Securing Cairn Housing Association

The Managed SOC & SIEM Service Blueprint

A structural specification for 24x7x365 Microsoft-native threat detection, automated response, and comanaged governance.

March 2026

The Executive Mandate

Procure a fully managed 24x7x365 SOC and SIEM service operating in a co-managed model for a Microsoft-only cloud environment.

The Tech
Microsoft Sentinel Native (Leveraging existing M365 E5 licensing).

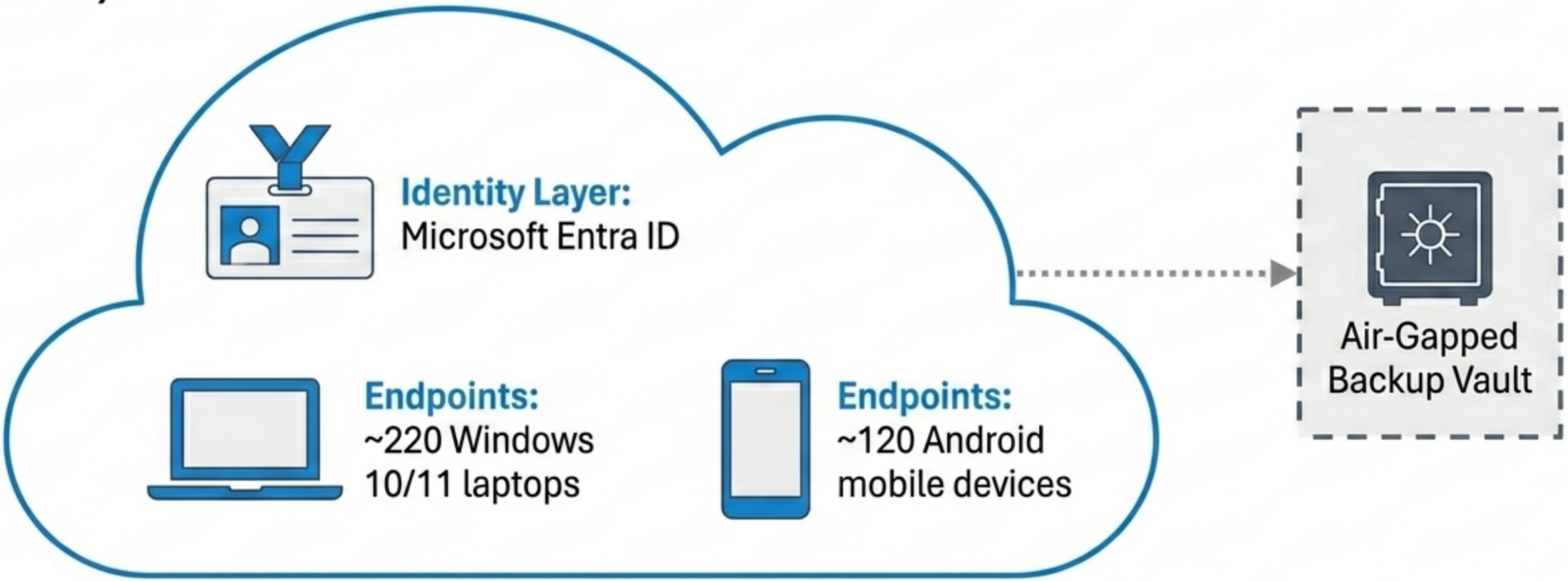
The Term
3-Year Initial Contract (+ Optional 4th Year).

The Budget Constraint
Under £30,000 per annum (Max £90,000 for the initial 3-year term).

PROJECT:	DRAWING TITLE:	REVISION:	DRAWN BY:	SIGNATURE:	DRAWING NO.:
Managed SOC/SIEM Service Procurement	Executive Mandate & Core Requirements	A	Security Architect		SL-001
		DATE: 2024-10-26	APPROVED BY: Executive Board		

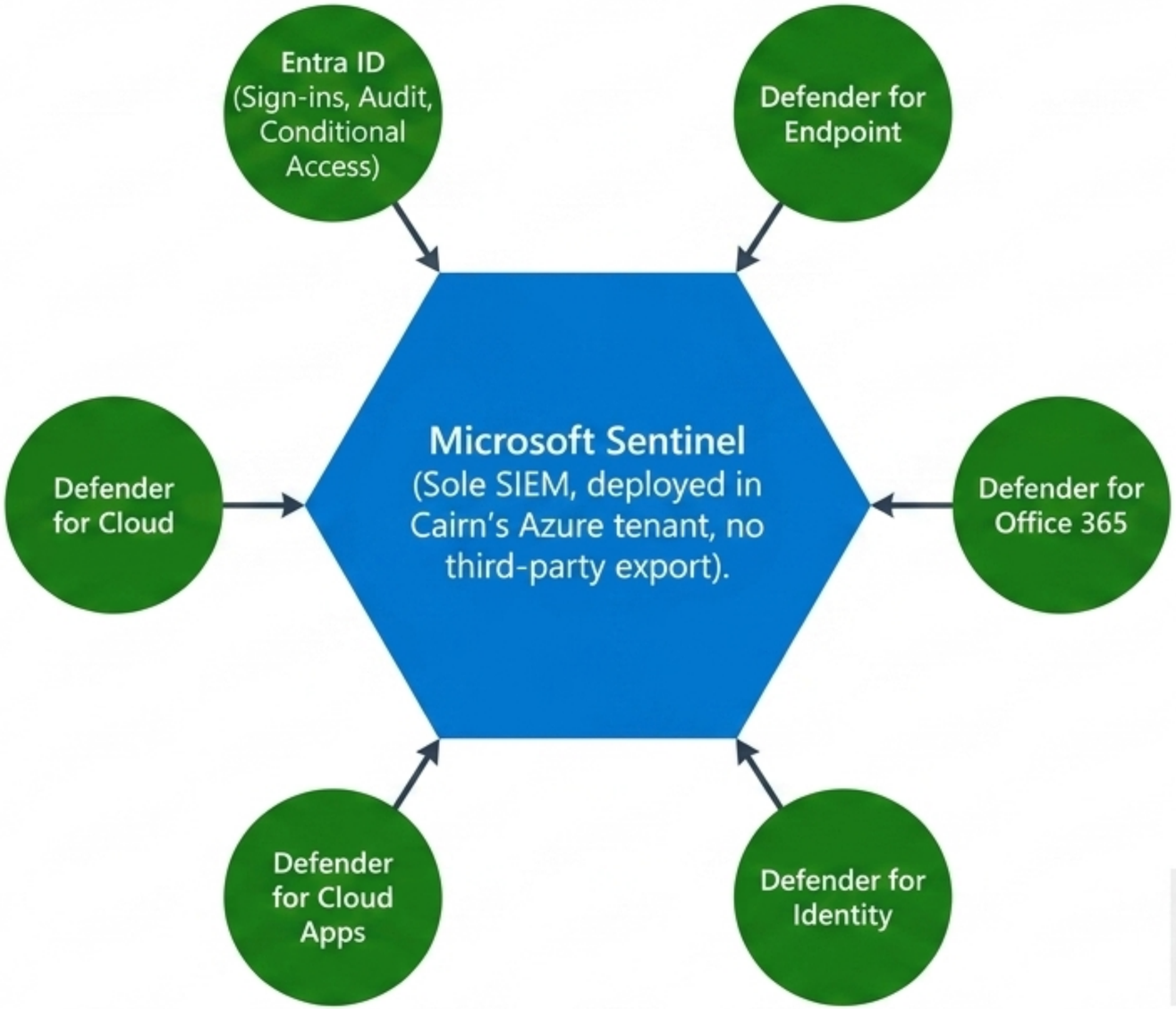
The Operational Topography

100% Cloud-Only Infrastructure (No on-premises footprint, PaaS SQL Server).



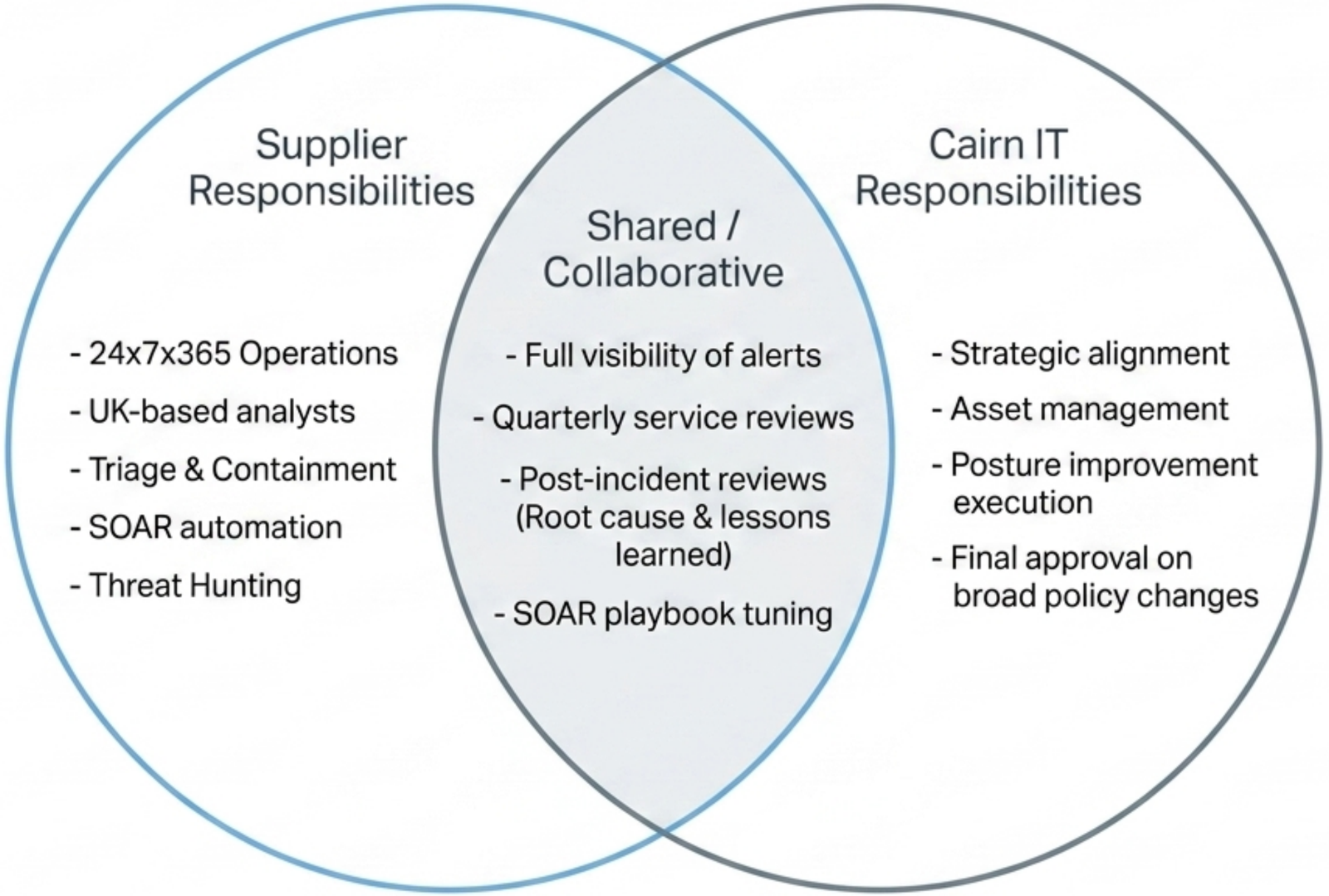
Boundary Rule: Non-Microsoft SIEM platforms and non-native security tooling are strictly out of scope.

The Technology Engine: Maximizing E5 Value



Compliance Constraint: Must support FOISA-compliant record keeping (Data sovereignty retained).

The Co-Managed Operating Model



Human Accessibility: The Anti-Call-Center Model

The Rejected Model

- Ticket-only communication
- Queue-based call handling
- Call-center style front ends
- Outsourced offshore tiers

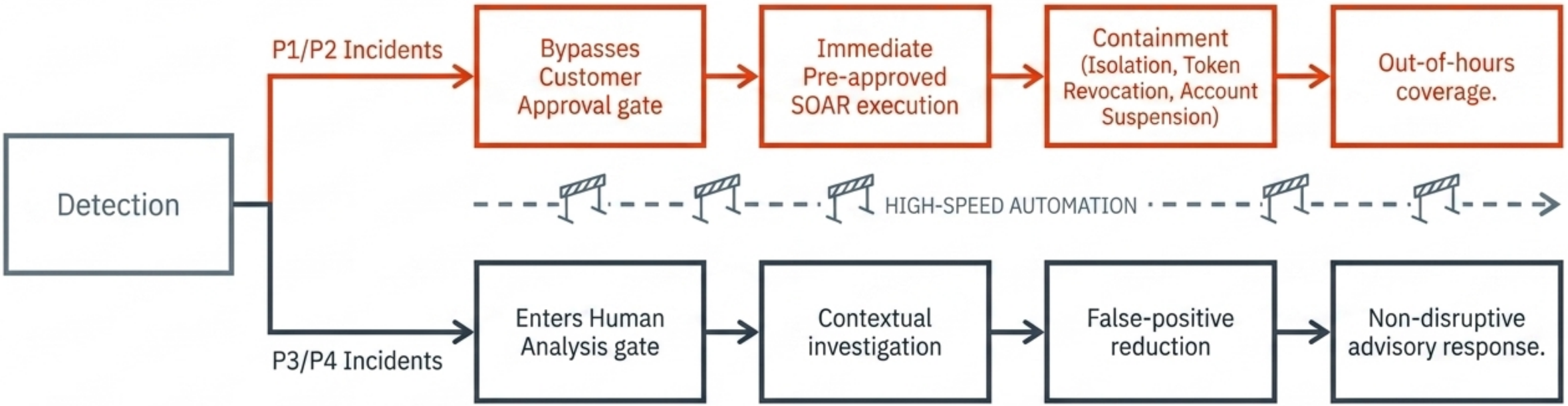
The Required Model

- **Direct and timely access to appropriately skilled human SOC analysts.**
- **Direct engagement within 30/60 minutes for P1/P2 incidents.**
- **Named Service Manager available during UK business hours (same-day response).**
- **Proactive collaboration as an extension of the Cairn IT team.**

The Incident Classification & Response Matrix

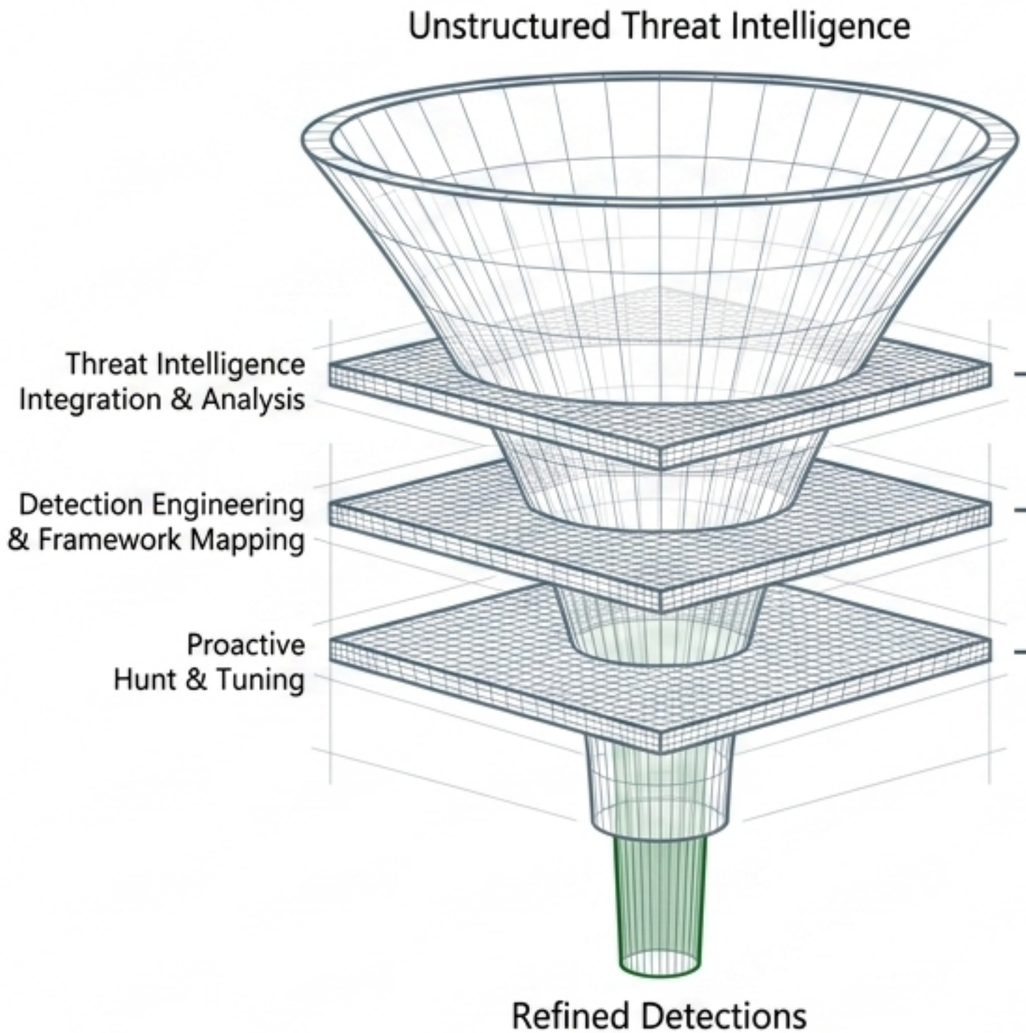
Priority	Definition	Triage SLA	Initial Response / Action SLA
P1 - Critical	Active compromise, ransomware, exfiltration	10 mins	30 mins (Immediate SOAR Execution, no approval needed).
P2 - High	Confirmed malware, high-risk suspicious behavior	30 mins	60 mins (Automated or analyst-led containment).
P3 - Medium	Low-risk/blocked malicious activity	4 hours	8 hours (Investigation/Tuning, non-disruptive).
P4 - Informational	Benign alerts, advisory events	24 hours	48 hours closure.

Automated Response (SOAR): The Defend-First Mandate



Mandatory Playbook Coverage: Compromised user, Endpoint isolation, Malicious email containment, Ransomware indicators.

Proactive Security: Threat Hunting & Detection Engineering



Engineering SLA

New KQL detections deployed within 5 working days of approval. False positives tuned within 10 working days.

Framework Alignment

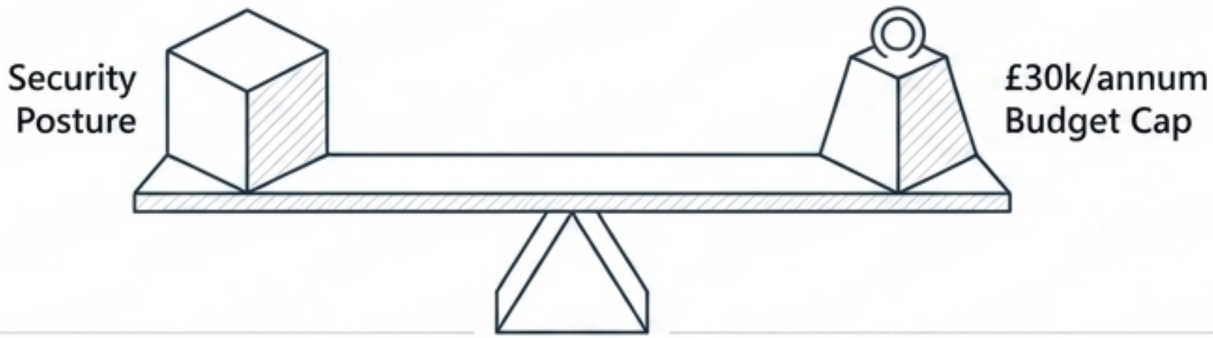
100% of new detections mapped to the MITRE ATT&CK framework within 5 days.

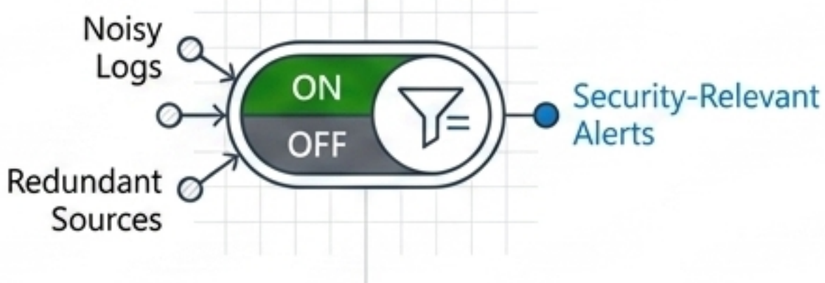
Hunting Cadence

Minimum of 1 proactive hunt per month (identity- and endpoint-centric), yielding documented findings.

The Cost Optimization Engine

Managing Sentinel ingestion dynamically without sacrificing visibility.





Lever 1: Tiered Storage Architecture

Strategic utilization of Basic Logs, Archive tiers, and Pay-As-You-Go models to minimize static costs.

Lever 2: Telemetry Culling

Reduction of noisy/redundant log sources; ingesting only security-relevant alerts from external SaaS platforms (e.g., backup).

Lever 3: Active Governance

Monthly cost reviews, investigation of ingestion spikes within 24 hours, and optimization actions applied within 10 days.

Service Level Agreements: Operations & Availability

Uptime

99.9% SOC operational availability (24x7x365).

Telemetry Health

>98% healthy ingestion status for all Microsoft Defender and Sentinel connectors.

Ingestion Alerting

Sentinel ingestion failures detected and alerted within 15 minutes.

Communication Pulse: Customer notified within 60 mins (P1) or 90 mins (P2). P1/P2 cases updated every 30 minutes until contained.

Service Level Agreements: Governance & Reporting

Post-Incident Rhythm

Post-Incident Reviews (PIR): Delivered within 5 working days for P1; 10 working days for P2.

Monthly Rhythm

Service reports (volumes, trends, SLAs) delivered within 5 working days of month-end.

Quarterly Rhythm

Service review meetings within 10 working days of quarter-end.

Comprehensive SOAR playbook reviews.

Roadmap and improvement planning updated.

Evidence Retention: All case evidence retained for a minimum of 12 months (or per regulatory requirement).

Legal & Compliance Context: Scots Law & Public Procurement

The Framework

Devolved Scottish authorities are governed by the Procurement Reform (Scotland) Act 2014 and Public Contracts (Scotland) Regulations 2015.

The Impact

Affects contractual interpretation, remedies, audit rights, and accountability in ways distinct from England and Wales.

FOISA Compliance

The Freedom of Information (Scotland) Act requires robust, auditable incident handling and compliant data residency. Logs must be highly retrievable.

Data Protection

Least-privilege access and strict adherence to UK data protection legislation.

Onboarding & Implementation Roadmap

Workshops to map environment, align playbooks, and define exact escalation matrices.

Enablement of Microsoft Sentinel and data connectors.

Building and documenting mandatory automated playbooks.

Conducting simulated P1/P2 scenarios to prove Defend-First mechanisms.

Transition to 24x7x365 active monitoring.

The Deliverables Summary

Operational Capability

- [x] Fully implemented Microsoft Sentinel SIEM architecture.
- [x] 24x7x365 managed SOC service (UK-based analysts).
- [x] Automated P1/P2 SOAR playbooks (Defend-First).
- [x] Documented runbooks and escalation matrices.

Governance & Posture

- [x] Proactive KQL threat hunting (Monthly).
- [x] Monthly and quarterly service reporting.
- [x] Sentinel cost optimization management.
- [x] Continuous knowledge transfer and collaborative posture improvement.