Managed Security Diligence Checklist

Use this checklist to compare managed security providers consistently before a scope call or tender shortlisting.

1) Accountability and Operating Model

- Is there one named owner across firewall, endpoint/XDR, SIEM or SOC, and recovery?
- Are escalation paths documented by severity and after-hours coverage?
- Is response ownership contractual, not implied in marketing copy?
- Is reporting cadence defined (monthly or quarterly) with fixed attendees and actions?

2) SOC and SIEM Depth

- Do they provide triage workflows and use-case tuning, not just log ingestion?
- Are suppression rules and tuning decisions recorded and reviewed?
- Can they show examples of root-cause remediation from repeated alert classes?
- Do they provide clear SLA definitions for detect, triage, and escalation?

3) XDR and Endpoint Operations

- Who monitors and tunes endpoint policies weekly?
- Are rollback and containment procedures documented and rehearsed?
- Is endpoint telemetry integrated into SIEM or SOC workflows?
- Are exceptions documented with owner, expiry date, and remediation plan?

4) Identity and Email Security

- Are conditional access and MFA policies operated as part of managed service?
- Is break-glass access controlled, tested, and auditable?
- Are phishing and mail-flow controls reviewed on a recurring schedule?
- Is identity posture included in the same risk report as endpoint and network controls?

5) Ransomware Recovery Alignment

- Is immutable backup in place and explicitly in scope?
- Are restore tests performed on schedule and evidenced?
- Are ransomware tabletop exercises run with business and technical owners?
- Are recovery RTO/RPO assumptions documented and accepted by leadership?

6) Governance and Evidence

- Can they provide board-ready reporting with open risks, exceptions, and trend movement?
- Are audit and assurance controls part of day-to-day operations?
- Is there a defined change management process tied to security controls?
- Can they map controls to Essential Eight and your sector obligations where relevant?

7) Procurement and Commercial Clarity

- Is scope explicit for in-scope vs out-of-scope activities?
- Are tool costs and operational service costs clearly separated?
- Are onboarding phases and handover milestones documented?
- Are reference customers available in a similar industry and scale?

8) Final Decision Questions

- If an incident happens at 2am, do you know exactly who acts first?
- If auditors ask for evidence, can the provider produce it quickly and clearly?
- If ransomware hits, are restore and containment owned in one operating thread?

If you want a fast gap review, share your current firewall/XDR/SIEM stack, recovery approach, and reporting expectations via:
/contact/?service=managed-security-services&intent=security-scope-call