

Service Definition

Security Engineering Tooling Setup, Automation, and Detection Engineering Support (Lot 3 – Cloud Support)

1. What the service is

A hands-on security engineering service to help you deploy, configure, and automate security tooling, and to build practical detection and response capabilities. We work with your security and IT teams to design secure configurations, implement alert logic, and create automated workflows for triage and user communications.

Typical use cases include: endpoint privilege management rollouts, SaaS security posture monitoring (CSPM) deployments, alerting and automation improvements, detection engineering, and operationalising log analysis to reduce risk and response time.

2. What's included

Security tooling design and deployment (as applicable to scope):

- Secure configuration design for selected security platforms and integrations
- Deployment planning (phased rollout, pilot groups, rollback approach)
- Role-based access control and least-privilege administration design
- Configuration baselining and hardening aligned to operational requirements
- Support for stakeholder workshops (Security, IT, Service Owners, Business)

Detection engineering, alerting, and automation (as applicable to scope):

- Creation of security alerts based on defined use cases and telemetry sources
- Alert tuning to reduce false positives and improve signal quality
- Automated alerting workflows (routing, enrichment, escalation logic)
- Automated user communications triggered by detections (e.g. email notifications)
- Log analysis support to validate detections and identify patterns of risk
- Runbooks and triage guidance to support consistent operational response

Example Deliverables:

- Executive summary of key risks, priorities, and decisions required

- Security tooling design pack (configuration intent, scope, and access model)
- Alert catalogue (use cases, severity, triggers, and response actions)
- Automation workflows (user comms triggers, escalation paths, runbooks)
- Rollout plan (phasing, pilot approach, testing and rollback steps)
- Handover notes and operational guidance for BAU support

3. Data backup/restore and disaster recovery

This is a consultancy service and does not provide hosting, data backup, or disaster recovery. Where we implement tooling or configuration changes, we follow your change control and rollback approach (for example: configuration export, staged rollout, pilot testing, and documented rollback steps).

4. Onboarding and offboarding

Onboarding:

- Kick-off to confirm objectives, scope, stakeholders, and timelines
- Access method agreed (least privilege; read-only where possible)
- Tooling and telemetry sources confirmed (logs, APIs, connectors, retention)

Offboarding / exit:

- Final deliverables supplied in agreed formats
- Access removed (accounts revoked, guest access removed if used)
- Working files handled per data retention section below

5. Service constraints

- Delivered remotely by default (onsite by agreement).
- Requires access to key stakeholders for workshops, approvals, and decisions.
- Requires access to relevant documentation where available (HLDs, LLDs, diagrams).
- Findings and effectiveness depend on access granted and log/telemetry retention.
- Implementation support requires buyer approvals, change windows, and testing time.
- Scope is limited to agreed systems/tooling and agreed tenant(s)/environments.

6. Service levels and support hours

- Support/engagement hours: Mon–Fri 09:00–17:00 UK
- Channels: Email, Microsoft Teams, phone (as agreed)
- Target response to questions during business hours: within 8 working hours
- No enhanced/out-of-hours support unless explicitly agreed in a call-off.

7. After-sales support

We can provide follow-up support including alert tuning, rollout check-ins, automation enhancements, and validation reviews after the main engagement. All time is delivered and charged in line with the Lot 3 rate card for the relevant role.

8. Technical requirements

Buyer provides:

- A named technical contact and decision-maker for approvals
- Appropriate access to the relevant platforms (read-only preferred initially)
- Access to required logs/telemetry sources for detection and alerting design
- Workspace for collaboration (Teams and document sharing)
- Access to service/application owners for impact assessment and testing

9. Outage and maintenance management

We do not operate any buyer production service. Where tooling changes, policy deployments, or automation updates are implemented, we plan changes within your maintenance windows and change control process and support testing, pilot rollout, and rollback steps.

10. Hosting options and locations

No hosting is provided. Delivery is remote. Documentation and outputs are shared using buyer-approved tooling and locations (e.g. buyer SharePoint/Teams or agreed secure transfer).

11. Access to data on exit

All outputs (designs, alert logic, automation workflows, runbooks) are provided to the buyer. We will securely delete any buyer data held as working material.

12. Security

- Least-privilege access
- Buyer-controlled accounts and approval for changes
- Secure handling of information (controlled sharing and storage)
- No intrusive testing unless explicitly in scope
- Data minimisation: access only what is required for delivery
- Compliance with buyer security policies and reasonable assurance requirements

13. Commercials (high level)

The service is delivered on a time-and-materials basis and charged at the relevant hourly rates listed on the Lot 3 rate card, aligned to the role(s) provided. We provide an estimate for the basis of a purchase order, and provide regular burn-down information against that.