



GUIDE

The Complete SIEM Migration Checklist

A 9 Stage Field-Tested Framework

Table of Contents

Introduction and How to Use this Guide	3
Stage 1: Know Why You're Moving Before You Move	4
Stage 2: Align the Organization Before Aligning the Technology	5
Stage 3: Conduct a Rigorous Current-State Inventory	6
Stage 4: Reject the Lift-and-Shift Mentality	7
Stage 5: Plan the Architecture and Infrastructure Foundation	8
Stage 6: Build a Rigorous Validation Framework	9
Stage 7: Address the Skills Gap Before It Becomes a Crisis	10
Stage 8: Plan the Cutover and Go-Live Strategy	11
Stage 9: Measure, Maintain, and Continuously Improve	12
Quick Reference: Migration Checklist at a Glance	13



Introduction

Migrating to a modern Security Information and Event Management (SIEM) platform is one of the most consequential decisions a security organization can make. Done right, it elevates your threat detection capabilities, modernizes your security operations center (SOC), reduces costs, and positions your team to tackle tomorrow's adversaries. Done wrong, it creates months of disruption, blows past budget, leaves detection gaps wide open, and — worst of all — may leave you no more secure than when you started.

This guide distills real-world experience from SIEM migrations of every scale — from six-figure engagements to multi-million-dollar, multi-stage transformations — along with insights from UltraViolet industry practitioners. Whether you are just beginning to evaluate a new platform or you are already mid-migration, use this checklist to avoid the most common pitfalls and build a migration that actually delivers on its promise.

How to Use This Guide

These stages are presented in sequence, but real migrations are rarely linear. Expect to revisit earlier stages as client requirements evolve, new information surfaces in the course of the engagement, and ownership and decision-making structures become clearer. Every checkbox represents a real decision point where migrations commonly derail. Work through them with your team and use the callout boxes throughout for deeper context on the issues that matter most.



STAGE 1

Know Why You're Moving Before You Move

The single most important step in any SIEM migration has nothing to do with technology. It has everything to do with clarity of purpose. Teams that skip this step often complete the migration and find themselves in exactly the same situation — just with a different logo on the login screen.

1.1 Identify and Document the Specific Pain Points Driving the Migration

Before anything else, your team needs to articulate precisely why the current SIEM is no longer sufficient. Vague dissatisfaction is not a strategy. Documented, specific shortcomings are.

- ☐ Is the platform too expensive — licensing, storage, or infrastructure costs?
- ☐ Does the current SIEM lack modern capabilities such as AI-assisted detection, behavioral analytics, or flexible storage options?
- ☐ Is the team suffering from alert fatigue due to excessive false positives and poor signal-to-noise ratio?
- ☐ Are there scalability limitations — does the system struggle during threat spikes or high-volume ingestion events? Are there industry buying cycles to consider? Industry buying cycles can compound this: retail organizations, for example, face concentrated operational pressure during Q4, when change windows are limited and risk tolerance is at its lowest.
- ☐ Is there an inability to connect detections across hybrid and multi-cloud environments?
- ☐ Has the platform been under-maintained, leading to degraded performance that may be mistaken for a product limitation?

Critical Insight:

Is It the Tool or the Maintenance?

Before committing to a full migration, honestly assess whether your current SIEM's shortcomings stem from the platform itself or from years of deferred maintenance. Neglected correlation rules, untuned alerts, orphaned dashboards, and stale data sources can make even a capable SIEM appear broken. Like a car without oil changes or tire rotations, a SIEM without ongoing care will underperform, and switching vendors won't fix a maintenance problem. If maintenance has lapsed, understand that the new platform will face the same fate without a long-term operational commitment.

1.2 Define What Success Looks Like — Before Day One

Many migrations complete the technical work but fail to deliver measurable security improvements. Avoid this by establishing clear, measurable outcomes at the outset.

- ☐ Define quantitative success metrics: target cost reduction percentage, alert volume reduction, mean time to detect (MTTD), and mean time to respond (MTTR).
- ☐ Establish a security posture baseline before the migration begins — document your current detection coverage, gap areas, and risk exposure. This is your pre-migration benchmark.
- ☐ Plan a post-migration security posture assessment using the same framework to measure improvement objectively.
- ☐ Confirm that the new platform can realistically meet your defined objectives — do not assume capability; validate it.
- ☐ Align success criteria with your organizational framework based on coverage targets such as, MITRE ATT&CK, NIST CSF, Unified Kill Chain, or others.



STAGE 2

Align the Organization Before Aligning the Technology

Technology migrations fail when the humans involved are not aligned. Some of the most painful SIEM migrations in practice result not from technical complexity, but from organizational misalignment — different teams pulling in different directions, or a decision made at the top that the people doing the work never bought into.

2.1 Bridge the Gap Between the Reason to Buy and the Reason to Use

There is a fundamental difference between the executive who decides to purchase a new SIEM and the analyst who will live inside it every day. When those two perspectives are not reconciled early, resistance slows the project and the new platform gets under-utilized.

- ☐ Identify all stakeholders: executive sponsors (CIO, CISO), project owners, SOC analysts, SIEM engineers, data owners, compliance leads, and IT operations teams.
- ☐ Hold alignment sessions where both the “reason to buy” (strategic, financial, modern capability) and the “reason to use” (day-to-day analyst workflow, familiarity, use case coverage) are explicitly discussed.
- ☐ Acknowledge that team members who are highly skilled in the legacy platform will experience a disruption to their expertise — plan for this proactively, not reactively.
- ☐ Once the decision to migrate has been made at the leadership level, establish a clear organizational position: the migration is proceeding. Channel the team’s energy into making it successful rather than re-litigating the decision.

2.2 Build Your RACI and Define Data Ownership Early

One of the most underestimated sources of migration delays is the absence of clear ownership, particularly around data validation. Without it, teams fall into cycles of “that’s not my job” that consume weeks of project time.

- ☐ Build a RACI (Responsible, Accountable, Consulted, Informed) chart that covers each major work stream: data source onboarding, parsing and normalization, use case migration, validation, cutover, and post-go-live support.
- ☐ Distinguish between data users (analysts who query the data daily) and data owners (those with authority to validate and approve data as accurate and complete). These are often different people.
- ☐ For each critical data source, identify all parties involved in validation — there may be 3 to 4 people per source across technical, business, and compliance functions.
- ☐ Establish who has the authority to sign off on data validation. Record count matches are a starting point, but the data also must make sense to the humans reading it in the new system.
- ☐ Document escalation paths for validation disputes before they happen, not during them.

From the Field: Internal Resistance is Real

A common challenge on migration engagements is influencing teams that are deeply skilled in a legacy SIEM. When a decision is made six months prior and teams are still resisting, momentum stalls. The key is ensuring both the strategic rationale and the day-to-day operational benefits are communicated clearly and repeatedly. The goal is mutual alignment — not just compliance.



STAGE 3

Conduct a Rigorous Current-State Inventory

You cannot accurately plan a migration if you do not know what you are migrating. A thorough inventory of your existing environment is not optional — it is the foundation of every subsequent decision.

3.1 Audit Your Data Sources

- ☐ Inventory every active log source being ingested by the current SIEM: source name, type, volume (events per day), and business or security purpose.
- ☐ Identify which data sources are actively used in correlation rules, dashboards, and alerts versus those that are being ingested but rarely or never queried.
- ☐ Flag data sources that are voluminous but low-value for security purposes — these are candidates for routing to lower-cost data lakes or object stores rather than the new SIEM.
- ☐ Understand whether your current SIEM uses normalized log formats or retains raw logs — this has direct implications for how correlation rules and parsers must be rebuilt in the new platform.
- ☐ Determine whether your current platform uses live correlation or batch query architecture, as this fundamentally changes detection timing behavior in the new system.

3.2 Audit Your Use Cases, Rules, and Content

Migrations routinely surface years of accumulated content that is no longer relevant, was never validated, or was built for a business context that no longer exists. Do not pay to migrate content that is not earning its keep.

- ☐ Catalog all correlation rules, detection use cases, dashboards, and reports currently in production.
- ☐ Evaluate each rule and dashboard: when was it last triggered? Is it generating actionable alerts or contributing primarily to alert noise? Has the underlying business requirement changed?
- ☐ Identify and retire content that has not produced a useful result in a timeframe relevant to your organization — typically six to twelve months, though this should be adjusted for your operational context and risk profile. There is no business case for migrating abandoned dashboards or rules that no one checks.
- ☐ Prioritize use cases by criticality: Tier 1 (must be live at cutover), Tier 2 (migrate within 30 days post-cutover), Tier 3 (migrate within 90 days or re-evaluate).
- ☐ Map your use cases to the MITRE ATT&CK framework to identify coverage gaps you can address in the new platform rather than simply replicating the gaps from the old one.

Avoid Migrating Technical Debt

It is tempting to move everything into the new SIEM as quickly as possible. Resist this. Organizations that perform a thorough content audit before migration consistently report better outcomes: lower ingestion costs, fewer false positives, and faster analyst response times. Use the migration as a forcing function to clean house.



STAGE 4

Reject the Lift-and-Shift Mentality

This is arguably the most dangerous mindset error in SIEM migrations. A lift-and-shift approach — moving everything from the old system to the new one unchanged — sounds efficient. In practice, it transfers all of your existing problems while adding new ones, and it misses the entire value of the new platform.

4.1 Understand That No Two SIEMs Are the Same

- ☐ Accept that detection rules, correlation logic, and parsers built for the legacy system will not translate directly. Plan for a rewrite, not a copy-paste. This effort typically consumes 40 to 60 percent of total project timeline.
- ☐ Research the new platform's native detection capabilities, pre-built content library, and out-of-the-box integrations — you may find that existing use cases are covered by native content that is more capable than what you built in-house.
- ☐ Understand the new platform's data handling approach: does it index raw logs, normalize on ingestion, or use a schema-on-read model? This affects query language, retention costs, and correlation logic.
- ☐ If migrating from on-premises to cloud-native SIEM, plan for a complete architectural shift — not just a hosting change. Firewall rules, collection agent deployment, data routing, and access controls all require rethinking.

4.2 Rebuild, Don't Replicate

Think of the migration as an opportunity to build the SIEM your team always wanted — one that reflects your current business requirements, current threat landscape, and current team capabilities.

- ☐ For each migrated use case, ask: what was this detection trying to accomplish? Then find the best way to achieve that objective in the new platform, which may differ from the original implementation.
- ☐ Do not port dashboards that no one was using. Interview your SOC analysts — what information do they actually need to investigate threats efficiently?
- ☐ Rebuild parsers for the new platform from scratch, using the vendor's supported parser library where available. Do not assume custom parsers from the legacy system will function correctly.
- ☐ Evaluate whether new AI-assisted features (behavioral analytics, automated case summarization, natural language search) change how certain use cases should be structured.

Lift-and-shift transfers all of your existing problems while adding new ones, and it misses the entire value of the new platform.



STAGE 5

Plan the Architecture and Infrastructure Foundation

Your SIEM is only as strong as its underlying architecture and its business purpose. Decisions made at this stage determine your ingestion costs, query performance, scalability, and long-term operational overhead. Cutting corners here is expensive to reverse.

5.1 Design the Data Architecture

- ☐ Select your deployment model: cloud-native SaaS, cloud-hosted (IaaS), hybrid, or on-premises. Each carries different cost structures, data residency implications, and operational responsibilities.
- ☐ Select your cloud platform if applicable: GCP, AWS, or Azure. Consider where your existing workloads reside and what native integrations are available.
- ☐ Determine your ingestion volume requirements: current events-per-day, projected 12-month growth, and peak load capacity needed.
- ☐ Design your data routing strategy: which data goes directly into the SIEM, which is tiered to lower-cost storage, and which is routed to alternative platforms such as observability tools or data lakes.
- ☐ Model your total cost of ownership honestly — cloud SIEMs use consumption-based pricing that is notoriously difficult to forecast. Model ingestion costs, storage costs, and query costs under realistic and worst-case scenarios before signing contracts.
- ☐ Establish retention policies for each data type, balancing compliance requirements (which mandate specific retention periods) against cost and operational utility.

5.2 Plan the Collection Architecture

- ☐ Determine your collection methods for each data source: agent-based collection, agentless syslog, API-based integration, or cloud-native connector.
- ☐ Validate that installing collection agents alongside existing agents does not introduce CPU or memory contention that could cause system instability.
- ☐ Confirm that all data sources are compatible with the new SIEM's collection capabilities — especially sources that were custom-integrated into the legacy system.
- ☐ Establish identity verification and access controls for each data source to prevent injection of spoofed or malicious data into the SIEM.
- ☐ Plan for secure data transmission: encryption in transit, access controls on collection endpoints, and authentication for log forwarding.

Architecture Tip: Run Both SIEMs in Parallel

Before cutting over any data feed, stand up the new SIEM in parallel ingestion mode. This allows your team to validate parsing, data quality, and alert fidelity against the known-good baseline of the legacy system. Accepting the risk of single-SIEM operation during validation is one of the most preventable causes of post-cutover incidents.



STAGE 6

Build a Rigorous Validation Framework

Validation is the most misunderstood stage of a SIEM migration. Teams often treat it as a formality — run a record count, see that numbers match, declare success. In reality, data validation is a multi-stakeholder, multi-layered process that requires both technical verification and business sign-off.

6.1 Define Your Validation Process Before You Start

- ☐ Document your validation methodology before any data is migrated. Define what “validated” means for each data source: record count match, field mapping correctness, schema compliance, and visual review by business stakeholders.
- ☐ Establish date range alignment: validation queries in the legacy system and the new system must use identical time windows.
- ☐ Plan for data format differences — differences in field names, timestamp formats, and event structure between the two systems are expected and must be accounted for in validation.
- ☐ Build testing tools or scripts to automate record count comparison across major data sources, reducing manual effort and human error.

6.2 Involve the Right People in Validation

- ☐ Before requesting validation sign-off, confirm that each approver has received hands-on training in the new platform. A common and costly failure mode: a key stakeholder is asked to approve data they have no experience querying. Identify and close this gap at project kickoff, not when the sign-off request arrives.
- ☐ Involve both data users and data owners in validation. The analyst who queries data daily can confirm format and field accuracy. Only the data owner has the authority to certify the data as correct and complete.
- ☐ Do not assume the person with the most technical knowledge of a data source has the authority to sign off on it. Identify the approver for each source explicitly at the start of the project.
- ☐ For complex data sources, schedule structured validation review sessions rather than relying on asynchronous email approvals — misunderstandings are caught faster in real-time discussion.
- ☐ Document every validation decision, including what was reviewed, who approved it, and any known gaps or deviations accepted as part of the approval.

Validation War Story

On a real UltraViolet SIEM migration engagement, the validation process surfaced a critical gap: the technical team who knew the data best had no authority to sign it off. When the actual data owner was brought in, they could confirm the data appeared visually correct but lacked the technical context to verify field-level accuracy. The result was weeks of back-and-forth, internal disputes over ownership, and a delay that could have been avoided by mapping the RACI at project kickoff. Do not let this happen to your team.



STAGE 7

Address the Skills Gap Before It Becomes a Crisis

Modern SIEM platforms — especially those with AI-driven detection, behavioral analytics, and data engineering capabilities — require skill sets that differ materially from what legacy SIEM administration demanded. Underestimating this gap is one of the most common causes of post-migration underperformance.

7.1 Assess Your Team's Current Capabilities

- ☐ Conduct an honest skills assessment against the requirements of the new platform. Include: query language proficiency, data engineering capabilities, parser development, detection engineering, and cloud platform administration.
- ☐ Identify which team members have adjacent skills that can be developed and which gaps require external expertise, new hiring, or ongoing managed services.
- ☐ Do not assume that mastery of the legacy SIEM translates to competency in the new platform. The operational model may be fundamentally different.

7.2 Build and Execute a Training Plan

- ☐ Schedule platform training for all SIEM users — analysts, engineers, and administrators — before the migration cutover date, not after.
- ☐ Invest in hands-on training using your own data in a development or staging environment. Theoretical training without practical application does not produce operational readiness.
- ☐ Leverage vendor certification programs and training resources. Most modern SIEM vendors provide structured learning paths.
- ☐ Plan for a productivity dip immediately following cutover. This is normal and expected. Establish escalation paths during the adjustment period so analysts have support when working in the new environment.
- ☐ Consider embedding experienced professional services resources alongside your team during the first 30 to 60 days post-cutover to accelerate knowledge transfer.

Don't Make Services an Afterthought

One of the most consistent observations from experienced UltraViolet SIEM migration practitioners: professional services should be engaged during the sales and planning cycle, not as a post-purchase add-on. Teams that rely solely on their internal staff — who may be deeply skilled in the legacy system but unfamiliar with the new platform — dramatically underestimate the time and risk involved. Engage services early, while the client is still shaping requirements, so that expertise is integrated from the start.

STAGE 8

Plan the Cutover and Go-Live Strategy

The cutover is the highest-risk moment in any SIEM migration. A well-planned cutover is nearly invisible to the security operations team. A poorly planned one creates detection gaps, loses data, and can leave the organization blind to active threats for hours or days.

8.1 Define Your Cutover Criteria

- ☐ Establish a clear set of go/no-go criteria for cutover: which Tier 1 use cases must be validated and operational before the legacy SIEM is retired.
- ☐ Set a realistic cutover date that reflects actual project progress — do not allow contractual or budget pressures to force a cutover before the new environment is ready.
- ☐ Define an explicit rollback plan: if critical issues emerge within 24 to 48 hours of cutover, what are the steps to restore legacy SIEM function while issues are resolved?

8.2 Execute a Parallel Run Period

- ☐ Run both SIEMs simultaneously — ingesting the same data into both — for a defined parallel period before fully cutting over. Compare alert outputs to validate detection fidelity.
- ☐ Do not shut down the legacy SIEM until Tier 1 use cases have been validated in production, not just in testing.
- ☐ Communicate the cutover schedule to all stakeholders, including business units that depend on SIEM reporting for compliance purposes.
- ☐ Plan for increased monitoring during the first 30 days post-cutover and have escalation contacts available for rapid response to anomalies.

A well-planned cutover is nearly invisible to the security operations team. A poorly planned one creates detection gaps, loses data, and can leave the organization blind to active threats for hours or days.



STAGE 9

Measure, Maintain, and Continuously Improve

The migration is not the finish line. A modern SIEM is a living system that requires ongoing investment in tuning, maintenance, and evolution. Organizations that treat the go-live date as the end of the project consistently underperform in security outcomes compared to those that treat it as the beginning of the operational stage.

9.1 Conduct a Post-Migration Security Posture Assessment

- ☐ Using the baseline security posture assessment conducted before the migration, perform a formal post-migration assessment using the same methodology and framework.
- ☐ Measure and document improvement across key dimensions: threat detection coverage, mean time to detect, mean time to respond, false positive rate, and analyst efficiency.
- ☐ Identify remaining gaps and build a roadmap for addressing them — the migration may have closed some gaps while revealing others.

9.2 Build a Sustainable Maintenance Model

- ☐ Establish a regular cadence for rule tuning and alert threshold adjustment based on operational feedback from SOC analysts.
- ☐ Implement a log source health monitoring process to detect when data sources stop reporting or experience volume anomalies.
- ☐ Schedule periodic system performance reviews and audits to catch configuration drift, orphaned content, and underperforming integrations before they become problems.
- ☐ Maintain current documentation: data source inventory, use case library, RACI, and runbooks. Documentation that falls out of date becomes a liability.
- ☐ Establish a process for evaluating and applying new platform features and capabilities on a regular cadence — modern SIEM vendors ship new capabilities frequently.
- ☐ Plan for periodic re-assessment of your data routing strategy as ingestion volumes grow and new data sources are added — cost optimization is an ongoing discipline, not a one-time exercise.

A modern SIEM is a living system that requires ongoing investment in tuning, maintenance, and evolution.



QUICK REFERENCE

Migration Checklist at a Glance

Stage	Key Actions
1. Know Your Why	Document pain points. Establish success metrics and baseline security posture before touching anything.
2. Align the Org	Reconcile reason to buy vs. reason to use. Build RACI. Map data owners.
3. Inventory Everything	Audit all data sources, rules, dashboards. Retire what you aren't using. Understand "why" you are using them.
4. Reject Lift and Shift	Plan for full rewrites of rules and parsers. Rebuild, don't replicate.
5. Design the Architecture	Choose deployment model. Design data routing. Model TCO honestly.
6. Validate Rigorously	Define validation methodology. Ensure approvers are trained before sign-off. Involve data owners. Document sign-offs.
7. Close the Skills Gap	Assess team capabilities. Train before cutover. Engage services early.
8. Plan the Cutover	Define go/no-go criteria. Run parallel. Have a rollback plan.
9. Maintain and Measure	Post-migration posture assessment. Ongoing tuning and health monitoring.

START WITH A SIEM HEALTH CHECK

Understand your current state before you migrate.



Data Collection Audit

Understand exactly what data is being collected and where gaps exist in your current environment.



Detection Coverage Review

Identify where detections are duplicated, weak, or unused across your current SIEM deployment.



Future-State Blueprint

Define what a future-state SIEM should look like for your organization's specific needs and threat landscape.

Contact UltraViolet to get started with a SIEM Health Check.

ABOUT ULTRAVIOLET



UltraViolet Cyber is a leading platform enabled unified security operations company providing a comprehensive suite of security operations solutions. Founded and operated by security practitioners with decades of experience, the UltraViolet Cyber security-as-code platform combines technology innovation and human expertise to make advanced real time cybersecurity accessible for all organizations by eliminating risks of separate red and blue teams. By creating continuously optimized identification, detection and resilience from today's dynamic threat landscape, UltraViolet Cyber provides both managed and custom-tailored unified security operations solutions to the Fortune 500, Federal Government, and Commercial clients. UltraViolet Cyber is headquartered in McLean, Virginia with global offices across the U.S. and in India.