Duration
5 to 10 days

Effort
30 to 50 Business hours

Dependencies
Client availability during the kick-off meeting, and details requested in order to perform assessment

Security assessments help you identify the risks in organizations' infrastructure that can potentially avoid cyberattacks and these security assessments are periodic exercises that test your organization's security preparedness and defines the security posture of the organization. The assessment includes checks for vulnerabilities in your IT systems and business processes, as well as recommending steps to lower the risk of future attacks. Security assessments are also useful for keeping your systems and policies up to date.

Scope of Assessment:

Perimeter Security Assessment

Conduct Vulnerability assessment on all the perimeter devices to know all the existing vulnerabilities on those devices:

- Highlight all identified critical & high vulnerabilities as they pose a greater risk to the organization's IT assets.
- Provide a detailed report on how to remediate the identified vulnerabilities to increase overall organization security posture

Host/End Point Security Assessment

Conduct Vulnerability assessment on all the servers/end point devices to know existing vulnerabilities on those systems/endpoints:

- Highlight all identified critical & high vulnerabilities as they pose a greater risk to the organization's IT assets
- Provide a detailed report on how to remediate the identified vulnerabilities to increase overall organization security posture

Vulnerability Assessment

This technical test identifies different vulnerabilities that can be found within your IT environment as of date. During the Vulnerability Assessment, we look at the (potential) severity of a possible attack on different system, as well as recovery options and scenarios

Assessment Summary

- Understand threats and vulnerabilities exists in the entire organizations infrastructure that your business could face based on the reports generated during the assessment
- Determine each identified potential risk as "Critical", "high," "medium," or "low and estimate the impact of the risk that could damage the organization like monetary loss, loss of clients, or loss of brand value or credibility
- List the existing control systems in place and outline further actions that can help mitigate the identified risks

Assessment Advantages

- With a cyber security assessment, you can accurately determine potential exposure to cyber threats that fits best with the company depending on the level of security and previous tests performed.
- Security assessment helps in mapping and identifying potential risks to the assets of a company and how the organization wants to protect those assets.
- Security assessment show cases the entire organizations security posture in protecting the systems from different types of attacks