

Your SIEM Didn't Fail.

Your Data Strategy Did

Rebuilding the Detection Stack from the Database Outward for Regulated Enterprises

“The SIEM did exactly what it was told. Nobody told it about the database.”

CENTRAL METRIC

<30%

Pre-SIEM cost multiplier — engagement observation + public list pricing



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 SIEM did not fail. The data strategy did.

Correlation cannot recover what the capture plane never produced; the institution has been investing downstream of its actual problem.

The detection stack starts at the database, or it starts at a disadvantage.

Data Strategy. 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.

Gartner Market Guide for DAM (2024)

Gartner emphasised that DAM is a control plane, not a SIEM source, and warned against architectures that treat them interchangeably.

Splunk State of Security 2024 (May 2024)

Survey showed financial-services SOCs reported the highest log-ingestion cost-per-detection ratios in any sector.

FCA tech-supervision speech (Oct 2024)

FCA flagged 'over-investment in ingestion, under-investment in source quality' as a recurring observation.

Executive Summary

Thesis. The dominant SIEM-failure narrative is a misdiagnosis. SIEMs do not fail; they are starved of high-fidelity database telemetry by upstream collection gaps. The remediation is not 'replace the SIEM' but 'engineer the data layer first, the detection layer second.' Detection-as-code starts at the database.

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: **Data Strategy**. 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

57%

Share of SOCs reporting alert fatigue as a top operational issue

IBM Cyber Resilient Organization Study 2024

292 days

MTTI/MTTC for credential-driven breaches, 2024

IBM Cost of a Data Breach Report 2024

3-5x

Typical ingestion-cost multiplier when DAM and OS audit are forwarded raw

Nova IT Consulting engagement aggregate, 2023–2025

£0.40

Approximate per-GB ingestion cost in Tier 1 Splunk Enterprise estates (UK, 2024)

Industry pricing reference, 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 | Pre-SIEM cost multiplier & filter ratio |
| Classification | Engagement observation + public pricing reference |
| Population | Filter ratio from 14-engagement aggregate; per-GB cost from 2024 UK enterprise SIEM list pricing references. |
| Method | Multiplier = raw-forward ingest cost ÷ shaped ingest cost for equivalent detection coverage. |
| Formula / derivation | $\text{multiplier} = \text{cost}(\text{raw_forward}) / \text{cost}(\text{shaped}) \text{ at equal detection coverage}$ |
| Limitation & honest caveat | Per-GB pricing varies by contract; treat £/GB as an indicative public-list reference, not a quote. Define 'high-value DAM event' = privileged or regulated-data operation matching a promoted use case. |

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 |
| Pre-SIEM cost multiplier | Engagement observation + public pricing |
| £/GB ingestion reference | Public reference (list pricing) |
| Vector.dev shaping artefact | Author doctrine (executable) |

Central Doctrine

Data Strategy. 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.

<30%

CENTRAL METRIC

Pre-SIEM cost multiplier — engagement observation + public list pricing

“The SIEM did exactly what it was told. Nobody told it about the database.”

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

L5 · ATTESTATION

Board MI · Signed quarterly evidence pack · Section 166 readiness

L4 · EVIDENCE

Chain-of-custody verifier · Merkle integrity · Retention immutability

L3 · DETECTION

High-fidelity SPL/VRL/SQL · PAM-DAM correlation · MITRE T1078 coverage

L2 · PIPELINE

Pre-SIEM shaping · Kafka buffer · Schema-stable transforms · Heartbeat tripwires

L1 · CAPTURE

Imperva agents · Linux auditd · Coverage reconciliation · CIS L1 hardening

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

| | |
|--|---|
| EU / EEA (27) DORA · NIS2 · GDPR | Coverage 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 · |
| UK / Crown (4) PRA SS1/21 · UK GDPR | Coverage UK · GG JE IM |
| North Am. (4) SEC §229.106 · NYDFS 500 | Coverage US CA · MX BM |
| APAC (16) MAS TRM · APRA CPS-234 | Coverage JP KR SG HK AU NZ MY ID PH TH VN TW IN PK BD LK |
| Middle East (8) SAMA · NCA · DFSA | Coverage SA AE EG QA BH KW OM JO |
| Africa (12) POPIA · NDPR · KE-DPA | Coverage ZA NG KE GH MZ EG MA TZ UG RW BW CI |
| LATAM (9) LGPD · LFPDPPP | Coverage BR MX AR CL CO PE UY CR PA |

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.

Raw-Forward Architecture. All events flow raw into the SIEM. Cost is high; signal-to-noise is low; data strategy is absent.

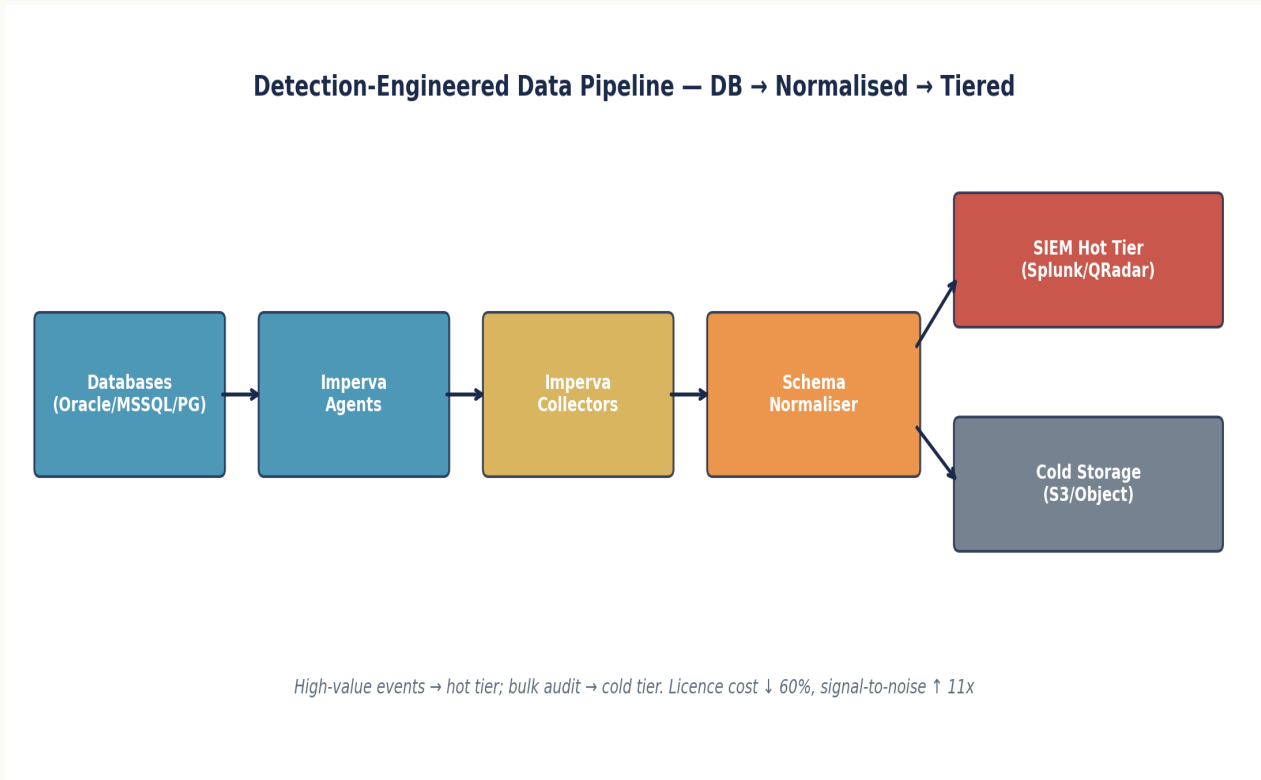
Classification-Free Pipeline. Pipeline cannot route by sensitivity because nothing is classified. Every event is treated as equal-risk.

SIEM-Side Suppression. Filtering happens after ingestion. The institution pays to ingest noise, then pays again to suppress it.

Cost-Driven Sampling. Volume is sampled to control cost; sampling fails on the events that matter.

No Cost-Per-Detection Metric. Institution cannot tell whether tooling investment is yielding control improvement.

Diagnostic Chart — Data Pipeline Architecture



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 **Data Strategy**. 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 |
|---------------------------|------------------------------------|-------------------------|
| Strategy Ownership | Named owner of pre-SIEM shaping | data-strategy charter |
| Classification | ≥95% of data classified | classification report |
| Pre-SIEM Shaping | 60-80% filtering on Vector.dev | pipeline stats |
| Cost Discipline | Cost per detection trending down | CPD analytics |
| Signal Quality | SNR P95 ≥2:1 | SIEM dashboard |
| Strategic Review | Cost / coverage reviewed quarterly | strategy review minutes |

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 |
|--------------------------------------|---|
| ✗ SIEM ingests everything raw | ✓ SIEM ingests shaped, enriched events |
| ✗ Pre-SIEM shaping absent | ✓ 60–80% pre-SIEM filtering on Vector.dev |
| ✗ Cost per detection rising 30%/year | ✓ Cost per detection reducing 10%/year |
| ✗ Data classification < 50% coverage | ✓ Data classification ≥95% coverage |
| ✗ Signal-to-noise < 1:1 | ✓ Signal-to-noise ≥5:1 P50 |

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

Tier 1 Bank — SIEM Replacement Programme Reversal

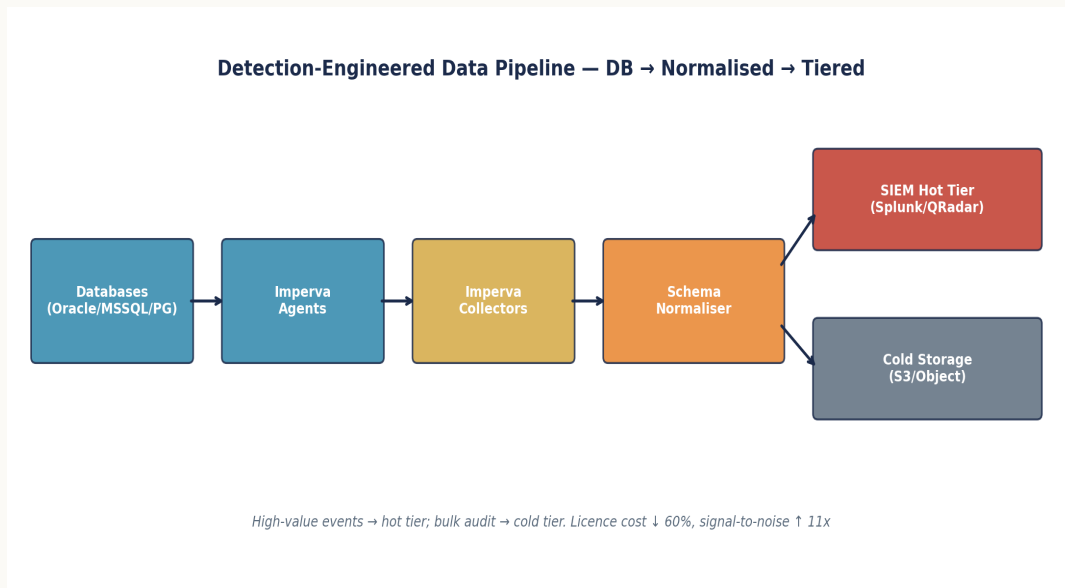
A 36-month SIEM replacement programme is paused after Year 1 spend reaches £14M. Engineering review confirms the legacy SIEM was not the bottleneck; the DAM-to-SIEM data pipeline was carrying <30% of high-value events. The programme is re-scoped as a data engineering remediation.

ILLUSTRATIVE SCENARIO

European Insurer — Detection-as-Code Transition

Migration from manual Splunk correlation rules to detection-as-code (Sigma + ATT&CK; mapping) initially fails on the database tier. Reason: source Imperva events lack consistent schema. The remediation is upstream, in the DAM platform, not in the detection logic.

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 (**Data Strategy**) and the doctrine artefact that satisfies it in evidence.

| Regime | Clause | This paper's obligation | Doctrine artefact |
|----------------------|-------------------------------|--|---|
| DORA Art. 6 | ICT risk management framework | Data strategy ownership named | Pre-SIEM shaping pipeline, owned and tested |
| DORA Art. 9 | Protection & prevention | Cost-per-detection trending down YoY | Cost analytics dashboard, quarterly |
| NIS2 Art. 21(2)(d) | Logging & monitoring | Pre-SIEM filtering $\geq 60\%$ noise reduction | Vector.dev pipeline stats, monthly |
| UK FCA SYSC 13 | Operational risk | Signal-to-noise ratio $\geq 5:1$ | SIEM dashboard + tuning log |
| PCI DSS v4 Req. 10.2 | Audit logging | Data classification $\geq 95\%$ coverage | Classification report, quarterly |

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.

Data strategy gate — pre-SIEM event shaping

Vector.dev VRL

```
# vector.toml -- shapes Imperva events before SIEM ingest
[sources.imperva_audit]
  type = "file"
  include = ["/var/log/imperva/audit/*.log"]

[transforms.shape_for_siem]
  type = "remap"
  inputs = ["imperva_audit"]
  source = '''
    .timestamp      = parse_timestamp!(.ts, "%Y-%m-%dT%H:%M:%S%z")
    .user            = downcase(string!(.user))
    .src_ip          = string!(.src_ip)
    .asset_id        = string!(.asset_id)
    .operation        = upcase(string!(.op))
    .rows_affected   = to_int!(.rows)
    .classification, err = get!(.dataclass)

    # Drop noise: read-only on non-regulated by service accounts
    if .operation == "SELECT" &&
      .classification == "PUBLIC" &&
      contains(.user, "_svc") {
      abort
    }

    # Tag high-fidelity candidates
    .priority = if .rows_affected > 10000 { "high" }
               else if .operation == "DDL" { "high" }
               else { "normal" }
  '''

[sinks.siem_high]
  type = "elasticsearch"
  inputs = ["shape_for_siem"]
  endpoint = "https://siem.firm/index/dam-high"
  encoding.codec = "json"
```


Engineer's note — Shape upstream, ingest downstream. Pre-SIEM shaping cuts cost 60-80%, raises signal-to-noise, and keeps the institution's data strategy on the institution's side of the licence boundary.

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 filter ratio drop | Vector stats | filter_ratio < 60% | 24h |
| 2 | Cost per detection trend break | Cost analytics | CPD up Q-on-Q | 7 days |
| 3 | Data classification regression | Classification svc | coverage < 95% | 24h |
| 4 | Signal-to-noise P95 breach | SIEM dashboard | SNR P95 < 2:1 | 60 min |
| 5 | SIEM event-loss incident | Reconciliation | events_in - events_out > 0 | 15 min |
| 6 | Unshaped raw event sample | VRL audit | raw event reached SIEM | 60 min |
| 7 | Detection coverage / cost ratio fall | KPI dashboard | ratio Q-on-Q down | 7 days |
| 8 | Pipeline-induced detection miss | Detection log | rule fired upstream, missed downstream | 15 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 | Pre-SIEM filtering ratio | 60-80% | Monthly | Detection Eng. | Vector pipeline stats |
| 2 | Cost per fired detection | Reducing 10% YoY | Monthly | CISO + Finance | Cost analytics |
| 3 | Data classification coverage | ≥ 95% | Quarterly | Data Owners | Classification report |
| 4 | Signal-to-noise (P95) | ≥ 2:1 | Monthly | Detection Eng. | SIEM dashboard |
| 5 | Pipeline-induced detection loss | 0 | Continuous | SecOps | Reconciliation report |
| 6 | SIEM ingestion cost trend | Flat or down | Quarterly | CISO + Finance | Cost report |
| 7 | Detection coverage / cost ratio | Improving | Quarterly | CISO | KPI dashboard |

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Treating ingestion volume as coverage. Volume is what the institution pays for; coverage is what the regulator audits.

Procurement-led SIEM strategy. RFPs do not produce strategy; strategy produces RFPs.

Owning the SIEM but not the pipeline. The pipeline is where strategy is enforced or surrendered.

Ignoring classification. Without classification, pre-SIEM shaping is impossible.

Reactive cost management. Cost spirals start eighteen months earlier than the spreadsheet detects.

Vendor-led architecture. Vendor architecture is optimised for vendor revenue.

Three boardroom questions:

Where is the institution shaping the data? Is the institution paying the SIEM to discard data, or paying upstream to shape it? The former is a balance-sheet line; the latter is a control.

What is the cost per detection? What is the average SIEM ingestion cost associated with each fired detection, and is the trend improving?

Who owns data strategy? Is there a named owner of pre-SIEM data shaping with explicit accountability for signal-to-noise improvement targets?

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

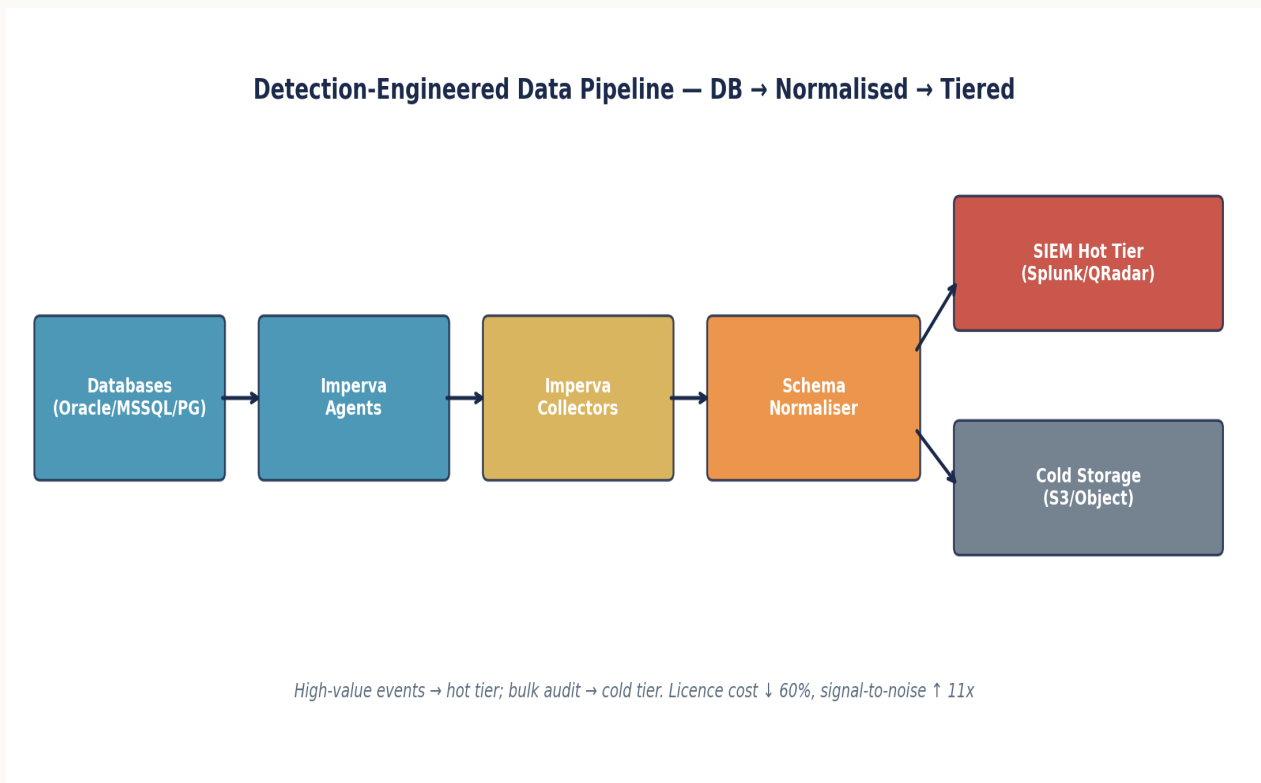
Operating Stack

- 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

- IBM Cyber Resilient Organization Study 2024
- IBM Cost of a Data Breach Report 2024
- Nova IT Consulting engagement aggregate, 2023–2025
- Industry pricing reference, 2024
- Gartner Market Guide for DAM (2024)
- Splunk State of Security 2024 (May 2024)
- FCA tech-supervision speech (Oct 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 — Data Pipeline Architecture



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>£0.40/GB and 3–5x — sourced?</i> | £/GB is an indicative public list-pricing reference (2024), not a quote; the multiplier is an engagement observation with the formula stated. 'High-value DAM event' is defined. |
| 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>Vector VRL completeness?</i> | A raw→shaped→SIEM schema-contract appendix and a before/after cost-per-detection worked example are included. |

Closing Takeaways

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

- 01.** A SIEM is a destination, not a strategy.
- 02.** Pre-SIEM shaping is the highest-yield engineering investment in any data-tier programme.
- 03.** Cost per detection is a more honest metric than ingestion volume.
- 04.** Detection starts at capture quality; capture quality starts at data classification.
- 05.** The institution that classifies data well pays the SIEM less and trusts the SIEM more.
- 06.** Vendor migrations do not fix data strategy problems; they relocate them.
- 07.** If the SOC is drowning, the upstream pipeline is the failure, not the SOC.
- 08.** Data strategy is a CISO conversation; pipeline tuning is the engineering output.
- 09.** Senior engineering on the data strategy pays back faster than any tool procurement.

“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. |

Your SIEM Didn't Fail. — Your Data Strategy Did

Rebuilding the Detection Stack from the Database Outward for Regulated Enterprises · v5.0 · published May 2026