CLARUS

Vulnerability Risk Assessment

The First Step in Cybersecurity Compliance and Improving Your Company's Data Security

Vulnerability Risk Assessments identify security weaknesses in networks, systems, and applications. Vulnerabilities can originate from unpatched applications or operating systems, small misconfigurations in a firewall or router, or from other areas in your networks or systems.

Cyber attackers can easily find vulnerabilities and are always looking to exploit easy targets. It can be difficult to defend against an attack if you are unaware of the vulnerabilities currently present in your systems. This is why Vulnerability Risk Assessments are required for most compliance regulations, such as NYDFS, NY SHIELD Act, HIPAA & CCPA.

Completing your Vulnerability Assessment is the first step in keeping your company and client data safe from external threats.

Minimize the risk of a security breach by providing insights and guidance to properly secure your networks

We will assess the security and integrity of your infrastructure to identify the vulnerabilities and provide recommendations on how to improve your overall security posture.

With our web-based scanning portal tool, we can schedule the scans around your schedule and provide re-scans after remediation of the high and medium level risks.

Proactively assess your networks to identify and prioritize your security threats

While reactive IT departments spend their time covering security weaknesses with cyber "band-aids", proactive IT teams use vulnerability assessments to discover the severity of their vulnerabilities.

Industry best practice is to perform vulnerability assessment scanning at least once per quarter. Quarterly vulnerability scans often catch any major security holes that need to be addressed. But depending on your unique business needs and compliance requirements, you may need to scan more often.

The Vulnerability Assessment Process

STEP 1

Plan and define scope

STEP 2

Gather information on the network infrastructure

STEP 3

Scan, detect, and assess the network vulnerabilities

STEP 4

Report on the vulnerabilities and provide detailed recommendations

Our Clarus team will work closely with your company to understand your business, IT and compliance requirements, identify the infrastructure and applications that will be in scope for the vulnerability scan, and schedule the scanning. Our scanning software assesses the hosts identified in the scan criteria against our threat intelligence and signatures, identifying any existing threats, vulnerabilities, or weaknesses.

The scan results are recorded in reports so that together we can review the results and remediation steps and take any necessary actions. After remediating high and medium level security risks based on the CVSS 1-10 scores, we then rescan and provide a certified pass report.

Your Assessment Includes

- ☑ Executive Vulnerability Risk Management Summary
- ☑ Vulnerability Summary Report
- ☑ Detailed Findings Report with CVSS Scores
- ☑ Remediation Recommendations Report in Excel Format
- ☑ Re-scans up to 30 days
- ☑ Certified Pass Report after Remediation