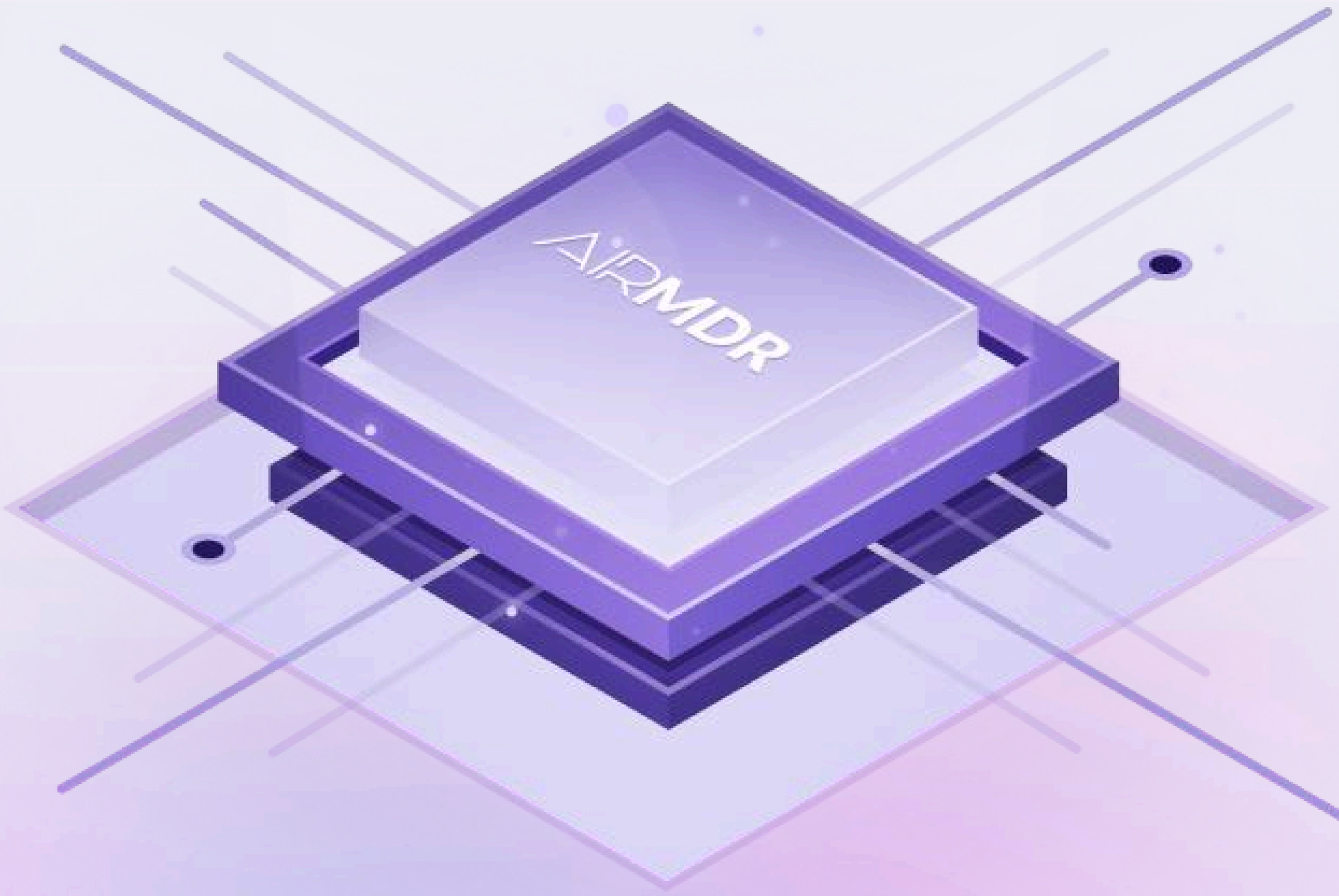
AIRMDR

Case Quality Scoring Toolkit

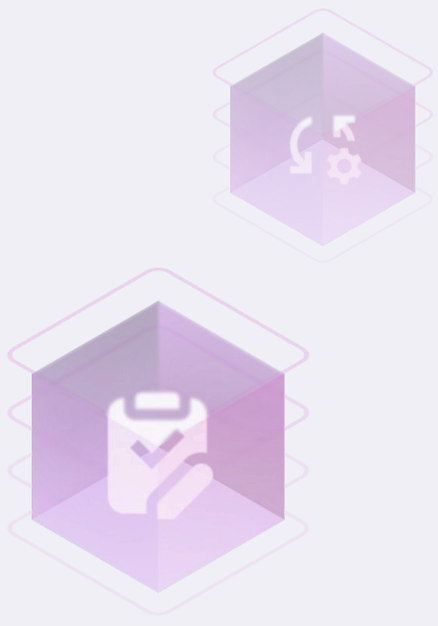
Scorecard & Checklist



The Hidden Foundation of the SOC

This document and the companion spreadsheet describe and use a scorecard and checklist to make case quality measurable and coachable. This toolkit is the manual version of the scoring approach that our open-source tool, **SOC Grader** applies automatically and at scale.

Toolkit Contents



Implementation Guide	How to turn case reviews into a repeatable coaching loop: sample → score → coach → improve.
Checklist	The observable things a high-quality case should contain so that a case reviewer can independently verify the work.
Scorecard	A method that converts the checklist into a repeatable 0-10 score for each case, plus flags to note when key evidence is missing.
Interactive Scorecard spreadsheet	This document explains what gets scored and what "good" looks like. Use the accompanying spreadsheet template to automate calculations described in this document.

Anatomy of a quality SOC case

A quality SOC case turns noisy telemetry data into a decision you can trust - and a next step you can take. The four key components of a quality case include:

1. **Investigation plan**
   What you set out to validate and why – your hypothesis.
2. **Evidence + context**
   The specific telemetry and context that supports (or refutes) the hypothesis.
3. **Conclusion + confidence**
   A clear disposition and why you are confident.
4. **Next action**
   What should happen next (contain, monitor, notify, remediate) and who owns it.

Implementation Guide: How to use this Toolkit

Score a sample of cases. For example, select 10 recent cases a single MDR provider delivered or that are destined for a single SOC queue. Do not pick only your best cases - true near-random sampling reveals a more accurate quality level.

Goal

Case reviews become a repeatable coaching loop. Consistent scoring creates clear coaching signals, and quality improves over time.

Method

1 **Pick a sample**

Choose 10 recent cases from the same provider or workflow.

2 **Score each case**

For each item in the Case Quality Checklist, mark it: Complete / Partial / Missing and note where the evidence appears in the case.

Important Note: You'll want to adapt generic labels in the Case Quality Checklist below to specific alerts. The checklist uses universal cybersecurity concepts (e.g., "Infrastructure Trust"), but the specific evidence required changes based on the alert type. You must adapt these categories to the scenario.

- ↳ Example 1: Login Alerts. For these alerts, "Infrastructure Trust" in the Case Quality Checklist means checking VPN logs, Geolocation, and ASN reputation.
- ↳ Example 2: Malware/Network Alerts: For these alerts, "Infrastructure Trust" means checking for Command & Control traffic patterns and DNS requests.

3 **Roll up**

Compute an average score and list the most common critical and minor gaps.

4 **Coach**

Turn the top 1-2 recurring gaps into a short playbook or template update; re-score next week/month to confirm improvement.

Case Quality Checklist

Use this table to review each case and determine whether it contains the minimum auditable decision context.

Investigation Area	Case Requirement	Tier	Weight
Alert trigger validation	States the specific condition/event pattern that caused the alert to fire.	Critical	5
Alert trigger validation	Validates the trigger using primary telemetry (log excerpts, query output, screenshots, or equivalent).	Critical	5
Identity/source validation	Identifies the actor (user/service/device/workload) and confirms legitimacy (expected owner, role, and context).	Critical	5
Identity/source validation	Checks for direct compromise indicators for the actor/source (auth anomalies, prior alerts, suspicious sequences) and records results.	Critical	5
Impact & scope	Enumerates affected assets/accounts/resources and confirms scope boundaries (what is and is not impacted).	Critical	5
Impact & scope	Confirms whether sensitive actions/data access occurred (or documents that it was checked and not found).	Critical	5
Baseline/historical context	Compares activity to historical baseline (new vs normal) for the entity involved.	Important	3
Baseline/historical context	Provides a short timeline (before/during/after) so the sequence of events is verifiable.	Important	3
Infrastructure trust (if applicable)	Validates source location/path trust (VPN/corp ranges, geo/ASN, known infra) when network/access is part of the alert.	Important	3
Access path legitimacy (if applicable)	Confirms access method and posture (app, auth method, device posture, MFA) match expected behavior.	Important	3
IoCs & threat context (if applicable)	Checks relevant artifacts (IPs/domains/files/URLs/hashes) against reputation/TI and records outcomes.	Important	3
Next action	Documents the next step (contain/monitor/notify/remediate) and who owns it; includes deadlines if time-sensitive.	Important	3
Auditability	Includes references to data sources or queries run (enough for another analyst to reproduce key validations).	Nice-to- have	1
Additional context	Adds secondary enrichment (peer comparisons, broader hunting, related cases) when it materially increases confidence.	Nice-to- have	1

Legend

Investigation Area: Logical grouping: Trigger, Identity, Baseline, Impact, IoCs, Disposition, Next Action, Auditability.
Case Requirement: Must be explicit and verifiable in the write-up.

Tier / Weight: Critical=5, Important=3, Nice-to-have=1
Action Item: Yes only if the Grade is Partial (i.e., 1) or Missing (i.e., 0) and explicitly called out as a next step.

Scorecard: How to Grade

The scorecard helps convert the checklist into a repeatable numeric score, while still preserving evidence-based review.

STEP 1

Grade each Case Quality Checklist item using the evidence in the case

Label	Meaning	Value
Complete	The case explicitly addresses the Case Requirement with verifiable evidence.	2
Partial	The case touches on the Case Requirement but misses key validation or evidence.	1
Missing	The Case Requirement is not addressed in the case.	0
Action item	If Partial or Missing, record whether it is explicitly listed as an Action Item/Next Step. That's because a case can be incomplete but still operationally responsible if it clearly documents what remains to be done (especially for items that are MDR customer responsibilities, or where the analyst lacks access).	Yes/No

STEP 2

Compute the weighted score and normalize to 0-10

These calculations are explained here, and captured as formulas in the associated spreadsheet. The weighting (i.e., Grade / 2) is based on scores that range from 0 to 2; because 2 means "100%" we normalize by dividing everything by 2.

Total points possible	SUM (Checklist Item Weights)
Weighted points earned	SUM (Checklist Item Weight × (Grade Value / 2))
Normalized score (0-10)	(Weighted points earned / Total points possible) × 10

Next Steps

When you're ready to operationalize the scorecard and checklist, you can use the spreadsheet template that accompanies this document. The approach taken in this document and calculated in the spreadsheet is the same methodology the SOC Grader tool uses.

AirMDR built the tool to help accelerate and scale the scoring process, and **it's free to use**.

Try the Tool