COHESITY | Service Brief

Cohesity CERT Ransomware Resilience Assessment

Cyber resiliency is an emergent organizational capability developed by putting the right governance, people, processes, and technologies in place to handle today's ransomware and wiper attacks.

The **Cohesity CERT Ransomware Resilience Assessment**, delivered by **Cohesity Cyber Resilience Consulting**, provides a data-driven, comprehensive evaluation of the maturity of your organization's operational cyber resilience capability. The engagement establishes a clear baseline of your preparedness for destructive cyberattacks and identifies opportunities for measurable improvement.

Key Benefits

- Holistic insight into your organization's current resilience
- Actionable improvement roadmap
- Benchmark practices against leading frameworks

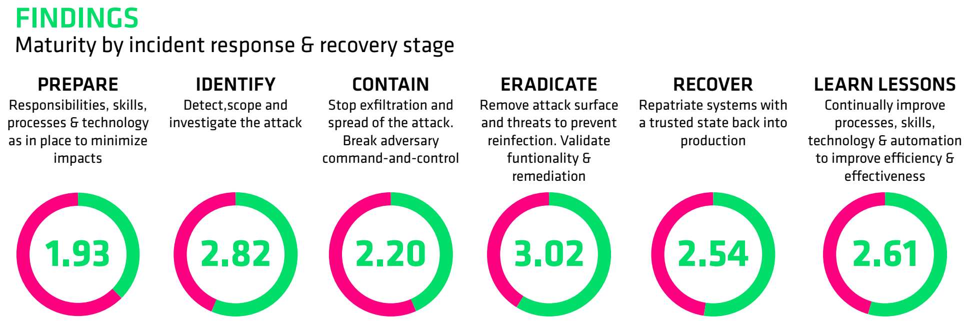

Figure 1: Sample assessment report excerpt

Consulting expertise and assessment scope

The assessment is delivered by consultants with extensive, hands-on experience helping hundreds of customers investigate, contain, eradicate, and recover from destructive cyberattacks. This expertise provides an opportunity not only to assess your current state, but also to discuss the applicability of relevant risk management strategies to your organization. It also allows senior stakeholders to engage with specialists who have seen the real-world impact of cyberattacks across peer organizations in your industry and region.

The scope of the assessment is comprehensive, covering over 100 operational areas from common cyber incident response and recovery frameworks, including:

- NIST SP 800-61 Computer Security Incident Handling
- SANS Institute 6-Step Incident Handling Process
- RE&CT Framework
- MITRE D3FEND
- ISO 27035 Information Security Incident Management
- Forum of Incident Response and Security Teams (FIRST) Framework
- UK National Cyber Security Centre Incident Response Process

Your organization's operational capabilities are graded using the **Destructive Cyberattack Maturity Model** aligned with the well-established **Capability Maturity Model Integration (CMMI)** principles.

Engagement Approach

- **On-site assessment (2 days)** - A structured workshop engaging cross-functional teams including IT, Security Operations, Legal, PR, and executive sponsors
- **Remote analysis and reporting** - A comprehensive evaluation and roadmap recommendation, presented remotely

Deliverables

At the conclusion of the assessment, you'll receive an extensive report that details:

- The maturity of your people, process, and technology elements of cyber resilience
- Your preparedness for an attack and your ability to investigate, contain, remediate threats, and recover or rebuild systems to a secure state
- A detailed three-phase roadmap of areas of pragmatic improvement, helping your organization to focus efforts on the areas that will deliver the greatest improvement in resiliency and build a strategic plan for improvement. The roadmap is designed to be actionable, with the value of the improvements and detailed work items that can be assigned and tracked.
- A remote presentation of summary findings and recommendations following the delivery of the report. This session is tailored to the audience of your choice, whether executive leadership, technical teams or broader stakeholders, ensuring alignment with organizational priorities and next steps. By clearly outlining risks, opportunities and recommended actions, the presentation creates a common understanding, allows informed decision-making, helps prioritize initiatives, and gain executive sponsorship that strengthens your organization's cyber resiliency posture.

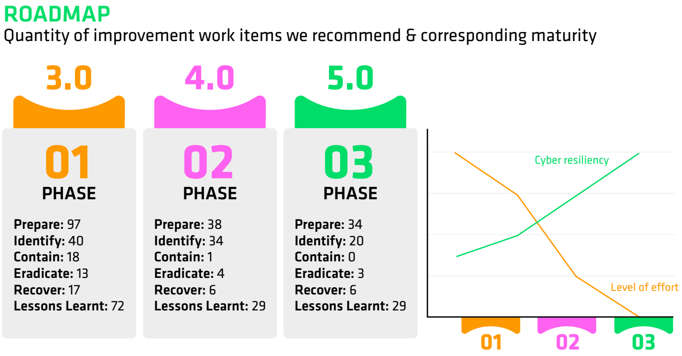

Figure 2: Sample three-phase roadmap

Service Summary

Component	Details
Duration	2 days on-site engagement + remote analysis and reporting
Participants	Availability of cross-functional resources required during the assessment, including IT and Security Operations, executive sponsors, Legal, and Public Relations
Deliverable	Draft findings and report shared 5 – 10 working days after assessment conclusion. High-level findings and recommendations presented remotely to stakeholders.
Delivered as	Time and materials
Service Units	Consumes 5 service units

Contact the Cyber Resiliency Consulting team at CERTConsulting@cohesity.com
to schedule a ransomware resilience assessment.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

3000182-001-EN 12-2025