vijilan
IT Security: Enabled

ENTERPRISE SIEM MIGRATION PROGRAM

A structured 7-step framework for migrating off legacy SIEMs without losing visibility or breaking detections

MOVE FROM LEGACY TO MODERN

Splunk · ArcSight · QRadar · Rapid7 InsightIDR → CrowdStrike Falcon LogScale & Next-Gen SIEM

OUR MIGRATION APPROACH

Two core principles guide every SIEM migration we execute

1

No Visibility Loss

Parallel run validates coverage before cutover. Detection quality improves during migration, not after.

2

No Big Bang Cutover

Controlled, phased waves by source criticality. Rollback options at every stage. Proof before commitment.

THE 7-STEP MIGRATION FRAMEWORK

STEP 01 Discovery & Inventory · STEP 02 Pipeline Design · STEP 03 SIEM Foundation · STEP 04 Ingest in Waves · STEP 05 Detection Migration · STEP 06 Parallel Run · STEP 07 Cutover

1 MIGRATION DISCOVERY & INVENTORY

GOAL

Establish the truth about what you ingest today, what you need tomorrow, and what you can safely drop.

WHAT VIJILAN DOES

- Log source inventory — current SIEM data map, sources, parsers, index/dataset layout, retention
- Use case mapping — what detections matter, what compliance requires, what leadership reports need
- Volume and cost baseline — ingest per source, noisy sources, high-value sources
- Data pipeline assessment — where logs originate, where they route, where they fail

DELIVERABLES

- Current state ingest map
- Coverage heat map by domain (endpoint, identity, network, cloud, SaaS)
- Priority use case list
- Migration plan with phased cutover order

2 TELEMETRY PIPELINE DESIGN

GOAL

Decouple telemetry from the legacy SIEM so you control data routing, shaping, and destinations.

WHAT VIJILAN DOES

- Select pipeline pattern — Cribl or Falcon Onum as the pipeline layer
- Design routing paths — dual destination support so legacy SIEM and new SIEM run in parallel
- Segmented routing — by source and criticality with controlled rollout to avoid data floods
- Define data shaping rules — normalize key fields, enrichment, noise reduction, masking for sensitive data

DELIVERABLES

- Pipeline architecture diagram
- Routing plan with source groups, phases, and rollback options
- Data shaping and normalization standard

3 STAND UP NEW SIEM FOUNDATION

GOAL

Make the destination operational before moving critical data.

WHAT VIJILAN DOES

- Deploy and configure CrowdStrike Falcon LogScale
- Configure access — roles, least privilege, audit visibility
- Establish naming standards — datasets and data taxonomy
- Set baseline operational dashboards
- Validate ingestion endpoints — initial source connectivity

DELIVERABLES

- Production-ready LogScale environment
- Access model and roles defined
- Baseline views and reporting framework

4 INGEST MIGRATION IN WAVES

GOAL

Move data in controlled stages with proof at each stage.

WAVE PLAN

WAVE 1: NON-CRITICAL, HIGH-SIGNAL Core identity logs, critical SaaS audit logs	**WAVE 2: HIGH-VOLUME OPERATIONAL** Server syslog, network device logs, cloud audit trails
WAVE 3: ENDPOINT & CORRELATION Endpoint telemetry, DNS, proxy, firewall, cloud control plane	**WAVE 4: LONG TAIL INTEGRATIONS** Niche apps, custom syslog, special compliance feeds

FOR EACH WAVE

- Route logs to both SIEMs during parallel run
- Validate completeness, parsing, normalization
- Validate search speed and usability
- Track ingestion health and data loss indicators

DELIVERABLES

- Wave-based cutover checklist
- Ingestion validation report per wave
- Source acceptance criteria sign-off

5 DETECTION TRANSLATION & MODERNIZATION

GOAL

Don't copy legacy noise into the new platform — rebuild what matters with higher fidelity.

VIJILAN DOES IT DIFFERENTLY

- Detection triage — keep, rebuild, retire
- Use case mapping — map rules to real threats and business risk
- Correlation redesign — build cross-domain correlation across identity, endpoint, cloud, network
- Noise reduction tuning — make detections environment-aware, not generic
- Severity and escalation model — define what is actionable and who owns response

DELIVERABLES

- Detection migration matrix
- Prioritized detection backlog
- New detection library with tuning plan
- Escalation and severity framework

6 PARALLEL RUN & PROOF PERIOD

GOAL

Prove the new SIEM can fully replace the legacy one before cutover.

WHAT VIJILAN DOES

- Run both platforms in parallel for a defined proof window
- Compare signal quality and detection coverage
- Validate SOC workflows, escalation, and reporting
- Confirm compliance evidence, retention, and audit needs
- Document gaps and close them before cutover

DELIVERABLES

- Parallel run scorecard
- Coverage gap remediation plan
- Cutover readiness sign-off

7 CUTOVER & DECOMMISSION

GOAL

Shut off legacy SIEM ingestion without losing visibility or breaking processes.

WHAT VIJILAN DOES

- Final routing switch — transition all data flow to new SIEM
- Confirm alerting and response workflows — validate end-to-end operational readiness
- Confirm reporting and compliance exports — ensure no gaps in required outputs
- Decommission plan for legacy SIEM — structured shutdown process
- Archive plan if required — for legal or compliance reasons

DELIVERABLES

- Cutover checklist
- Rollback plan
- Decommission and archive runbook

WHAT SETS VIJILAN APART

Parallel run validates coverage before cutover. Detection quality improves during migration, not after. Managed services keep ingestion, detections, investigations, and reporting continuously healthy.

READY TO MIGRATE WITHOUT LOSING VISIBILITY?

Vijilan migrates enterprises off Splunk, ArcSight, QRadar, and Rapid7 by decoupling telemetry from legacy platforms using Cribl or Falcon Onum, then onboarding, tuning, and operating next-gen SIEM in controlled waves.

LET'S DISCUSS YOUR MIGRATION

Schedule a Discovery Call

vijilan
IT Security: Enabled

www.vijilan.com · info@vijilan.com · +1 (954) 334-9988

AICPA SOC · ISO 27001 · A-LIGN