SIEM MIGRATION SERVICES

Modernize your SIEM without losing detection.

Migrating logs is easy. Preserving security outcomes is not.

SIEM migrations are often driven by cost, aging platforms, or the need for modern analytics. In complex environments, even well-planned transitions can introduce risk when detections behave differently, alert volume increases, or visibility gaps appear during and after cutover.

UltraViolet Cyber provides end-to-end SIEM Migration services for organizations operating in complex, regulated environments. Our approach is designed to maintain visibility throughout the transition, improve detection quality, reduce alert noise, and support long-term operational efficiency. Each engagement delivers a SIEM platform that provides high value, is easily supportable, maintainable, and aligned to how security teams actually operate.

SIEM MIGRATION SERVICES

Each engagement is led by detection engineers and SIEM practitioners with experience operating at enterprise scale across legacy and modern platforms.

HOW WE MIGRATE SIEMS

Our methodology is proven in complex, deadline-driven environments where maintaining detection coverage during migration is critical.

1. **Assess Current Environment**
   Perform a comprehensive discovery of the existing SIEM, validating data sources, ingestion methods, dashboards, alerts, and operational integrations.
2. **Planning & Scope Validation**
   Align stakeholders, document security and compliance requirements, and define the migration roadmap, milestones, and cutover priorities.
3. **Architecture Review & Parallel Log Shipping**
   Evaluate the current architecture, design the target SIEM environment, and establish parallel ingestion to verify data integrity and coverage.
4. **Content Migration & AI Optimization**
   Deploy the platform, migrate and enhance detection rules, and apply AI-driven analytics to improve signal quality and reduce noise.
5. **Validation & Decommissioning**
   Conduct structured testing and stakeholder validation to ensure operational readiness before retiring legacy infrastructure.
6. **Maintenance & Sustainability**
   Provide training, documentation, and runbooks to ensure teams can operate, tune, and sustain the SIEM long after migration.

What You'll Get

Every SIEM Migration engagement delivers:

- Project governance, structured milestones, and ongoing status reporting
- SIEM architecture and log collection strategy documentation
- Health assessment of current detections, dashboards, and content
- Requirements gathering and development of new industry and company-aligned detection use cases
- Inventory and validation of data sources and logging coverage
- Detection engineering migration, testing, and optimization
- End-to-end validation of searches, dashboards, and reporting performance
- Data migration and retention strategy recommendations
- Transition guidance for ongoing operations, runbooks, and managed services

WHY ULTRAVIOLET CYBER

- ☑ **Built for Operations, Not Just Migration**
  Our work is led by highly certified practitioners who build and run SIEMs daily. Migration success is measured by post-cutover performance, not project completion.
- ☑ **Detection-First Execution**
  We focus on detection quality, alert relevance, and response readiness throughout the engagement.
- ☑ **Proven at Scale**
  UltraViolet has executed large-scale SIEM migrations involving hundreds of dashboards, thousands of detection panels, and immovable business deadlines.
- ☑ **Vendor-Agnostic Expertise**
  We support legacy and modern SIEM platforms without bias, enabling customers to choose what fits their environment and strategy.
- ☑ **Part of a unified security model**
  SIEM Migration connects directly to UltraViolet's broader services, including detection engineering, managed SOC, and dedicated defense, enabling long-term sustainability

REAL-WORLD RESULTS

Customer: Global Fintech
Industry: Financial Services
Location: North America

Goals:

- ➔ Reduce SIEM-related licensing and infrastructure costs
- ➔ Centralize alerting and response workflows across the enterprise
- ➔ Streamline and optimize legacy content for performance and clarity
- ➔ Support cross-functional teams with a modern, scalable analytics

> **"I am embracing the singularity, AI, purple, and everything that goes with that. You're really taking us to the next level in terms of a modern SIEM."**
>
> **CISO**
> Fortune 500 Fintech Provider

Key Outcomes:

- ☑ Reduced SIEM-related licensing and infrastructure costs
- ☑ Improved detection performance and platform responsiveness
- ☑ Consolidated security operations into a unified, scalable ecosystem
- ☑ Rebuilt 4,000+ saved searches, alerts, and dashboards for clarity and speed
- ☑ Eliminated legacy inefficiencies and redundant content
- ☑ Equipped cross-functional teams with targeted training and enablement
- ☑ Maintained full operational continuity throughout migration

START WITH A SIEM HEALTH CHECK

Understand what data is being collected, where detections are duplicated, weak, or unused, and what a future-state SIEM should look like. **Contact UltraViolet Cyber to schedule a SIEM Health Check and migration readiness review.**

Continuously Assess. Consistently Defend.

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

443.351.7630 / info@uvcyber.com / UltraViolet Cyber / @uv_cyber