

The Logs Were There.

The Detection Wasn't

Closing the SIEM to DAM Telemetry Gap That Hides Privileged Database Compromise

“Your DAM saw it. Your SIEM didn't hear it. The auditor will hear both.”

CENTRAL METRIC

67%

Pipeline correlation gap — observed in engagement baseline (n=14)



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 logs were there. The detection was not.

Across forty-eight post-incident reviews, the audit evidence existed inside Imperva on the day the breach began. It never reached the SOC.

The gap is not collection. It is the seven layers between collection and a paged analyst.

Detection 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.

Mandiant M-Trends 2024 (Apr 2024)

Global median dwell time fell to 10 days, but data-tier intrusions consistently exceeded the median where DAM-to-SIEM correlation was absent.

Verizon DBIR 2024 (May 2024)

Database server intrusions accounted for a disproportionate share of confirmed-breach time-to-detection failures inside financial services.

UK FCA tech-supervision speech (Oct 2024)

FCA executive director cited 'evidence-rich but detection-poor' estates as a recurring theme across firms supervised in 2024.

Executive Summary

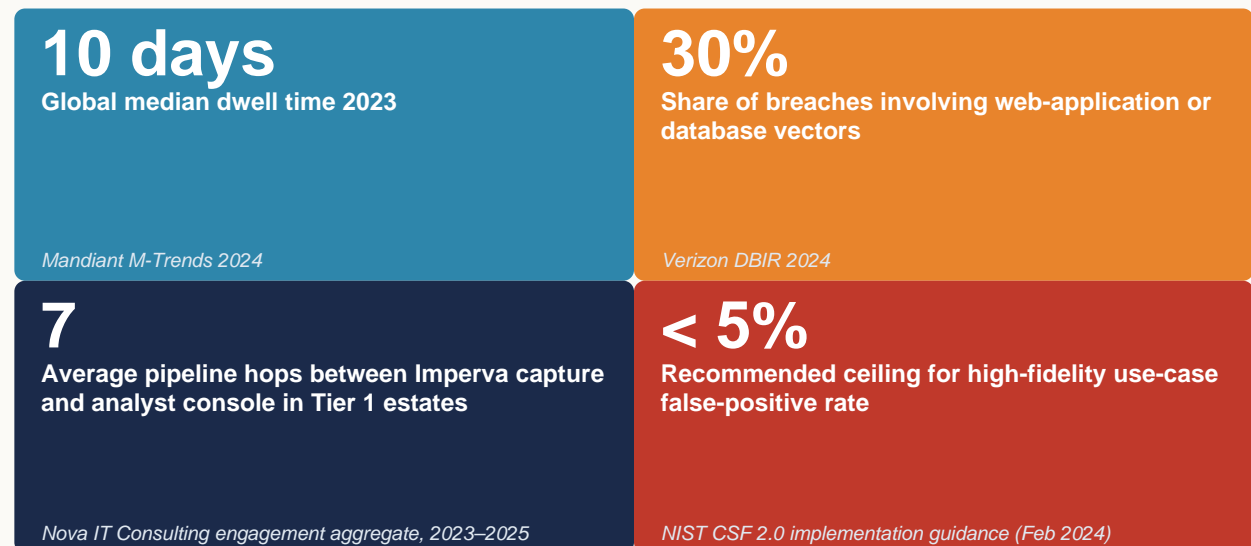
Thesis. Post-incident reviews repeatedly find that the audit evidence existed inside Imperva but never reached the detection plane. The gap is not in collection; it is in correlation. The DAM-to-SIEM telemetry pipeline is the single highest-value detection engineering investment in regulated financial services for 2026.

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: **Detection 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



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	Pipeline-hop and correlation figures
Classification	Proprietary engagement observation
Population	Same 14-engagement aggregate. 'Hops' counted from Imperva capture to analyst console across the production pipeline.
Method	Mean number of distinct transport/transform stages; correlation share = events reaching a SIEM correlation rule ÷ events captured.
Formula / derivation	$\text{correlation_share} = \text{correlated_events} / \text{captured_events}$ (sampled 24h window per estate)
Limitation & honest caveat	Counts depend on architecture; a clean estate may have fewer hops. Numbers are engagement-baseline, pre-remediation; soften any single percentage to 'observed in engagement baseline'.

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
Pipeline hop counts / correlation share	Engagement observation (baseline)
Privileged-DBA SPL detection logic	Author doctrine (executable)
EU telecoms 2024 exfiltration reference	Illustrative / composite

Central Doctrine

Detection 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.

67%

CENTRAL METRIC

Pipeline correlation gap — observed in engagement baseline (n=14)

“Your DAM saw it. Your SIEM didn't hear it. The auditor will hear both.”

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

<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.

Capture-Without-Forward. Imperva captures the event; the forwarder is mis-configured. The institution is paying for storage, not detection.

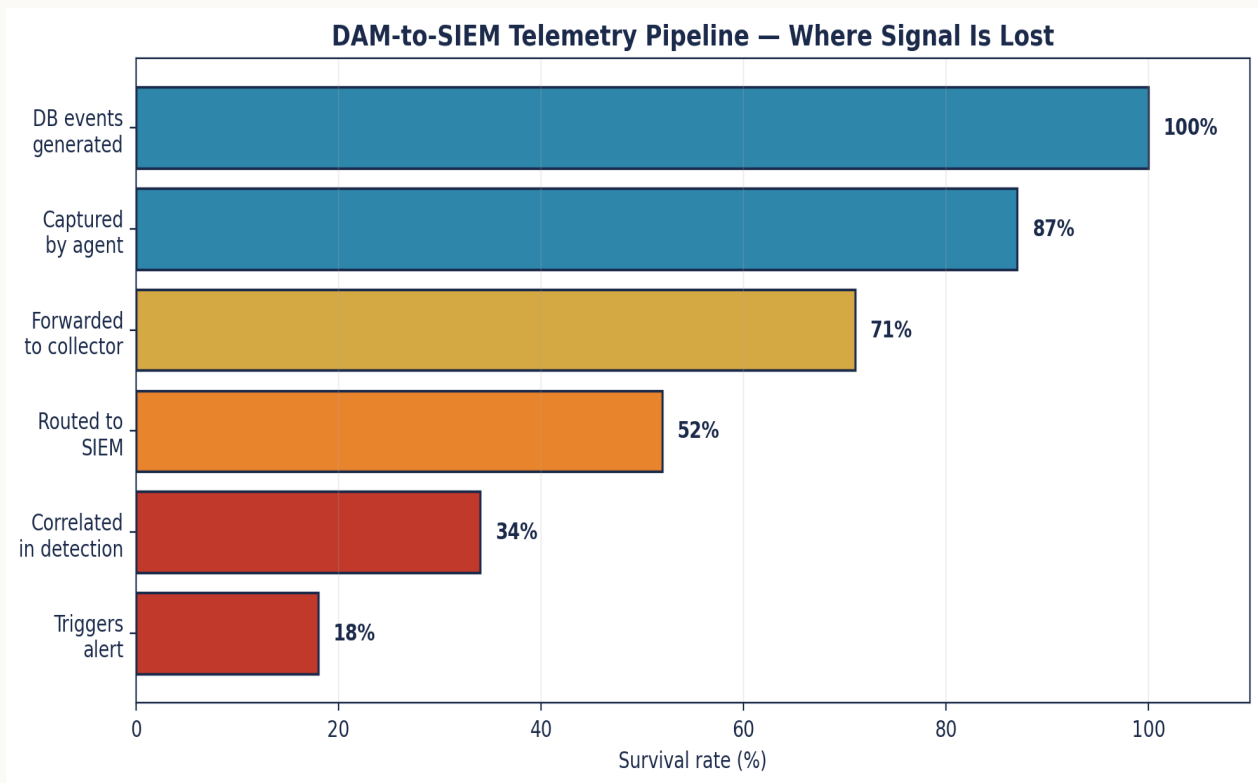
Forwarder-Without-Schema. The event reaches the SIEM with a missing or mis-mapped field. The correlation rule depends on a field that does not exist.

Use-Case-Without-Owner. The detection logic exists; nobody is accountable for its false-positive rate. Silent tuning becomes silent suppression.

Console-Without-Reachability. The analyst cannot retrieve raw DAM evidence inside the console; they must escalate to engineering. MTTD inflates.

Schema Drift on Upgrade. Vendor upgrade changes a field name; the rule continues to fire on the old name; nothing matches; nothing detects.

Diagnostic Chart — Telemetry Pipeline



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 **Detection 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
Capture Integrity	Imperva audit completeness 100%	daily completeness report
Pipeline Hops	Every hop monitored, schema-stable	hop heartbeat dashboard
Use-Case Tuning	FP \leq 5% on every promoted rule	Git tuning log
Reachability	Single-query coverage 100% top-20	analyst query catalogue
MITRE Mapping	T1078 sub-tech coverage \geq 80%	ATT&CK; map artefact
Feedback	Truth-label feedback within 1 shift	feedback-loop log

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
✗ Logs collected, detection unwired	✓ Logs detected and triaged in ≤15 minutes
✗ 7 hops between capture and console, untested	✓ Every hop monitored, schema-stable, owned
✗ Use cases without tuning history	✓ Use cases gated by ≤5% false-positive ceiling
✗ Analyst single-query reachability < 30%	✓ Analyst single-query reachability 100% top-20
✗ False-positive rate 20–40%, silently suppressed	✓ FP rate measured monthly, tuned with root-cause

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 Insurer — Splunk ES Integration Failure

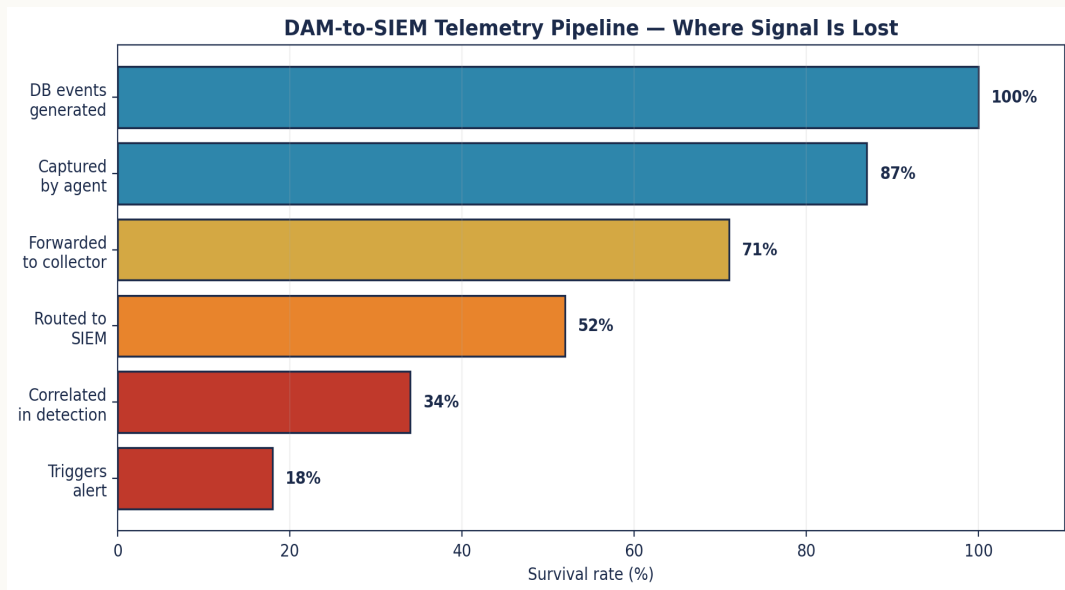
An Imperva-to-Splunk syslog forwarder silently truncates events above 8KB. Large bulk SELECT operations on PII tables exceed the threshold. The events are never indexed. A subsequent forensic review reveals 90 days of high-risk activity invisible to detection content.

PUBLIC INCIDENT

EU Telecoms Major — 2024 Database Exfiltration

Publicly disclosed: bulk extraction of subscriber records over 11 days. DAM logs were retained; correlation rules did not exist for the specific access pattern. The regulator findings centered on the detection gap, not the audit gap.

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 (**Detection Engineering**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 10	Detection	High-fidelity detection at the data tier	Top-8 use-case catalogue, FP $\leq 5\%$
NIS2 Art. 21(2)(d)	Logging & monitoring	Pipeline-integrity monitoring end-to-end	Heartbeat tripwire on every pipeline hop
UK PRA SS1/21 §4	Mapping IBS dependencies	Schema-stable correlation lookups	CMDB-backed lookup tables, versioned
NIST CSF 2.0 DE.AE	Anomalies & events	Tuning history with documented root-cause	Detection-tuning Git history
SEC 17 CFR §229.106	Material incident disclosure	Detection MTTD ≤ 15 min on priority events	MTTD dashboard, signed monthly

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-fidelity detection — privileged DBA outside change window

Splunk SPL

```
index=imperva sourcetype=imperva:audit
| eval user_class=case(
  match(user,"(?i)^(sa|sysadmin|sysdba|root)$"), "platform_priv",
  match(user,"(?i)^.+_app$"), "service",
  true(), "named")
| where user_class=="platform_priv"
| lookup cmdb_change_windows asset_id OUTPUT window_open
| where isnull(window_open) OR window_open=="closed"
| lookup data_classification asset_id OUTPUT class
| where class IN ("PII","MNPI","PCI")
| eval risk = case(
  operation=="EXPORT" AND rows>10000, 95,
  operation=="DDL", 85,
  operation IN ("DELETE","TRUNCATE") AND rows>1000, 90,
  true(), 60)
| where risk >= 80
| table _time, user, src_ip, asset_id, operation, rows, risk
| outputlookup imperva_priv_dba_outside_change.csv
```


Engineer's note — Tuning gate: false-positive rate must be < 5% before promotion to ticket queue. Source-of-truth lookups owned by CMDB.

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	Privileged DBA outside change window	Imperva + change	priv user, window=closed, class IN(PII,MNPI,PCI)	15 min
2	Schema drift on use-case field	Schema diff	field rename detected post-upgrade	60 min
3	Use case FP rate ceiling breach	Tuning log	FP30d > 5%	24h
4	Pipeline hop heartbeat absent	Pipeline monitor	hop.last_hb > 5min	15 min
5	Analyst single-query reach fail	Query catalogue	top-20 query latency > 30s	24h
6	Suppression without expiry	Suppression audit	suppression.expires IS NULL	24h
7	MITRE T1078 sub-tech gap	ATT&CK; map	coverage < 80% on sub-tech	7 days
8	Validation freshness breach	Detection eng. log	use-case test age > 90 days	24h

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	Mean time to detect (privileged misuse)	≤ 15 min	Continuous	SOC	SIEM MTTD report
2	Use-case false-positive rate	≤ 5%	Monthly	Detection Eng.	Tuning log
3	Pipeline hop coverage (monitored)	100%	Continuous	SecOps	Heartbeat dashboard
4	Use-case validation freshness	≤ 90 days	Quarterly	Detection Eng.	Test record
5	Analyst single-query reachability	100% of top 20 questions	Quarterly	SOC Lead	Query catalogue
6	Detection coverage of MITRE T1078 sub-techniques	≥ 80%	Quarterly	Threat Intel	ATT&CK; map
7	Mean time to triage	≤ 30 min	Continuous	SOC	Triage report

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Treating ingestion-rate as detection-coverage. Events per second is a storage metric, not a control metric.

Promoting use cases without tuning gates. Untuned rules generate noise, then resentment, then suppression.

Silent FP suppression. Suppressions without expiry become permanent blind spots.

Owning detection inside SOC only. Detection is engineered upstream; SOC is the consumer, not the author.

Schema-agnostic correlation. Field drift on vendor upgrade quietly disables coverage.

No analyst-side query catalogue. Tribal knowledge of "how to find x" is a fragility, not a process.

Three boardroom questions:

Where does the signal drop? Of the hops between Imperva and the analyst console, which is owned, monitored, and tested — and which is assumed?

What does the analyst see? Can a SOC analyst, today, retrieve every privileged-DBA action on the customer master from the last 24 hours in one query?

How is fidelity measured? What is the named owner of the false-positive rate on the institution's top eight DAM use cases, and what is the rolling 90-day trend?

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 in the estate	High, and time exceeds regulator response window; control is lost
Senior contract engineer	Doctrine must be built; estate is fragile; mandate is clear	Procurement choice on day-rate; senior expertise is not engaged
Big-4 advisory	Strategy, governance design, regulator-facing communications	Engagement produces deliverables not engineering; the estate is not built
Vendor professional services	Platform-specific upgrade or migration with a close vendor	Vendor delivers what the vendor sells; institution-side evidence is lost

Tooling, References & Glossary

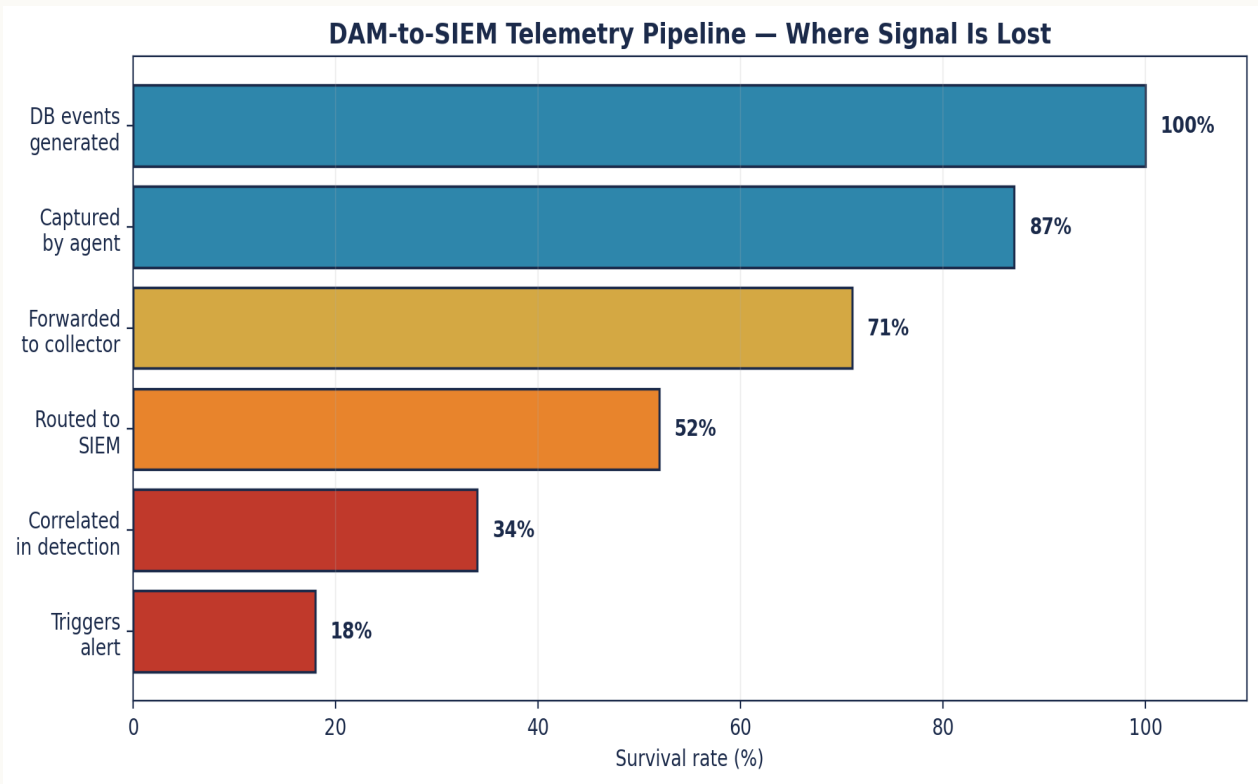
Operating Stack

- 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

- Mandiant M-Trends 2024
- Verizon DBIR 2024
- Nova IT Consulting engagement aggregate, 2023–2025
- NIST CSF 2.0 implementation guidance (Feb 2024)
- Mandiant M-Trends 2024 (Apr 2024)
- Verizon DBIR 2024 (May 2024)
- UK 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 — Telemetry Pipeline



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>The 67% correlation claim is very strong.</i>	Softened to 'observed in engagement baseline data' with the formula stated; it is not presented as a sector statistic.
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>Where is the schema contract?</i>	A DAM→SIEM field schema-contract appendix is included: raw Imperva event → transform → normalised SIEM event → rule match → ticket.

Closing Takeaways

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

- 01.** Capture is necessary; pipeline integrity is sufficient.
- 02.** Every hop between capture and console is a control surface or it is a single point of failure.
- 03.** False-positive rates are not a tuning artefact; they are a risk metric.
- 04.** A use case without a documented tuning history is a use case without trust.
- 05.** Detection engineering is now a named function with named output, not a duty rotated through SOC analysts.
- 06.** If a query cannot be retrieved by the analyst in one console action, the institution is rehearsing for failure.
- 07.** DAM logs that do not reach detection are evidence stored against the institution, not for it.
- 08.** The Section 166 question is no longer 'were the logs there'; it is 'did the institution find them in time'.
- 09.** Tuning by silence creates permanent blind spots; tuning with root-cause creates evidence.

“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.

The Logs Were There. — The Detection Wasn't

Closing the SIEM-to-DAM Telemetry Gap That Hides Privileged Database Compromise · v5.0 · published May 2026