CYBERSECURITY CONSULTANCY AND IMPLEMENTATION

Service Definition

19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

Regus Atterbury Lakes Fairbourne Drive, Atterbury, Milton Keynes, Buckinghamshire, England, MK10 9RG

TRIDENT
INTELLIGENT SOLUTIONS

Contents

Service Overview

The Cybersecurity Consultancy and Implementation service provides end-to-end advisory, design, deployment, and operational support to secure enterprise environments, applications, data, and platforms. The service supports risk management, compliance, and governance requirements across cloud, on-premises, and hybrid infrastructures.

It also addresses the security implications of advanced workloads, including AI, generative AI, and agentic AI systems, data pipelines, and analytics platforms.

Capabilities include:

- Cybersecurity strategy, risk assessment, and governance advisory
- Threat modelling, vulnerability assessment, and penetration testing
- Security architecture design and implementation
- Identity and access management (IAM), role-based access control, and least-privilege enforcement
- Secure DevOps (DevSecOps) integration
- Data protection, encryption, and privacy-by-design
- AI and agentic AI security governance and model assurance
- Incident response planning and security operations support
- Compliance with regulatory frameworks, ISO/IEC 27001, NIST CSF, GDPR, and industry-specific standards

The service can be delivered as advisory engagements, project-based implementations, or ongoing managed security support.

Scope of Services

Cybersecurity Strategy and Governance

- Enterprise security risk assessment and prioritisation
- Security policy, standard, and procedure development
- Governance advisory for AI, agentic AI, cloud, DevOps, and data platforms

- Compliance mapping to ISO/IEC 27001, ISO/IEC 42001 (for AI), GDPR, NIST CSF, and other regulatory frameworks

Security Architecture and Implementation

- Security design for networks, cloud, applications, data platforms, and AI/agentic AI solutions
- Threat modelling and mitigation strategies
- Secure configuration of infrastructure, applications, and cloud services
- Identity and access management (IAM), multi-factor authentication, and privileged access controls
- Implementation of monitoring, logging, and alerting controls

DevSecOps and Cloud Security

- Integration of security controls into CI/CD pipelines and automated deployments
- Infrastructure-as-Code (IaC) security hardening
- Container and orchestration security for cloud-native applications
- Automated vulnerability scanning and remediation workflows

AI/Agentic AI Security

- Security and ethical controls for AI/agentic AI models, data flows, and integration points
- Model integrity assurance, bias and adversarial risk mitigation
- Human oversight and decision authority frameworks
- Secure deployment and lifecycle management of AI systems

Incident Response and Operational Security

- Security monitoring, alerting, and threat intelligence integration
- Incident response planning, playbooks, and simulation exercises
- Remediation and recovery support for cyber incidents
- Continuous improvement and security posture monitoring

Engagement Approach and Deliverables

Cybersecurity engagements are tailored to client requirements and may include:

- Risk assessment and gap analysis reports
- Security architecture and design blueprints
- Policies, procedures, and governance frameworks
- Threat modelling and penetration testing reports
- Secure configuration and hardening guides
- Incident response plans and operational playbooks
- Recommendations for AI/agentic AI, analytics, and cloud security

Deliverables are actionable, auditable, and aligned to client governance and compliance frameworks.

Onboarding and Engagement Initiation

Following contract agreement, a Security Lead and team are assigned. A kick-off session establishes objectives, scope, governance, roles, and access requirements.

A Statement of Work (SOW) or Engagement Definition is agreed, specifying:

- Scope and deliverables
- Timelines and milestones
- Client responsibilities and access requirements
- Governance and approval processes

Service Constraints

- Security delivery relies on client-provided access to systems, networks, data, and applications
- Effectiveness depends on availability of key stakeholders and timely provision of information
- Cybersecurity controls cannot guarantee absolute prevention of threats; risk is managed and mitigated

- Cloud, DevOps, and AI security recommendations assume deployment on supported platforms with agreed configurations

Service Levels and Support

Unless otherwise agreed in writing, the service and ongoing support shall be provided during standard business hours (9-5), Monday to Friday. Support outside of these hours, including 24/7 support, may be provided subject to a separately agreed arrangement.

Support levels are defined per engagement:

Standard Support: Advisory guidance and remote assistance during business hours for security configuration or minor incident response.

Enhanced Support: Extended hours, proactive monitoring, vulnerability scanning, and guidance on security improvements.

Premium Support: 24/7 coverage for mission-critical systems, rapid escalation, dedicated Security Lead, threat intelligence integration, and full incident response support.

Severity Classifications:

- **Severity 1 (Critical):** Active breach or compromise impacting critical systems; immediate response
- **Severity 2 (High):** Significant vulnerability or configuration issue affecting operations; rapid remediation
- **Severity 3 (Medium):** Non-critical security issues or recommendations; addressed within standard response times
- **Severity 4 (Low):** Minor security advisory, reporting, or configuration adjustments

After-sales Support

After implementation, handover includes all security documentation, operational procedures, configurations, and monitoring dashboards. Knowledge transfer ensures client teams can maintain, monitor, and operate securely.

Ongoing support may include:

- Vulnerability scanning and remediation

- Patch management
- Security posture monitoring
- AI/agentic AI model and platform security reviews

Technical and Client-side Requirements

The client is responsible for:

- Providing access to systems, networks, applications, and data required for security assessment and implementation
- Identifying stakeholders and subject-matter experts for governance and decision-making
- Providing relevant policies, standards, and regulatory obligations
- Ensuring network, identity, and access integration to enable monitoring and automation

Security, Governance, and Compliance

Security and governance are embedded throughout the lifecycle:

- Role-based access, least-privilege enforcement, and secure coding practices
- Data protection, encryption, and secure storage
- Continuous monitoring, logging, and alerting for security events
- AI/agentic AI governance and ethical controls
- Compliance with ISO/IEC 27001, ISO/IEC 42001, NIST CSF, GDPR, and industry-specific regulations

Responsibilities are shared between the service provider, client, and third-party providers, with clear allocation per engagement.

Offboarding and Exit

At engagement conclusion, a formal close-out session confirms:

- Delivery of all security documentation, configurations, and artefacts

- Residual client data, access credentials, or temporary accounts are securely deleted or revoked
- Recommendations for ongoing security improvements and risk management