A RICOH Company

29 January 2026

CYBER ASSESSMENT & PROFESSIONAL SERVICES PORTFOLIO

Ref no: G-Cloud 15

PREPARED BY

MTI Technology

COPYRIGHT

TABLE OF CONTENTS

1.0 SERVICE DEFINITION

This document provides an overview of MTI's cyber security assessments and cyber professional services, outlining the key capabilities, service categories, and consultancy offerings that support organisations in assessing, strengthening, and maturing their cybersecurity posture.

1.1. EXECUTIVE SUMMARY

MTI Technology delivers a comprehensive portfolio of Cyber Assessment and Professional Services designed to strengthen security maturity, reduce risk, and enhance organisational resilience. These services span several core categories, including Identity & Access Management, Vulnerability and Risk Management, Threat Detection and Incident Response, Cloud Security and Network Protection, Penetration Testing, and Governance and Risk Management.

Both assessment services—such as reviews, health checks, maturity assessments, and strategic evaluations—and professional services—including configuration, implementation, optimisation, and specialist consultancy—are available across each category to support customers at every stage of their cybersecurity journey.

A wide range of services is offered, including examples such as Active Directory Reviews, MFA Review, Vulnerability Assessment, Incident Response Tabletop Exercises, Firewall Health Checks, Cloud Security Assessments, and Gap Analysis & Strategy engagements.

1.2. CYBER ASSESSMENT AND PROFESSIONAL SERVICES PORTFOLIO

The Cyber Assessment and Professional Services Portfolio table below provides a broad range of security services designed to help organisations understand their current security posture and improve it where needed.

The portfolio table below provides a brief overview of each service, while detailed service descriptions and statements of work are available to offer further insight and support your decision to engage with MTI.

IDENTITY & ACCESS MANAGEMENT		
Protecting User and Privileged Identities, control and monitor access to critical systems.		
Discovery and Assessment Services	Active Directory Review (On-prem) (AD Security Review)	Assesses Active Directory to identify security gaps, role-based privilege weaknesses, and configuration risks. Evaluates domain health, trust relationships, and attack paths, providing prioritised recommendations to reduce cyber risk and strengthen overall domain security posture.
	Active Directory Review (Entra-ID) (AD Security Review)	Identifies security weaknesses and misconfigurations in Entra ID, including identity governance, conditional access, authentication, privileged roles, and Zero Trust considerations. Complements on-prem AD reviews and can include

		assessment of hybrid identity connectors to reduce cloud and cross-directory attack risk.
	MFA Review	Assesses your organisation's MFA policies and technical implementation across identity providers, authentication coverage, MFA methods, conditional access, and legacy systems. It delivers a gap analysis report aligned to agreed standards, a prioritised remediation plan, and practical guidance to strengthen authentication and reduce compromise risk, including practical guidance for alternative controls where direct MFA is not supported.
	Privileged Access Management Gap Analysis and Strategic Review	Evaluates how privileged accounts are managed, protected, and used within the customer's PAM solution. Assesses whether the organisation is maximising the use of available features and security controls, aligns findings with business objectives, and provides a strategic roadmap for remediation and enhanced PAM security. Includes quick wins and medium-term improvements.
Professional Services	MFA Configuration and/or policy improvements	Improve/update policies, standards, and configurations to better align with good security practice and improve defences against identity-based attacks.
	Entra ID Improvement Services	Enhances Entra ID environments through identity enforcement, synchronisation, and policy optimisation.
	Active Directory Remediation	Remediates Active Directory weaknesses to better align with good security practice and reduce overall risk posture.
	Role Based Authority (RBA) Accelerator - Domain and Server Boundaries	Implements role-based access across domain and server boundaries for an order of magnitude increase in security and governance. This service can be delivered across multiple merging or digitally collaborating organisations to standardise RBA across the group.
	Role based Authority (RBA) Accelerator - Domain Boundary	Establishes domain-level role-based access controls to enforce segregation of duties. Delivers an order of magnitude increase in Active Directory security and governance.
	Role Based Authority (RBA) Accelerator – Server Boundary Extension	Extends role-based access controls to servers, enhancing privilege management and visibility. Delivers an order of magnitude increase in Active Directory security and governance.
VULNERABILITY AND RISK MANAGEMENT		
Asset discovery and assessment, vulnerability remediation, continuous threat exposure management		
Discovery and Assessment Services	Vulnerability Assessment	Identifies technical vulnerabilities across systems and networks, and applications providing actionable insights for remediation.

	Vulnerability Management Maturity Assessment (VMMA)	The Vulnerability Management Maturity Assessment (VMMA) aims to address the problem of cyber attackers exploiting vulnerabilities in people, processes, and technology by providing a structured assessment of an organisation's vulnerability management maturity. MTI review Vulnerability Management policy & process, aligned to NCSC & CAF principles, through analysis of completed VMMA questionnaire, workshop, and documentation review, to deliver a formal report & actionable recommendations.
	Cyber Maturity Assessment	Provides strategic cyber consultancy, assessing organisational maturity, leveraging applicable standards and maturity model, going beyond technical vulnerability findings.
	Risk Assessment	Evaluates organisational cyber risk, providing recommendations to strengthen governance and controls.
	Threat Assessment	Identifies and assesses potential threats to the organisation, enabling informed mitigation strategies.
Professional Services	Vulnerability Scanning Platform, Deployment, configuration, improvement	Deployment of the Vulnerability Scanning Platform, to conduct Network and Server Vulnerability Assessment Scans, Web Application Scans, Cloud Platform Assessments, Attack Surface Reduction scanning, as well as passive scanning for sensitive OT and IoT environments.
THREAT DETECTION AND INCIDENT RESPONSE		
Proactive and reactive management of threats and alerting. Real time monitoring, Threat detection, incident response. Proactive Threat hunting and rapid containment		
Discovery and Assessment Services	SIEM, SOAR, EDR, MDR and XDR Health Check	Provides an independent assessment of Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) SOAR, and MDR platforms reviewing data ingestion, log coverage, detection rules, analytics, tuning, response actions, endpoint coverage, and integration maturity. Identifies configuration gaps and optimisation opportunities to improve threat detection, investigation, and response effectiveness.
	Table Top Exercises (TTX) Incident Response Preparedness	Tabletop exercises are consultant-led simulations where key stakeholders discuss their organisation's response to realistic cyber incidents, such as phishing attacks, ransomware outbreaks, or data breaches. The consultant facilitates the session, introducing "injects" or "grenades" to evolve the scenario and observe how participants react under changing conditions, helping to assess decision-making, communication, and overall resilience.
	SIEM Capacity & Readiness Review	A SIEM Capacity, Readiness, and Planning Review is a pre-deployment consultancy engagement that helps organisations assess expected log ingestion volumes, data sources, and retention needs to inform accurate sizing and funding

		decisions. It also evaluates operational readiness, including the resources and capabilities required to run and support a SIEM 24×7, ensuring the solution is feasible, scalable, and aligned with business and security objectives.
	Protective Monitoring Review	Typically appended to ITHC / penetration test projects to verify that attacks / scans are being detected and reported on in the SIEM tool.
	Threat Simulation and Detection Assessment	Replicates threat actor Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK framework in controlled exercises to evaluate detection and response effectiveness. Identifies gaps across SIEM, Managed Detection & Response (MDR), Extended Detection & Response (XDR), and Endpoint Detection & Response (EDR), informing optimisation and managed service requirements.
Professional Services	Design & Deploy	SIEM, EDR, XDR and MDR Design & Implementation Services. Includes log collection strategy, detection rule development, alert tuning, incident workflow configuration, and integration with existing security controls to ensure effective monitoring, rapid detection, and streamlined incident response.
	Microsoft Sentinel and LevelBlue USMA Configuration and optimisation	Configures and optimises Microsoft Sentinel and LevelBlue USMA SIEM deployments to maximise visibility, detection, and response capabilities.
	Microsoft Defender for Endpoint (MDE) configuration, Optimisation, and Integration	Provides configuration, optimisation, and integration services across the MDE suite to strengthen endpoint security.
	TrendMicro VisionOne Configuration, Optimisation, Migration	Configures, optimises, and migrates TrendMicro Vision One XDR deployments to enhance detection and response capabilities.
CLOUD SECURITY AND NETWORK PROTECTION		
Public and private cloud security, secure configuration, network segmentation, and protecting north/south and east/west traffic flows.		
Discovery and Assessment Services	Security Architecture Review (or Network Security Design Review)	Evaluates network and system architecture against best practices, including NCSC's Secure by Design principles. Identifies design weaknesses, misconfigurations, and potential attack vectors, providing actionable recommendations for remediation, secure product implementation, and enhanced resilience against cyber threats.
	Network Security Audit	The network security audit assesses network architecture, configurations, firewall rules, segmentation, and exposed

		services to identify misconfigurations, vulnerabilities, and control gaps, validating alignment with security standards, policies, and threat-driven best practice.
	Firewall Health Check	Reviews firewall configurations to identify weaknesses such as overly permissive rules, unused services, misapplied policies, default settings, and misconfigured NAT or VPNs. Provides optimisation recommendations to enhance security, performance, and compliance.
	Network Segmentation Review	Evaluates network segmentation design and implementation to identify gaps, misconfigurations, and weaknesses. Provides recommendations to improve access control, isolate critical assets, reduce attack surface, and strengthen overall network security.
	NSX Review - Broadcom (VMware)	Assesses VMware / NSX network segmentation to ensure alignment with best practices and compliance requirements.
	Zero Trust Maturity Assessment	Evaluates Zero Trust maturity across Identity, Devices, Networks, Applications & Workloads, and Data using CISA ZTMM, NIST 800-207, ISO 27001, and CIS Controls; provides prioritised recommendations.
	Firewall Deployment, configuration, improvements	Provides end-to-end firewall deployment, configuration, optimisation, and feature maximisation for on-premises or cloud firewalls.
	NDR deployment, configuration	Deploys and configures Network Detection & Response appliances, integrating them with SIEM or monitoring platforms.
Professional Services	Cloud Security Tool implementation	Implementation of cloud security tools configuring CSPM, CIEM, CNAPP, and cloud workload security to assess misconfigurations, identity risk, runtime threats, and policy compliance across cloud platforms, improving visibility, control, and risk posture.
	Compliance and Policy Audit & Maximising License/Features	Reviews firewall deployments to identify compliance gaps, policy weaknesses, and opportunities to maximise licences and features.
PENETRATION TESTING		
Proactive Social and Technical assessments simulating real-world attacks to uncover vulnerabilities, misconfigurations, and weaknesses across systems, applications, networks, cloud platforms, and people. Supports risk reduction, strengthens security posture, and drives regulatory and compliance objectives.		
Professional Services	Code Review	Security review of source code to identify vulnerabilities and coding flaws.
	Cloud Security Assessments	Reviews cloud environments (e.g. Azure, AWS, OCI) for misconfigurations, vulnerabilities, and compliance gaps.

	Red Teaming	Simulates realistic, multi-layered adversary attacks across people, processes, and technology to test organisational detection, response, and resilience. Techniques include social engineering, phishing, physical intrusion, network exploitation, application attacks, and lateral movement, highlighting gaps and informing improvements in security controls, incident detection, and response capability
	Social Engineering	Evaluates human and process vulnerabilities through controlled social engineering exercises. Includes phishing, vishing (telephone), physical access attempts, tailgating, pretexting, and remote impersonation. Identifies awareness gaps, procedural weaknesses, and potential attack vectors.
	Third-Party Attack via IPSec VPN	Simulates attacker using VPN access to perform reconnaissance, exploitation, lateral movement, and potential domain compromise over a dedicated assessment period.
	Structured SIEM / XDR / MDR Assessment	Tests SIEM/XDR/MDR effectiveness by simulating adversary techniques, validating detection, response, coverage, and producing MITRE-mapped findings and remediation guidance.
	Simulated Ransomware Attack	Conducts controlled ransomware kill-chain simulation to test detection, containment, response and recovery, using reversible encryption and detailed activity logging.
	Focused Remote Red Team Attack	Simulates targeted remote intrusion to assess detection, response, privilege escalation, lateral movement, and resilience against real-world attacker techniques.
	Telephone Social Engineering	Uses caller impersonation and scripted scenarios to elicit credentials, MFA codes, system access, or sensitive information, testing staff awareness, and process robustness.
	Physical / Internal Offensive Network Attacks	Attempts onsite intrusion, workstation compromise, lateral movement and privilege escalation using physical access, USB insertion, tailgating and living-off-the-land techniques.
	Overwatch – Continuous Remote Red Team Attack	Ongoing six-month or 12 month red-team monitoring and exploitation of emerging vulnerabilities to validate detection, patching, and defensive readiness.
	External Infrastructure Assessment	Assesses internet-facing assets for vulnerabilities and misconfigurations.
	Internal Infrastructure Assessment	Evaluates internal networks and systems for vulnerabilities and misconfigurations.
	Application Assessment (Web Apps, APIs, Thin Clients, Thick Clients)	Tests applications for security weaknesses, including SQL injection, cross-site scripting, authentication and session flaws, and insecure configurations, providing recommendations to reduce risk and strengthen overall application security.
	Backup Compromise Assessment	Reviews backup systems for vulnerabilities and potential compromise paths.

	CI / CD Assessment	Evaluates continuous integration and deployment pipelines for security weaknesses.
	Database Security Assessment	Assesses databases for encryption, misconfigurations, vulnerabilities, and weak access controls.
	Mobile Application Assessment	Reviews mobile apps for data leakage, insecure storage, and other security weaknesses.
	Malicious File Protection Assessment	Evaluates protection controls against malicious file threats.
	Wireless Network Assessment	Tests Wi-Fi networks for encryption strength, rogue access points, and unauthorised access.
	Cloud Service (Azure/AWS/Google/ Private Cloud) Review	Reviews cloud platform configurations and resources to reduce security risk.
	Microsoft / Office 365 Review	Audits O365 settings, permissions, and security controls for weaknesses.
	Firewall Configuration Review	Reviews firewall rules and configurations for security gaps.
	Operating System Build Review	Assesses OS builds against Cyber Security standards and security best practices.
	CAF-Aligned-DSPT NHS ITHC	Security testing to meet NHS England compliance requirements.
	PSN / PSN-P ITHC	Gap analysis and review to meet UK government and Police cybersecurity certification requirements.
	WAF Validation Testing	Tests web application firewalls for correct configuration, blocking, detection, and effectiveness.
	Cyber Essentials/ Cyber Essentials Plus	Assesses foundational cyber hygiene against Cyber Essentials controls, including firewalls, secure configuration, access controls, malware protection, and patch management, providing evidence, recommendations, and verification for certification readiness.
	IT Security Review	Comprehensively assesses internal and external networks, cloud environments, applications, and IT infrastructure, including Vulnerability Assessments, and reviews of OS Builds, firewalls, switches, databases, and backup systems. Evaluates security gaps, misconfigurations, and detection capabilities to enhance resilience against ransomware and cyber threats.
	SCADA / Operational Technology Testing (OT) / ICS / IoT	Reviews operational technology systems for vulnerabilities without disrupting live services.

	Ransomware Readiness Assessment	Evaluates preparedness and response plans for ransomware attacks.
GOVERNANCE AND RISK MANAGEMENT		
Discovery, assessment, consulting, and policy to deliver governance and compliance and reduce risk. Driving towards a Cyber Target Operating Model.		
Discovery and Assessment Services	Supply Chain Risk Assessment	MTI's Supply Chain Risk Assessment evaluates individual suppliers against NCSC's 12 Supply Chain Principles to identify vulnerabilities that could impact your organisation's data and operations. The service delivers a detailed risk profile, RAG status, and actionable recommendations to strengthen supplier security and reduce overall supply chain risk
Professional Services	Gap Analysis & Strategy	MTI's Gap Analysis benchmarks your organisation's policies, processes, and technical controls against applicable standards such as ISO/IEC 27001, CIS Critical Security Controls, NCSC CAF, NIST Cyber Security Framework etc. as applicable to the customer, to identify compliance gaps. The service delivers a clear remediation plan, detailed findings, and actionable steps to help customers improve their security posture and resilience, build robust Information Security Management Systems and controls.
	Tabletop Exercises	Tabletop Exercises simulate real-world cyber incidents in a controlled, discussion-based format to test organisational response plans and decision-making under pressure using agreed scenarios such as (Heightened Cyber Threat, Ransomware Attack, Supply Chain Software, Threatened leak of sensitive data, Insider Threat resulting in a Data Breach). These exercises help identify gaps in processes, improve coordination between teams, and strengthen overall incident readiness without impacting live systems.
	Cyber Target Operating Model (CTOM)	Consultancy to design a cyber target operating model (CTOM) defining governance, risk ownership, control frameworks, operating processes, metrics, and assurance mechanisms aligned to business objectives, regulatory obligations, and threat-driven security maturity.
	Cyber Security Posture Review	The review assesses an organisation's technical security posture through structured workshops and documentation analysis, examining network architecture, endpoint protection, vulnerability management, identity controls, backup, firewalls, patching, encryption, remote access, and disaster recovery. Findings inform risk identification and technical recommendations to strengthen controls, improve resilience, and align security practice with policy.

	Remediation Action Plan	We review outputs from audits, risk registers, risk-assessments, compliance submissions, IT Health Checks, penetration tests, vulnerability reports, and organisational strategy to develop a prioritised Remediation Action Plan (RAP). Risks are addressed in priority order, aligned with organisational imperatives, consolidating activities into Quick Wins, and three-, six-, twelve-month, and 3- and 5-year plans.
	Virtual CISO	The Virtual CISO service provides customers with scheduled and on-demand access to senior-level cyber security leadership without the cost of a full-time hire. Acting as a strategic advisor, the vCISO develops and oversees security policies, risk management frameworks, compliance programmes, and incident response strategies, ensuring alignment with business objectives and regulatory requirements. The vCISO service provides access to technical/risk/governance specialists in different domains providing access to greater skills/knowledge than is limited to one individual. vCISO typically starts with a Gap Analysis against relevant technical/compliance standards, such as CIS Critical Security Controls, NCSC CAF, ISO27001 to get a solid understanding of the organisation and help create a prioritised improvement roadmap.

2.0 ABOUT MTI

MTI Technology is a technology services and solutions provider with over 200 staff, operating across EMEA with offices in the UK and Germany. Over the last 36 years, MTI has helped thousands of organisations transform their IT operations, enabling them to leverage the latest technologies, reduce operating costs, become more flexible, and mitigate risk.

MTI has considerable experience in designing, delivering, and managing cybersecurity and data centre solutions for our customers across various industry sectors, including Commercial, NHS, central government, local government, Banking, Defence, Finance, and Insurance. This extensive experience ensures your solution is designed and installed by industry-leading MTI experts, guaranteeing a smooth, accurate, and on-time project delivery.

MTI specialise in cybersecurity, data centre modernisation, IT managed services and IT transformation. By employing proven methodologies and best practices, and adopting a consultative approach, MTI helps its customers solve business challenges and provides secure, compliant management of their applications, data, infrastructure, and system environments.

2.1. ACCREDITATIONS

MTI hold the following ISO Standards and Certifications

- ISO 27001 Information Security Management system
- ISO 9001 Quality Management System
- ISO 20000 IT Service Management
- ISO 45001 Occupational Health and Safety Management
- ISO 22301 Business Continuity Management System
- ISO 14001 Environmental Management System
- Cyber Essentials & Cyber Essentials Plus
- NCSC CHECK Scheme Member (CHECK 'Green Light' company since 2003)
- CREST Scheme Member

2.2. AWARDS

Our dedication to maintaining high standards is reflected in our numerous industry awards, including Dell Specialist Partner of the Year 2024, Dell Exceptional Services Delivery Performance 2024, Dell Advanced Services Delivery Partner 2024, Cyber Security Customer Service Award at the Computing Security Awards 2024, Cybersecurity/Data Protection Partner of the Year Award at the CRN Awards 2024, CRN MSSP/Security Reseller of the Year 2023, CRN Security Value Added Reseller (VAR) of the year for 2018, 2019, and 2020, and Penetration Tester of the Year for 2018 and 2020. We have won the UK Service Partner of the Year award twice for excellence in service delivery, in 2023/2024. MTI is committed to delivering exceptional customer service, which is why we have an industry-leading 98% customer satisfaction rating.

2.3. KEY PLATFORMS

MTI is proud to be a Dell Technologies Titanium Black Partner, the highest tier in Dell's Global Partner Program. This elite recognition positions MTI among a select group of global partners that demonstrate exceptional technical expertise, strategic alignment, and a consistent ability to deliver transformational outcomes for customers in today's data-driven, multi-cloud world.

Other key partners include:

2.4. ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG), CSR & SOCIAL VALUE

MTI integrates ESG, CSR and Social Value principles into our business values and operations to meet the expectations of customers, employees, investors, suppliers, the community, and the environment. Our Policy governs responsible and ethical conduct, a positive working environment, support for local communities, fair dealings with suppliers, and respect for human rights.

Environmental Management

MTI maintains a documented Environmental Policy Statement, approved by senior leadership, and reviewed annually. Our **ISO 14001 Environmental Management System** incorporates policies and procedures to manage, reduce, and report environmental impacts. We are committed to **Net Zero by 2050** and have achieved **EcoVadis Gold** standard for Social Value policies and procedures.

Sustainability Activities and Achievements

- **Planting of ~600 trees annually** to neutralise our carbon footprint (in partnership with Treedom). Treedom plants a tree on our behalf across Africa, South-East Asia, and South America to offset MTI's carbon emissions. They are a certified B Corporation, and every tree on their site has its own online page for tracking. To date, MTI has planted 3,299 trees, resulting in a 6.17 mt CO2e reduction and driving positive social and environmental impact.
- Reduction targets for business travel, including a digital-first approach, increased virtual meetings, and reduced travel emissions.
- **In 2023, we took one step closer as we are proud to say all our company vehicles are electric.**
- Transition to homeworking/hybrid models, reducing commuting and office energy consumption.
- Use of renewable energy sources for office electricity and optimisation of lighting, heating, and cooling systems.
- Eradication of single-use plastics in all offices.
- Implementation of cloud-based applications to reduce energy consumption.
- Collaboration with carbon-neutral suppliers and annual Supplier Sustainability Assessments.
- Comprehensive waste management systems, with recycling and mandatory staff training.
- Ongoing achievement of ISO 14001:2015 Certification.

Social Responsibility and Value Creation

- Dedicated ESG committee overseeing strategy, risk management, compliance, stakeholder engagement, and continuous improvement.
- Social Value Development Plan tracked by an ESG Manager, with regular reviews and reporting.
- Employer-supported volunteering, offering employees charity days tracked via our ESG application. MTI employees have completed 1,088 hours of volunteering.
- Initiatives supporting disadvantaged groups, including participation in the Disability Confident Scheme.

- Commitment to equal opportunity, diversity, and inclusion in the workplace.
- MTI support Cystic Fibrosis Charity through fundraising events, employee challenges, and donations.

Governance and Assurance

- Regular supplier assurance activities and annual Supplier Code of Conduct refresh.
- Compliance with ILO standards, UN Global Compact, and Universal Declaration of Human Rights.
- Board-level reporting of CSR compliance and performance.

Public Disclosure and Transparency

- Annual publication of Carbon Reduction Plan/ESG Report on MTI's website - https://mti.com/about/corporate-social-responsibility/
    - https://mti.com/wp-content/uploads/2025/10/MTI_Carbon-Reduction-Plan_FY2024.pdf
- Enhanced reporting of ESG performance and promotion of industry certifications - https://mti.com/wp-content/uploads/2025/12/ESG-Report-FY24.pdf

Head Office

MTI Technology Limited

3 Lotus Park First Floor

The Causeway

Staines-Upon-Thames

TW18 3AG

Reception: +44 (0) 1483 520 200

Service Desk: +44 (0) 1483 520 349

Web: www.mti.com

About MTI

MTI provides award-winning, end-to-end technology solutions and services across cybersecurity and data centre infrastructure, supporting customers for over 35 years. With over 250 specialists across the UK, France, and Germany, we deliver expert consultancy, project delivery, and scalable managed services.

Our mission is to build a secure digital future for our customers. We do this by combining deep technical expertise with a consultative, proven approach – helping organisations accelerate and de-risk transformation while ensuring secure, compliant management of applications, data, and IT systems.