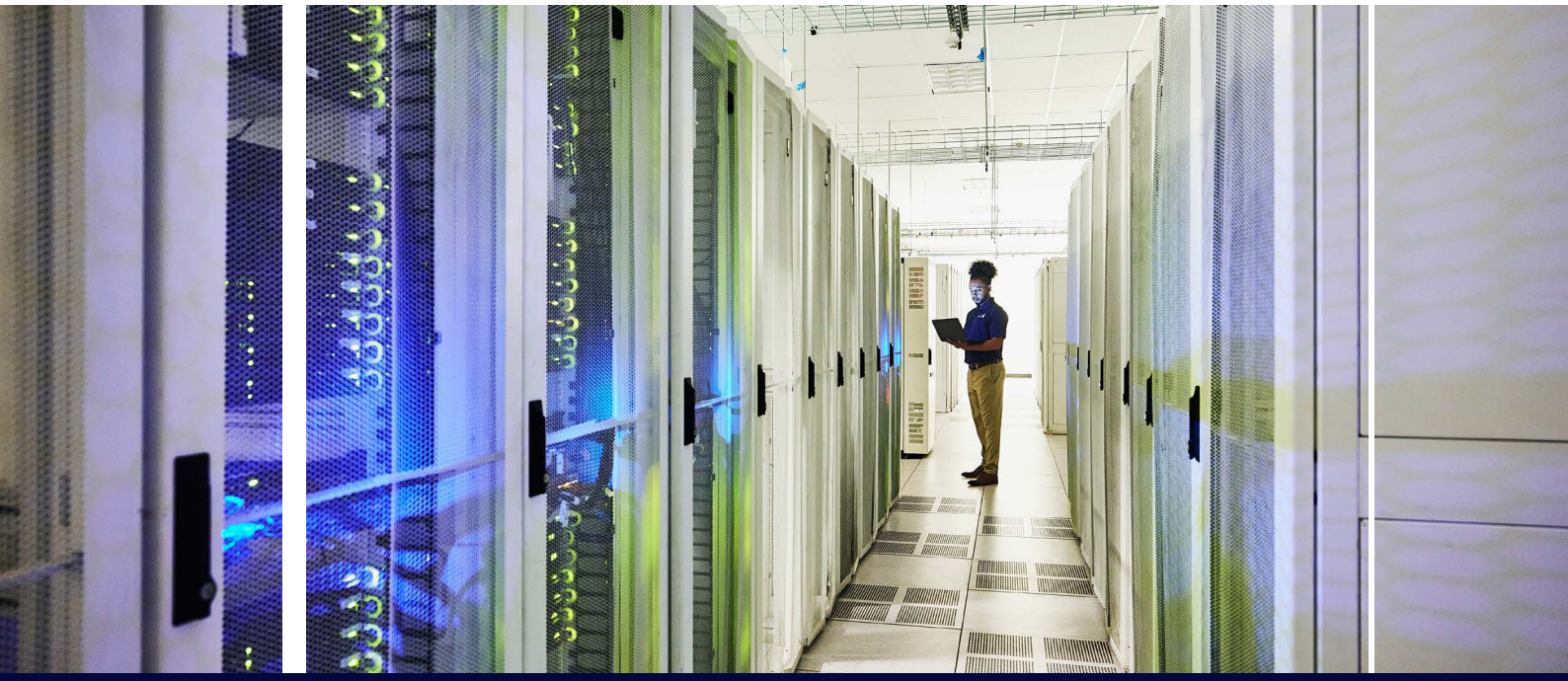
We confirm the technology estate and agree the scope of the Vulnerability Management Service. For example:

- Internal facing - applications running on the internal network
- External facing – all applications outside the network boundary (internet facing)
- Network
- Operating systems

Vulnerability scanning and remediation

With the scope agreed we begin the process of regular scanning, reporting and remediation when requested, Capita can provide consultants who can advise on how best to remediate the identified vulnerabilities

- Vulnerability scans using automated tools to monitor updates that are published by technology providers.
- Provide clear reports outlining the risks and vulnerabilities categorised to show severity of risks
- Install relevant patches and fixes and maintain documentation and audit.



For more information please contact:

Jim Fox CISM, MBCS, MSyI
James.fox2@capita.com

Capita