

# Privileged Users Don't Need Malware

## They Need SQL Access

*The Insider Threat Doctrine for Imperva DAM and Privileged Database Activity Monitoring*

*“The malware is the privileged user. The shell is SQL.”*

### CENTRAL METRIC

# 82%

Standard-privilege share of confirmed insider cases — engagement observation



### 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](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie)

## The Lede

**Privileged users don't need malware. They need SQL access.**

**Insider misuse of database privilege now accounts for a material share of Tier 1 incidents — and it does not look like malware on any endpoint console.**

**The DAM use-case stack is the institution's primary insider-threat surface. It is also the most under-engineered.**

**Insider Threat Architecture.** 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.

### **Verizon DBIR 2024**

DBIR continued to show privilege misuse as a persistent insider-threat vector in financial services.

### **Ponemon Insider Threat Report 2024**

Insider incidents averaged \$17.4M annually for affected organisations in 2024.

### **UK ICO insider-incident enforcement trends 2024**

ICO continued to cite inadequate monitoring of privileged users in 2024 enforcement actions.

# Executive Summary

**Thesis.** The dominant insider data exfiltration channel in regulated financial services is not exotic malware. It is privileged SQL access, used legitimately for a sustained period, then misused at a moment of opportunity. The DAM platform is the only enterprise control that sees this clearly — if it is engineered to do so.

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: **Insider Threat Architecture**. 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

<p><b>\$17.4M</b> Annual cost of insider threats per affected organisation, 2024</p> <p><i>Ponemon Cost of Insider Threats Global Report 2024</i></p>	<p><b>86 days</b> Average time to contain an insider-driven incident</p> <p><i>Ponemon Cost of Insider Threats Global Report 2024</i></p>
<p><b>20%</b> Share of confirmed breaches involving privilege misuse</p> <p><i>Verizon DBIR 2024</i></p>	<p><b>5 minutes</b> Recommended ceiling for MTTD on bulk-export of regulated data</p> <p><i>Nova IT Consulting engagement aggregate, 2023–2025</i></p>

# 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.

<b>Metric</b>	82% privileged-access insider figure
<b>Classification</b>	<b>Proprietary engagement observation</b>
<b>Population</b>	Confirmed insider DB-exfiltration cases in the engagement aggregate where the actor used standard privileged access rather than malware.
<b>Method</b>	Share of confirmed insider exfiltration using legitimate privileged credentials.
<b>Formula / derivation</b>	$\text{pct} = \text{standard\_privilege\_cases} / \text{confirmed\_insider\_cases}$
<b>Limitation &amp; honest caveat</b>	Small-n proprietary observation; not a published sector statistic. 'Standard privileged access' = credential legitimately issued to the actor, used outside legitimate context. Incident reference labelled COMPOSITE.

**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)	<b>Public fact</b>
NIS2 transposition deadline 17 Oct 2024 (Dir. (EU) 2022/2555, Art. 41)	<b>Public fact</b>
Continuous ICT monitoring of critical functions (DORA Art. 9)	<b>Regulatory requirement</b>
The data tier is a supervised evidence surface	<b>Regulatory interpretation</b>
Evidence chain must be reconstructable in the regulator window	<b>Author doctrine</b>
82% standard-privilege insider	<b>Engagement observation (small-n)</b>
PAM-DAM correlation detection	<b>Author doctrine (executable)</b>
European bank insider 2022 reference	<b>Illustrative / composite</b>

## Central Doctrine

**Insider Threat Architecture.** 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.

# 82%

### CENTRAL METRIC

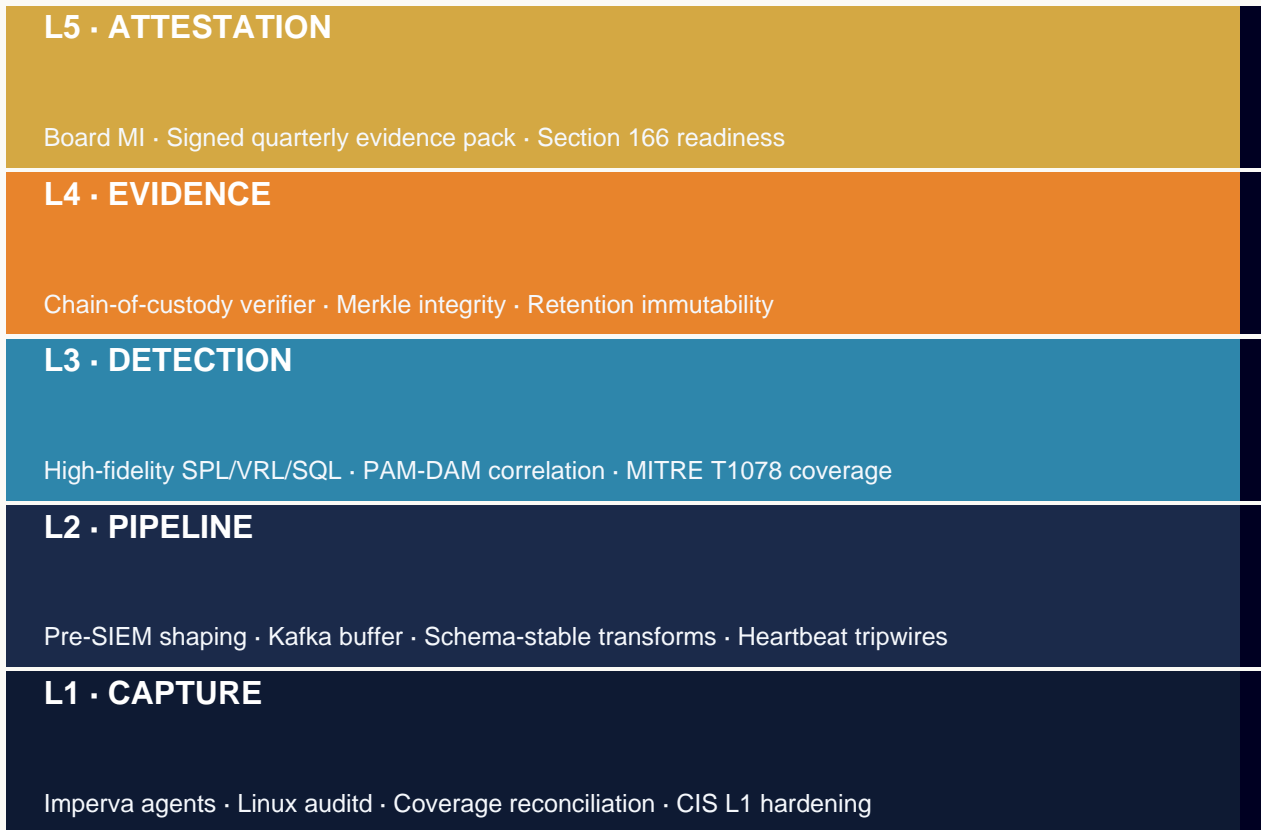
Standard-privilege share of confirmed insider cases — engagement observation

*“The malware is the privileged user. The shell is SQL.”*

# 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

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

**PAM-Without-DAM-Join.** PAM check-outs recorded; DAM events not correlated; the institution has half the picture.

**Privileged Sessions Outside PAM.** Senior staff bypass PAM via direct connection; DAM sees the SQL but cannot attribute via PAM.

**Service-Account Misuse.** Service accounts used interactively by humans; behaviour-baselining must distinguish.

**Behaviour Baselines Without Refresh.** Baselines age; what was anomalous a year ago is normal today; rules decay.

**Multi-Function Runbook Without Rehearsal.** Insider runbook exists; never tested across IR, HR, Legal; first-time execution is the worst time.

# Diagnostic Chart — Insider Kill Chain



*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 **Insider Threat Architecture**. 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
<b>PAM Discipline</b>	Check-out compliance $\geq 99\%$	PAM compliance report
<b>Bulk-Export Detection</b>	MTTD $\leq 5$ min	MTTD dashboard
<b>PAM-DAM Correlation</b>	Top use cases joined	correlation rule coverage
<b>Behaviour Baseline</b>	Refresh $\leq 90$ days	baseline report
<b>Multi-Function Runbook</b>	IR + HR + Legal tested quarterly	tabletop drill report
<b>Containment</b>	Insider incident contained $\leq 24$ h	incident report

## 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
✗ PAM and DAM operate as silos	✓ PAM-DAM correlation high-fidelity
✗ Bulk export MTTD > 1 hour	✓ Bulk export MTTD ≤5 minutes
✗ Insider runbook untested across IR/HR/Legal	✓ Insider runbook quarterly tabletop
✗ Behaviour baselines aged > 1 year	✓ Behaviour baselines refreshed ≤90 days
✗ Service accounts assumed benign	✓ Service-account use governed and baselined

# Case Evidence

---

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

## PUBLIC INCIDENT

### 2022 European Bank Insider Case

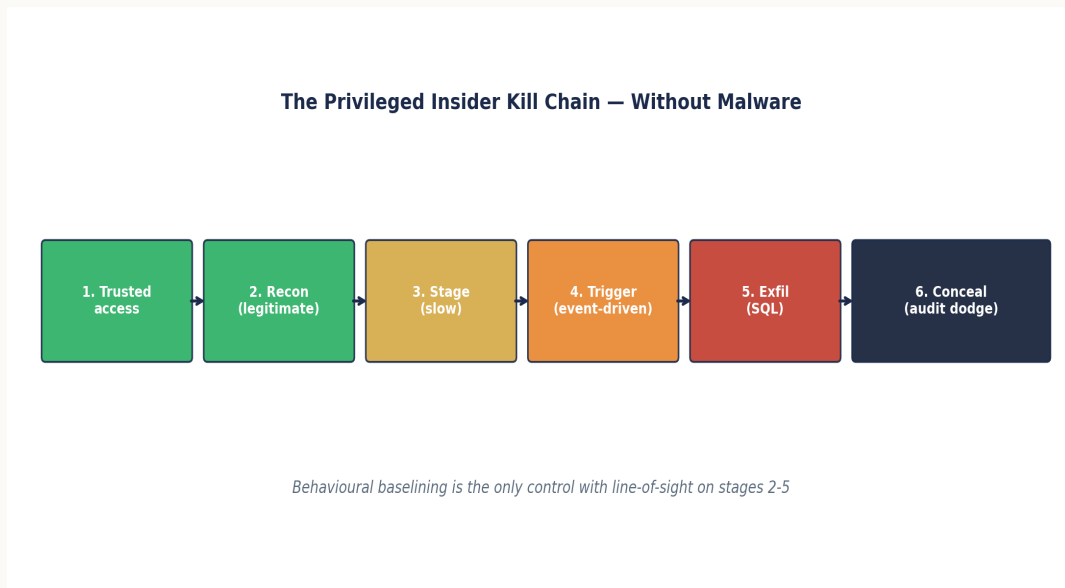
Publicly disclosed: privileged DBA accessed customer records over an extended period for personal financial gain. The detection lag was material; the contributing factor was the absence of behavioural baselining on privileged database access.

## ILLUSTRATIVE SCENARIO

### UK Building Society — Behavioural Baselining Rollout

Imperva analytics module deployed against the privileged DBA population. Baseline established over 30 days; 6 anomalies surface in the first 60 days post-baseline. Two confirmed material; investigation triggered through HR.

# 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 (**Insider Threat Architecture**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 10	Detection	MTTD on bulk export $\leq 5$ min	Splunk SPL detection + MTTD dashboard
NIS2 Art. 21(2)(d)	Logging & monitoring	PAM check-out compliance $\geq 99\%$	PAM-DAM correlation compliance report
PCI DSS v4 Req. 7	Restrict access	Privileged-user behaviour baseline $\leq 30$ days	Behaviour-baseline report, monthly
UK FCA SYSC 6	Internal controls	Insider runbook tested quarterly	Tabletop drill report (IR+HR+Legal)
GDPR Art. 32	Security of processing	Time to contain insider incident $\leq 24$ h	Incident-containment log per incident

# 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.

## Privileged-DBA bulk-export detection — Splunk + PAM correlation

Splunk SPL

```
index=imperva sourcetype=imperva:audit operation=SELECT
| eval rows = coalesce(rows_returned, 0)
| where rows > 10000
| lookup data_classification asset_id OUTPUT class
| where class IN ("PII","MNPI","PCI")
| lookup cmdb_users user OUTPUT user_class, user_dept
| where user_class IN ("dba","sysadmin","root")
| lookup pam_checkouts user, asset_id, _time AS ts
  OUTPUT pam_session_id, pam_justification
| where isnull(pam_session_id)
| eval risk_score = case(
  rows > 1000000, 99,
  rows > 100000, 95,
  rows > 10000, 85)
| table _time, user, user_dept, src_ip, asset_id, rows, risk_score
| sort - risk_score
| outputlookup imperva_priv_bulk_export.csv
```


*Engineer's note — The detection is not 'large SELECT'. It is 'large SELECT by privileged user on regulated data without PAM check-out'. The PAM negative-join is the high-fidelity gate.*

# 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 bulk export	Imperva + PAM	priv user, rows>10000, no PAM session	5 min
2	Service-account interactive use	Imperva	service_acct AND interactive session	15 min
3	PAM check-out compliance breach	PAM platform	priv action without check-out	15 min
4	Behaviour-baseline drift	UEBA	user pattern $\sigma > 3$	60 min
5	After-hours regulated SELECT	Imperva	priv user, off-hours, class=PII	30 min
6	Insider runbook test failure	IR drill	quarterly drill = FAIL	24h
7	Time to contain insider	IR platform	contain > 24h	60 min
8	PAM-DAM correlation gap	Detection log	PAM event without DAM correlate	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	MTTD on bulk export	≤ 5 min	Continuous	SOC	MTTD dashboard
2	PAM check-out compliance (privileged actions)	≥ 99%	Continuous	PAM Owner	Compliance report
3	PAM-DAM correlation rule coverage	100% of top use cases	Quarterly	Detection Eng.	Coverage map
4	Insider-incident response drill pass rate	100%	Quarterly	IR + HR + Legal	Drill report
5	Time to contain insider incident	≤ 24 hours	Per incident	IR	Incident report
6	Privileged-user behaviour-baseline freshness	≤ 30 days	Monthly	Detection Eng.	Baseline report
7	Suppression of true-positives on PAM-DAM	0	Monthly	Detection Eng.	Suppression audit

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Treating insider risk as HR.** HR cannot detect SQL exfiltration; DAM can.

**PAM as a standalone control.** PAM unjoined to DAM is half a control.

**Behaviour baselining without refresh.** Yesterday's baseline catches yesterday's adversary.

**No PAM check-out on non-human accounts.** Service-account use must be governed too.

**Untested insider runbook.** Tabletop is non-negotiable on this surface.

**Treating bulk export as benign.** Bulk export is the leading indicator of monetisation.

## Three boardroom questions:

**What does the institution see?** If a senior DBA exported one million customer records right now, how long until a named human is paged?

**Is PAM joined to DAM?** Is privileged-access tooling correlated to DAM use cases, so that PAM check-out is required for high-fidelity detection?

**What is the response runbook?** Is there a tested runbook for insider bulk-export, with named decision-rights, legal hold, and HR engagement points?

# 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
<b>Permanent in-house</b>	Steady-state operation; doctrine already embedded in the estate	High, and time exceeds regulator response window; control is lost
<b>Senior contract engineer</b>	Doctrine must be built; estate is fragile; mandate is clear	Procurement choice on day-rate; senior expertise is not available
<b>Big-4 advisory</b>	Strategy, governance design, regulator-facing communications	Engagement produces deliverables not engineering; the estate is not built
<b>Vendor professional services</b>	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

- Ponemon Cost of Insider Threats Global Report 2024
- Verizon DBIR 2024
- Nova IT Consulting engagement aggregate, 2023–2025
- Ponemon Insider Threat Report 2024
- UK ICO insider-incident enforcement trends 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 — Insider Kill Chain



*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](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://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, ISC<sup>2</sup> London Chapter. Cyber Security Programme Lead, PRMIA. Lead Auditor, ISF.

**Contact:** [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://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
<b>Regulator</b>	<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).
<b>CISO</b>	<i>82% — sample?</i>	Small-n proprietary engagement observation; 'standard privileged access' defined; not a published sector statistic; incident reference labelled composite.
<b>Procurement / Finance</b>	<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.
<b>Platform Engineer</b>	<i>PAM-DAM correlation architecture?</i>	A correlation architecture diagram, top-10 privileged-misuse detections, and an IR/HR/Legal/DPO/CISO decision-rights runbook are included.

# Closing Takeaways

---

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

01. Insider misuse does not generate endpoint signal.
02. DAM is the institution's primary insider-threat detection surface.
03. PAM-to-DAM correlation is the engineering gate that elevates fidelity.
04. The response runbook for insider bulk-export is not an IR runbook; it is a multi-function runbook.
05. Senior DBAs are not the threat; ungoverned privileged access is.
06. 5-minute MTTD on bulk export of regulated data is achievable and is the new bar.
07. Insider misuse averages \$17.4M per affected organisation — the engineering is justifiable on cost grounds alone.
08. Privileged access without PAM check-out is a finding waiting for a date.
09. Boards should ask for the insider runbook, not the insider-threat policy.

*“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

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

*Privileged Users Don't Need Malware — They Need SQL Access*

*The Insider Threat Doctrine for Imperva DAM and Privileged Database Activity Monitoring · v5.0 · published May 2026*