Machine Learning Threat Detection Readiness Checklist

Instructions

Use the checklist below to assess your organisation's readiness for AI-driven cybersecurity monitoring and operational resilience.

Score your organisation using:

- Yes = 2 points
- Partial/In Progress = 1 point
- No = 0 points

Assessment Questions

Visibility & Monitoring

☐ We maintain centralised visibility across endpoints, users, and cloud systems.

☐ We actively monitor authentication activity and login anomalies.

☐ We have tools capable of detecting unusual behavioural patterns.

☐ Our organisation reviews security alerts consistently.

☐ We can identify suspicious user activity quickly.

Identity & Access Security

☐ Multi-factor authentication is enabled across critical systems.

☐ Privileged account access is limited and reviewed regularly.

☐ Former employee accounts are removed promptly.

☐ Third-party access permissions are monitored carefully.

☐ Remote access activity is logged and reviewed.

Employee Awareness

☐ Employees receive regular phishing awareness training.

☐ Staff understand how to report suspicious activity.

☐ Executives participate in cybersecurity awareness initiatives.

☐ Employees understand social engineering risks.

☐ Cybersecurity awareness is treated as an ongoing operational priority.

Incident Response Readiness

☐ We maintain a documented incident response process.

☐ Roles and escalation responsibilities are clearly defined.

☐ Critical systems and operational priorities are identified.

☐ Backup and recovery procedures are tested regularly.

☐ Leadership understands incident communication procedures.

AI & Vendor Governance

☐ We understand how our AI security tools generate alerts.

☐ We evaluate cybersecurity vendors beyond marketing claims.

☐ Security monitoring systems are reviewed for effectiveness regularly.

☐ We understand the limitations of machine learning detection.

☐ Human oversight exists for major security decisions.

Scoring Results

40–50 Points — Strong Maturity

Your organisation demonstrates strong operational cybersecurity awareness and appears to maintain a mature approach toward monitoring, governance, and resilience planning.

Continue refining:

- visibility,
- employee awareness,
- vendor oversight,
- and operational readiness.

20–39 Points — Moderate Exposure

Your organisation has foundational cybersecurity measures in place but may still face operational gaps that increase risk exposure.

Focus on:

- improving monitoring visibility,
- strengthening employee awareness,
- clarifying response procedures,
- and reviewing identity security controls.

0–19 Points — High Vulnerability

Your organisation may face significant exposure to preventable cyber incidents.

Immediate priorities should include:

- visibility improvements,
- phishing awareness training,
- incident response preparation,
- access control reviews,
- and stronger operational governance.

Cybersecurity resilience improves through steady operational progress.