Hybrid Identity Cyber Accelerator

Hybrid cloud environments are common to all public service providers who have struggled to adopt 'cloud only' when critical services have been supported by on-premise IT for decades. The partial shift to cloud and underinvestment in core identity security over 25 years has left a critical legacy of security debts. Active Directory and Microsoft Entra, used to govern access to digital systems, are compromised in 90% of successful ransomware attacks. Closing down these common attack paths and blocking tactics and techniques used by threat actors is the objective of this service.

Our Approach

1. Identity Security Review

Specialist discovery tooling and scripts are used to interrogate Active Directory and Entra to highlight vulnerabilities and risks in a detailed report.

2. Identity Strategy and Design

Identity systems are often complex and have evolved without good security principles. We produce a secure identity architecture and a plan to transform.

3. Remediate and Transform

Close all critical and high vulnerabilities, implement the principle of least privilege, consolidate domains, and execute the plan.

4. Sustained Identity Resilience

Ongoing support services from specialists using incumbent tooling; periodic test-resolve or continuous service options available.

What We Need From You

- Access to key stakeholders for interviews and workshops (e.g., IT and cybersecurity specialists, senior digital leadership for more transformational and enduring services).
- Relevant documentation, including existing cybersecurity policies, IT architecture diagrams, risk assessments, and compliance reports.
- Information on current and planned digital transformation initiatives.
- Details on your organisation's business objectives and critical services.
- Availability for scheduled meetings and feedback sessions throughout.

Service Objectives

- Break common attack paths and remediate vulnerabilities in Active Directory and Entra.
- Stop attacks near the surface of the onion. Prevent them from becoming existential events.
- Address architectural design flaws that hamper collaboration and digital or AI adoption.
- Achieve compliance with CAF with sustained Identity & Access Management maturity levels.

Service Options

Foundation: £5-10,000 ex VAT

Discovery and reporting of key identity security vulnerabilities and design issues.

Enhanced: £25-50,000 ex VAT

Strategic planning and design for improved resilience and user identity experience. Tactical remediation of critical issues.

Strategic: £150-250,000 ex VAT

Remediate critical and high vulnerabilities on a single AD domain plus Entra OR annual Sustained Identity Resilience services.

Key Features

- **Component-based** service and solutions to move resilience forward whatever your budget.
- Reports clearly identify risk and link to wider business initiatives for clear articulation to the board and in business cases.
- Specialist teams with long experience in critical public service providers and established methodology to support complex change.
- Simplified identity platforms and reduced privilege sprawl enable zero trust and more secure AI adoption.

Benefits to your organisation

Risk Reduction

Cut both impact and likelihood of severe ransomware events by disrupting the most common attack paths.

Cash Release

Reduce unnecessary privilege and associated license costs. Improve user experience and access to systems.

AI Enabling

Deploying agents to environments with uncontrolled IAM rights will prevent AI benefits and increase risks.

About us

- SME with highly experienced subject matter experts.
- Security clearance to BPSS, NPPV3 and SC.
- Specialists in delivery of end-to-end resilience.
- Wide-scale cyber programmes for UK Government.
- Public Sector first and mission-driven.

onionio.com

www.onionio.com

info@onionio.com

0330 223 6663