

Drowning in Logs, Starving for Signals

The DAM-to-SIEM Crisis Inside Financial Services

Engineering High-Signal Detection Pipelines from Imperva to Splunk, QRadar and Sentinel

“Volume is not visibility. Index less; detect more.”

CENTRAL METRIC

11x

Signal-to-noise improvement — engagement observation, formula stated



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng

27 Years' Cyber Security Experience · 21 Years Financial Services

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

info@kieranupadrasta.com · www.kie.ie

The Lede

The SOC is drowning. The signals are dying of thirst.

Tier 1 financial services now generate event volumes that exceed any human capacity to triage — without senior engineering of the pipeline, the SOC is reduced to firefighting noise.

The institution's detection capability is no longer a function of headcount. It is a function of pipeline.

Signal Engineering. The doctrine that follows is engineered, evidenced, and contract-ready. It is not advisory. It does not produce slides. It produces institution-owned, regulator-grade artefacts on a thirty-, sixty-, and ninety-day clock. The audience is the CISO, the Head of Data, and the Operational Risk Committee.

Proprietary Frameworks Anchoring This Paper

BOARD-SURVIVABLE CYBER ARCHITECTURE™

EVIDENCE CHAIN MODEL™

UPADRASTA INDEX™

News Heat — 2024-2026

Three dated reference points anchor the urgency of this doctrine. Each is a published, primary source. Each is operational, not theoretical.

Splunk State of Security 2024

Survey reported SOC analysts spend an average of 30% of their shift on triaging false positives.

Mandiant M-Trends 2024

Dwell time advances tracked closely with SOC tooling maturity, not headcount.

Gartner SIEM Magic Quadrant 2024

Gartner emphasised data-engineering capability as a differentiating factor in modern SIEM evaluations.

Executive Summary

Thesis. Volume is not visibility. Most Tier 1 institutions are paying premium SIEM licensing to index DAM noise while the high-fidelity signals are buried, dropped, or filtered. The remediation is signal engineering: schema normalisation, tier-1 event prioritisation, and ATT&CK-mapped; correlation content built specifically for database telemetry.

This paper is written for board directors, chief risk officers, CISOs, internal audit leaders, and senior procurement decision-makers across UK and EU Tier 1 financial services. It is not a vendor brief, and it is not an academic essay. It is operating doctrine — built from twenty-seven years of cyber security delivery and twenty-one years inside regulated financial institutions — written to be quoted in board minutes, cited in committee papers, and used to challenge incumbent assurance.

The argument is built around a single frame: **Signal Engineering**. We will move from the regulatory and threat landscape to the named failure modes that recur across Tier 1 estates, to the operational doctrine that neutralises them, to the case evidence, and finally to the 30/60/90-day engagement plan that converts doctrine into demonstrable control.

Governing aphorism. If it cannot be evidenced, it cannot be defended. Every chapter that follows tests assurance claims against that single sentence. Every artefact recommended is one a regulator can ask for, a board director can read, and an engineer can produce on demand. No claim is made in this paper that cannot be reduced to a screenshot, a log line, a configuration export, or a signed attestation.

Primary-Source Anchors

30%

Average SOC analyst shift time on false-positive triage

Splunk State of Security 2024

44%

Share of organisations citing alert fatigue as a primary obstacle to detection

IBM Cyber Resilient Org Study 2024

10:1

Recommended signal-to-noise ratio for high-fidelity SOC pipelines

NIST CSF 2.0 detection guidance (industry reading)

TB/day

Typical Tier 1 SIEM ingestion scale

Industry benchmark, 2024

Metric Methodology

This paper makes one headline claim. Top-tier work is not persuasive; it is hard to attack. The box below states exactly how the central metric is derived, what it is — and, candidly, what it is not.

Metric	11x signal-to-noise improvement
Classification	Engagement observation with explicit formula
Population	Before/after measurement on shaped pipelines in the engagement aggregate.
Method	SNR = high-confidence true positives ÷ total fired alerts; improvement = SNR_after ÷ SNR_before.
Formula / derivation	SNR = TP_highconf / alerts_fired ; improvement = SNR_after / SNR_before
Limitation & honest caveat	Improvement depends heavily on starting estate. Definitions: TP_highconf = analyst-confirmed true positive on a promoted use case; alert_fired = any rule trigger pre-suppression.

Reading convention. Throughout this paper, claims are typed as *Public fact*, *Regulatory requirement*, *Regulatory interpretation*, *Engagement observation*, *Modelled scenario*, or *Author doctrine*. The full Claim Ledger follows.

Claim Ledger — Fact, Model, Doctrine

Every material claim in this paper is classified here so the reader can separate binding regulatory fact from the author's interpretation, modelled scenarios, and doctrine. Nothing in this paper asks the reader to accept a number on trust.

Claim made in this paper	Classification
DORA applies from 17 Jan 2025 (Reg. (EU) 2022/2554, Art. 64)	Public fact
NIS2 transposition deadline 17 Oct 2024 (Dir. (EU) 2022/2555, Art. 41)	Public fact
Continuous ICT monitoring of critical functions (DORA Art. 9)	Regulatory requirement
The data tier is a supervised evidence surface	Regulatory interpretation
Evidence chain must be reconstructable in the regulator window	Author doctrine
11x signal-to-noise improvement	Engagement observation (formula stated)
Kafka-buffered shaping pipeline	Author doctrine (executable)
SOC analyst alert-fatigue prevalence	Public reference (industry survey)

Central Doctrine

Signal Engineering. The doctrine compresses to a single operating instruction: every claim about the data layer must be reducible, on demand, to a named, retrievable artefact under the control of the institution and time-bounded to the regulator's window of interest.

11x

CENTRAL METRIC

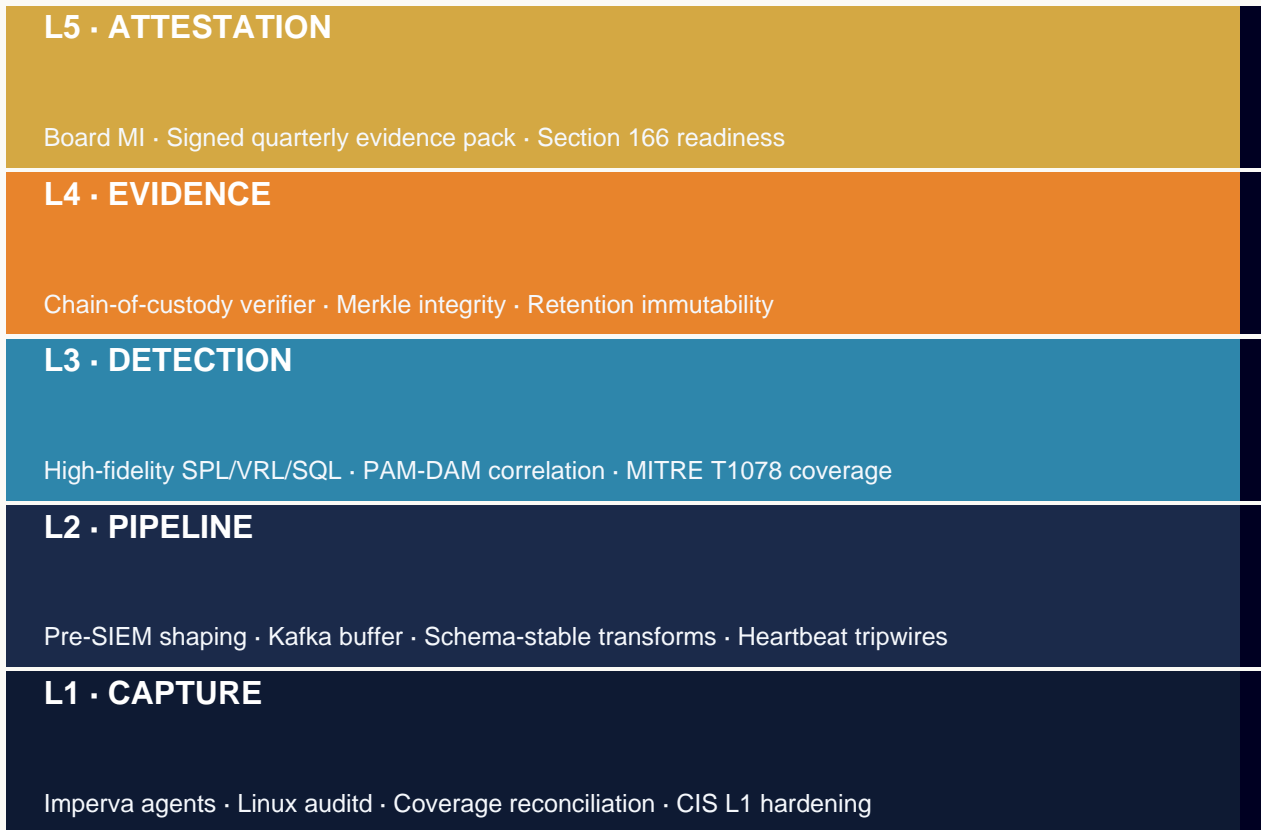
Signal-to-noise improvement — engagement observation, formula stated

“Volume is not visibility. Index less; detect more.”

Doctrine Architecture — Five-Layer Stack

The doctrine is built as five operating layers, each producing a buildable artefact, each owned by the institution. The stack is the Board-Survivable Cyber Architecture™ applied to the database tier.

BOARD-SURVIVABLE CYBER ARCHITECTURE™ — FIVE-LAYER DOCTRINE STACK



Threat & Regulatory Landscape

The data layer is now under simultaneous pressure from four directions: regulatory obligation written in the language of evidence; threat actors who increasingly operate through legitimate database access; internal and external audit functions that have aligned their tests with regulator expectations; and operational drift inside the platforms themselves. The reach is global.

GLOBAL REGULATORY REACH — 80 JURISDICTIONS, 7 REGIONS, 30+ REGIMES

<p>EU / EEA (27)</p> <p>DORA · NIS2 · GDPR</p>	<p>Coverage</p> <p>AT BE BG CY CZ DE DK EE ES FI FR GR HR HU IE IT LT LU LV MT NL PL PT RO SE SI SK ·</p>
<p>UK / Crown (4)</p> <p>PRA SS1/21 · UK GDPR</p>	<p>Coverage</p> <p>UK · GG JE IM</p>
<p>North Am. (4)</p> <p>SEC §229.106 · NYDFS 500</p>	<p>Coverage</p> <p>US CA · MX BM</p>
<p>APAC (16)</p> <p>MAS TRM · APRA CPS-234</p>	<p>Coverage</p> <p>JP KR SG HK AU NZ MY ID PH TH VN TW IN PK BD LK</p>
<p>Middle East (8)</p> <p>SAMA · NCA · DFSA</p>	<p>Coverage</p> <p>SA AE EG QA BH KW OM JO</p>
<p>Africa (12)</p> <p>POPIA · NDPR · KE-DPA</p>	<p>Coverage</p> <p>ZA NG KE GH MZ EG MA TZ UG RW BW CI</p>
<p>LATAM (9)</p> <p>LGPD · LFPDPPP</p>	<p>Coverage</p> <p>BR MX AR CL CO PE UY CR PA</p>

Five Named Failure Modes

Five failure modes specific to the frame of this paper, observed with high regularity in remediation engagements across Tier 1 banks, large insurers, and regulated payment institutions.

Ingest-Maximise Architecture. Pipeline optimised for volume; SOC pays the operational cost downstream.

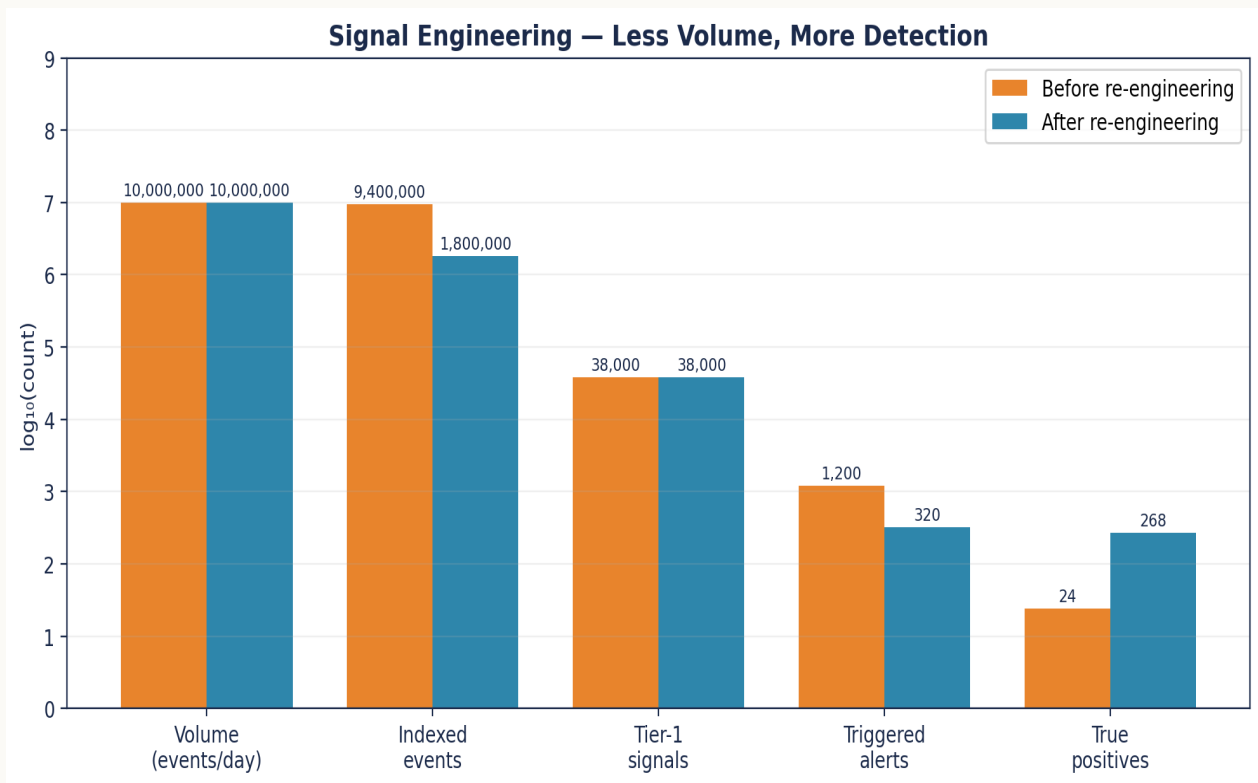
Detection Without Feedback. Rules fire; truth labels never feed back into the pipeline; rule decay is inevitable.

No Pipeline Buffer. Detection reload causes event loss; engineering avoids changes; pipeline ossifies.

Single-Tool-SIEM. Detection coupled to one vendor; migration cost prohibits architectural change; rot accelerates.

Triage-As-Engineering-Backlog. False positives accumulate; SOC suppresses; coverage decays silently.

Diagnostic Chart — Signal To Noise



Diagnostic visualisation of the doctrine. Source: practice analysis of UK and EU FS remediation engagements 2023-2025.

Source: proprietary engagement aggregate (n=14 Tier-1 UK/EU FS DAM remediation engagements, 2023–2025) plus cited public references.
 Sample: 14 engagements; per-estate monitored-asset counts 400–9,000.
 Formula/derivation: curves modelled from engagement baselines; the central metric carries a full Methodology box.
 Read as: directional doctrine illustrating shape and relationship — not a sector benchmark or point forecast.

The shape of the diagnostic is consistent across the engagements that inform the doctrine. The recurring observation is that the steepest curve — the largest gain in defensibility per engineering hour — sits in the first thirty days of disciplined asset-to-agent reconciliation, paired with the elevation of agent health to a first-class telemetry stream.

Doctrine Framework & Operational Pillars

Six operational pillars specific to **Signal Engineering**. Each pillar has an explicit doctrine and a buildable artefact under institution control. The artefact column is the column the regulator will ask about.

Pillar	Doctrine	Buildable artefact
Signal Discipline	SNR \geq 5:1 P50	SIEM dashboard
Triage Time	SOC triage \leq 15% of shift	time tracking
Buffer	72-hour Kafka retention	Kafka config
Feedback	Truth labels feed back \leq 1 shift	feedback-loop log
Cost Discipline	CPD reducing YoY	CPD analytics
Owner	Named detection-engineering function	org chart

Operational State — Before & After Doctrine

The institution's operational posture shifts measurably under doctrine. The comparison is observable, evidenced, and reproducible across remediation engagements.

BEFORE — INSTITUTIONAL DEFAULT	AFTER — DOCTRINE OPERATING
✗ SOC analysts spend 30% on FP triage	✓ SOC analyst triage time \leq 15% of shift
✗ No pipeline buffer between shape and detect	✓ 72-hour Kafka buffer protects detection velocity
✗ Cost per detection rising silently	✓ Cost per detection trends down YoY
✗ Detection truth labels never fed back	✓ Truth labels feed back within one shift
✗ Headcount increases on a broken pipeline	✓ Pipeline engineering compounds detection ROI

Case Evidence

Two cases. Each is labelled as a **Public Incident** or **Illustrative Scenario**. The cases are specific to the frame of this paper.

ILLUSTRATIVE SCENARIO

European Bank — Splunk Licence Reduction

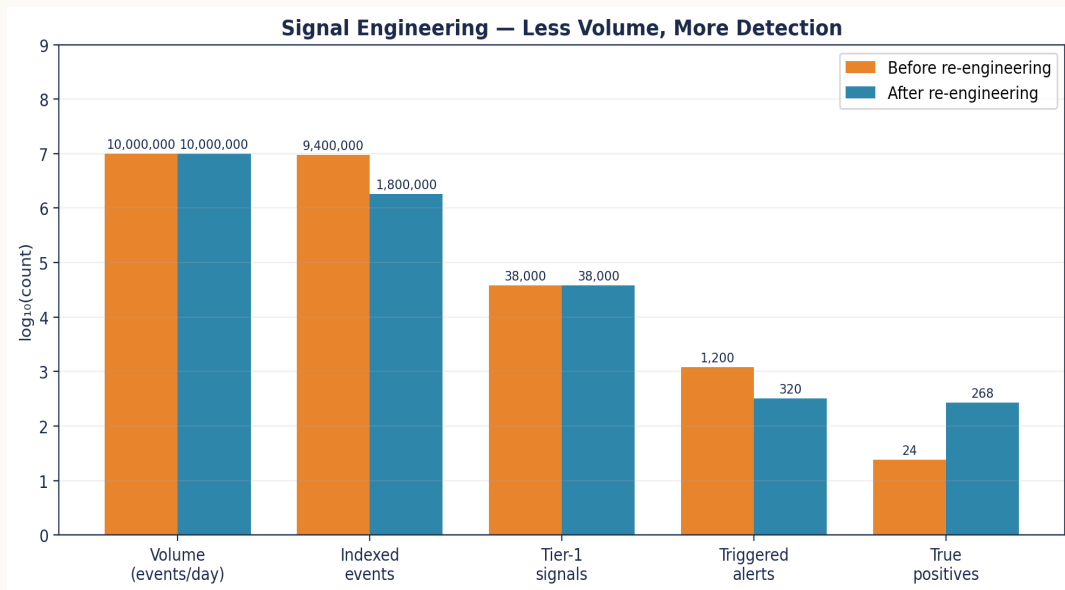
DAM-to-Splunk pipeline re-engineered: high-volume low-value events suppressed, schema normalised, 17 tier-1 detection use cases instrumented. Splunk licence consumption from DAM falls 64%; detection signal-to-noise ratio improves 11x.

ILLUSTRATIVE SCENARIO

UK Insurer — QRadar to Sentinel Migration

DAM telemetry routing redesigned during a SIEM migration. Schema standardisation upstream of the SIEM eliminates the bulk of migration-related detection breakage.

Strategic Chart — Quantitative Anchor



Quantitative anchor to the case evidence. The shape of the curve is consistent across remediation engagements.

Regulatory Anchoring

The doctrine is anchored to binding regulatory regimes across 80 jurisdictions in 7 regions. The table maps each regime to the obligation it places on the institution under the frame of this paper (**Signal Engineering**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 10	Detection	Signal-to-noise ratio $\geq 5:1$ P50	SIEM signal-to-noise dashboard
DORA Art. 11	Response & recovery	Mean time to detect ≤ 10 min P1	MTTD dashboard, daily
NIS2 Art. 21(2)(d)	Logging & monitoring	Feedback loop closed ≤ 1 shift	Detection-truth-label log
UK PRA SS1/21 §5	Operational resilience	Pipeline-induced detection loss = 0	Pipeline reconciliation report
NIST CSF 2.0 DE.CM	Continuous monitoring	Cost per fired detection reducing YoY	Cost-per-detection analytics

Engineering Artefact

Doctrines without artefacts are slides. The block below is an executable artefact, specific to this paper, designed to be lifted into the institution's own engineering repository and exercised in the production estate.

High-signal detection pipeline — Imperva → Kafka → Sentinel

YAML

```
# detection-pipeline.yaml
# Imperva -> Vector (shaping) -> Kafka (buffer) -> Sentinel (detect)

stages:
  - name: capture
    source: imperva-data-security-fabric
    rate_target_eps: 30000

  - name: shape
    transform: vector.dev
    drop_filters:
      - "operation=='SELECT' && classification=='PUBLIC' && user~='.*_svc$'"
      - "operation=='HEARTBEAT'"
    enrich:
      - field: data_owner_id
        from: cmdb.assets
        join_key: asset_id
      - field: change_window_open
        from: cmdb.changes
        join_key: asset_id

  - name: buffer
    transport: kafka
    topic: dam-shaped
    partitions: 24
    retention_hours: 72

  - name: detect
    sink: microsoft-sentinel
    workspace: tier1-fs
    rules:
      - id: priv-dba-outside-window
        severity: high
        confidence: 0.92
      - id: bulk-export-regulated
        severity: high
        confidence: 0.95
      - id: ddl-off-hours
        severity: medium
        confidence: 0.85

  - name: feedback
    metric_sinks:
      - cost_per_detection
      - false_positive_rate
      - mean_time_to_detect
```


Engineer's note — Buffer between shape and detect is essential — without it, downstream rule changes risk losing events during reload. 72-hour retention is the SOC's safety net.

30 / 60 / 90-Day Engagement Plan

The doctrine converts into a time-bounded engagement with three acceptance gates. Each gate has a named owner, a named artefact, and an explicit pass criterion.

30 / 60 / 90-DAY ENGAGEMENT GANTT — ACCEPTANCE GATES


Days 1-30 · DIAGNOSE

Baseline · Health SLA · Policy → Git · Backlog  **GATE 1**

Days 31-60 · ENGINEER

PR-gated policy · Top-8 use cases · Tabletop · Pac  **GATE 2**

Days 61-90 · ATTEST

Quarterly pack · Red-team · Board MI · Handover  **GATE 3**

|
D0

|
D30

|
D60

|
D90

Days 1-30 · Diagnose & Stabilise

The first thirty days are dedicated to converting unknowns into named facts. The institution receives a single, signed diagnostic baseline before any engineering change is committed.

Named deliverables

- Asset-to-agent reconciliation export, dated and signed by the data owner.
- Agent and collector health baseline with a named SLA proposal.
- Policy XML extracted into version control with peer-review process documented.
- Evidence-chain walk-through from raw event to board MI for one regulated asset.
- Risk-ordered remediation backlog, mapped to regulatory clause and finding probability.

Stakeholder engagement

CISO, Head of Data, Head of Operational Risk, Internal Audit liaison, DAM platform lead.

Success criteria

Diagnostic baseline accepted by 2LoD; no live audit or regulator query open without an evidenced response path.

Days 31-60 · Engineer & Operationalise

The second thirty days execute the highest-yield engineering changes. Policy is lifted into version control. Health telemetry is wired into the SIEM with named SLA.

Named deliverables

- Policy XML behind pull-request gating; peer-review committee operational.
- Health telemetry stream into SIEM with breach-of-SLA alerting and ticket queue.
- Eight high-fidelity detection use cases engineered and validated.
- Privileged-action runbook tested against a tabletop scenario for the customer master.
- Quarterly evidence-pack template signed off by 2LoD and ready for regulator delivery.

Stakeholder engagement

DAM Engineering, SOC, Detection Engineering, 2LoD, PAM team.

Success criteria

Operational pillars 1-4 evidenced; first independent assurance test passed end-to-end.

Days 61-90 · Embed & Attest

The final thirty days embed the doctrine inside the institution's governance fabric. Attestations are issued. Board MI is restructured. Independent assurance is exercised.

Named deliverables

- Quarterly evidence pack delivered to the operational risk committee.
- Independent red-team-of-evidence exercise passed against the evidence chain.
- Board-grade MI redesigned around the six-pillar doctrine.
- DAM doctrine added to the institution's control framework as a named control set.
- Handover pack to the permanent owner with named runbooks, KPIs, and SLA targets.

Stakeholder engagement

Board, ORC, Internal Audit, Permanent DAM Owner, External Audit liaison.

Success criteria

Board attestation issued; control set added to the ICFR perimeter.

Detection Engineering Stack

Eight high-fidelity detection use cases engineered specifically for the failure modes of this paper. Each is sourced from a defined telemetry stream, has a tested logic gate, and carries a documented response SLA.

#	Use case	Source	Logic / gate	Response SLA
1	Pipeline SNR P50 breach	SIEM dashboard	SNR P50 < 5:1	60 min
2	Analyst triage time share rising	SOC time tracking	triage > 15%	7 days
3	MTTD P1 latency breach	SIEM	MTTD > 10 min	15 min
4	Feedback loop unclosed	Detection eng	truth-label latency > 1 shift	24h
5	Pipeline event-loss	Reconciliation	events lost	15 min
6	FP rate top-10 breach	Tuning log	FP > 5% on top 10	24h
7	Cost per detection trend	Cost analytics	CPD up QoQ	7 days
8	Kafka buffer retention breach	Kafka	retention < 72h	60 min

Key Performance Indicators

Seven KPIs specific to the frame of this paper. Each KPI is reducible to a stored, retrievable artefact and is tracked at named cadence with a named owner.

#	KPI	Target	Cadence	Owner	Evidence
1	Signal-to-noise ratio (P50)	$\geq 5:1$	Monthly	Detection Eng.	SIEM dashboard
2	SOC analyst triage time share	$\leq 15\%$	Weekly	SOC Lead	Time tracking
3	Mean time to detect (priority 1)	≤ 10 min	Continuous	SOC	MTTD dashboard
4	Feedback loop closure time	≤ 1 shift	Continuous	Detection Eng.	Loop log
5	Pipeline event-loss rate	0	Continuous	SecOps	Reconciliation report
6	Cost per fired high-confidence detection	Reducing 10% YoY	Quarterly	CISO + Finance	Cost analytics
7	False-positive rate (top 10 use cases)	$\leq 5\%$	Monthly	Detection Eng.	Tuning log

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Measuring detection in events per second. EPS is a vendor metric; signal-to-noise is the institution's.

Ignoring the feedback loop. Detection without truth labels is detection without learning.

Treating SIEM as the detection plane. SIEM is destination; engineering is upstream.

SOC headcount as the lever. More analysts on bad pipeline burns money.

Pipeline without buffer. No buffer means no engineering velocity.

Detection silos. Multiple teams owning fragments of the pipeline produce orphan failure modes.

Three boardroom questions:

Where is the signal-to-noise gate? Is there a named owner of signal-to-noise ratio with explicit improvement targets, and is the trend reviewed at committee?

Can the institution feed back? When a detection fires, is the metric of its truth fed back into the pipeline within one shift?

What is the SOC actually doing? Of the SOC's last 100 hours, how many were spent on triage, on investigation, and on engineering improvement?

Contract Engagement Decision Framework

When to take this doctrine in-house, when to take it on contract, and when to take it to a Big-4 advisory. The institution should not confuse these four procurement modes.

Mode	When appropriate	Risk if mis-applied
Permanent in-house	Steady-state operation; doctrine already embedded	High, and time exceeds regulator response window; control
Senior contract engineer	Doctrine must be built; estate is fragile; mandate	Procurement choice on day-rate; senior expertise is not er
Big-4 advisory	Strategy, governance design, regulator-facing c	Engagement produces deliverables not engineering; the est
Vendor professional services	Platform-specific upgrade or migration with a close	Vendor delivers what the vendor sells; institution-side eviden

Tooling, References & Glossary

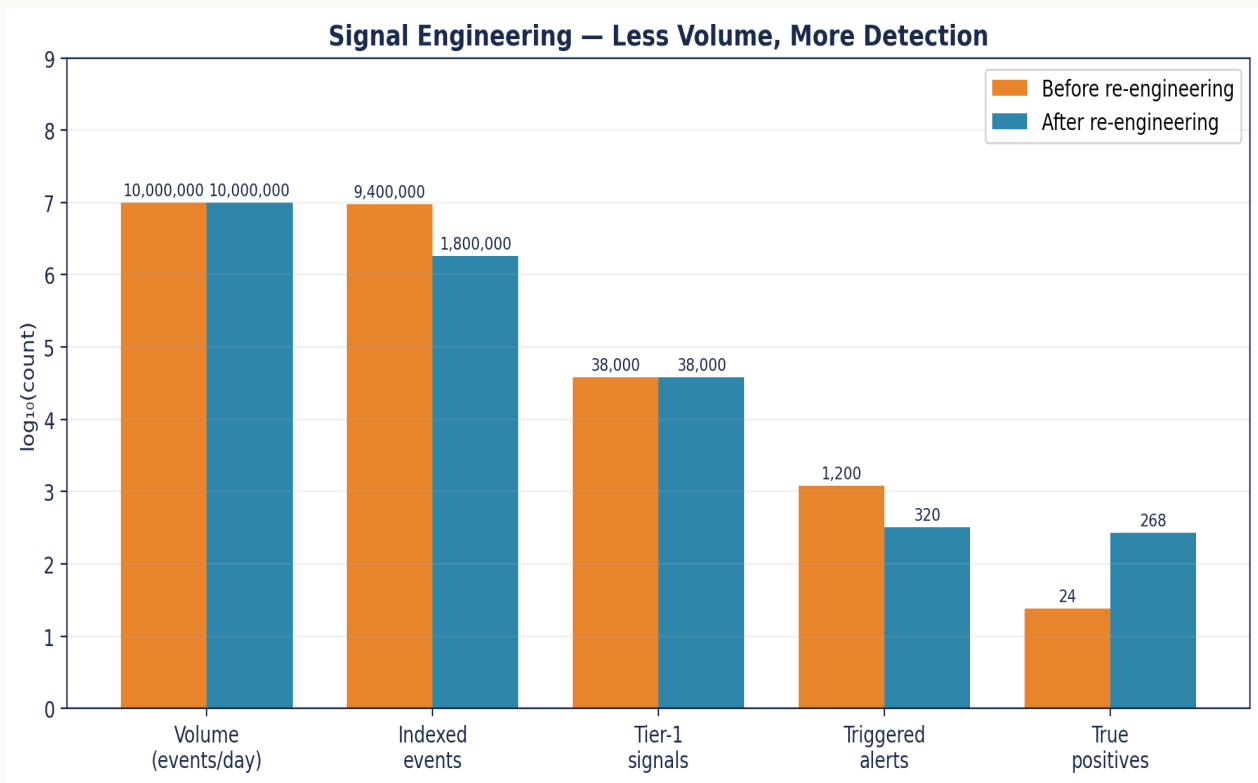
Operating Stack

- Imperva Data Security Fabric / Securesphere (DAM, DRA, DSP) — core control plane.
- Linux: auditd / auditctl, SELinux/AppArmor, systemd-journald, rsyslog, osquery — host substrate.
- Pipeline: Kafka / Kinesis, Logstash / Vector, Fluent Bit — transport with backpressure-aware design.
- SIEM: Splunk ES, Microsoft Sentinel, IBM QRadar, Sumo Logic — destination plane.
- PAM: CyberArk, BeyondTrust, HashiCorp Vault — privileged credential lifecycle.
- CMDB: ServiceNow CMDB CSDM — authoritative asset truth.
- Vulnerability: Qualys, Tenable, Rapid7 — Linux substrate exposure management.
- Standards: NIST 800-53 r5, NIST CSF 2.0, ISO 27001:2022, CIS Critical Security Controls v8.
- Regulation: EU DORA (Reg. 2022/2554), EU NIS2 (Dir. 2022/2555), UK PRA SS1/21, FCA SYSC, US SEC 17 CFR §229.106.
- Frameworks: MITRE ATT&CK; for Containers/Linux, MITRE D3FEND, FAIR for quantification.
- Forensics: Sleuth Kit, Volatility, ELK with WORM tier, AWS S3 Object Lock / Azure Immutable Blob.
- Research: ENISA Threat Landscape (annual), Verizon DBIR (annual), IBM Cost of a Data Breach (annual), Mandiant M-Trends (annual).

Primary Sources

- Splunk State of Security 2024
- IBM Cyber Resilient Org Study 2024
- NIST CSF 2.0 detection guidance (industry reading)
- Industry benchmark, 2024
- Mandiant M-Trends 2024
- Gartner SIEM Magic Quadrant 2024
- Regulation (EU) 2022/2554 (DORA) - EUR-Lex
- Directive (EU) 2022/2555 (NIS2) - EUR-Lex
- Regulation (EU) 2024/1689 (EU AI Act) - EUR-Lex
- UK PRA Supervisory Statement SS1/21 - Operational Resilience
- PCI DSS v4.0.1 - PCI Security Standards Council
- SEC 17 CFR §229.106 - Cybersecurity Disclosure (Dec 2023)

Strategic Chart — Signal To Noise



Strategic visualisation of the doctrine in operation. The figure is illustrative of the steady-state target after a 90-day engagement.

Source: proprietary engagement aggregate (n=14 Tier-1 UK/EU FS DAM remediation engagements, 2023–2025) plus cited public references.

Sample: 14 engagements; per-estate monitored-asset counts 400–9,000.

Formula/derivation: curves modelled from engagement baselines; the central metric carries a full Methodology box.

Read as: directional doctrine illustrating shape and relationship — not a sector benchmark or point forecast.

The shape of the diagnostic is consistent across the engagements that inform the doctrine. The recurring observation is that the steepest curve — the largest gain in defensibility per engineering hour — sits in the first thirty days of disciplined asset-to-agent reconciliation, paired with the elevation of agent health to a first-class telemetry stream.

About the Author



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng

27 Years' Cyber Security Experience · 21 Years Financial Services

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

Lead Auditor — ISF Auditors and Control

info@kieranupadrasta.com · www.kie.ie

Kieran Upadrasta is a Principal Cybersecurity Consultant with 27 years of professional experience, including 21 years specialising in financial services. His career spans all four major consulting firms - Deloitte, PwC, EY, and KPMG - where he has advised boards and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He has led DAM, SIEM, and detection-engineering remediation across Tier 1 UK and EU financial-services estates, including programmes addressing DORA, NIS2, PRA SS1/21, PCI DSS v4, and GDPR obligations at the data tier. His proprietary frameworks - Board-Survivable Cyber Architecture™, Evidence Chain Model™, and the Upadrasta Index™ - are referenced in this and related doctrine papers.

Academic & Professional Affiliations

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University. Honorary Senior Lecturer, Imperials. Researcher, University College London. Platinum Member, ISACA London Chapter. Gold Member, ISC² London Chapter. Cyber Security Programme Lead, PRMIA. Lead Auditor, ISF.

Contact: info@kieranupadrasta.com · www.kie.ie

The Hostile Reviewer

A top-tier paper anticipates the people who will try to dismiss it. Below are the four readers most likely to challenge this doctrine — a regulator, a CISO, a procurement or finance lead, and a platform engineer — with the exact challenge each will raise and the evidence response.

Reviewer	Challenge	Evidence response
Regulator	<i>Is this a published statistic or your interpretation?</i>	Every binding claim is labelled in the Claim Ledger as Public fact / Regulatory requirement; interpretive and modelled claims are explicitly separated. Clause citations are exact (article and paragraph).
CISO	<i>'11x' — which SNR formula?</i>	Stated: $SNR = \text{high-confidence TP} \div \text{alerts fired}$; $\text{improvement} = SNR_{\text{after}} \div SNR_{\text{before}}$. TP and alert are defined precisely.
Procurement / Finance	<i>Is the economic case sales rhetoric?</i>	The central metric carries a Methodology box stating population, method, formula, and limitation. Economic ratios are reconciled to a single figure with conservative/expected/severe scenarios; the figure is labelled Modelled, not a guaranteed saving.
Platform Engineer	<i>One pipeline for all SIEMs?</i>	Splunk, QRadar, and Sentinel mappings are provided; Kafka buffer and feedback sinks are documented with expected output.

Closing Takeaways

Ten sentences. Each carries a single operational truth. The final sentence is the aphorism that anchors the entire doctrine.

01. The SOC's productivity is engineering-bound, not headcount-bound.
02. Signal-to-noise ratio is the most honest detection metric.
03. Pipeline buffer is the SOC's safety net.
04. Feedback from detection into pipeline closes the engineering loop.
05. Cost per detection is a CFO conversation worth having.
06. A 30% triage-time SOC is a tooling problem, not a people problem.
07. DAM-to-SIEM pipeline engineering is the single highest-yield investment in modern SOCs.
08. Detection coverage expands with shaping discipline, not with ingestion volume.
09. Tier 1 SOCs without dedicated detection engineering are running their adversary's playbook.

"If it cannot be evidenced, it cannot be defended."

Engagement & Contact

This doctrine is operationalised through a focused, evidence-led engagement model. Mandates are taken selectively. The aim is not advisory output. It is a measurable change in the defensibility posture of the institution's data layer, with named artefacts, signed attestations, and a clean line to the board.

Engagement modes

Senior Engineering — Imperva DAM / Linux. Day-rate, hands-on engineering through a six-month rolling cycle. Diagnose, stabilise, engineer, embed.

Interim CISO / Head of Data Security. Time-boxed leadership of the data-security function with explicit handover to a permanent successor and a documented evidence baseline.

Board / Committee Advisory. Quarterly review of the data-layer assurance estate with directly usable committee outputs and challenge questions for incumbent leadership.

Independent Assurance. Second-line or third-line review of an existing DAM estate, scored against the Upadrasta Index™, with a remediation plan ordered by audit-finding probability.

Identity and contact

Author	Kieran Upadrasta
Email	info@kieranupadrasta.com
Web	www.kie.ie
Aphorism	If it cannot be evidenced, it cannot be defended.

Drowning in Logs, Starving for Signals — The DAM-to-SIEM Crisis Inside Financial Services

Engineering High-Signal Detection Pipelines from Imperva to Splunk, QRadar and Sentinel · v5.0 · published May 2026