SMRT Assessment

Security Maturity, Risk & Threat Assessment
Company 86 | www.c86.tech

Executive Summary

The SMRT Assessment (Security Maturity, Risk & Threat Assessment) is a comprehensive, risk-led security assessment delivered by C86 (Company86). It provides an organisation with a clear understanding of their security posture by combining threat intelligence, security maturity benchmarking, and business risk analysis. The assessment supports informed decision-making across both technical teams and senior leadership.

The Evolving Threat Landscape

The cyber threat landscape is evolving at an unprecedented pace. Threats are becoming more wide-ranging, more targeted, and increasingly sophisticated in nature. Organisation's face a diverse mix of threats, which is increasing in complexity with the adoption of AI. These threats include, advanced persistent threats, ransomware, supply chain compromise, insider risk, and automated attacks leveraging modern tooling and techniques.

Rapid technological advancement is reshaping how organisations operate. Innovations such as cloud platforms, automation, and artificial intelligence (AI) offer significant business benefits, but also introduce new threat vectors and risks if not adopted securely. Many also face a mirid of regulatory obligations requiring clear documented reporting of adherence within their own environment and that of their supply chain.

A structured security maturity assessment enables an organisation to understand how changing threats, regulatory requirements and complexity apply to their specific environment and business model. The SMRT Assessment enables organisations to identify realistic threat scenarios, understand their exposure, and develop practical, prioritised

recommendations to protect against current threats while preparing for future technological change.

Service Overview

The SMRT Assessment ensures that security maturity is assessed in the context of real-world threats, regulatory requirements and business impact. Rather than focusing solely on compliance, the assessment takes a risk-based approach that aligns security investment to the threats an organisation faces and the outcomes that matter most to the business.

Assessment Components

i) Threat Assessment

The threat assessment identifies and evaluates the threat landscape most relevant to the organisation, its industry, and operating environment. This includes:

- Threat research aligned to the organisation and sector
- Facilitated threat workshop with key business and technical stakeholders
- Analyst-led and tool-based threat hunting activities

This approach provides a tailored view of threat actors, attack techniques, and realistic threat scenarios that are most likely to impact the organisation.

ii) Security Maturity Assessment

The security maturity assessment measures current security capabilities against a customer-selected set of requirements, ensuring flexibility and relevance. These may include:

- Industry benchmarks
- Recognised security frameworks such as ISO/IEC 27001 or the NIST Cybersecurity Framework (CSF) CAF etc.
- Regulatory and compliance obligations specific to the customer's industry

The outcome is a clear view of current maturity levels, strengths, and gaps across people, process, and technology.

iii) Risk-Based Assessment & Analysis

The risk-based assessment contextualises security maturity against identified threats and potential business impact. This ensures that maturity gaps are prioritised based on risk, likelihood, and impact, enabling practical and defensible security decision-making.

Assessment Deliverables

The SMRT Assessment includes the following deliverables:

- Full detailed assessment report covering threats, maturity, and risk analysis
- Executive summary assessment suitable for senior leadership and board-level audiences
- Risk-prioritised findings and observations
- Clear, actionable recommendations and next steps roadmap

Recommendations & Next Steps

C86 provides clear, practical recommendations based on the outcomes of the SMRT Assessment. Recommendations are designed to help organisations protect against current threats while also enabling the secure adoption of future technologies, including AI and automation.

- Immediate risk reduction and quick-win improvements
- Medium-term security maturity enhancements
- Strategic initiatives to support secure, assured technology adoption

Why C86

C86 specialises in security, risk, and IT transformation services in the private and public sector. Our consultants combine deep technical expertise with strong business insight, enabling organisations to improve security maturity, reduce risk, and adopt new technologies with confidence.

Contact Us

www.c86.tech
info@c86.tech