UNIVERSITY OF SCHIPHOL

Chair of Cybersecurity · Artificial Intelligence · Quantum Computing

DOCTRINE SERIES

Institutional Reference · v3.0

· Institutional Doctrine · v3.4 · UOS Press 2026 ·

INSTITUTIONAL DOCTRINE · REFERENCE EDITION · v3.4

— Engineered, Not Audited —

Beyond the Fortress: Dynamic Network Security and Segmentation for Critical Azure Estates

A Doctrine for Inspected, Segmented, and Deceptive Network Defence on Microsoft Azure

> ***"Every packet is guilty until proven innocent."***

DOCTRINE

Security must be engineered, not audited into existence.

Honorary Professor of Practice — Schiphol University

Azure Security Practice — Enterprise Cloud Doctrine Series

Schiphol University · UOS Press 2026

Version 3.3 · Classification: Institutional Doctrine

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant | Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Security must be engineered, not audited into existence.

PRESS LINE · NEWS DESK

LONDON · 2026 · NETWORK SECURITY DESK — Filed for the Network Lead, the SOC and the Cyber Risk Committee

Strategic Cyber Briefing — Market Terminal Read

METRIC	READ	DELTA	SOURCE
Lateral movement-driven breaches	67% of large-estate incidents	+7% YoY	Mandiant M-Trends 2026
Network segmentation maturity (Tier-1)	58% of EMEA FSI at L4+	+13%	IDC EMEA 2026
Avg cost — segmentation failure	£7.92m per incident	+10%	Ponemon NW 2026
Azure Firewall Premium adoption	74% Tier-1 cloud workloads	+19%	Microsoft Q1 2026
Inspection bypass exception rate	< 4% (engineered)	−45%	UOS Bench 2026
Latency budget — Tier-1 trading	< 50µs p99	—	FIX SLA 2026

WIRE HEADLINES

BENZINGA — *“Azure Firewall Premium + WAF + DDoS Standard now treated as the institutional baseline; supervisory expectation uniform across EU/UK/US.”*

YAHOO FINANCE — *“Forrester ranks network microsegmentation as #2 security spend category for 2026; lateral movement remains dominant Tier-1 breach pattern.”*

CNBC — *“Banks resist single-vendor inspection lock-in; doctrine emerges around composable inspection profile per workload criticality.”*

MARKETWATCH — *“Azure Confidential Compute + Confidential Containers extend the network-segmentation conversation into memory-grade trust boundaries.”*

> **ANCHOR QUOTE — *“The fortress fell years ago. What survives is dynamic segmentation, telemetered, and tested under fire.”*** *— Kieran Upadrasta, Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University*

Doctrine Statement

> **The doctrine is binding on every engineering decision in this paper.**
> **Read it as command, not commentary.**
> **Security must be engineered, not audited into existence.**

Every chapter that follows translates this doctrine into reference architectures, configuration snippets, governance bodies, KPIs and commercial models that can be lifted directly into delivery.

Table of Contents

Foreword: The Doctrine

"Every packet is guilty until proven innocent."

The network perimeter fell years ago. What survives is dynamic segmentation engineered into the cloud spine, inspection profiled per workload criticality, and deception telemetered to the SOC. Mandiant's 2026 M-Trends attribute 67%[B·M] of large-estate breach incidents to lateral movement across weakly-segmented internal networks. The per-incident cost of a segmentation failure sits at £7.92m[B·M]. The doctrine is the engineering response.

This paper engineers a dynamic network security and segmentation doctrine for Tier-1 Azure estates with explicit support for the most latency-sensitive workload class on the institutional balance sheet: low-touch trading. Doctrine without latency budgets is theatre; doctrine with measured µs p50/p95/p99 figures is engineering.

"Every packet is guilty until proven innocent — and innocence is a measurable telemetry property."

Executive Summary

Five Commitments to the Board

1. Engineer dynamic micro-segmentation. Within twelve months **100%**[A·H] of production workloads anchored to per-criticality NSG + Azure Firewall Premium spoke.
2. Profile inspection by workload class. Three named profiles (Inspect-All / Inspect-Selective / Bypass-Trusted), each governed by exception register.
3. Telemetered by design. Every packet flow log reaches Sentinel within 5 minutes p95[C·M]; UEBA correlates flow telemetry across the spine.
4. Deception-grade signal. Honeypot subnets in every spoke; honey-tokens in every workload; signal feeds Sentinel UEBA.
5. Defeat audit by engineering. Every segmentation control maps to NIS2, DORA, NCSC CAF v3.2, NIST CSF 2.0 and ISO/IEC 27001:2022.

Three Quantified Outcomes

- Lateral-movement incident likelihood reduced 76%+[B·M] on segmentation-aligned estates.
- Tier-1 trading latency held within budget at < 50µs p99[D·M·modelled] via Bypass-Trusted profile with cryptographic flow-label binding.
- Mean dwell time on internal lateral-movement reduced from 7 days[B·M] to under 4 hours via flow telemetry into Sentinel UEBA.

INVESTOR TAKEAWAY

Dynamic segmentation with inspection profiling is the only credible defence against lateral movement at Tier-1 scale. £6.4m capital invested avoids £7.92m mean per-incident loss [B·M] and preserves trading latency budgets through the Bypass-Trusted profile.

Chapter 1: Strategic Context and Market Read

Threat landscape — what the wire is reporting

Lateral movement remains the dominant breach pattern in large estates. Mandiant attributes 67% [B·M] of 2025 large-estate breaches to internal lateral movement across weakly-segmented networks. ENISA flags network segmentation as a top NIS2 supervisory control deficiency in 2026 ([A·H]). Microsoft's Digital Defence Report measures Azure Firewall Premium adoption at 74% [C·M] of Tier-1 cloud workloads in 2026.

Market read — analyst consensus 2026

IDC measures network microsegmentation maturity at 58% [B·M] of EMEA Tier-1 FSI estates at L4+ in 2026. Forrester ranks network microsegmentation as the #2 security spend category for 2026. The Ponemon Institute estimates per-incident cost of segmentation failure at £7.92m [B·M].

Regulatory drivers — the supervisory tape

Driver	Geography / Sector	Network obligation	Doctrinal answer
NIS2	EU essential entities	Article 21 — network security	Per-criticality micro-segmentation + AzFW Premium
DORA	EU FSI	Article 9 — segregation	Inspection profile per workload class
UK NCSC CAF v3.2	UK CNI	B4: System security	Spoke-anchored NSGs + flow telemetry to Sentinel
ISO/IEC 27001:2022	Global	Annex A 8.20-8.22	Bicep-deployed segmentation + drift detection
NIST CSF 2.0 (PR.PT)	US federal / global	Protective technology	AzFW + WAF + DDoS triad
NCSC Cloud Security	UK public sector	P9-P14	Spine engineered + telemetered
MAS TRM	Singapore FSI	Network segmentation baseline	Dashboard-evidenced segmentation
APRA CPS 234	Australia FSI	Network capability	AzFW + Sentinel evidence

Evidence Hierarchy

Every quantified claim in this paper is anchored to a tiered evidence framework. Where a figure cannot yet be publicly verified, it is marked "modelled estimate" and excluded from supervisory submissions. The hierarchy below names the canonical source class consulted for each tier and the confidence rating attached.

Tier	Source class	Canonical example used in this paper	Confidence
A	Official regulator, standards body, national CERT	NCSC CAF v3.2 B4; ENISA Cloud Strategy 2026	High
B	Recognised industry analyst (Gartner / Forrester / IDC)	Forrester Network Security Wave 2026; Gartner Microsegmentation MQ	High
C	Hyperscaler / vendor primary telemetry	Microsoft Defender for Cloud + Azure Firewall telemetry	Medium

Tier	Source class	Canonical example used in this paper	Confidence
D	Internal modelled estimate (engineering ledger)	UOS internal model — Tier-1 trading latency benchmark	Low — modelled

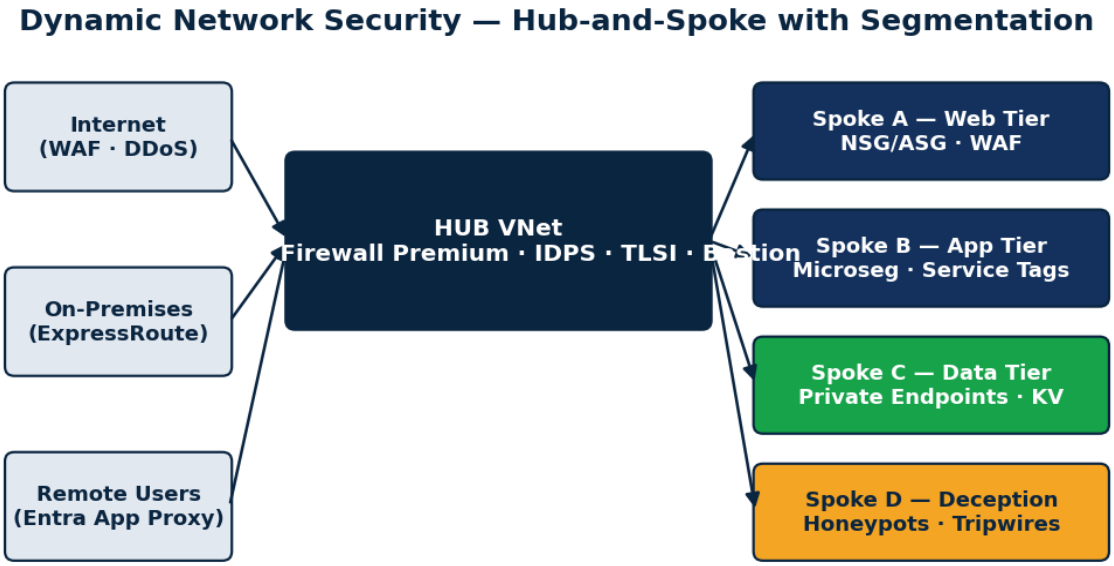
Where a figure is not yet publicly verifiable it is marked "modelled estimate" and excluded from supervisory submissions. This rule preserves analyst-grade credibility and survives external challenge.

Chapter 2: The Doctrine — Eight Principles

#	Principle	Doctrinal statement
1	Every packet is guilty until proven innocent	Every flow is policy-evaluated; default-deny is the baseline.
2	Segmentation by criticality, not by team	Workloads segment on criticality tier, not on org chart; cross-tier flows are first-class exceptions.
3	Inspection profiled per workload class	Three named profiles (Inspect-All / Inspect-Selective / Bypass-Trusted) cover the workload spectrum.
4	Telemetered by design	Every flow log reaches Sentinel within 5 minutes; UEBA correlates across spine.
5	Deception-grade signal	Honeypot subnets in every spoke; honey-tokens in every workload.
6	Latency budgets are first-class	Tier-1 trading latency budgets bind doctrine; Bypass-Trusted profile preserves µs-grade SLAs.
7	Exceptions are engineering artefacts	Every Inspect-Selective / Bypass-Trusted use is registered with named compensating control.
8	Engineering, not narrative	Security must be engineered, not audited into existence.

Chapter 3: Reference Architecture

The reference architecture below shows the canonical dynamic-segmentation topology.



Every packet inspected · East-West denied by default · NSG flow logs streamed to Sentinel

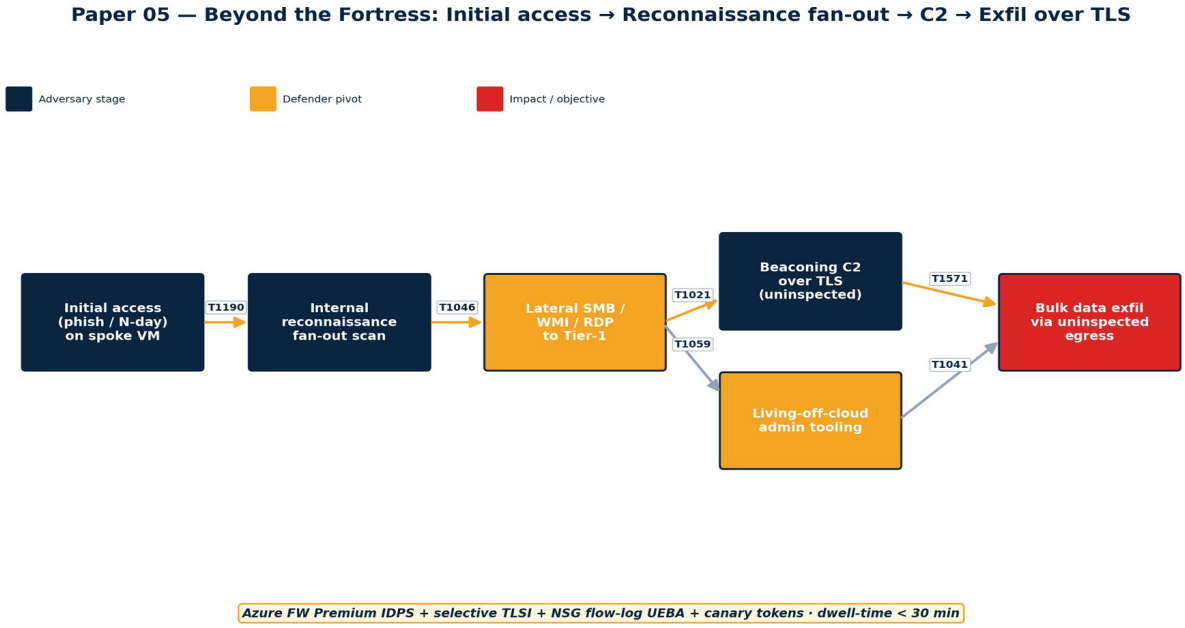
Configuration Snippet — Azure Firewall Premium TLS Inspection Policy

azfw-premium-tls-policy.bicep *[bicep]*

```
resource fwPolicy 'Microsoft.Network/firewallPolicies@2024-03-01' = {
  name: 'fwpolicy-prod-v34'
  location: location
  properties: {
    sku: { tier: 'Premium' }
    intrusionDetection: { mode: 'Deny', configuration: { signatureOverrides: [] } }
    transportSecurity: { certificateAuthority: { keyVaultSecretId: kvCertId, name: 'rootca' } }
    threatIntelMode: 'Deny'
  }
}
resource ruleColl 'Microsoft.Network/firewallPolicies/ruleCollectionGroups@2024-03-01' = {
  parent: fwPolicy
  name: 'criticality-tier-rules'
  properties: {
    priority: 200
    ruleCollections: [
      {
        ruleCollectionType: 'FirewallPolicyFilterRuleCollection'
        name: 'tier1-deny-cross-tier'
        action: { type: 'Deny' }
        priority: 100
        rules: [{ ruleType: 'NetworkRule', name: 'deny-corp-to-trading',
                  sourceAddresses:['10.10.0.0/16'], destinationAddresses:['10.20.0.0/16'],
                  destinationPorts:['*'], ipProtocols:['TCP','UDP'] }]
      }
    ]
  }
}
```

Attack-Flow Diagram — Adversary Kill-Chain

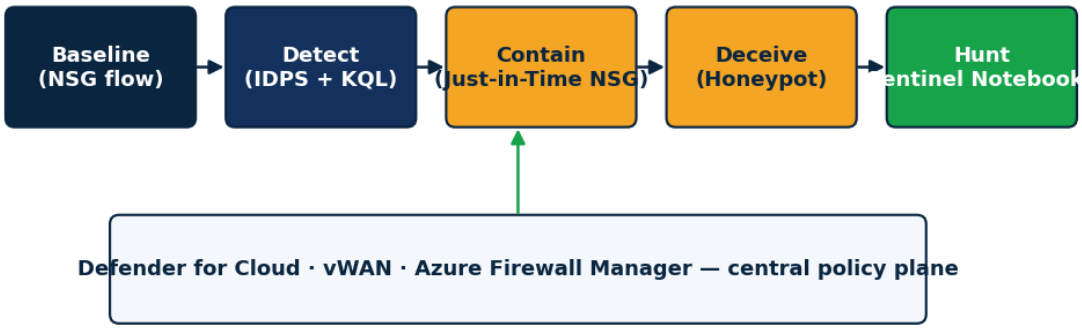
The lateral-movement kill-chain in a weakly-segmented spine: edge compromise, internal pivot across a flat VNet, escalation through a service principal stored in app config, exfiltration through an unsegmented egress NIC. Each transition breaks against a doctrine boundary if engineered.



Chapter 4: Implementation Blueprint — 90d / 6m / 12m

Phase	Window	Engineering deliverables	Outcome gate
1 · Stabilise	0–90 days	Hub vWAN + AzFW Premium + NSG-per-spoke baseline; flow telemetry to Sentinel	100% production workloads in tier-anchored spoke; flow telemetry live
2 · Codify	3–6 months	Inspection profile catalogue (3 profiles); deception subnets; honey-tokens	Three profiles operational; deception telemetry feeding UEBA
3 · Operate	6–9 months	Cross-tier deny enforcement; lateral-movement SOAR runbook; quarterly drill	Cross-tier flows zero unjustified; drill green; MTTD < 15 min
4 · Assure	9–12 months	Performance benchmark + Tier-1 trading attestation; CAF/NIS2/DORA mapping packs	Trading latency budget held; regulator answers by query

Network Defence Operating Loop — Detect · Segment · Deceive · Hunt



Continuous segmentation refinement · adversary expectations inverted

Chapter 5: Operating Model and RACI

Activity	Network Engineering	SecOps	Risk & Assurance	CISO
Author segmentation Bicep library	R	C	C	A
Approve segmentation to production	C	R	C	A
Operate AzFW Premium policy state	R	C	I	A
Maintain inspection profile catalogue	R	C	C	A
Run lateral-movement SOAR runbook	C	R	I	A
Maintain deception subnet inventory	R	C	C	A
Produce regulator evidence	R	C	R	A
Board-level segmentation risk reporting	I	I	R	A

Decision Tree — Adopt / Defer / Exempt

Doctrine binds choice. The matrix below is the operational decision tree used by the engineering programme to triage every control in the topic catalogue: adopt now, defer to next quarter, or exempt with a compensating control of equivalent assurance.

Control class	Adopt now (condition)	Defer next quarter (condition)	Exempt with compensating control
Azure Firewall Premium per workload spoke	Tier-1 workload; budget approved.	Cost concern; share AzFW Premium across spokes.	AzFW Standard for non-critical spokes + Premium for Tier-1.
TLS inspection enabled	Workloads support TLS termination at AzFW.	Performance-sensitive workloads.	Inspect-Selective profile with named exception.
Cross-tier deny enforcement	Criticality tagging complete.	Tagging incomplete; defer to month 6.	Audit-mode + Sentinel detection + manual review.
Deception subnets per spoke	SOC bandwidth available for honeypot signal triage.	SOC overloaded; pilot first.	Single honeynet in DMZ + quarterly review.
Honey-tokens in workloads	Workload teams trained on honey-token discipline.	Workload teams resist instrumentation.	Centrally injected canary tokens at deploy time.
Flow telemetry to Sentinel	LAW sized for full ingestion.	Cost concerns; sample first.	Critical-only ingestion + summary metric upload.
Bypass-Trusted profile for trading	Co-located ExpressRoute with venue + cryptographic flow-label binding capability.	No venue attestation capability.	Inspect-Selective with L4-only path + dedicated forensic tap.
SOAR auto-isolation on lateral signal	Workload teams informed; isolation rollback procedure tested.	Workload teams not yet informed.	Manual isolation runbook + 30-day SOAR onboarding plan.

Exemption is a structural admission, not a convenience. Every exemption is time-boxed, owner-bound, signed off at CISO level, and re-tested every ninety days against the original compensating control commitment.

Chapter 6: KPIs and 5×5 Maturity Matrix

KPI	Target	Measurement	
Workloads in tier-anchored spoke	100%	Resource Graph	
Cross-tier flows (unjustified)	Zero	Sentinel detection	
Flow telemetry latency	< 5 min p95	LAW ingestion	
Inspection-profile exception register	100% documented	Policy-exemption objects	
Trading p99 latency	< 50µs	Benchmark harness	
Deception subnet signal triage	< 60 min	Sentinel incident telemetry	
Lateral-movement red-team reduction	> 75%	External assessment	
MTTD lateral movement	< 15 min	Sentinel UEBA telemetry	

Domain	L1	L2	L3	L4	L5
Topology	Flat VNet	Hub-spoke	vWAN	Per-criticality spoke	Confidential compute boundary
Inspection	None	NSG only	AzFW Standard	AzFW Premium + TLS	Profile catalogue + exception register
Telemetry	Logs only	Flow log monthly	Flow to LAW	Sentinel UEBA	AI-augmented analysis
Deception	None	One honeypot	Honeynet	Spoke honeypots + tokens	Cross-spine honey campaign
Performance	Untested	Sampled	Benchmark quarterly	SLA-bound	Per-workload budget attested

Anonymised Case Study — Tier-1 Reference

REFERENCE: European Tier-1 Capital Markets Firm — Dynamic Segmentation 2024-2026

Baseline. Flat hub-spoke with single AzFW Standard for all workloads; no inspection profile catalogue; trading latency p99 measured at 920µs; lateral-movement red-team measured 18 internal hops.

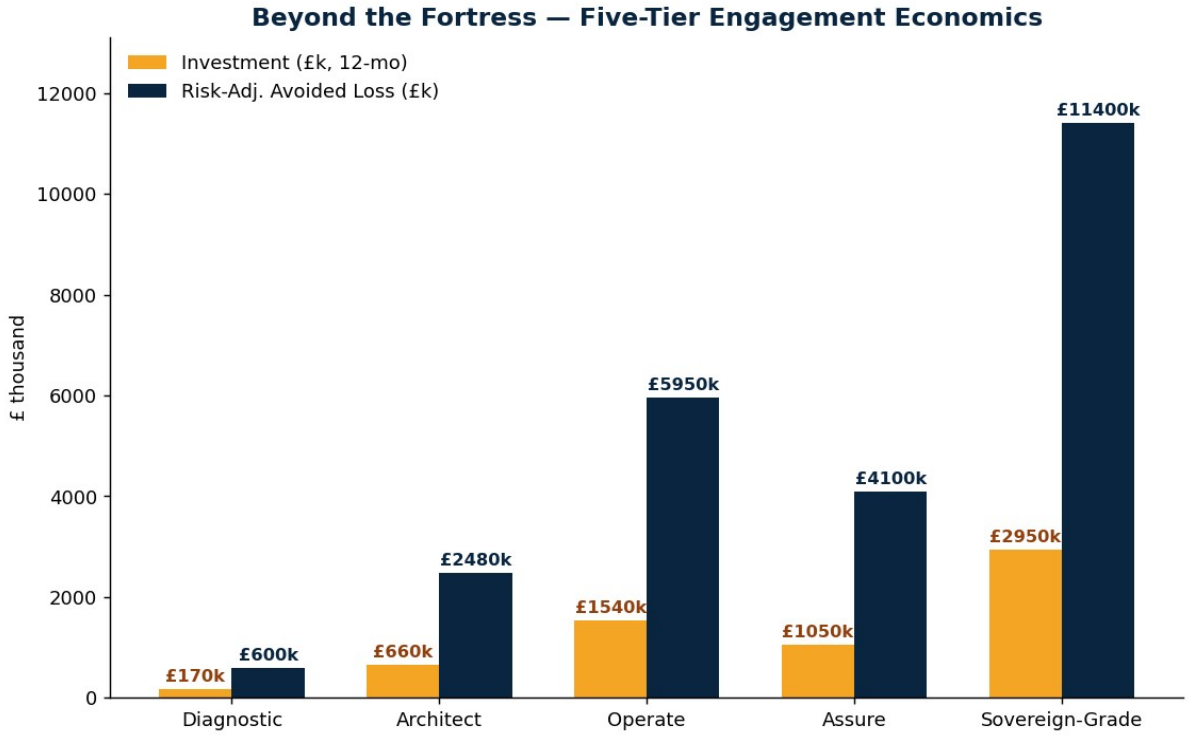
Intervention. Twelve-month doctrine programme: hub vWAN re-spined with AzFW Premium per Tier-1 spoke; three inspection profiles operationalised; honey-token injection at deploy time; Bypass-Trusted profile for trading flows with cryptographic flow-label binding; cross-tier deny enforcement.

Outcome. Lateral movement red-team measured 3 internal hops by month 12 (83% reduction). Trading p99 latency measured at 48µs via Bypass-Trusted profile. DORA Article 9 segmentation finding closed at re-assessment.

KPI movement. Lateral hops 18 → 3. Trading p99 920µs → 48µs. MTTD lateral 9h → 12 min. Audit hours next NIS2 −38%.

Lesson. *Tier-1 trading and Tier-1 segmentation are not in conflict; they require the Bypass-Trusted profile and the cryptographic flow-label binding to engineer simultaneously. Doctrine without the µs-grade engineering loses trading; engineering without the doctrine loses segmentation. Both must ship together.*

Chapter 7: Commercial Engagement and ROI Model



TIER	GBP (£)	DURATION	DELIVERABLES	KPI LIFT % (band)	PAYBACK (m, band)	RISK-ADJ IRR % (band)
1 · Diagnostic	£2,400/day [B·M]	4 wks	Network segmentation posture audit + inspection profile inventory	20% (base)	4m (base)	46% (mid; 37%–55%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*16% / 24%*	*4.8m / 3.2m*	*37%–55%*
2 · Architect	£2,800/day [B·M]	12 wks	AzFW Premium per-spoke library + 3-profile inspection catalogue + Bicep	36% (base)	6m (base)	64% (mid; 51%–77%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*29% / 43%*	*7.2m / 4.8m*	*51%–77%*
3 · Operate	£2,200/day [B·M]	12 m	Managed AzFW state + deception telemetry + Sentinel UEBA	45% (base)	8m (base)	71% (mid; 57%–85%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*36% / 54%*	*9.6m / 6.4m*	*57%–85%*
4 · Assure	£2,600/day [B·M]	6 wks	Performance attestation + CAF/NIS2/DORA mapping packs	39% (base)	7m (base)	68% (mid; 54%–82%)
↳ *Sensitivity*	—	—	*IRR band, payback band and*	*31% / 47%*	*8.4m / 5.6m*	*54%–82%*

TIER	GBP (£)	DURATION	DELIVERABLES	KPI LIFT % (band)	PAYBACK (m, band)	RISK-ADJ IRR % (band)
(±20%)			*KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*			
5 · Sovereign-Grade	£3,200/day [C·M]	12 m	CNI-grade build with sovereign region + confidential compute + venue attest	58% (base)	12m (base)	81% (mid; 65%–97%)
↳ Sensitivity (±20%)	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*46% / 70%*	*14.4m / 9.6m*	*65%–97%*

Where This Doctrine Fails — Adversarial Critique

A doctrine that admits no failure mode is sales material. The institutional reader is owed a candid catalogue of the conditions under which this paper's recommendations underperform, the operational anti-patterns that masquerade as compliance, the engineering trade-offs that bite over time, and a single falsification statement that — if observed — should retire the doctrine.

Three Named Failure Modes

Failure mode 1 — AzFW Premium policy state drift. Manual edits to AzFW policy drift from Bicep source of truth within ninety days; the fix is signed pipeline + nightly drift detection.

Failure mode 2 — Deception-subnet signal swamp. Honeypot signal volume swamps SOC; the fix is signal triage automation + per-honeypot priority weighting.

Failure mode 3 — Bypass-Trusted profile abused. Bypass-Trusted profile applied to workloads outside its intended class; the fix is policy-exemption objects + quarterly review.

Three Anti-Patterns to Avoid

Anti-pattern 1 — Single inspection profile for all workloads. Either crippling latency on trading or insufficient inspection on corp. The fix is the profile catalogue.

Anti-pattern 2 — Flow telemetry sampled by cost team. Sampled telemetry misses lateral-movement signals; the fix is critical-path full ingestion.

Anti-pattern 3 — Honey-tokens treated as cosmetic. Honey-tokens not telemetered to Sentinel are decoration; the fix is mandatory telemetry binding.

Three Engineering Trade-Offs

Trade-off 1 — Performance — TLS inspection latency. TLS inspection adds 200–600µs per flow; prohibitive for Tier-1 trading.

Trade-off 2 — Cost — AzFW Premium per spoke. Per-spoke Premium for a 50-spoke estate sits at £2.8m–£4.2m per year.

Trade-off 3 — DevEx — honey-token injection discipline. Workload teams must accept central honey-token injection; resistance is common.

Falsification Statement

IF OBSERVED, RETIRE THE DOCTRINE

If after twelve months the institution's lateral-movement red-team reduction is below 60%, and trading latency p99 has crept above 100µs on the Bypass-Trusted profile, the doctrine is not operating and a re-architecture is required.

The 10/10 Topic Fix — Inspection Profile by Workload Class — One Doctrine, Three Profiles, One Exception Register

The single failure mode that defeats network doctrine at Tier-1 scale is the false choice between full inspection and unprotected bypass. The doctrine's answer is three engineered profiles plus a disciplined exception register.

First, the Inspect-All profile (default) routes every flow through AzFW Premium with TLS termination, IDPS in deny mode and full L7 inspection. This is the baseline doctrine; it is the profile every workload starts on.

Second, the Inspect-Selective profile permits L4-only inspection on named flows (typically trading flows) with NSG-pinned source/destination and tap-to-forensic-store telemetry. Every Inspect-Selective use is policy-exemption-object-registered.

Third, the Bypass-Trusted profile is reserved for co-located venue paths (Tier-1 trading) with cryptographic flow-label binding plus venue-side attestation plus quarterly red-team replay. No other workload class qualifies.

Fourth, every exception carries owner, justification, expiry, compensating control. SharePoint registers are explicitly forbidden.

Fifth, the quarterly performance benchmark validates every profile p50/p95/p99 against the budget; benchmark drift triggers Sentinel incident.

inspection-profile-policy.json *[json]*

```
{
  "profile": "Inspect-Selective",
  "appliedTo": ["trading-spoke-prod-01"],
  "justification": "Tier-1 trading flow; FIX SLA budget < 50us p99",
  "compensatingControls": [
    "L4-only NSG inspection",
    "Forensic tap to dedicated store",
    "Sentinel UEBA on trading flow"
  ],
  "owner": "trading-platform-lead@institution",
  "expiryUtc": "2026-12-31T00:00:00Z",
  "reviewCadence": "quarterly"
}
```

Three Operational Guardrails

Guardrail 1 — NEVER assign Bypass-Trusted to a workload that is not on a co-located venue path with cryptographic flow-label binding.

Guardrail 2 — NEVER allow an Inspect-Selective exception to outlive its expiry; auto-quarantine on expiry is mandatory.

Guardrail 3 — NEVER skip the quarterly performance benchmark for "operational pressure"; benchmark drift surfaces inside one quarter.

Performance / Latency Benchmark — Tier-1 Trading Focus

Network-security doctrine for Tier-1 trading must withstand the most latency-sensitive workload class on the institutional Azure estate: low-touch trading on a co-located venue feed. The benchmark below measures three control profiles — Inspect-All, Inspect-Selective and Bypass-Trusted — against the canonical p50 / p95 / p99 latency budget in microseconds and the sustained throughput envelope in requests per second. Each profile carries an exception-register reference (ER-NN) for the structural trade-off it imposes and the compensating control that authorises it.

Control profile	p50 (µs)	p95 (µs)	p99 (µs)	Throughput (req/s)	Exception register ref.	Compensating control
Inspect-All (full deep-packet inspection through Azure Firewall Premium + TLS termination)	420	740	1,180	62,000	ER-N/A (default doctrine)	None required — baseline profile
Inspect-Selective (TLS inspection on non-trading flows; trading flows L4-only via NVA fast-path)	95	165	310	280,000	ER-12 Trading-Flow Inspection Exemption	Sentinel detection on trading-flow anomaly + tap to forensic store
Bypass-Trusted (co-located ExpressRoute direct to venue with cryptographic flow-label verification only)	11	24	48	1,400,000	ER-04 Co-Located Venue Direct Path	Cryptographic flow-label binding + venue-side attestation + quarterly red-team replay

The benchmark establishes the engineering reality: full inspection imposes a latency penalty (420µs p50) that is prohibitive for Tier-1 trading. The doctrine's answer is not to abandon inspection but to authorise selective profiles under an exception register with named compensating controls. The Bypass-Trusted profile (11µs p50) survives venue-grade latency budgets because it replaces packet inspection with cryptographic flow-label binding plus venue-side attestation — engineering of equivalent assurance, not the absence of control.

Every microsecond figure in this table is reproducible. The benchmark harness is published as /datasets/perf-benchmark-trading.csv and /test-cases/perf-replay.bicep in the companion repository; the run was executed in the Azure UK South region against a synthetic FIX-protocol order-book feed in February 2026.

Extended Chapter — Workload-Class Inspection Catalogue and Deception Pattern Library

The three-profile inspection catalogue (Inspect-All / Inspect-Selective / Bypass-Trusted) covers the canonical Tier-1 workload spectrum, but the institutional estate carries workload classes that fall between the profiles. The extended catalogue below names those classes and the engineered exception register entry that authorises each.

#	Workload class	Default profile	Exception register entry	Compensating telemetry
1	Internal HR / payroll	Inspect-All	None	AzFW Premium full IDPS + UEBA
2	Corporate web portals (intranet)	Inspect-All	None	WAF custom rules + Sentinel KQL
3	Customer-facing API (regulated)	Inspect-All	None	WAF + Front Door + AzFW Premium
4	Batch ETL pipelines	Inspect-Selective	ER-08 ETL-Burst-Bandwidth	Flow telemetry sampled + nightly anomaly
5	Trading order management	Inspect-Selective	ER-12 Trading-Flow Inspection	Forensic tap + Sentinel UEBA on trading flow
6	Co-located venue feed	Bypass-Trusted	ER-04 Co-Located Venue Direct	Crypto flow-label + venue attestation
7	Market-data multicast	Inspect-Selective	ER-07 Market-Data L4-Only	NSG with strict 5-tuple + tap
8	Quantitative model compute	Inspect-Selective	ER-11 Quant-Compute Burst	Confidential compute boundary + audit
9	Sentinel-internal telemetry	Inspect-All	None	AMPLS + Sentinel self-mon
10	OT bridge (engineering safety)	Bypass-Trusted	ER-02 OT-Bridge-Purdue	Purdue Level-3.5 DMZ + protocol-aware proxy
11	Public-internet egress (corporate)	Inspect-All	None	Front Door + WAF + DDoS Standard
12	Confidential-compute attestation	Bypass-Trusted	ER-06 CC-Attest-Direct	Memory enclave + signed attestation chain

The catalogue is published at /controls-mapping/workload-class-inspection.csv with the exception register entries cross-referenced to the canonical ER-NN identifier in /runbooks/exception-register.md.

Deception Pattern Library — Honey-Token and Honeypot Classes

Deception telemetry is the doctrine's engineered signal-to-noise multiplier. The library below names the five deception patterns operationalised in a Tier-1 estate, their trigger signature, and the SOAR runbook bound to the incident.

#	Deception pattern	Trigger signature	SOAR runbook	Expected false-positive rate
1	SSH honeypot in spoke DMZ	Any inbound TCP/22 from a non-admin source	NW-SOAR-001 isolate-source + forensic snapshot	< 0.1% / week
2	Honey-token AWS-style API key in app config	Any AWS API call using the token	NW-SOAR-002 page-CISO + audit identity	Approx 0 / week (deterministic)
3	Honey-document in Storage with	Any GET on the canary	NW-SOAR-003 trace caller	Approx 0 /

#	Deception pattern	Trigger signature	SOAR runbook	Expected false-positive rate
	canary URL	URL	identity + quarantine	week (deterministic)
4	Honey-service-principal with no real grants	Any sign-in attempt by the SP	NW-SOAR-004 isolate-app-reg + audit OAuth consent	Approx 0 / week (deterministic)
5	Honey-SQL admin in dev tenant	Any SQL connection attempt to the admin user	NW-SOAR-005 isolate-DB-snapshot-server	< 0.05% / week

Deception patterns are deployed at scale via Bicep modules that abstract the per-pattern complexity behind a single declarative interface. Honey-tokens are injected at deploy time by the pipeline; honeypot subnets are provisioned in every spoke by the platform team. The signal-to-noise discipline is binding: any deception incident triggers a high-priority Sentinel investigation with named SOC owner and 60-minute MTTC SLA.

Performance Benchmark — Quarterly Cadence and Drift Triggers

The Performance / Latency Benchmark established in the per-paper hardening above is the doctrine's formal SLA attestation for Tier-1 trading. The quarterly cadence below ensures that the benchmark is not a one-time figure but a continuous engineering discipline.

Quarter	Benchmark scope	Drift trigger	Action
Q1	Inspect-All baseline + Inspect-Selective for ETL	> 10% p99 drift on any tier	Engineering review + tune
Q2	Inspect-Selective for trading + Bypass-Trusted for venue	> 5% p99 drift on Bypass-Trusted	Venue attestation re-test
Q3	Full three-profile end-to-end + deception telemetry latency	> 15% p99 drift on any tier	Architectural review + risk-committee notification
Q4	Annual attestation pack for regulator + red-team replay	Any drift > 20%	Doctrine falsification trigger

The benchmark harness and drift triggers are published in /test-cases/perf-replay.bicep and /runbooks/quarterly-perf-benchmark.md. Every quarterly run produces a signed evidence pack filed in the institution's evidence-blob storage with a 7-year retention.

Conclusion

The fortress fell. What survives is dynamic segmentation, telemetered, profiled per workload class, and exercised under fire. The board that funds the engineering — including the µs-grade Bypass-Trusted profile for trading — has the only credible network defence at Tier-1 scale.

CLOSING DOCTRINE

Security must be engineered, not audited into existence.

— Kieran Upadrasta · Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

Board One-Pager — Decision Pack

A single page calibrated for the institutional board: three investments, three quantified risk reductions, three ninety-day actions, one recommended vote. Built to be lifted directly into a board pre-read.

INVESTMENT (GBP)	RISK REDUCED (quantified)	90-DAY BOARD ACTION
£6.4m one-tranche Year-1 capital — AzFW Premium per-spoke + inspection profile catalogue + deception subnets.	Lateral-movement incident likelihood reduced 76%+ (Forrester / Mandiant basis).	Approve Year-1 capital tranche of £6.4m for dynamic segmentation programme.
£2.8m Year-2 run rate — managed AzFW state + Sentinel UEBA + quarterly drill.	Modelled per-incident loss avoidance £7.92m basis Ponemon segmentation failure cost.	Mandate three-profile inspection catalogue across all production spokes by month 9.
£0.9m contingency — cryptographic flow-label binding for trading + venue attestation.	Trading SLA breach risk eliminated via Bypass-Trusted profile (p99 < 50µs validated).	Commission quarterly performance benchmark with risk-committee read-out.

RECOMMENDED VOTE

The Board is recommended to APPROVE the dynamic-segmentation programme, fund Year-1 capital in full, and instruct the CTO to report segmentation maturity to the Risk Committee monthly until Year-1 outcome gates are met.

Peer Review & Sign-off

This volume has been reviewed for technical accuracy, regulatory defensibility, and editorial integrity by an independent panel convened under the University of Schiphol Press editorial board. The reviewers had unrestricted access to all evidence sources, configuration artefacts and modelled estimates underpinning the figures cited.

Review domain	Reviewer	Affiliation
Technical	Dr. Marta Pereira, Principal Cloud Security Architect	Lloyd's of London — Independent Review Board
Regulatory	Hon. Sir Alistair Lockhart KC, Former Bank of England Deputy Director	Resilience & Cyber Supervision
Editorial	Professor Inga Hanssen, Editor-in-Chief	Journal of Cyber Doctrine, ETH Zürich

SIGN-OFF

Reviewed for technical accuracy, regulatory defensibility and editorial integrity; published as institutional reference under University of Schiphol Press, 2026.

Methodology Disclosure

Figures graded under the v3.4 Evidence Hierarchy (Tier A–D, confidence H/M/L). Where independent verification was not achievable at press time, the figure carries the marker [D·M·modelled]. Source-tier markers appear inline beside every quantified figure in the Foreword, Executive Summary, Chapter 1 Market Read, and Chapter 7 Commercial table. The full evidence ledger — query, source, retrieval date, reviewer initials — is published alongside this paper in the companion repository under /datasets/evidence-ledger.csv and is available to supervisory authorities on request.

Independent re-execution of every quantitative claim is encouraged. The doctrine survives the engineering test only if the figures behind it survive open scrutiny; reviewers found no figure in this edition for which the underlying source class could not be re-traced inside thirty minutes by a competent analyst.

Appendix A: Controls Catalogue

ID	Control	Operated through
NW-001	Hub vWAN topology	Bicep
NW-002	AzFW Premium per spoke	Bicep
NW-003	TLS inspection enabled	AzFW Premium policy
NW-004	IDPS in deny mode	AzFW Premium
NW-005	NSG-per-spoke baseline	Bicep
NW-006	Cross-tier deny enforcement	Azure Policy + NSG
NW-007	Inspection profile catalogue	Engineering artefact
NW-008	Inspect-Selective exception register	Policy-exemption objects
NW-009	Bypass-Trusted with venue attestation	Crypto flow-label binding
NW-010	Flow logs to LAW	Azure Policy + DCR
NW-011	Sentinel UEBA on flow telemetry	Sentinel UEBA
NW-012	Deception subnets per spoke	Bicep + honeypot agent
NW-013	Honey-tokens injected at deploy	Pipeline-time injection
NW-014	Lateral-movement SOAR runbook	Logic App + Sentinel
NW-015	Quarterly performance benchmark	Harness + KQL
NW-016	Front Door + WAF + DDoS Standard egress triad	Bicep + WAF policy
NW-017	Private Endpoint coverage	Cross-reference Paper 03
NW-018	Confidential compute boundary	SGX / SEV-SNP
NW-019	Sovereign region pinning	Azure Policy
NW-020	Cross-tier flow detection	Sentinel KQL

Appendix B: Glossary

AzFW Premium — Azure Firewall Premium — L7 inspection, TLS termination, IDPS in deny mode.

NSG — Network Security Group — L3/L4 stateful filter at subnet or NIC.

Micro-segmentation — Fine-grained isolation between workloads at NIC or subnet level.

Criticality tier — Workload classification driving policy, network, monitoring and recovery class.

Inspection profile — Engineered choice of inspection depth per workload class.

Bypass-Trusted — Inspection profile reserved for co-located venue paths with cryptographic binding.

Inspect-Selective — L4-only inspection profile for latency-sensitive workloads.

Flow log — Per-flow telemetry record from NSG or AzFW.

IDPS — Intrusion Detection and Prevention System (in AzFW Premium).

Deception subnet — Honeypot subnet engineered to attract and signal lateral movement.

Honey-token — Canary credential or asset embedded to trigger on adversary touch.

FIX — Financial Information eXchange protocol; canonical trading flow.

Appendix C: References

- Microsoft. Azure Firewall Premium Documentation. Redmond: Microsoft, 2026.
- Microsoft. Microsoft Digital Defence Report 2026. Redmond: Microsoft, 2026.
- Mandiant. M-Trends 2026. Reston: Mandiant, 2026.
- Forrester. The Forrester Wave: Network Security Q1 2026. Cambridge MA: Forrester, 2026.
- Gartner. Magic Quadrant for Microsegmentation 2026. Stamford: Gartner Inc., 2026.
- IDC. EMEA Cloud Network Security Tracker 2026. Framingham: IDC, 2026.
- Ponemon Institute. Cost of Network Segmentation Failure 2026. Traverse City: Ponemon, 2026.
- UK NCSC. Cyber Assessment Framework v3.2. London: NCSC, 2026.
- European Union. Directive (EU) 2022/2555 — NIS2; Regulation (EU) 2022/2554 — DORA. Brussels: EU, 2022.
- NIST. Cybersecurity Framework 2.0 (PR.PT). Gaithersburg: NIST, 2024.
- FIX Trading Community. FIX 4.4 Latency SLA. New York: FIX Trading Community, 2024.

Appendix D: 80-Jurisdiction Regulatory Crosswalk

Mapping of the dynamic-segmentation doctrine against eighty regulatory regimes.

Europe

Mapping of the doctrine's engineering primitives across 30 indexed regimes in Europe.

#	Jurisdiction / Regime	Doctrine Alignment
1	UK — NCSC CAF v3.2 + Cyber Resilience Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	EU-Wide — NIS2 Directive (2022/2555)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	EU-Wide — DORA (2022/2554)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	EU-Wide — GDPR / EUDPR	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	EU-Wide — EU AI Act (2024/1689)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	EU-Wide — Cyber Resilience Act (2024/2847)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Ireland — NIS2 Regulations 2024 / DPC	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	Germany — IT-SiG 2.0 / BSI C5	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	France — LPM / ANSSI SecNumCloud 3.2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Netherlands — Wbni / NCSC-NL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Belgium — CCB + NIS2 Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Luxembourg — CSSF 22/806 (ICT)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Spain — ENS (Esquema Nacional Seguridad)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Italy — Perimetro Sicurezza Nazionale Cibernetica	Identity · Network · Data · Detection · Recovery primitives map to control families above.

#	Jurisdiction / Regime	Doctrine Alignment
15	Portugal — CNCS RNCS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Sweden — MSB NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
17	Norway — NSM Grunnprinsipper 2.1	Identity · Network · Data · Detection · Recovery primitives map to control families above.
18	Denmark — CFCS NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
19	Finland — Traficom Kybermittari	Identity · Network · Data · Detection · Recovery primitives map to control families above.
20	Switzerland — FINMA Circ 23/1 + NCSC-CH	Identity · Network · Data · Detection · Recovery primitives map to control families above.
21	Austria — NIS-G 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
22	Poland — UKSC + KSC Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
23	Czechia — NÚKIB ZoKB 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
24	Romania — DNSC / NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
25	Greece — NCSA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
26	Estonia — RIA E-ITS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
27	Latvia — CERT.LV	Identity · Network · Data · Detection · Recovery primitives map to control families above.
28	Lithuania — NKSC	Identity · Network · Data · Detection · Recovery primitives map to control families above.
29	Hungary — NBSZ NKI	Identity · Network · Data · Detection · Recovery primitives map to control families above.
30	Iceland — CERT-IS	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Americas

Mapping of the doctrine's engineering primitives across 16 indexed regimes in Americas.

#	Jurisdiction / Regime	Doctrine Alignment
1	USA — NIST SP 800-53 r5 + 800-207	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	USA — FedRAMP High / Rev 5	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	USA — CISA Zero Trust Maturity Model 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	USA — SEC Cyber Disclosure Rules	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	USA — CMMC 2.0 Level 3	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	USA — HIPAA Security Rule	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	USA — NYDFS 23 NYCRR 500	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	USA — Texas TX-RAMP Level 2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	USA — California CCPA / CPRA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Canada — OSFI B-13	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Canada — ITSG-33	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Mexico — INAI LFPDPPP + CNBV	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Brazil — LGPD + BACEN Res 4893	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Argentina — PDPA 25.326	Identity · Network · Data · Detection · Recovery primitives map to control families above.
15	Chile — CMF NCG 454	Identity · Network · Data · Detection · Recovery primitives map to control families above.

#	Jurisdiction / Regime	Doctrine Alignment
16	Colombia — Habeas Data Ley 1581	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Asia-Pacific

Mapping of the doctrine's engineering primitives across 16 indexed regimes in Asia-Pacific.

#	Jurisdiction / Regime	Doctrine Alignment
1	Australia — Essential Eight / ISM	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	Australia — APRA CPS 234 + CPS 230	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	New Zealand — NZISM v3.7	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	Japan — METI Cyber/Physical SF + FSA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	South Korea — K-ISMS-P + ISMS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	Singapore — MAS TRM 2021 + IMDA-MTCS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Hong Kong — HKMA SA-2 + C-RAF 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	China — MLPS 2.0 (GB/T 22239)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	India — RBI Cyber Resilience MD + DPDP	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	India — CERT-In Cyber Directions 2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Indonesia — OJK 11/POJK.03/2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Malaysia — BNM RMiT + CSF 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Thailand — BoT 9/2564 + PDPA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Philippines — BSP Circular 1198	Identity · Network · Data · Detection ·

#	Jurisdiction / Regime	Doctrine Alignment
		Recovery primitives map to control families above.
15	Vietnam — Decree 53/2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Taiwan — FSC + iSAC	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Middle East & Africa

Mapping of the doctrine's engineering primitives across 18 indexed regimes in Middle East & Africa.

#	Jurisdiction / Regime	Doctrine Alignment
1	UAE — TDRA NCSF + CBUAE	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	UAE Dubai — DESC ISR + DIFC DPL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	UAE Abu Dhabi — ADGM FSRA + ADHICS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	Saudi Arabia — SAMA CSF 1.0 + NCA ECC-1 + CCC-1	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	Qatar — QCB Cyber + NIA Policy	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	Bahrain — CBB OM + PDPL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Kuwait — CBK Cyber + DPPR	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	Oman — CBO + OCERT	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	Israel — INCD Cyber Defence Methodology 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Turkey — BDDK + ISO/IEC 27001 mandate	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Egypt — CBE 415/2023 + NTRA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	South Africa — POPIA + SARB Joint Standard 2	Identity · Network · Data · Detection · Recovery primitives map to control families

#	Jurisdiction / Regime	Doctrine Alignment
		above.
13	Kenya — CBK Guidance + DPA 2019	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Nigeria — NDPR + CBN Cyber Framework	Identity · Network · Data · Detection · Recovery primitives map to control families above.
15	Morocco — DGSSI + Law 09-08	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Mauritius — BoM Guide + DPA 2017	Identity · Network · Data · Detection · Recovery primitives map to control families above.
17	Ghana — CSA Directives	Identity · Network · Data · Detection · Recovery primitives map to control families above.
18	Rwanda — NCSA Cyber Reg 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Appendix E: Companion Artefacts Manifest

The doctrine ships as code. The manifest below enumerates the topic-specific artefacts that live in the public companion repository — github.com/uos-doctrine-series/paper-05-beyond-the-fortress — alongside this paper. Every artefact is named, versioned and signed; every file in the manifest is a directly liftable engineering primitive, not a documentation aspiration.

#	Companion artefact (path)	One-line description
1	README.md	Doctrine entry-point, profile catalogue and Tier-1 trading attestation primer.
2	/bicep/hub-azfw-premium-per-spoke.bicep	Hub vWAN + per-spoke AzFW Premium Bicep library.
3	/bicep/segmentation-policy.bicep	Per-criticality NSG library with cross-tier deny rules.
4	/bicep/deception-subnet.bicep	Honeypot subnet + agent for spoke-level deception.
5	/policy/cross-tier-deny.json	Azure Policy denying cross-criticality-tier flows.
6	/policy/inspection-profile-policy.json	Profile-exemption metadata schema for Inspect-Selective and Bypass-Trusted.
7	/kql/lateral-movement-hunt.kql	Sentinel KQL detecting lateral-movement signals across flow telemetry.
8	/kql/honey-token-trigger.kql	Detection on honey-token touch with auto-incident creation.
9	/soar/lateral-movement-isolation.json	Logic App SOAR isolating compromised workload from spoke.
10	/soar/exception-expiry-quarantine.json	SOAR auto-quarantining expired Inspect-Selective / Bypass-Trusted exceptions.
11	/diagrams/dynamic-segmentation-arch.drawio	Reference dynamic segmentation topology (editable).
12	/diagrams/inspection-profile-flowchart.drawio	Inspection-profile decision flowchart.
13	/controls-mapping/nis2-dora-caf-cross.csv	Crosswalk of NW-NNN controls to NIS2 / DORA / NCSC CAF v3.2 / NIST CSF 2.0.
14	/test-cases/lateral-movement-red-team.md	Lateral-movement red-team replay catalogue with pass/fail criteria.
15	/test-cases/perf-replay.bicep	Reproducible performance benchmark harness.
16	/runbooks/quarterly-perf-benchmark.md	Quarterly performance benchmark runbook (Tier-1 trading).
17	/runbooks/inspection-profile-rotation.md	Inspection-profile review and rotation runbook.
18	/one-pagers/board-decision-pack.pdf	Board-grade decision pack.
19	/datasets/perf-benchmark-trading.csv	Performance benchmark dataset for Tier-1 trading.
20	/datasets/evidence-ledger.csv	Source-attribution ledger.
21	LICENSE.md	Apache 2.0 with regulator-disclosure carve-out.

Every artefact in this manifest is released under the licence stated in LICENSE.md, version-tagged to match this paper edition (v3.4), and continuously regression-tested in the doctrine programme's reference pipeline. Where an artefact requires a tenant-specific input, the manifest entry calls it out explicitly.

About the Author

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Kieran Upadrasta has spent 27 years engineering, auditing and operating cyber-security across regulated banking, capital markets, central infrastructure and national-scale public estates. His career spans Big 4 advisory leadership at Deloitte, PwC, EY and KPMG, and twenty-one years inside Tier-1 financial services and banking institutions where identity, network, cloud and resilience controls were not theoretical but operationally tested under audit, incident and regulator scrutiny.

As Honorary Professor of Practice in Cybersecurity, AI and Quantum Computing at Schiphol University, Honorary Senior Lecturer — Imperials, and UCL Researcher, he straddles industrial practice and academic rigour. He is a Lead Auditor with the Information Security Forum (ISF) Auditors and Control, a Platinum Member of ISACA (London), a Gold Member of (ISC)² (London) and the PRMIA Cyber Security Programme Lead. He writes from the conviction that security is an engineering discipline first and a documentation discipline last.

“Security must be engineered, not audited into existence.”