

Vendor Security Evaluation Checklist

For teams evaluating, renewing, or replacing a cybersecurity vendor, go through before signing anything.

⚠ = treat as a dealbreaker if the vendor can't answer this clearly



PROOF OF CONCEPT & ONBOARDING

- ☐ Push back on a standard 14-day trial window
Most behavioural detection tools need ~90 days to baseline accurately, a shorter window can't effectively prove fit.
- ☐ Request a walkthrough of the first 90 days of onboarding
- ☐ Confirm what "go live" actually means and when it happens
- ☐ Confirm what's required from your own team during rollout



INCIDENT RESPONSE READINESS

- ☐ Ask vendor to walk through a real past incident similar to your risk profile
- ☐ Confirm how response times are measured and reported
- ☐ Confirm escalation path for nuanced or ambiguous incidents
- ☐ Run a **tabletop exercise** with the vendor before signing
(Reveals single points of dependency that demos and slide decks won't show)



VENDOR STABILITY & GROWTH RISK

- ☐ Check whether core capability was built organically or bolted on via acquisition
- ☐ Assess whether product focus has been diluted by portfolio growth
- ☐ Ask what the vendors roadmap and growth strategy is over the next 36 months including M&A and changes of ownership



EXIT & OFFBOARDING

- ☐ Confirm data ownership and export rights in writing before signing
- ☐ Confirm you can export full incident history and security metrics
(Without this, a replacement platform has to start baselining from zero)
- ☐ Get the offboarding process documented, not just described verbally



COMPLIANCE & SUPPLY-CHAIN LIABILITY

- ☐ Check whether the vendor's compliance posture becomes your liability
Especially relevant under the **UK Cyber Security and Resilience Bill**, especially in financial services, utilities, or public sector.
- ☐ Verify subprocessors and fourth-party dependencies are disclosed
- ☐ Confirm AI capabilities and data subprocessing locations



EVALUATION PROCESS & GOVERNANCE

- ☐ Commission an **independent gap analysis** and baseline before any vendor conversations
- ☐ Re-confirm the original organisational gap you're trying to close, has it changed?
- ☐ Treat adoption as an ongoing process to plan for, not a checkbox at contract signature
- ☐ Ask: "What's the most common reason customers don't renew?"
A specific, honest answer is a green flag; deflection is a red flag.

Suitability, not size or brand, should be the entire basis of a vendor decision.