SIEM Migration Checklist: How to Avoid Detection Gaps

By: Jaiz Anuar

25 July 2026 · Cybersecurity · Security Operations · 7 min read

A SIEM migration is only successful when the organisation can demonstrate that meaningful threats will still be detected, investigated and escalated throughout the transition.

Migrating a Security Information and Event Management platform is often treated as a technology replacement.

The organisation selects a new platform, connects the log sources, rebuilds the dashboards and plans a cutover date.

But a SIEM migration is not complete simply because logs are visible in the new system.

The real question is whether the organisation can still detect, investigate and respond to threats throughout the transition.

A migration may look successful from a project perspective while silently creating detection gaps. Critical logs may be missing. Correlation rules may not behave as expected. Alerts may not reach the right team. Historical evidence may become inaccessible just when investigators need it.

This is why a SIEM migration checklist should focus on security outcomes, not only technical activities. As discussed in A SIEM Migration Is Not Just a Technology Refresh. It Is a Security Risk Event., the transition itself creates risk that must be identified, controlled and formally governed.

1. Define What “Ready” Means

Before migration begins, establish measurable readiness criteria.

“Logs are flowing” is not enough.

The new SIEM should only be considered operationally ready when:

Critical log sources are connected and stable.

Priority detection use cases have been tested.

Alerts reach the correct monitoring team.

Investigation procedures are documented.

Escalation paths are working.

Analysts can access sufficient historical data.

Response teams understand their responsibilities.

Without clear acceptance criteria, project pressure may cause the organisation to declare success too early.

A platform can be technically available but operationally unready.

2. Identify Critical Log Sources

Not every log source carries the same security value.

Start by identifying the systems that are most important for detecting high-impact attacks. These commonly include:

Identity and authentication platforms.

Privileged access systems.

Domain controllers.

Firewalls and internet gateways.

Endpoint detection platforms.

Cloud environments.

Critical applications.

Databases containing sensitive information.

Email and collaboration platforms.

Vulnerability management systems.

Each critical source should have an owner, expected event volume, retention requirement and validation method.

A connector showing a green status does not prove that the correct security events are being received. Sample events should be examined to confirm that timestamps, usernames, source addresses, event categories and other important fields are correctly parsed.

3. Prioritise Detection Use Cases

Many organisations attempt to migrate every existing detection rule at once.

This may not be realistic.

Instead, classify use cases according to risk and business importance. Priority should be given to scenarios such as:

Privileged account misuse.

Multiple failed authentication attempts.

Suspicious administrative changes.

Malware or ransomware activity.

Endpoint isolation events.

Unusual outbound traffic.

Data exfiltration indicators.

Disabled security controls.

New accounts added to privileged groups.

Access from unexpected locations.

Critical application attacks.

The objective is not immediate rule-for-rule duplication. The objective is to preserve the ability to identify the organisation’s most serious threat scenarios.

Each migrated rule should be tested using known events, controlled simulations or previously observed incidents.

A rule that exists but has never been triggered during testing should not automatically be assumed to work.

4. Compare Detection Coverage

Different SIEM platforms process data differently.

Field names, correlation logic, enrichment sources, query languages and alert thresholds may change. An identical-looking rule may therefore produce different results.

Create a detection coverage matrix that records:

Existing use case.

Threat scenario addressed.

Required log sources.

Status in the new SIEM.

Test evidence.

Known limitations.

Compensating controls.

Responsible owner.

This makes detection gaps visible and allows management to understand what remains incomplete.

The comparison should focus on coverage, not simply the number of rules. Hundreds of low-value rules cannot compensate for a missing high-risk detection scenario. As explored in When Security Tools Become the Noise, alert volume is not the same as useful visibility; noise can hide the events that matter.

5. Maintain Parallel Monitoring

Where possible, operate the old and new SIEM platforms in parallel for an agreed period.

Parallel monitoring allows the security team to compare:

Alert volumes.

Detection accuracy.

Missed events.

False positives.

Processing delays.

Analyst workflows.

Escalation performance.

Differences should be investigated before the old platform is retired.

When parallel operation is not possible, stronger compensating controls are required. These may include direct monitoring from endpoint, network, identity and cloud security platforms, supported by manual correlation and clearly assigned alert ownership.

The transition risk should be formally acknowledged rather than hidden behind the migration schedule.

6. Protect Historical Investigation Data

Security incidents are not always discovered immediately.

An investigation may require authentication records, network activity or application logs from several months earlier. The Most Dangerous Incidents Start as Normal Days, and evidence from an apparently routine period may later become essential to understanding an attack. If historical data becomes unavailable during migration, the organisation may lose the ability to determine what happened.

Confirm:

How long historical logs remain accessible.

Whether data will be migrated or archived.

Who can retrieve archived evidence.

How quickly it can be restored.

Whether timestamps and integrity are preserved.

Whether retention meets legal, regulatory and investigation requirements.

Historical access should be tested before the previous SIEM is decommissioned.

A written statement that logs have been retained is less valuable than proof that investigators can retrieve and use them.

7. Confirm Monitoring Team Readiness

A new platform also creates a new operating model.

Internal analysts and managed security service providers must understand:

Alert ownership.

Triage expectations.

Severity classification.

Escalation timeframes.

Incident declaration criteria.

After-hours responsibilities.

Communication channels.

Regulatory notification processes.

Runbooks should reflect the actual platform and team structure.

If a new service provider is involved, mobilisation should include access provisioning, platform training, environment familiarisation, use-case walkthroughs and live escalation exercises.

Contract commencement does not automatically mean monitoring readiness.

8. Monitor the Monitoring Platform

The SIEM itself must be monitored.

The organisation should detect when:

A critical connector stops sending logs.

Event volume drops unexpectedly.

Parsing fails.

Processing is delayed.

Storage limits are reached.

A detection rule is disabled.

Alert forwarding fails.

Administrative configurations are changed.

Without platform health monitoring, a detection capability can fail silently.

Log-source health should be reviewed continuously, with critical failures escalated like other security incidents.

9. Establish a Cutover and Fallback Plan

The final cutover should include clear decision points.

The plan should state:

Who authorises the cutover.

Which readiness conditions must be met.

What unresolved gaps are accepted.

Which compensating controls remain active.

When the old platform will be switched off.

What will trigger rollback or fallback.

Who makes the final risk decision.

Fallback planning is particularly important when contracts, licences or infrastructure dependencies limit access to the previous SIEM.

The organisation should know what monitoring capability remains available if the new platform becomes unstable immediately after cutover.

10. Continue Tuning After Go-Live

Go-live is not the end of the migration.

Detection logic must be tuned using actual operational data. Analysts should review false positives, missed activity, parsing problems, event delays and investigation difficulties.

The first weeks after implementation should include frequent reviews of:

Critical alerts generated.

Use cases that have not triggered.

Failed log sources.

Escalation performance.

Analyst feedback.

New threat scenarios.

Outstanding detection gaps.

The migration should only be considered complete when the new operating model is stable and security coverage has been demonstrated.

The Migration Checklist

Before retiring the previous SIEM, confirm that:

Critical log sources are connected and validated.

Priority detection use cases are operational.

Detection coverage has been compared.

Alert routing and escalation have been tested.

Monitoring teams are fully onboarded.

Historical evidence remains accessible.

Log-source failures can be detected.

Compensating controls cover known gaps.

Cutover and fallback decisions are documented.

Post-go-live tuning has clear ownership.

A SIEM migration is not just the movement of logs from one platform to another.

It is the transfer of an organisation’s ability to see threats.

The migration is successful only when the organisation can demonstrate that meaningful threats will still be detected, investigated and escalated without interruption.

Question assumptions. Share knowledge. Build trust.