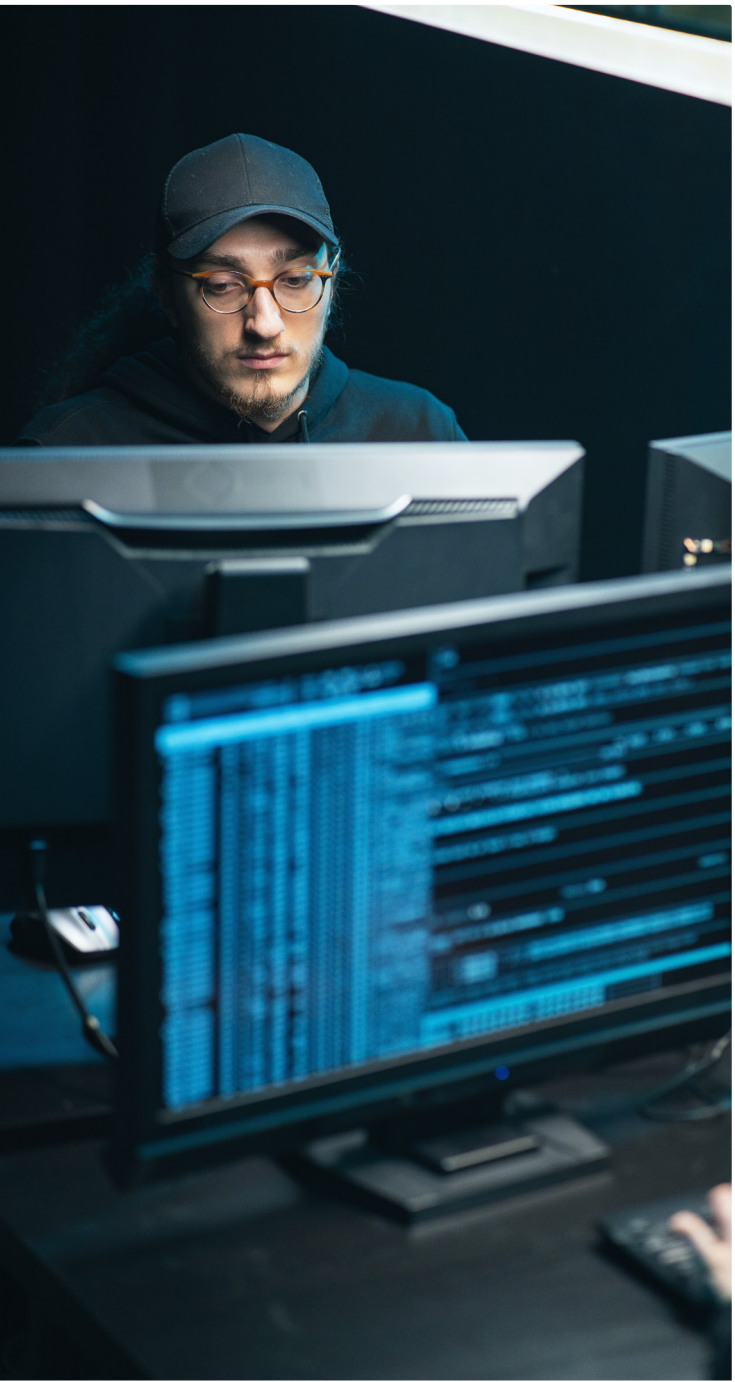
HCLTech | Supercharging Progress™

Ransomware readiness assessment

The challenge

Ransomware has proven to be both extremely prevalent and effective at disrupting business in today's technology landscape. The greater scale of today's environments and the vast expansion of a remote workforce has made it increasingly difficult to prevent Ransomware and related threats. These difficulties can range from raising user awareness about the threat and recovery, to preparing the environment in case of an incident and even defending against active Ransomware threats.



Who should leverage this service?

- Clients looking to improve their resilience against Ransomware threats
- Critical Infrastructure
- Medical/Healthcare
- Past victims of Ransomware attacks

Why HCLTech Global Product Consulting?

- We are the Security experts!
- HCLTech Global Consultants have experience with a comprehensive scope of the security landscape
- Our Team understands the specific needs of different industries and can provide the required expertise to meet your cyber security demands

Solution

Our experienced Cyber Security experts work with our clients to ensure that they understand the scale and depth of what should be done to prevent Ransomware attacks. Our team also understands and delivers the best practices involved in minimizing the likelihood of Ransomware threats and mitigating the damage and accelerating recovery, should an incident occur.

With a vast range of industry experience and insight, our experts will review existing implementations, security platforms and strategies. We then provide detailed reports on findings, feedback and suggestions, tailored to your business, on how to improve your Ransomware Readiness, Response and Recovery.

Our team's broad skillset in defense and readiness across the entire threat landscape will support your business and mission with industry-leading security practices. The team is extremely skilled in reviewing software suites including antimalware, EDR, intrusion prevention and intrusion detection platforms. Also, we have depth in network security platforms that include data loss prevention, proxy servers, web isolation services and firewalls.

With our team's guidance, your business will be stronger, more defensible and ready to thwart any Ransomware attacks that attempt to lay siege to your environment.

How ransomware readiness, reaction and recovery works

Our tailored and proven methodology ensures consistent service delivery, which means that you will always have an expert who can help you reach your business outcomes on time and on target. HCLTech's Fortius cybersecurity consulting provides a proven framework with a solution driven approach by leveraging our best practices in key areas encompassing business and technical objectives/processes, all to derive the most value out of the solution for current and future needs.

The following outlines typical assessment topics:

Our tailored and proven methodology ensures consistent service delivery, which means that you will always have an expert who can help you reach your business outcomes on time and on target. HCLTech's Fortius cybersecurity consulting provides a proven framework with a solution driven approach by leveraging our best practices in key areas encompassing business and technical objectives/processes, all to derive the most value out of the solution for current and future needs.

Endpoint security best practices

Assessment

- Review infrastructure attack surface
- Review Business Continuity/Disaster Recovery/Incident Response
  - Includes data Backup/Restore, System Re-imaging, Offline Spares
- Review staff communication and collaboration
- Review KPI's and Baselining

Preventive

- Implement/Enhance Host-based security solutions for system hardening and detection
- Implement/Enhance policies and best practices to ensure effective coverage
- Implement/Enhance deployment to client systems
- Implement/Enhance remote workforce best practices and preparedness
- Implement/Enhance Business Continuity planning to optimize Disaster Recovery

Network security best practices

Assessment

- Review infrastructure attack surface
- Review Business Continuity/Disaster Recovery/Incident Response
  - Backup/Redundant network pathing, port flow data, quick ACL/Port blocking
- Review KPI's and Baselining

Preventive

- Implement/Enhance client connectivity best practices
- Implement/Enhance remote workforce best practices
- Implement/Enhance Network Administration Rapid Response capability

User awareness best practices

Assessment

- Review Acceptable Behavior policies
- Review End User training and communications

Preventive

- Implement/Enhance user awareness processes and effectiveness
  - Spotting spoofed links, phishing emails
  - Impact awareness

As a result of the review process, a detailed report on findings, feedback, suggestions and best practices will be provided. This report can be used as a guideline and planning document for the process of hardening the environment and bolstering your defenses. You will find industry-targeted best practices for security platforms, hosts, network-based security platforms and user awareness improvements that can be implemented. Our team will also detail any red flags and security or configuration concerns that may be noteworthy. With years of security and industry experience, our team's improvement reports are second to none.

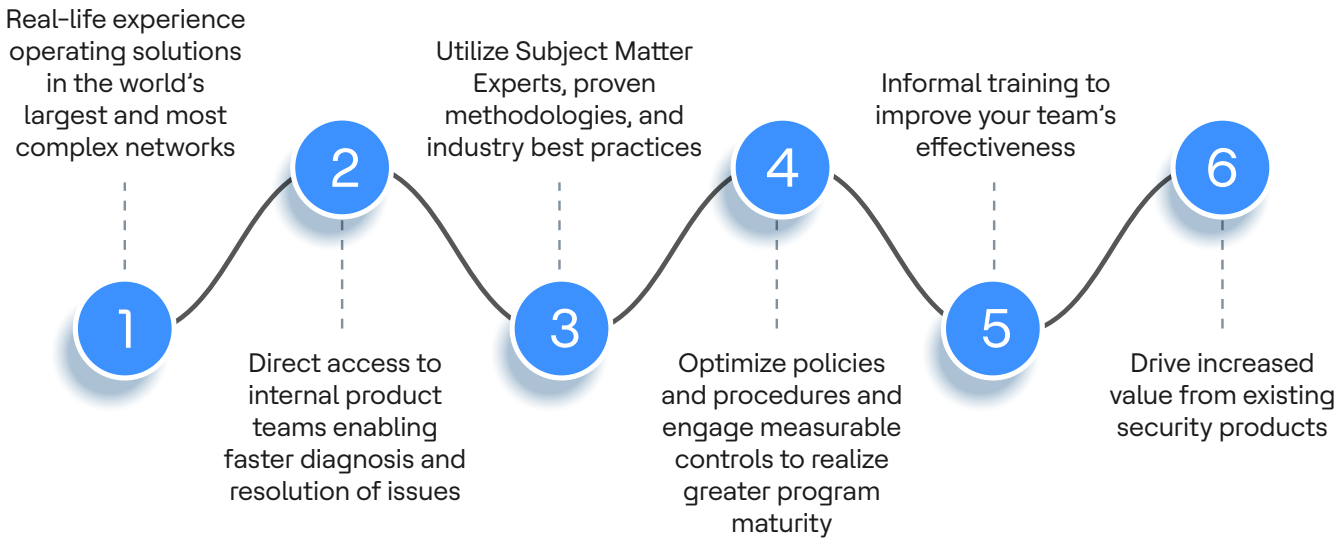
We will help you understand the "Read, Write and Delete" method used by most Ransomware, as well as enumeration of available SMB (File Share) targets. With a better understanding of how your attacker works, you will be better prepared to mitigate and minimize any negative impact. Implementing a better security posture against Ransomware will also provide additional security against other common cyber-attack methods. Improving your prevention and accelerating your response and recovery can make the difference between an inconvenience and a catastrophe.

Further reading

Building Your Remote Workplace Environment's Fort Knox in the Age of Remote Workplaces | HCLTech Blogs (hcltech.com) Email Security as the First Line of Defense: Is Your Drawbridge Down? | HCLTech Blogs (hcltech.com) "Trust But Verify" is Obsolete: Zero Trust Networking | HCLTech Blogs (hcltech.com)

Why HCLTech's Fortius cybersecurity consulting?

Our consultants deliver real world value to help guide organizations in improving their security posture through:



For more information or to get started, please contact us:
Fortius@hcl.com | hcltech.com