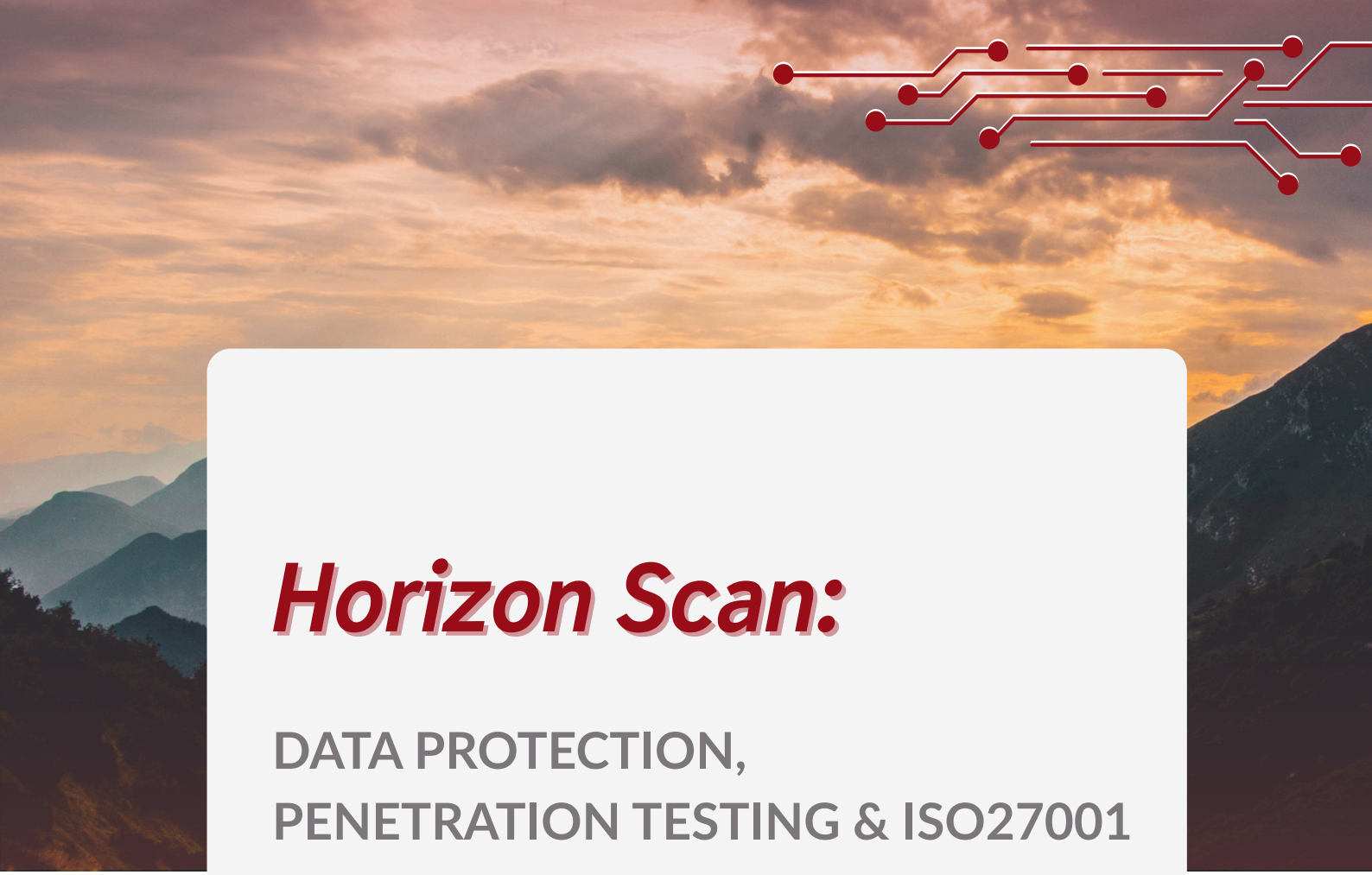

Horizon Scan:

DATA PROTECTION, PENETRATION TESTING & ISO27001

What's changing or coming up in the world of Data Protection, Pentesting and ISO27001?

October 2025

Contact

Phone +44 (0) 1789 608708.
Website www.istormsolutions.co.uk
Email info@istormsolutions.co.uk

iSTORM®
Privacy • Security • Pentesting

Penetration Testing

EMERGING TRENDS

- **Mandatory Testing for Compliance:** Regulatory bodies like HIPAA are moving toward requiring annual penetration tests for covered entities and business associates.
- **Shift from Vulnerability Scanning to Exploitation Testing:** Regulators and auditors increasingly expect proof that vulnerabilities are not just identified but actively tested and remediated.

THINGS TO WATCH

- **Zero-Day Exploits**: Exploitation of unpatched vulnerabilities is surging—now accounting for 20% of breaches.
- **Integration with DevSecOps**: Expect more demand for continuous testing integrated into development pipelines, not just annual assessments.

Data Protection

EMERGING TRENDS

- **Stricter Enforcement of GDPR Article 32:** Regulators are emphasising the need for "regularly testing, assessing and evaluating" security measures, which includes penetration testing.
- **Rising Cost of Breaches:** The average cost of a data breach in the U.S. has hit $10.22 million, pushing organisations to invest more in proactive data protection.

THINGS TO WATCH

- **AI and Privacy Risks**: As AI adoption grows, expect new scrutiny around data minimisation, algorithmic transparency, and automated decision-making.
- **Cross-border Data Transfers:** Ongoing legal challenges to mechanisms like Standard Contractual Clauses and adequacy decisions could disrupt global data flows.

ISO/IEC27001

EMERGING TRENDS

- **ISO/IEC 27001:2022 Update:** The latest version merges several controls and introduces A.8.29 for "Security testing in development and acceptance," reinforcing the role of penetration testing.
- Pen Testing as Best Practice: While not mandatory, penetration testing is increasingly recommended to meet Annex A controls like A.12.6.1 and A.8.29.

THINGS TO WATCH

- **Alignment with Other Frameworks:** ISO27001 is being linked with other standards like NIST and SOC 2, making cross-framework compliance more achievable.
- Tooling and Automation: Expect more emphasis on automated compliance tooling to streamline audits and evidence collection.

Phone +44 (0) 1789 608708
Website www.istormsolutions.co.uk
Email info@istormsolutions.co.uk

iSTORM® Privacy • Security • Pentesting