RANSOMWARE READINESS

What is a Ransomware Readiness Assessment?

Ransomware Readiness Assessments from SEVN-X help organizations understand their risk and defense postures against ransomware attacks.

The assessment components are selected based on the specific objectives of the organization and may include:

Ransomware Simulation

SEVN-X can deploy a custom payload that simulates ransomware behavior seen in the wild without putting your systems and data at risk. See how your organization's controls stand up to real-world techniques.

Impact Mapping

SEVN-X crawls the internal network using multiple test user roles to enumerate file shares and assess write permissions, identifying potential exposure to ransomware propagation through overly permissive access.

Endpoint Controls

Strong endpoint detection and response (EDR) controls can thwart ransomware execution and propagation. Managed Detection can provide timely alerting.

Processes

SEVN-X can examine your organization's data backup and restore strategy, incident response (IR) capabilities, security awareness training, and patching / vulnerability management strategies.

Is it Right for My Organization?

SEVN-X typically recommends this assessment for organizations with mature cybersecurity programs. Ransomware Assessments are highly targeted and provide maximum value when evaluating existing security controls the organization has in place.

If your cybersecurity program is less mature, or just getting started, talk to us about our Cybersecurity Program Assessment so SEVN-X can help you identify critical issues and define your security roadmap.

Why Use SEVN-X for Your Next Assessment?

When assessing your environment for ransomware readiness, you need clear answers to basic questions not fluff, non-answers, and consulting jargon. Our customers trust us to provide actionable and practical recommendations.

info@sevnx.com

484.989.0911

ACHIEVE BETTER CYBERSECURITY