ENTERPRISE PRACTICE STANDARD

SIEM Modernization & TCO Architecture Blueprint

CrowdStrike Falcon Next-Gen SIEM Telemetry & Ingestion Sizing

PREPARED FOR:

FinTech Global

Date: October 29, 2026

1. Executive Modernization Overview

This Architecture Blueprint delivers an objective technical and financial evaluation for transitioning **FinTech Global** from legacy **Splunk Cloud** infrastructure to **CrowdStrike Falcon Next-Gen SIEM (LogScale)**.

Modern enterprise security operations are crippled by legacy SIEM cost spirals, where license bills scale punitively with uncompressed log ingestion while queries choke on bloated B-tree indices. Migrea guarantees a rapid, seamless modernization executing **100% inside your cloud tenant with Zero Customer Data Egress**.

DAILY INGEST	LEGACY STORAGE	LOGSCALE STORAGE	STORAGE SLASHED
650 GB/day	**296.5 TB**	**47.4 TB**	**249.1 TB**
237.2 TB/year raw throughput	1.25x with index overhead	~80% columnar compression	84% Total Reduction

2. Storage Compression & TCO Benchmark Matrix

Legacy SIEM architectures expand incoming events to build secondary search trees and index shards. In contrast, Falcon Next-Gen SIEM operates index-free, compressing raw telemetry by **80%** directly into cloud object storage buckets (Amazon S3, Azure Blob, Google Cloud Storage) while accelerating searches across petabytes to sub-second speeds.

Architectural Dimension	Legacy Splunk Cloud	CrowdStrike Falcon Next-Gen SIEM
Indexing & Ingest Engine	Pre-indexing B-Trees, forward index bloat (+25% to +50% overhead).	Index-free streaming grep with hardware-accelerated regex evaluation.
Storage Footprint (365 d)	296.5 TB required in hot/warm tiers.	47.4 TB in high-efficiency compressed object storage.
Search & Query Latency	35s to 90s+ for multi-terabyte retrospective investigations.	Sub-second streaming execution (< 0.9s across petabytes).
Storage Reduction	Baseline 0% (high disk expansion penalty).	**249.1 TB slashed (84% net reduction)**.
Estimated Annual TCO Savings	Ongoing index maintenance & runaway licensing fees.	**$294,000+ Estimated Net Annual Savings**.

The Migrea Dual-Run & SecOps Parity Guarantee

We safeguard operational continuity with a contractually bound **30-Day Dual Ingestion Run SLA**. Detection parity is rigorously proven via **Atomic Detection Parity Testing (Red-Team / Purple-Team Event Replay), Event**

Count Reconciliation (less than 0.01% variance), and CrowdStrike Parsing Standard (CPS / OCSF) Schema Validation, ensuring zero visibility blind spots before decommissioning legacy infrastructure.

3. Detection Modernization: Legacy Query vs. Falcon CQL

Migrea translates active correlation searches into native, MITRE ATT&CK-aligned CrowdStrike Query Language (CQL). Below is a verified translation benchmark for Obfuscated Process Execution (**T1059.001**):

LEGACY: Legacy Splunk Cloud Query

Legacy Query Syntax

```
index=windows
sourcetype=XmlWinEventLog:Microsoft-Windows-
Sysmon/Operational EventCode=1
| search CommandLine="* -enc *" OR CommandLine="*
-encodedcommand *"
| stats count min(_time) as firstTime max(_time)
as lastTime by host, user, CommandLine,
ParentCommandLine
| where count > 0
```

Forces expensive unindexed disk scans and distributed map-reduce shuffle.

ENGINEERED: Falcon LogScale CQL

Falcon Next-Gen Streaming CQL

```
#event_simpleName=ProcessRollup2
event_platform=Win
|            ImageFileName=/\\powershell(\.exe|
_ise\.exe)$/i
|       CommandLine=/.*(\s+-(enc|encodedcommand|
e)\s+[A-Za-z0-9+\/=]{20,}).*/i
|    groupBy([aid,    ComputerName,    UserName,
ParentBaseFileName, CommandLine],
           function=([count(as=executionCount),
min(@timestamp, as=firstSeen), max(@timestamp,
as=lastSeen)]))
|        select([ComputerName,        UserName,
executionCount, CommandLine, ParentBaseFileName,
firstSeen, lastSeen])
```

Sub-second evaluation via streaming tag #event_simpleName with 0% parse penalty.

4. Recommended Modernization Pathway

Based on the modeled throughput of **650 GB/day** and existing telemetry topology, Migrea recommends the following turnkey implementation package:

RECOMMENDED PACKAGE

Tier 2: Hybrid Cutover (\$38,500 USD)

Fixed Scope â€¢ Guaranteed Milestones â€¢ 100% In-Tenant Engineering â€¢ 30-Day Warranty

Core Implementation Deliverables:

- **1 Connector = 1 Data Source Standard:** Native CrowdStrike Marketplace connectors (M365, AWS Foundation, Palo Alto) count as 1 single data source regardless of sub-feeds.
- **Strictly One-Time Turnkey Delivery:** Zero 24/7 Managed SOC or MDR lock-in (**“Build, Validate, Transfer Keys”**). Client retains 100% operational ownership.

- **In-Tenant Data Ingestion:** Onboard active data feeds directly into Falcon unified schemas (CPS/OCSF) with pre-ingest noise suppression in Falcon Onum / Cribl Stream.
- **Rule Translation & Hardening:** Rewrite and validate legacy correlation rules to LogScale CQL with verified MITRE mapping and 20,000 groupBy() cardinality tuning.
- **Falcon Fusion SOAR Automation:** Deploy turnkey response playbooks (Endpoint Isolation, Entra ID / Okta session revocation, and ServiceNow/Jira ticket synchronization).
- **Cutover Parity Protocol:** Atomic detection replay, event count reconciliation, and formal sign-off triggering the 30-day warranty certificate.
- **30-Day Post-Cutover Logic Warranty:** Continuous query tuning and schema drift mitigation at zero extra fee.
- **Optional One-Time Engineering Sprints:** $5,000 1-Week CQL Audit Sprint & $7,500 2-Week Telemetry, Cribl & Falcon Onum Pipeline Sprint (zero retainers).

5. Security & Governance Commitments

ZERO DATA EGRESS

100% In-Tenant Access

Engineers connect via client-managed IAM with temporary least privilege. Zero telemetry ever exits your boundary.

CONTRACTUAL SLA

30-Day Dual Run Guarantee

Bound parallel run window eliminates dual-licensing traps and ensures zero operational disruption.

BILINGUAL DESK

Native EN / ES Delivery

Senior security architects fluent in English and Spanish for seamless LATAM & global collaboration.

AUTHORIZED SIGNATURES & EXECUTION

FOR CLIENT:

FinTech Global

Authorized Signature

Title: CISO / VP of Information Security

Date:

FOR SERVICE PROVIDER:

Migrea Telemetry Engineering Desk

Authorized Signature

Date: