DOWNLOADABLE WORKSHEET · CYBERSECURITY

MDR/SIEM Vendor *Scorecard*

A working document, not a brochure. Work through Step 1 before you talk to a single vendor — it settles whether you're shopping for a SIEM, an MDR service, or both, based on your staffing reality rather than a datasheet.

How to use this scorecard

Carry the scorecard in Steps 2–3 into every vendor call and score the answers while they're fresh. Work through it in order:

1. Decide the operating model — SIEM you run, MDR you buy, or both (8 yes/no questions).
2. Score each vendor — 22 criteria across the five pillars, scored 1–5, in live conversation.
3. Read out and decide — let the math argue with the demo glow, then record a recommendation you can defend.

Keep one copy per vendor so the comparison stays apples-to-apples. Vague answers score low — that's the point.

Step 1 — Decision path: SIEM, MDR, or both?

Answer honestly about where your team is today, not where the roadmap says it will be. Each Yes is a vote for running a SIEM in-house.

#	Question	Yes	No
1	Do you have (or have funded headcount for) 8–12 analysts to cover true 24/7 shifts?	☐	☐
2	Does someone on staff have SIEM engineering experience (rule tuning, parser upkeep, integration maintenance)?	☐	☐
3	Has your team handled a real security incident end-to-end (detect → investigate → contain) in the last 12 months?	☐	☐
4	Can your team triage alerts overnight and on holiday weekends without heroics or burnout?	☐	☐
5	Is security operations a core competency you want to build and retain in-house long term?	☐	☐
6	Can you absorb SOC analyst turnover (hiring, training, knowledge transfer) without losing coverage?	☐	☐
7	Do you have a documented, tested incident response process with named on-call owners?	☐	☐
8	Is your leadership prepared to fund detection engineering as an ongoing program, not a one-time project?	☐	☐

Tally: Yes / 8

Tally: No / 8

Read-out

- 0–3 Yes → MDR. You'd be buying a SIEM you can't staff. Buy the humans; evaluate MDR vendors with the scorecard below.
- 4–6 Yes → Hybrid / co-managed. You have real capability but not full coverage. Look at MDR with SIEM co-management, or MDR layered on a SIEM you keep for retention and audit. Score vendors on both service depth and how well they work with what you own.
- 7–8 Yes → SIEM in-house. You can genuinely run it. Evaluate SIEM platforms — and still use Pillars 4 and 5 below to pressure-test any co-managed or augmentation services you add.

One more gate before you shortlist

Does a compliance framework, insurer, or contract require you to retain and control your own logs? ☐ Yes ☐ No

If Yes, any MDR vendor you score must support your log ownership and retention requirement, or you keep a retention layer alongside them.

Write the requirement here:

Step 2 — Vendor scorecard (five pillars, 22 criteria)

Score each criterion 1–5 per vendor, in live conversation — not from the datasheet.

> Scoring guide: 5 = specific, verifiable answer, proven in the demo or in writing. 3 = adequate but generic. 1 = vague, deflected, or "that's on the roadmap." A 1–2 on any question marked ⚑ should make you nervous regardless of the total.

Pillar 1 — Who is actually watching the screen at 2 AM?

#	Criterion	Vendor A	Vendor B	Vendor C
1	⚑ Stated the number of analysts on shift overnight and on holiday weekends (a number, not “24/7 SOC”)	___	___	___
2	Overnight coverage is a staffed follow-the-sun / shift operation, not an on-call pager	___	___	___
3	Analysts are the vendor’s employees, not a subcontracted white-label SOC	___	___	___
4	Analyst tenure and turnover shared openly (who is actually looking at your alerts?)	___	___	___
5	Escalation path from overnight analyst to senior/IR staff is defined with timings	___	___	___

Pillar 1 subtotal _____ / 25

Pillar 2 — What their AI does vs. what their humans do

#	Criterion	Vendor A	Vendor B	Vendor C
6	⚑ Explained precisely what their AI does — detection, triage, or response — and where humans take over	___	___	___
7	⚑ Shared false-positive rates and who absorbs that noise (their analysts, not your inbox)	___	___	___
8	A human reviews what the AI auto-dismisses (sampled or full review — which, and how often?)	___	___	___
9	Missed detections have a defined path to a post-mortem and detection-engineering fix	___	___	___
10	Human escalation path from AI flag to analyst decision has stated time targets	___	___	___

Pillar 2 subtotal _____ / 25

Pillar 3 — Response authority: do they act, or just alert?

#	Criterion	Vendor A	Vendor B	Vendor C
11	⚑ Pre-authorized response actions (isolate host, disable account, block infrastructure) listed explicitly and contractually	___	___	___
12	Will contain a confirmed threat at 2 AM without waking you (and the notify-after process is defined)	___	___	___
13	The tier/package you're actually quoted includes response — not triage-and-forward	___	___	___
14	Response SLAs are stated for containment actions, not just for "notification"	___	___	___

Pillar 3 subtotal _____ / 20

Pillar 4 — Integration reality with your stack

#	Criterion	Vendor A	Vendor B	Vendor C
15	⚑ Ingests from the tools you already run (EDR, identity provider, M365/cloud, network) — verified against your actual list, not their logo page	___	___	___
16	No forced rip-and-replace of your existing endpoint agent (or the replacement is genuinely justified and costed)	___	___	___
17	Identity and conditional-access signals are covered (critical if zero trust is on your roadmap)	___	___	___
18	Coverage gaps stated honestly — what in your environment they won't see, in writing	___	___	___

Pillar 4 subtotal _____ / 20

Pillar 5 — Their last real incident

#	Criterion	Vendor A	Vendor B	Vendor C
19	⚑ Walked through a real incident for a client your size with specifics — timeline, decisions, who called whom — not a process diagram	___	___	___
20	Could say what they contained before the client was awake, and what they escalated	___	___	___
21	Admitted something that went wrong or almost went wrong (and what changed after)	___	___	___
22	References available from clients your size and industry who have had a real incident with them	___	___	___

Pillar 5 subtotal _____ / 20

Step 3 — Totals and read-out

Pillar	Max	Vendor A	Vendor B	Vendor C
1. Watching the screen at 2 AM	25	_____	_____	_____
2. AI vs. humans	25	_____	_____	_____
3. Response authority	20	_____	_____	_____
4. Integration reality	20	_____	_____	_____
5. Last real incident	20	_____	_____	_____
Total	110	_____	_____	_____

Read-out

- 90–110 — Delivers what the pitch promised. Verify the contract language matches the call, then proceed.
- 70–89 — Solid, with soft spots. Re-interview on every pillar that scored under 70% before you shortlist them as the finalist.
- 50–69 — The demo is writing checks the operating model can't cash. Only proceed if the low scores are in pillars you've consciously decided to own yourself.
- Below 50 — A dashboard with a sales team. Walk.

> Tie-breaker rule: If two vendors are within 5 points, the one with the higher combined score on Pillars 1 and 3 (humans + authority) wins. Those are the two you cannot patch after signing.

Final recommendation summary

Field	Entry
Operating model decided (Step 1)	☐ SIEM in-house ☐ MDR ☐ Hybrid / co-managed
Recommended vendor	_____
Total score (/110)	_____
Strongest reason to choose	_____
Biggest known gap (and who owns it)	_____
Pre-authorized response actions confirmed in contract?	☐ Yes ☐ No
Log ownership / retention requirement satisfied?	☐ Yes ☐ No ☐ N/A
Decision owner & date	_____

One-paragraph rationale (write it so leadership can read it cold):

Worksheet companion to "Every MDR Vendor Promises 24/7 Protection. Here's How to Tell Who Actually Delivers." Prepared by Plow Networks — Security.