

AI Attack Readiness Checklist

12 checks that reveal whether your business is ready for the AI-driven attack wave.

September 2026 proved AI attacks are real: one attacker breached 27 companies at a cost of only **\$25 a target**, ransomware weaponized an AI coding agent, and the first **fully autonomous AI ransomware** appeared. Work through these checks to find your gaps before attackers do.

A. Know your AI exposure

- ☐ **We've inventoried every AI tool employees use** — including personal accounts. One errant prompt took down a company's entire Salesforce.
- ☐ **Our developers' AI coding assistants can't leak code or screenshots.** 13,000 internal images ended up on public GitHub via agent tooling defaults.
- ☐ **No cloud secrets or credentials sit in public repos, tickets, or chat.** One leaked Azure secret let an AI delete 100+ cloud storage accounts in 7 minutes.

B. Survive the zero-day wave

- ☐ **We have real-time zero-day protection (virtual patching).** AI now discovers vulnerabilities faster than vendors ship patches.
- ☐ **Our network is segmented to contain breaches.** Segmentation trapped an AI intruder at a Dutch nonprofit before it reached anything important.
- ☐ **We know every vendor/partner connected to our network and what they can reach.** Spain's railway was breached through a partner — not directly.
- ☐ **MFA is phishing-resistant everywhere.** 12,000 inboxes fell to OAuth device-code phishing that bypassed standard MFA.

C. Detect, respond, recover

- ☐ **24/7 monitoring (MDR/SIEM) watches our environment.** AI attacks run at machine speed — often off-hours.
- ☐ **We have a tested incident response plan.** Ransomware groups are running double-extortion playbooks against SMBs right now.
- ☐ **Backups are isolated from the network and tested.** Attackers now wipe databases to cover their tracks.

D. Platform & maturity

- ☐ **We run an AI-enabled XDR platform — not standalone tools.** Point tools can't correlate attacks happening at AI speed.
- ☐ **We're moving toward compliance-level security** — framework in place, risk assessment in the last 12 months, prioritized roadmap. "Good enough for insurance" no longer survives the AI wave.

Score yourself: 10–12 checks — strong posture, keep it current. 6–9 — gaps attackers can find; prioritize the unchecked boxes. 0–5 — exposed; every unchecked box is an open door.

Missing checks? We can help.

eSecurity Solutions assesses your readiness, closes the gaps, and manages your defenses — within your budget.

Free AI security consultation: 866-661-6685 | Sales@eSecuritySolutions.com | www.esecuritysolutions.com