Managed Security Operations Centre from 2T Security

At 2T Security, we know government security is about relevance of the alerts. Our Managed Security Operations Centre service is engineered to align with your business risk profile. We translate your critical assets and threat landscape into custom detection rules, response playbooks and MITRE ATTCK mappings, ensuring every alert matters. 2T Security SOC offering is aimed at high stakes environments like Critical National Infrastructure (CNI), Industrial Control Systems (ICS) and OT. We eliminate the noise, focussing on what actually threatens your mission, and delivering a defence in depth strategy that includes AI as a proactive layer against unknown threats.

Capabilities

Commented [SV1]: Mention AI, TI (internal and external), SOC-in a box

Commented [SV2R1]: Risk driven and mapping, Mitre mapping, rules development and continuous improvement, tailored to customer needs

- Risk-First SOC Architecture: We map your business risk register directly to detection rules, threat intelligence, and MITRE ATT&CK frameworks—not vendor defaults. Your SOC only alerts on threats that impact your most critical assets
- AI as Your "Unknown Unknowns" Shield: Beyond traditional rules, we deploy AI-driven anomaly detection to identify stealthy, zero-day threats
- Designed to support high threats environments: designed for Critical National Infrastructure (CNI), Industrial Control Systems (ICS), and Operational Technology (OT) environments
- UK-Certified, UK-Based Operations: Fully UK hosted, and managed by UK based staff (including our ACSC CCP Lead Security Architect)
- Unified Security Operations: Monitor hybrid cloud operations and/or data centres, with multi-vendor and ISP/cloud vendor support
- Designed to satisfy your needs: We have a flexible delivery approach:
    - Use your existing monitoring tools
    - We can help you procure and deliver appropriate tooling
    - Fully managed SOC where we provide the platform, people and processes
- High-Threat Environment Expertise: our staff of architects, risk managers, engineers, analysts, and senior leaders have demonstrable expertise in protecting high risk environments
- Threat Intelligence customisation: Threat Hunting and data analysis based on your risk profile and your infrastructure

Key benefits

- Zero noise, maximum relevance: Alerts tied to your risk
- AI-assisted threat hunting: Spot emerging threats (e.g., lateral movement in OT networks) before they escalate
- Confidence in consistent delivery: Confidence that your security monitoring needs are being delivered consistently
- Insider threat detection: Proactive monitoring and analysis that spots misuse and security threats
- Predictable cost model: budget certainty for effective long-term planning

- Flexible/agile service: reflect changing business needs, with a flexible commercial framework available that can be tailored to meet your needs
- Services led by ACSC (CCP) Lead Security Architect
- Plug and play SOC: Complete deployable SIEM/SOC infrastructure available
- High threat environments: Designed to meet the requirements of high threat environments
- Seamless incident response: We integrate with your CIR process, reducing mean time to resolution
- Continuous improvement: Quarterly risk reviews and SOC optimisation aligned to your evolving threat landscape

Engagement Process

Our SOC service collaborates with you to deliver a SOC that works for you, providing high levels of value to your business:

- Engage: to identify business, technical, and supplier stakeholders
- Assess & Assure: Understanding existing security controls for effectiveness and response capabilities
- Risk assessments: to identify your most critical business assets, threats and business impact
- Developing response plans to protect your business assets in the most efficient way
- SOC Design & Build: Tailor detection rules, MITRE mappings, and AI-driven analytics to your risk profile
- Deploy & Integrate: Launch with your tools or our managed stack
- Operate, Optimise & Maintain: Monitoring with UK-based analysts and regular checkpoints to review performance and deliver continuous improvement