Ransomware Protection

PLETHORA offers in-depth Ransomware Preparedness Assessment to help you strengthen the processes and technology to mitigate the threat of ransomware.

Problem

- Most businesses that are attacked experience significant downtime, resulting in lost revenue. You may also lose customers and potential new business.
- Ransomware attacks degrade productivity, cause organizations to incur significant indirect costs, and mar their reputations.
- How do I ensure my **business is ready to mitigate the threat of ransomware?**

Service Overview

A detailed report including:

- Executive summary outlining key strengths and weaknesses of your security controls
- Technical details of testing performed
- Detailed findings, categorized by severity
- Executive briefing

Key Benefits

Our security engineers will identify your vulnerable assets and give you concrete steps to prioritize and fix major security risks.

- **Identify specific assets** that ransomware can reach
- **Realize security weaknesses** that can be exploited by ransomware
- **Minimize the impact** of ransomware attacks
- **Reduce your organization's ransomware attack surface**
- Recognize **operational deficiencies** in the management of ransomware-related risks

How it works

- CRPA Lite is an assessment against the **20 must have security controls and processes** for SME sector.
- CRPA Enterprise is a unique program that reviews risk, security preparedness, and existing controls utilizing the **NIST Cybersecurity Framework.** In addition, we review the technical security capabilities of your organization with Vulnerability Assessment and Penetration Testing on Information assets.

REQUEST A CONSULTATION

Scope Definition

Type of Ransomware Preparedness Assessment;

- **CRPA Lite (Y/N):**
- **CRPA Enterprise (Y/N):**

Name of the Organization/Company:	
Business Industry:	
Approx. Number of Total Employees:	
Approx. Number of the Subsidiaries or the Sister concerns of the Organization/Company:	
Approx. Number of the Vendors/Partners/Suppliers:	
List the Business Domain(s):	
List the Email Domain(s):	
Locations of Business Operations: All Locations of Business Operations included in Ransomware Assessment? (Y/N):	
Locations of Subsidiaries or the Sister concerns: All Locations of Subsidiaries or the Sister Concerns included in Ransomware Assessment? (Y/N):	