Managed Protection & Security Operations

Secure, Consistent Protection Across Platforms

This service delivers continuous security monitoring, threat detection, vulnerability oversight and operational governance across workplace, cloud and network environments.

It strengthens resilience, reduces organisational risk, enhances compliance and provides day-to-day incident triage, security posture improvement and structured operational protection aligned to industry and organisational security standards.

Service Benefits

- Enhanced resilience and risk reduction through continuous monitoring response
- Improved security posture and compliance via proactive governance assurance
- Increased visibility using consistent posture risk and incident reporting
- Reduced operational workload through managed triage reviews and automation
- Service adapts to existing environments with board-level reporting assurance

Areas We Support

A modular managed service delivering continuous, proactive and resilient security operations.

► Modern Workplace Security

Protection and monitoring across modern end-user environments:

Identity and access management governance

Endpoint security posture verification

Threat detection and incident alert triage

Policy, baseline and configuration assurance

► Hybrid Cloud Security

Unified controls, monitoring and operational governance across cloud and on-premise estates:

Cloud security monitoring and event triage

Configuration, patching and vulnerability oversight

Backup and business continuity readiness

Compliance and security posture reporting

► Intelligent Networking Security

Security aligned to networking models, including SD-WAN, edge and secure access:

Network event monitoring and escalation

Firewall, access and segmentation verification

Zero-trust policy enforcement checks

Operational risk and exposure analysis

Security Strategy & Architecture

Strategic planning and high-level design of organisational security direction and control frameworks:

- Security roadmaps and future-state models
- Policy and standards development
- Architectural security principles
- Alignment to ISO/NCSC best practice

Security Governance & Policy Alignment

Establishing and uplifting governance structures and compliance frameworks, including but not limited to Cyber Essentials, Cyber Essentials Plus, ISO 27001, NIST CSF, NCSC CAF and UK GDPR:

- Policy review and refinement
- Governance maturity assessments
- Compliance mapping and gap analysis
- Support for audit documentation

Security Risk Management

Continuous identification, assessment and mitigation of security risks:

- Vulnerability identification and prioritisation
- Configuration and posture reviews
- Risk registers and risk reporting
- Threat exposure and trend analysis

Security Design & Control Engineering

Designing secure architectures, platforms and technical controls:

- Secure cloud and network design
- Identity and access control design
- Hardening standards and patterns
- Control mapping to business needs

Identity & Access Assurance

Ensuring access to systems remains secure and appropriate:

- Privileged access oversight
- MFA and conditional access checks
- Access review and recertification support
- Detection of identity misuse

Security Monitoring & Detection

Continuous monitoring to identify malicious or abnormal activity:

- Log collection, enrichment and correlation
- Monitoring of cloud, network and endpoint events
- Detection of suspicious activity or anomalies
- Severity-based alerting and notification

Security Incident Management

Operational response to security alerts and events:

- Alert triage and investigation
- Impact assessment
- Escalation and coordinated response
- Incident reporting and recommendation

Vulnerability & Patch Governance

Structured oversight of vulnerabilities, patches and configuration drift:

- Vulnerability scanning and prioritisation
- Patch lifecycle tracking
- Baseline configuration comparison
- Exposure reporting

Continuity & Recovery Readiness

Assuring environments remain resilient and recoverable:

- Backup and restoration verification
- Recovery-path readiness checks
- Continuity risk identification
- Resilience improvement recommendations

Security Assurance & Testing

Assessing the effectiveness of security controls, posture and compliance alignment:

- Application security & code testing
- Penetration testing & red teaming
- Security QA & assurance frameworks

Threat Intelligence & Reporting

Providing insight into threats, trends and organisational exposure:

- Trend and pattern analysis
- Relevant threat intelligence summaries
- Monthly/quarterly reporting
- Exposure reduction recommendations

Security Hyperautomation

Automation of routine and high-volume security operations to improve speed and consistency:

- Automated alert triage and enrichment
- Orchestrated response workflows
- Integration across SIEM, EDR, cloud and identity
- Reduced manual workload and faster incident resolution

Deliverables

This service provides deliverables aligned to the specific areas selected in scope, which typically include:

- Monitoring, detection and incident triage
- Threat investigation and response guidance
- Vulnerability, configuration, identity and access governance
- Backup validation, continuity and recovery assurance
- Stronger compliance alignment across Cyber Essentials, ISO 27001 and UK security frameworks.
- Security risk, posture, compliance and governance reporting
- Strategy, architecture and policy uplift
- Security design, hardening and control engineering
- Identity and access assurance and recertification
- Application and code security testing, penetration testing and red teaming (scope dependent)
- QA frameworks, assurance testing and verification artefacts
- Threat intelligence summaries and exposure insights
- Hyperautomation workflow design and enhancements
- Documentation, runbooks and knowledge transfer
- Configuration and policy assurance reviews
- Control effectiveness assessments
- Threat and exposure dashboards
- Operational maturity insights and recommendations

Service Levels

Service levels depend on the service areas selected in scope and may include:

- 24×7 monitoring and alert triage (managed service options)
- 9–5 UK time, Monday to Friday, for assessment or uplift activities
- Severity-based response and escalation timelines
- Scheduled service reviews during UK business hours
- Monthly or quarterly reporting cadence

Pricing Model

- Fixed monthly managed service fee
- SFIA-aligned day rates for uplift or project work
- Fixed-price assessment packages available
- Scope and pricing finalised after scoping activities

Engagement Options

Supporting flexible delivery across Assessment, Implementation and Managed Operations:

- **Project Delivery -** Structured execution of security uplift, control deployment, configuration hardening or resilience improvements
- **Team Augmentation –** Security specialists, including but not limited to SOC analysts, security engineers, architects, governance and compliance practitioners
- **Specialist Resourcing -** Short-term, task-focused expertise for incident support, posture assessments, audits or workflow automation
- **Managed Service -** Multidisciplinary team that provides ongoing monitoring, response support, control upkeep and continuous security-posture improvement

Security & Compliance

- Staff screened to BS7858:2019.
- NPPV or SC clearance available on request and scoped separately (not included in standard rate card)
- Processes aligned to ISO 27001, 9001, 20000-1 and 14001
- GDPR-compliant handling of customer data

Customer Responsibilities

- Provide access to systems, tooling and stakeholders for operational support
- Maintain governance and change processes for configuration, patching or remediation actions
- Approve operational changes, recommendations and review outcomes
- Supply accurate architectural and operational information as environments evolve
- Participate in service reviews, reporting discussions and decision-making

Offboarding

- Handover of reports, artefacts and documentation
- Transfer of runbooks, configurations and workflow information
- Final posture, risk and service performance summary
- Access removal and secure service closure
- Next-step recommendations and transition guidance

Contact us to discuss your requirements.

0115 846 4000
outcomes@xma.co.uk
www.xma.co.uk

