resillion

Assure. Secure. Innovate.

Penetration Testing Services By Resillion

Resillion, your strategic quality partner - providing global quality engineering, testing, conformance, interoperability, and assurance services from initiation to launch across software systems, cyber security, devices, digital products, and media content.

Cybersecurity-Enhanced Total Quality 360 – The Resillion Advantage

Resillion stands in a unique position in today's digital assurance landscape. We bring together the full spectrum of cyber capabilities—penetration testing, vulnerability assessments, compliance, and security by design—and seamlessly combine them with our expertise in Conformance and Interoperability, end-to-end Content Testing, and Quality Engineering. The result? A comprehensive and secure assurance service we call Total Quality 360.

This unified approach allows us to not only test your products and systems thoroughly—but also to secure them by default. From streaming content to connected devices, every element of your digital ecosystem can be validated, certified, and cyber-hardened under one roof.

Cyber-Powered by AI and Data-Led Quality Engineering

We are also leading the way in applying Artificial Intelligence across the assurance lifecycle. Whether you're just beginning your AI journey or looking to expand its impact, we help you navigate the strategy, integration, and upskilling to get the most value.

With AI and data-led automation embedded throughout our Quality Engineering and Cyber services, you benefit from:

- **Quality Intelligence**: Deep insight into end-user experience, with real-time data helping you spot issues before they affect your customers.
- **AI-Driven Security Testing**: We detect and address cyber threats faster and more accurately, using smart tools that scan code, data, and behaviour patterns for vulnerabilities.
- **Automated Penetration & Vulnerability Testing**: Our cyber specialists simulate real-world attacks using actual usage data to uncover risks—before attackers do.

In short, Resillion delivers cyber-secure quality at scale, powered by intelligent automation and a holistic approach to assurance.

Our penetration testing capabilities

- **Network/Infrastructure Penetration Testing**
  Audit internal and external networks for misconfigurations, exposed services, and segmentation flaws using real-world attacker techniques.
- **Web Application and API Penetration Testing**
  Assess OWASP Top 10 risks, business logic vulnerabilities, and session flaws with a combination of automated and manual testing.
- **Client-Side Penetration Testing**
  Test endpoints for privilege escalation, insecure storage, DLL hijacking, and browser-based attacks.
- **Wireless Network Penetration Testing**
  Simulate rogue APs and encryption-breaking attacks to assess Wi-Fi segmentation and authentication security.
- **Social Engineering Penetration Testing**
  Evaluate human vulnerabilities through phishing, vishing, and impersonation-based attack simulations.
- **Cloud Penetration Testing**
  Identify risks in AWS, Azure, or GCP environments such as exposed storage, IAM misconfigurations, and insecure APIs.
- **DevOps Security**
  Maturity assessment, Automated SAST & DAST, SCA (software composition analysis), IaC scanning (infrastructure as code), agile penetration testing.
- **Agile Penetration Testing**
  Align security testing with sprints and CI/CD workflows to catch issues before deployment.
- **Other Testing types**

  Vulnerability Assessment (VA), Build Reviews, Configuration Reviews (cloud, containers, firewalls, databases and more), Thick Client testing, Hardware Device Testing (e.g. IoT devices, drones and other hardware) and more.

Some of the companies we work with:

Our Powerhouse PTaaS

Discover security vulnerabilities before attackers do. Understand and prioritise remediation by out how your applications, systems and people respond to real-world attack scenarios. Wherever your data assets are, they need constant protection from an ever-changing threat landscape.

Why choose Powerhouse Pentest-as-a-Service?

- **Recognised Industry Experts**
  Our testers regularly uncover critical vulnerabilities in widely used systems. Our dedicated Vulnerability & Exploit Development Lab ensures we stay ahead of attackers.
- **Faster & More Efficient Testing**
  35x faster than the industry standard, with full reports delivered within 5 days of test completion. This means quicker time-to-remediation and less exposure to risk.
- **Seamless Integration**
  Reports in PDF and CSV format. Our platform supports ticketing, workflow automation, and developer collaboration, simplifying your vulnerability management.
- **Cost-Effective Without Compromise**
  We deliver top-tier quality at lower costs through automation and expert validation. More value, less waste.
- **Ahead of the regulatory curve**
  We are helping our customers comply with all regulatory requirements such as DORA, NIS2 and TIBER
- **Industry-Recognised Accreditations**
  CREST Penetration Testing and CCV Keurmerk certifications ensure global security standards are met.

Why is security testing important?

Thousands of technical vulnerabilities are discovered every year. If undetected these can lead to unintentional loss or provide hackers with a point of weakness to initiate an attack. As well as this, your people remain, if not properly educated and aware, a significant weakness in your security control regime. Threats are evolving and increasing in technical assurance sophistication. Attackers increasingly have the motivation, resources, tools and time to crack through corporate defences, driven by the prospect of financial gain, hacktivism, or simply to cause mayhem. At stake is the potential compromise of your critical business information, and the privacy of your employees, clients and suppliers. An appropriate penetration testing programme, combining various approaches, should be an essential element of your information security management control framework. Testing should be carried out regularly and after any significant change to a system. The resulting insight into your vulnerabilities will allow you to make knowledge-based, considered risk management decisions on mitigation or risk acceptance.

Resillion's commitment is underscored by numerous certifications, including Cyber Essentials Plus, ISO 9001, ISO 27001, ISO 17025, CREST SOC, CREST Penetration Testing, CREST STAR, and a UK NCSC Assured CHECK Penetration Testing Team

Built for the future

- Continuous updates and cutting-edge research keeps your cybersecurity posture ready for tomorrow's threats.

What is Powerhouse Pentest-as-a-Service?

A standardised, off-the-shelf penetration testing solution designed for speed, efficiency, and effectiveness. Powerhouse PTaaS (Pentest-as-a-Service) makes security testing faster, leaner, and smarter for modern digital businesses.

Key features

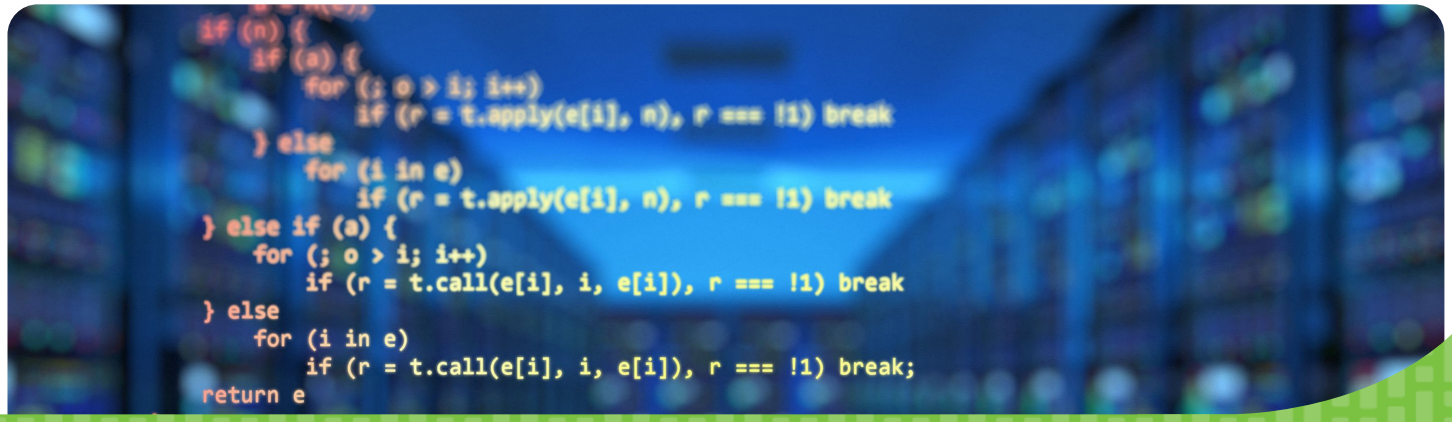
- On-demand availability with simple booking
- Combination of automated scanning and manual testing
- Ready for cloud-native, IoT, and API-heavy environments
- Real-time visibility via dashboards (SPOG) and integrations

How this helps you:

- Reduce time and effort to meet compliance goals
- Minimise risk exposure with faster identification of vulnerabilities
- Improve collaboration across your security and development teams
- Increase efficiency with test results that plug into your existing systems

Powerhouse vs Traditional Penetration Testing

Aspect	Traditional Penetration Testing	Powerhouse Pentest-as-a-Service
Engagement Type	Fully customised	Standardised, repeatable
Booking	Manual scoping, scheduling delays	Book via call or online portal
Start Time	1–3 weeks average	Same week or next-day availability
Testing Duration	2–6 weeks	1–2 weeks average
Reporting Time	10–15 days	Within 24 hours of test completion
Integration	Limited support for tools	Ready for CI/CD, JSON & API outputs
Ideal For	Deep-dive audits	Fast-moving environments, DevOps cycles



resillion

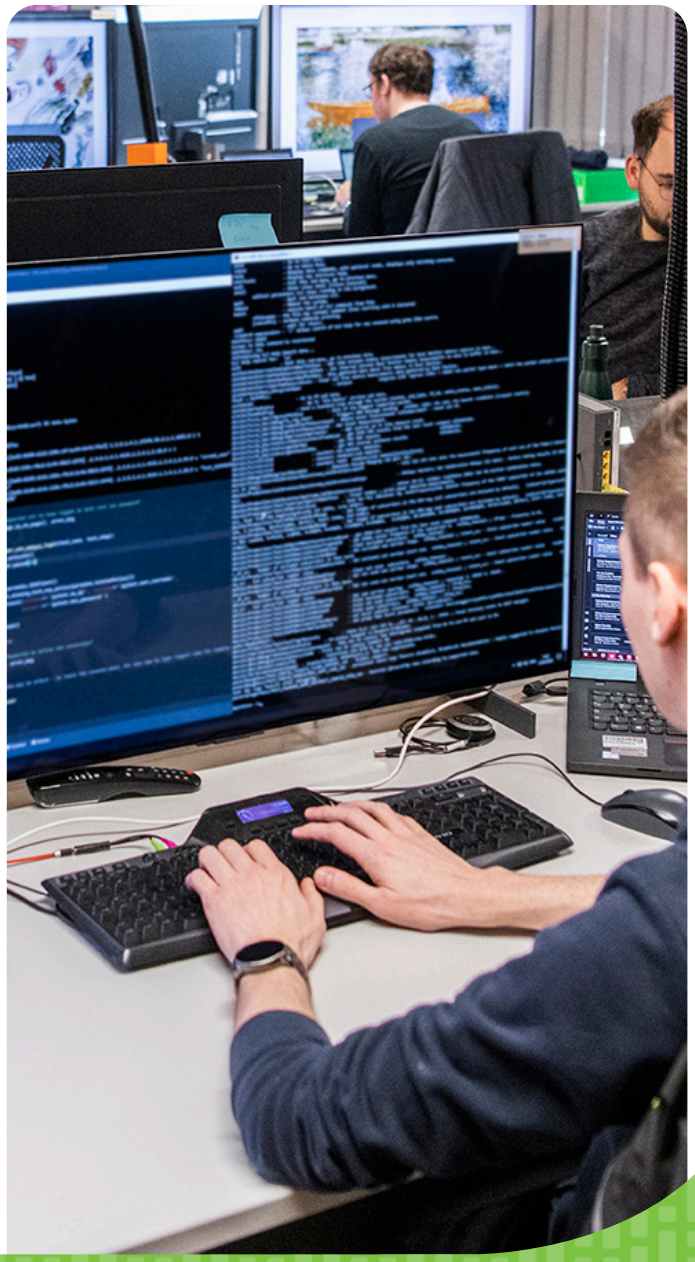
Assure. Secure. Innovate.

Common vulnerabilities addressed

- Insecure system and cloud configurations
- Unpatched software and outdated dependencies
- Weak authentication mechanisms (e.g., weak passwords, lack of MFA)
- Missing or improper access controls
- Exposure of sensitive data
- OWASP Top 10 vulnerabilities for web, API, and mobile applications

Included tests

- Network Infrastructure (Internal/External)
- Web & Mobile Apps (OWASP Top 10, ASVS)
- API Security (CREST-certified)
- Binary Application Security



Example Engagements

CREST Certified - Intelligence Led Penetration Testing (STAR)

Duration: 3–8 weeks
Complexity: High

Simulate real-world cyber threats and build operational resilience:

- **Red Teaming**
  Mimics APTs using stealth, phishing, and lateral movement to identify critical security gaps.
- **Blue Teaming**
  Strengthens internal defences, monitoring, and response capabilities in collaboration with your SOC and IT teams.
- **Purple Teaming**
  Combines red and blue strategies in real time to improve detection, visibility, and tactical readiness.

Aspect	Penetration Testing	Red-Team engagement
Primary Objective	Identify all vulnerabilities in a specific scope	Simulate a real-world adversary to test detection and response
Scope & Duration	Typically narrower scope, focussed on defined targets: Short to medium engagements (day/weeks). Point-in-time	Broader scope, can include multiple attack vectors: longer engagements (typically months). Whole organisation view
Methodology	Systematic testing of systems in scope. 'Noisy' and quick in an attempt to find all vulnerabilities	Creative, stealthy, multi-phase campaign mimicking actual threat actors
Team Focus	Exploit vulnerabilities to demonstrate risk	Test overall security posture, including people, processes and technology
Outcome	Detailed list of findings and remediation steps	Evaluation of blue teams ability to detect and respond to real attacks

Key benefits

- Mapped to MITRE ATT&CK and aligned with NIS2, GDPR, ISO 27001, DORA
- Validates tooling, playbooks, and detection maturity
- Promotes cross-team collaboration and a security-first culture

Internal Auditing (Penetration Testing Focus)

Duration: 4–12 weeks
Complexity: Medium

Go beyond compliance checklists with audits that simulate insider threats and lateral movement.

Scope Includes:

- Internal apps and infrastructure
- Domain trusts and escalation paths
- Log coverage and alerting gaps
- Patch, configuration, and access control weaknesses

Why It Matters:

- Uncover internal threat surfaces
- Validate real-world effectiveness of controls
- Demonstrate resilience for ISO 27001, CRA, DORA, NIS2, UNECE R155
- Strengthen audit-readiness and board-level assurance

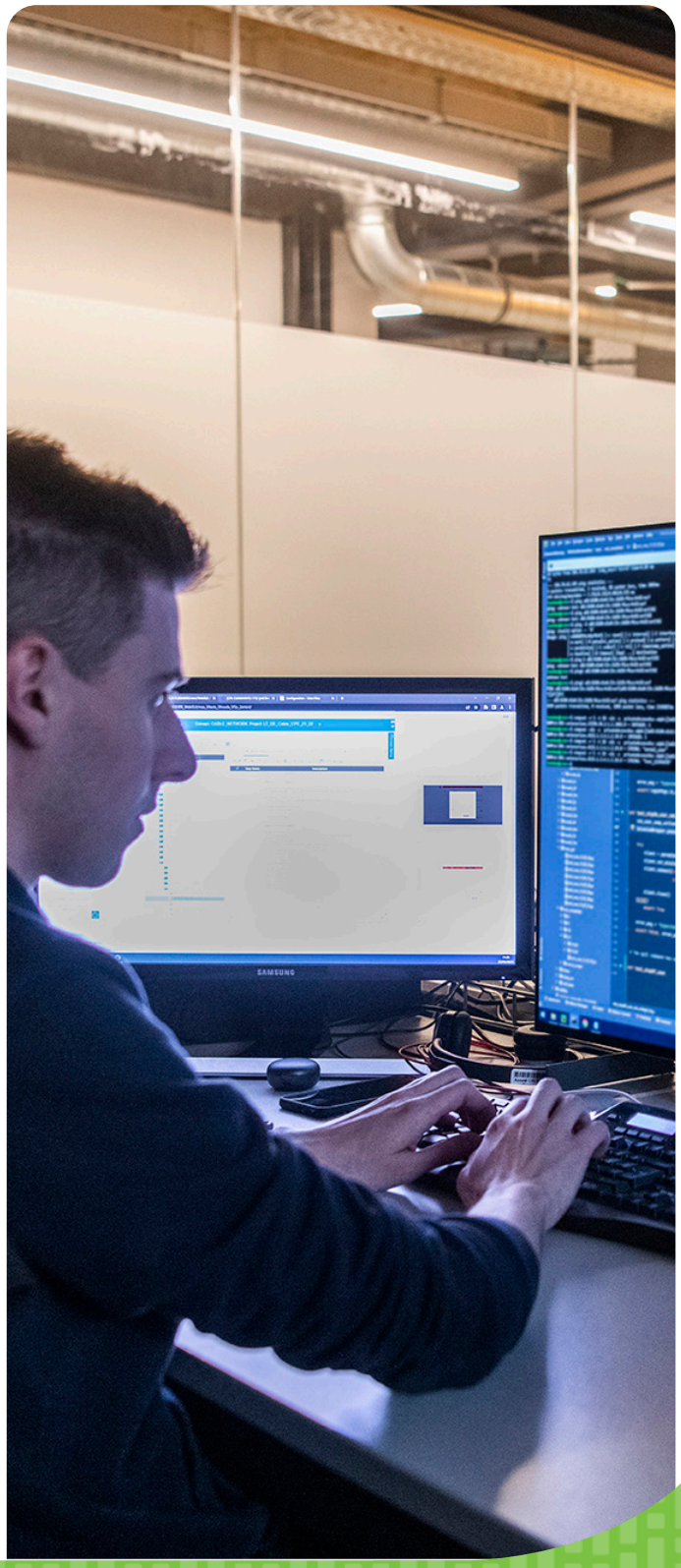
Compliance & Low Disruption

Supports Compliance With:

- PCI-DSS
- ISO 27001
- GDPR
- HIPAA

Disruption Level:

- Minimal Disruption.. High transparency. Testing is designed to be non-intrusive and business-aware, with real-time communication and alignment with operational windows.



Our experience - Banks and Financial Services

In today's evolving threat landscape, regulatory bodies across the globe mandate or strongly recommend **penetration testing (pen testing)** as a core component of cybersecurity and operational risk management. For banks and financial institutions, regular pen testing isn't just best practice—it's a **regulatory necessity** that directly supports compliance, customer trust, and systemic resilience.

At Resillion, we specialise in delivering advanced penetration testing and red teaming services that align with global and local financial regulations. Our expert teams and powerful **Penetration Testing-as-a-Service (PTaaS)** platform ensure you stay ahead of threats and aligned with regulatory expectations—no matter where you operate.

Regulation / Standard	Region	Pen Testing Requirement	How Resillion Helps
SWIFT CSP	Global	Annual independent assessment including pen testing (e.g. CSCF Control 6.4).	Certified, third-party testing aligned to SWIFT Customer Security Controls.
CBEST (Bank of England)	UK	Intelligence-led red teaming for systemically important financial institutions.	Our threat-led red teaming methodology meets CBEST standards using real-world TTPs.
TIBER-EU	EU	Threat Intelligence-Based Ethical Red Teaming.	Full-spectrum red teaming execution and threat simulations in line with TIBER-EU.
DORA (Digital Operational Resilience Act)	EU	TLPT (Threat-Led Pen Testing) at least every 3 years starting 2025.	DORA-aligned testing with evidence-based reporting for regulators.
FFIEC / GLBA / OCC	USA	Regular pen testing and vulnerability assessments strongly encouraged.	Services mapped directly to FFIEC IT Handbook requirements and GLBA data protection mandates.
PCI DSS	Global	Internal and external pen testing annually and after major changes.	Full PCI DSS compliance ensured with comprehensive network and application testing.
RBI Cybersecurity Guidelines	India	Regular VAPT (Vulnerability Assessment & Penetration Testing).	Support for Indian banks with RBI-aligned testing and detailed remediation guidance.
MAS TRM Guidelines	Singapore	Annual pen testing of critical systems.	Secure architecture reviews, system hardening, code validation & testing, and pen testing tailored to MAS TRM.

Our experience - Banks and Financial Services

Global and UK Banks and Financial Services companies

Penetration testing is not optional—it's a **strategic and regulatory** imperative for banks operating in the UK and across international markets:

- **UK banks** face intense scrutiny from regulators like the Bank of England and PRA, especially those classified as systemically important. CBEST testing is now a cornerstone of demonstrating resilience under real-world attack scenarios.
- **Global banks** operating in the EU must align with **DORA, TIBER-EU**, and local central bank requirements (e.g. Bafin, Banque de France), which emphasize **Threat-Led Pen Testing (TLPT)**.
- Multinational banks operating in North America, Asia, or Africa must meet a patchwork of frameworks from **FFIEC and GLBA to MAS, RBI, and SWIFT**—each requiring tailored penetration testing and ongoing vulnerability management.
- With increased regulatory coordination, global institutions are expected to harmonize their testing approach across geographies.

Resillion helps banks **unify and streamline** their **testing strategies across borders, business units, and compliance frameworks**—offering a single partner with global reach and local insight.

Why Choose Resillion?

- **Deep Regulatory Expertise**
  We bring years of experience supporting banks, asset managers, fintechs, and financial service providers through audits, threat simulations, and assessments across multiple jurisdictions.
- **Powerhouse PTaaS Platform**
  Our Penetration Testing-as-a-Service combines manual and automated testing, real-time dashboards, ticketing integration (e.g. Jira), and remediation tracking—all in one secure platform.
- **Global Coverage, Local Knowledge**
  With testing teams across Europe, the US, Middle East, and Asia, Resillion offers global delivery with regional compliance insight. Whether it's TIBER in the EU or CBEST in the UK—we've got you covered.
- **Beyond the Checkbox**
  We don't just test and report—we partner with your security and compliance teams to close gaps, elevate security maturity, and build long-term resilience.

Other services

As part of Resillion's Total Quality 360 solution, in addition to Penetration Testing, Resillion offers a full suite of services tailored to the needs of banks, fintech's, and financial institutions.

Cybersecurity Services

- Penetration Testing & Red Teaming (PTaaS)
- Cloud Security Assessments
- Threat Modelling
- Risk & Maturity Assessments
- Cyber Resilience, Incident Response Planning & Security Awareness Training
- Security Code Review & Secure SDLC

Quality Engineering & Testing

- End-to-End Functional Testing
- Test Automation Strategy & Execution
- Performance & Load Testing
- Data Migration & Integration Testing
- Regression Suite Development
- Quality Advisory & QA Transformation
- Total Quality 360 Framework

Compliance & Certification

- PCI DSS, SWIFT CSP, ISO 27001, SOC 2 readiness
- DORA and CBEST/TIBER support services
- Audit Support & Documentation
- Vulnerability Management & Hardening

Digital Platform Assurance

- Device & Browser Compatibility Testing
- Accessibility (WCAG) Compliance Testing
- App Store Readiness & UX Assurance
- AI & Algorithmic Bias Testing

Let's Secure Your Digital Future

Our Powerhouse-PT and PTaaS solutions are built to help your organisation move fast and stay secure. Whether you're a fintech startup, an automotive OEM, or a highly regulated enterprise, Resillion ensures you stay one step ahead of threats while meeting the highest compliance standards.

Resillion's commitment to excellence is underscored by our numerous certifications, including Cyber Essentials Plus, ISO 9001, ISO 27001, ISO 17025, CREST SOC, CREST Penetration Testing, CREST STAR

Let's Talk

If you're preparing for a regulatory assessment or looking to modernise your pen testing strategy, Resillion is here to help. From one-time tests to fully managed PTaaS engagements, we're ready to support your compliance and security goals

Contact us today to schedule a consultation or request a proposal.

CHECK IT Health Check Service
CREST
Cyber Essentials Certified Plus
Assured Service Provider in association with National Cyber Security Centre
ISO 27001 ISOQAR Registered
ISO 9001 ISOQAR Registered
Crown Commercial Service Supplier

Talk to us today about how Resillion can simplify and strengthen your cybersecurity posture - quickly, effectively, and without the hassle.

Get in touch: hello@resillion.com.

resillion

Assure. Secure. Innovate.