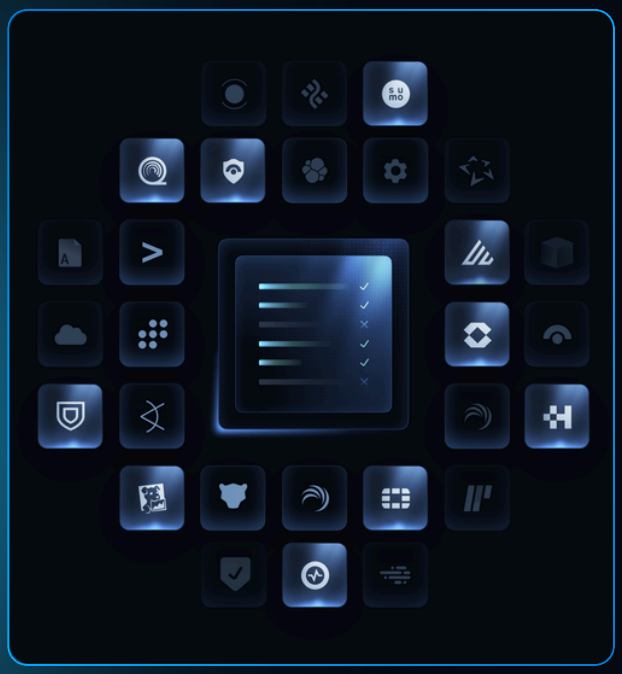
SIEM Evaluation Checklist & Scoring Matrix

This checklist is designed to guide your SIEM evaluation process and create a defensible, measurable record of results. Each criterion is weighted based on its strategic importance. Score each vendor from 0–5 using the rubric provided, and record notes or evidence. Weighted scores will help you compare vendors side by side.



Scoring guidance

Each SIEM should be scored on a 0–5 scale across the criteria in this checklist. Weights are assigned to reflect their relative importance, so the total score adds up to 100. This turns subjective impressions into measurable outcomes and gives you a defensible comparison across vendors.

0 = Absent or fails requirement
1 = Exists but immature or pilot-only
2 = Exists but unreliable or incomplete
3 = Adequate, meets minimum standard
4 = Strong, proven in production
5 = Excellent, mature, future-ready

Preparation for evaluation

Before scoring any SIEM, two steps will determine whether your evaluation reflects reality or sets you up for surprises later. These are not vendor features but prerequisites for a meaningful comparison:

1. Define objectives and risk profile

Clarify what success means for your organization. Is the priority faster investigations, broader detection coverage, or lowering the cost of ownership? Tie your evaluation criteria to those goals and compliance risks so the outcome is relevant.

2. Test with realistic, representative data

Run your evaluation with the same scale, variety, and quality of data your SOC manages every day. Avoid “clean” vendor-provided datasets that hide ingestion issues and performance bottlenecks. Use noisy logs, production-scale volumes, and synthetic edge cases where necessary.

SIEM Evaluation Checklist (Weighted 100%)

Category	Criteria	Why It Matters	Weight*	Score (0–5)	Weighted Score
Data Collection	Collection & normalization	Ensures logs are parsed/normalized automatically; prevents hidden engineering costs	18		
Detection & Control	Detection & threat hunting	Validates automated detection/correlation of real threats across sources	25		
	UEBA & AI-driven analytics	Identifies insider threats and anomalies missed by static rules	7		
Operations & Integration	Integration & operational fit	Confirms interoperability with SOAR, case mgmt, cloud-native/SaaS tools	12		
	Scalability & performance	Sustains ingestion/queries at enterprise & multi-cloud scale	15		
	Usability & manageability	Analyst/admin learning curve and day-2 ops burden	8		
Business & Compliance	Cost & TCO clarity	Models affordability (license, storage, infra, people costs)	5		
	Vendor reliability & compliance support	Vendor stability, roadmap, regulatory certifications (PCI, HIPAA, ISO, GDPR, etc.)	10		

TOTAL **100**

(*The logic behind these weights is explained in detail on page 4)

How to calculate weighted scores

For each criterion:
Weighted Score = (Score ÷ 5) × Weight
Add up all weighted scores for the vendor to get a total out of 100.

Example:
If a SIEM scores 4/5 on “Detection & Threat Hunting” with a weight of 25%,

Weighted score = (4 ÷ 5) × 25
= (0.8) × 25 = **20**

The weighted score is **20.** Repeat across all criteria and sum the results.

SIEM vendor comparison dashboard

Summarize evaluation results across vendors. It provides a single-page view for leadership discussions and decision-making.

- Total Weighted Score shows overall alignment to your priorities.
- Key Observations capture the most important findings or differentiators from the evaluation.

SIEM Vendor	Total Weighted Score	Key Observations
SIEM A		
SIEM B		

Summary

This checklist and scoring matrix are designed to help you cut through vendor noise and make decisions with clarity. By applying consistent weights, documenting evidence, and comparing vendors side by side, you gain the confidence that your choice will stand up in production and not just in a demo.

With DataBahn in place, you can simplify evaluation even further — our platform normalizes telemetry, removes parsing limitations before it reaches the SIEM, and enables multi-destination routing, giving you cleaner, safer data to test multiple SIEMs in parallel.

Ready to see how DataBahn can simplify your SIEM evaluation and migration? Request a demo today!

Logic behind the weights:

The weights in this checklist are designed to balance core technical capabilities with operational and business factors. They reflect the areas where a SIEM can either enable or undermine long-term success.

Core Technical Capabilities (58%)

These categories represent the fundamental "can it do the job?" aspects of a SIEM. They receive the largest share of the weight because if a platform fails here, its other features are irrelevant.

- **Detection & Threat Hunting (25%)** - This is the highest-weighted category because detection is the primary reason for a SIEM's existence. The platform must reliably surface real threats without overwhelming analysts with noise.
- **Collection & Normalization (18%)** - "You can't detect what you can't collect." Reliable ingestion and normalization prevent blind spots and ensure detections function as designed. A failure here undermines everything else.
- **Scalability & Performance (15%)** - A SIEM must perform at enterprise scale, remaining resilient under heavy load. If it collapses when volumes spike, it cannot be trusted in production.

Operational & Business Alignment (42%)

These categories determine how well the SIEM fits into your team and your broader business requirements.

- **Integration & Operational Fit (12%)** - The SIEM must be a team player, connecting seamlessly with SOAR, ticketing systems, and other security tools. Smooth integration reduces friction and speeds response.
- **Vendor Reliability & Compliance Support (10%)** - A SIEM is also a long-term partnership. The vendor must be stable, supportive, and able to meet regulatory requirements such as PCI DSS or HIPAA.
- **Usability & Manageability (8%)** - A tool only succeeds if analysts and administrators can use it effectively. Usability and manageability reduce training overhead and drive adoption.
- **UEBA & AI-Driven Analytics (7%)** - These capabilities provide forward-looking value by detecting insider threats and anomalies beyond rule-based correlation. They strengthen detection but are not yet the primary driver.
- **Cost & TCO Clarity (5%)** - Cost should always be considered, but it should not overshadow core security outcomes. This weight ensures long-term affordability is factored in without dominating the decision.

Note: These weights are recommended baselines. They may vary depending on your environment, industry, and priorities. For example, a regulated business may increase the weight of compliance, while a high-growth cloud-native company may emphasize scalability. Adjust the weights before scoring vendors so the results reflect your real requirements.

To see how disciplined evaluation sets up a smoother cutover, explore our SIEM Evaluation use case.