Your MSP cyber-insurance evidence pack

Domain: eliteaiempire.com
Checked: 2026-11-09T06:19:04Z
4 of 14 questions answered from scan evidence.

Do you use SPF, DKIM and DMARC to authenticate email sent from your domain?

Answer: Partly
Evidence: SPF: v=spf1 include:_spf.postal.eliteaiempire.com include:spf.brevo.com include:_spf.google.com ~all; DMARC: none; DKIM: none found at default, google, selector1, selector2, k1, s1, s2. DKIM was not found at common selectors; confirm the selector your mail provider uses.

Is DMARC set to quarantine or reject?

Answer: No
Evidence: DMARC policy: none

Do your public websites use HTTPS with a valid certificate and TLS 1.2 or later?

Answer: Yes
Evidence: Certificate valid: yes; version: TLSv1.3

Do your websites tell browsers to use HTTPS only (HSTS)?

Answer: No
Evidence: strict-transport-security: missing

Is remote desktop (RDP), SSH or VNC reachable from the internet?

Answer: Not checked
Evidence: Needs an active scan on a domain whose owner proved control.

Are database ports reachable from the internet?

Answer: Not checked
Evidence: Needs an active scan on a domain whose owner proved control.

Are configuration or credential files exposed on your public web servers?

Answer: Not checked
Evidence: Needs an active scan on a domain whose owner proved control.

Is multi-factor authentication required for all email accounts?

Answer: MSP to answer
Evidence: Export of the email tenant's MFA or conditional-access report showing every licensed user.

Is multi-factor authentication required for remote access and admin accounts?

Answer: MSP to answer
Evidence: Screenshot or export of the remote-access and admin MFA policy.

Is endpoint detection and response (EDR) installed on every workstation and server?

Answer: MSP to answer

Evidence: EDR console export listing protected devices, compared with the device inventory count.

Are backups kept offline or immutable, and was a restore tested in the last 12 months?

Answer: MSP to answer

Evidence: Backup job report showing an offline or immutable copy, plus the date and result of the last restore test.

Are critical security patches applied within 30 days?

Answer: MSP to answer

Evidence: Patch compliance report from your RMM for the last 30 days.

Do employees complete security awareness training at least once a year?

Answer: MSP to answer

Evidence: Training platform completion report for the last 12 months.

Do you have a written incident response plan?

Answer: MSP to answer

Evidence: The plan document with its last review date.

Pre-filled from outside-in scan evidence. Rows marked "MSP to answer" need evidence from your own tools. Review every answer before it goes to a carrier; a clean scan does not prove that a system is secure.