Ransomware Readiness 2026 Checklist

Assess where your organization stands. Fix what's red.

Attack Lifecycle — Where to Detect

1 Access	2 Persist	3 Lateral	4 Exfil	5 Encrypt	6 Demand
Phish/RDP/CVE	Backdoors set	Cred harvest	Data uploads	Files locked	Ransom note

Detection Signals to Monitor

SIEM
- ☐ Mass file renames
- ☐ vssadmin delete shadows
- ☐ Off-hours data spikes
- ☐ Log-clear events

EDR
- ☐ PowerShell → cmd → bin
- ☐ Mimikatz activity
- ☐ PsExec across many hosts
- ☐ AV disable events

NETWORK
- ☐ C2 to unusual domains
- ☐ Cloud storage exfil
- ☐ Beaconing patterns
- ☐ Internal port scans

BEHAVIORAL
- ☐ Service acct after-hours
- ☐ Backup jobs failing
- ☐ Mass account lockouts
- ☐ Canary files touched

Defense Readiness — Rate Yourself

- ☐ **Immutable Backups**
  Air-gapped, tested restore in last 90 days
- ☐ **Network Segmentation**
  Workload isolation, internal firewalls, no flat networks
- ☐ **Patch Cadence**
  Critical CVEs patched within 30 days (ideally 14)
- ☐ **MFA on Privileged Accts**
  Hardware keys for admins. No SMS. No exceptions.
- ☐ **EDR + Auto-Containment**
  Endpoint isolation on high-severity alerts
- ☐ **Tested IR Plan**
  Tabletop exercise completed in last 6 months
- ☐ **Endpoint Log Retention**
  ☐90 days for forensics. 12 months for compliance.

When the Note Appears — First 24 Hours

Isolate	Preserve	Notify	Assess	Decide
Disconnect affected systems from network — physically if needed	Do NOT power off. Memory holds forensic evidence.	Legal, executive team, IR firm, cyber insurance, law enforcement	Scope: how many systems, what data, is exfil confirmed	Restore path via clean backups — NOT via decryption tools you find online