

Security Monitoring Consultancy from 2T Security

2T Security recognises that security monitoring must align with your strategic objectives, risk posture and operational reality. Our Security Monitoring Consultancy delivers a bespoke strategy that defines what truly matters to monitor, why it matters and how to monitor it. We select and design your security monitoring ecosystem to prioritise high impact data sources, integrate actionable threat intelligence, and establish a SOC infrastructure that evolves with your business and threat landscape.

Capabilities

- Requirements assessment: Analyse your technology, risk profile and operational needs to define security monitoring priorities and requirements
- ACSC (CCP) Lead Security Architect Oversight: Service overseen by ACSC (CCP) Lead Security Architect, ensuring compliance, maturity and strategic alignment with national frameworks
- Threat-led Monitoring design: Identify what threats that can be mitigated through security monitoring and map them to business critical assets
- High impact log sources prioritisation: Focus monitoring efforts on log sources with the greatest business impact
- AI driven threat detection: build AI based solutions for anomaly detection, novel threat identification and intelligent alert triage
- Custom alerts and detection engineering: Development of business risk tailored detections, with extensive expertise in Critical National Infrastructure (CNI) environments.
- Threat Intelligence generation: generate actionable threat intelligence from observed alerts and threat data to inform an evolving threat landscape and continuous service improvement
- Playbook development: Development of security monitoring use cases for inclusion in your security playbook
- Security Operation Centre (SOC): design, implement, management of scalable SOC infrastructure which can be deployed into unique environments
- Vendor management: Assist with the selection of security monitoring suppliers and ongoing vendor management
- Requirements and design: document requirements , design, install and configure commercial and open-source software and SIEM monitoring solution
- Logs onboarding and tuning: integrate and optimise log sources with continuous alert refinement and development.
- Business risk mapping: map threat activity to business risk exposure, providing visibility into where threats reside and how risk shifts across your critical assets

Key benefits

- Proven sovereign expertise: Extensive experience in security design across public and private sectors and critical infrastructure (CNI)
- NCSC Trusted partner: endorsed by NCSC for high value and complex projects
- Extensive cross-domain experience
- Business aligned cost optimisation: Manage long term costs with a clear business linked strategy
- Risk visibility: threat to business risk mapping to inform on what's at stake
- Future proof operations: AI-enhanced detection, custom risk based alerts, scalable infrastructure to ensure resilience against evolving threats
- CNI specific maturity: deep expertise in building monitoring solutions for CNI infrastructure

Engagement Process

Our security operations service engages widely to deliver high levels of value to your business, this includes:

- Stakeholder alignment: Identifying business, technical, and supplier stakeholders
- Current state assessment: Review existing security controls and assets, and monitoring gaps to determine their security monitoring effectiveness
- Risk assessments: to identify and prioritise your most critical business assets and map monitoring coverage
- Identify log sources, mapping them for monitoring use and against business assets
- Strategy and Design: co-develop the monitoring strategy, AI-driven detection logic and SOC architecture, including design and installation of security monitoring software/SIEM
- Onboarding of log sources to security monitoring software and alert tuning
- Threat intelligence integrations: integrate and automate the ingestion of threat intelligence and automate threat intel generation from monitored data
- Integrating threat intelligence sources
- Continuous improvement: Regular checkpoints to review performance and alert efficacy