

# Vulnerability Assessment: Our Approach

## EXTERNAL



- ✓ Test of external perimeter of the networks, primarily internet facing devices like firewalls and web servers, web portals, gateways & VPN systems.
- ✓ We obtain a list of all IPs/ URLs in scope and request whitelisting of our IP addresses, if needed.

## INTERNAL NETWORKS



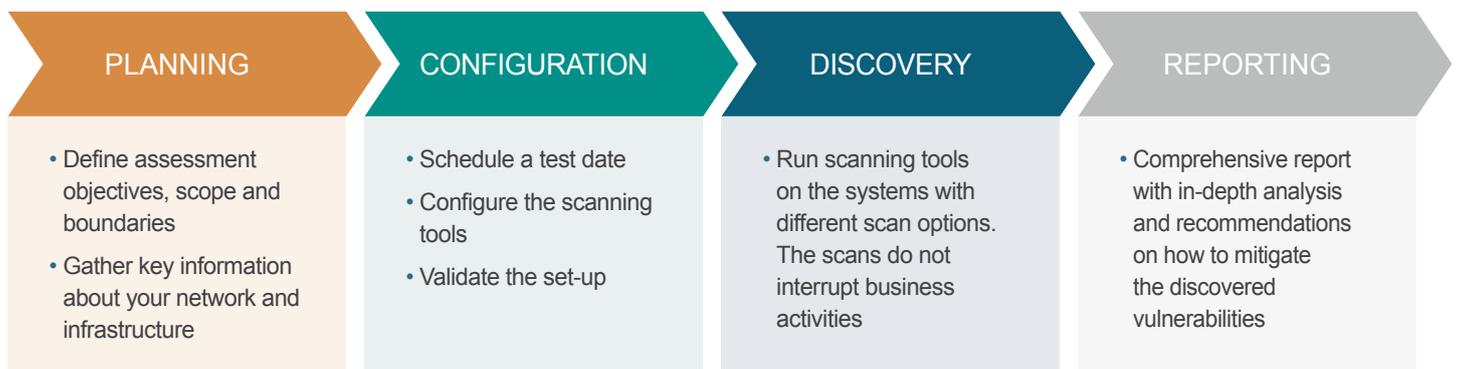
- ✓ Test of devices, PCs and servers within the networks. Duration of the scan varies and depends on number of devices, types and available bandwidth.
- ✓ This is usually a one-off assessment visit to a central location that can also provide access to any other office networks. We configure various scans through our scanning device connected to your network.

## REMOTE MONITORING



- ✓ Remote scanning of your network, and devices (defined as assets). This can be continuous, daily, monthly or any other frequency suitable to your business needs.
- ✓ We install a small tool (scanning agent) on each device and network and schedule the scans to run automatically.
- ✓ We continuously monitor the status and alert you for any critical and high risk issues.

## HOW IT WORKS



## DELIVERABLES

A report on the current state of your cyber security vulnerabilities, actions required and best practises. The report is prepared by a team of professionally qualified security and compliance experts who have a good understanding of business priorities. Our risk-based recommendations assist you in prioritising remediation efforts, achieve quick wins and address critical risks.

**Pricing:** Based on number of locations, unique IP addresses / assets scanned.