Integrity360

your **security** in mind

Penetration Testing as a Service (PTaaS)

Introduction

Cyber threats are constantly evolving—and so should your defences. Traditional penetration testing, often carried out once a year, is no longer sufficient for organisations with dynamic IT environments and continuous development cycles. Integrity360's Penetration Testing as a Service (PTaaS) changes that paradigm. It offers a flexible, scalable, and always-on model that embeds testing into your cyber defence programme throughout the year.

PTaaS is designed to meet the needs of organisations facing fast-moving threat landscapes, ongoing infrastructure changes, frequent software releases, and stringent compliance demands. Instead of relying on one-off reports, clients gain access to a continuous assessment model with self-service scheduling, real-time dashboards, integrated ticketing workflows, and expert remediation support.

With PTaaS, penetration testing becomes an operational security control—not just a compliance checkbox. It enables you to understand your exposures as they emerge, improve mean time to remediation, and prioritise actions based on risk—not calendar dates. Delivered through a secure SaaS platform and backed by seasoned penetration testers and technical leads, the service ensures that your testing programme is always aligned to your business needs.

Penetration Testing - key stats

Sources: Cobalt/Cyentia Research - Stare of Pentesting Report 2025

Whether you're focused on protecting customer data, validating new applications, or meeting regulatory obligations, PTaaS gives you the tools, intelligence, and expertise to stay secure. With Integrity360, security testing becomes a proactive, strategic advantage.

How it works

Integrity360's PTaaS is a managed subscription service that delivers regular, flexible penetration testing through an intuitive SaaS platform. At the core of the service is a pre-purchased block of testing days, used flexibly throughout the year—monthly or quarterly—depending on your chosen package. This gives you predictable budgeting and total control over when and where testing occurs.

The service begins with a detailed onboarding workshop led by your assigned Technical Test Lead (TTL). They'll capture your business objectives, align testing scopes, and establish a governance model to ensure continuous value. From there, you can schedule tests, track findings, request retests, and access detailed dashboards via the portal.

Available test types include internal and external infrastructure, web and mobile applications, APIs, Active Directory, IoT, wireless networks, and cloud environments. Identity/AD/Entra ID testing, user testing and training, vulnerability assessments, and configuration audit services are also available under the model.

Traditional CST vs Pen Testing as a Service

Traditional Pentesting	Pentesting as a Service
Project Based service	Subscription based service
Once-off testing events	Regular / Ongoing pen testing
Supports infrequent testing requirements	Supports regular/ongoing testing requirements
Manual request-based scheduling	Customer self-schedules according to their needs
Once off PDF-based reporting	SaaS-based interface for ongoing viewing and tracking findings
Point in time governance and coordination	Ongoing engagement and governance
Payment per engagement	Payment under subscription
Human-led	Human-led, but increased use of tools and automation

Pen Testing as a Service

Retesting is included at no additional cost, so you can validate fixes without using up your balance. **Findings are automatically mapped to assets and can be pushed into ticketing systems like Jira or ServiceNow, streamlining remediation workflows.** Real-time analytics and dashboards help track progress and identify patterns across your environment.

Whether you're facing compliance deadlines, launching new apps, or managing a hybrid infrastructure, PTaaS makes expert-level security testing part of your operational rhythm—cost-effective, continuous, and integrated.

All of the following services are the types of testing that are available under Pen Testing as a Service.

Penetration Testing Services

Internal/external infrastructure testing

Identifies vulnerabilities in internal and public-facing infrastructure. Internal tests simulate insider threats, while external tests focus on perimeter defences like firewalls, VPNs, and cloud interfaces. Misconfigurations, outdated software, and open ports are flagged. Delivered on demand via PTaaS with workflow integration.

Web application testing

Assesses web applications for issues like SQL injection, XSS, CSRF, and insecure authentication. Testing combines automation with expert validation, aligned to OWASP Top 10. Delivered through PTaaS with dev-ready reporting and CI/CD integration.

API testing

Examines REST and SOAP APIs for security flaws including broken auth, logic weaknesses, and excessive data exposure. Coverage includes token handling, input fuzzing, and privilege testing. PTaaS enables scheduled and scalable API testing aligned to your release cycle.

Mobile application testing

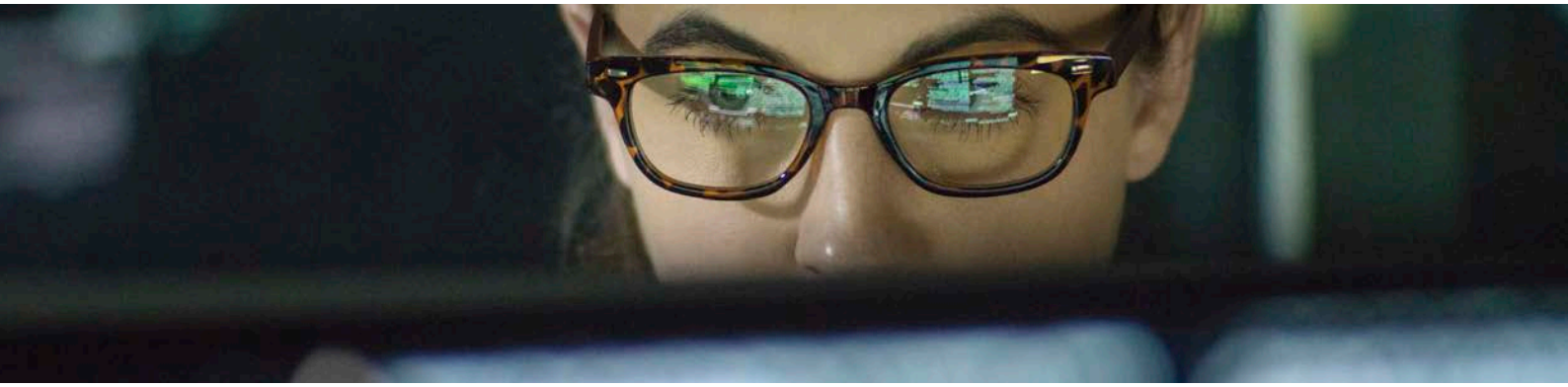
Evaluates Android and iOS apps for reverse engineering risks, insecure storage, and data leakage. Conducted using real devices and emulators, with findings mapped to OWASP Mobile Top 10. Available through PTaaS with automated reporting and integration capabilities.

Cloud security testing

Tests AWS, Azure, and GCP environments for misconfigurations, insecure access, and overly permissive roles. Includes Infrastructure-as-Code reviews and cloud-specific threat simulation. Results are aligned to CIS Benchmarks. PTaaS ensures continuous coverage as your cloud environment evolves.

Active Directory / Entra ID testing

Assesses identity infrastructure for misconfigurations, privilege escalation paths, and trust exploitation. Simulates real-world attack techniques like Kerberoasting and Pass-the-Hash. PTaaS supports regular identity reviews and remediation tracking.



Wireless network testing

Identifies risks like rogue access points, weak encryption protocols, and insecure guest access. Includes simulations of Evil Twin and WPA cracking attacks. PTaaS allows scheduled testing and integration into wireless infrastructure upgrades.

IoT security testing

Analyses smart devices and sensors for firmware flaws, insecure communications, and default credentials. Includes interface testing (e.g. Bluetooth, Zigbee). PTaaS supports ongoing security assurance for connected ecosystems.

AI penetration testing

Secures AI/ML models against manipulation, adversarial input, and data leakage. Evaluates training data, inference APIs, and model logic. Testing supports safe and ethical AI deployment. PTaaS enables routine checks aligned to model iteration.

Vulnerability Scanning and Assessment Services

External infrastructure scanning

Automated scanning of internet-facing systems like firewalls and cloud interfaces to detect known vulnerabilities and misconfigurations. Ideal for perimeter risk management and regulatory alignment. Available as part of PTaaS or standalone.

Internal infrastructure scanning

Covers internal devices including servers, endpoints, and printers. Identifies exposures such as unpatched software, risky services, and insider threat vectors. Delivered through PTaaS with scheduled automation and expert support.

Network segmentation testing

Validates that VLANs, firewalls, and routing rules properly isolate systems and restrict lateral movement. Ensures segmentation policies align with business and security needs. Available under PTaaS as part of broader infrastructure testing.

Web application scanning

Automated detection of application-layer flaws like XSS, SQLi, and insecure sessions. Validated to reduce false positives and aligned with OWASP Top 10. PTaaS delivers results with actionable advice for developers.

Managed vulnerability scanning & assessment

Vulnerability scanning and assessment is also available as a fully managed service, offering regular scans, risk-based prioritisation, and expert-led assessments. Includes compliance alignment (e.g. ISO 27001, PCI DSS, DORA). Reduces operational burden and ensures continuous visibility.

Other services available under PTaaS

In addition, User security awareness testing and training services, and comprehensive configuration audit services are also available under the PTaaS model.

Key features and benefits

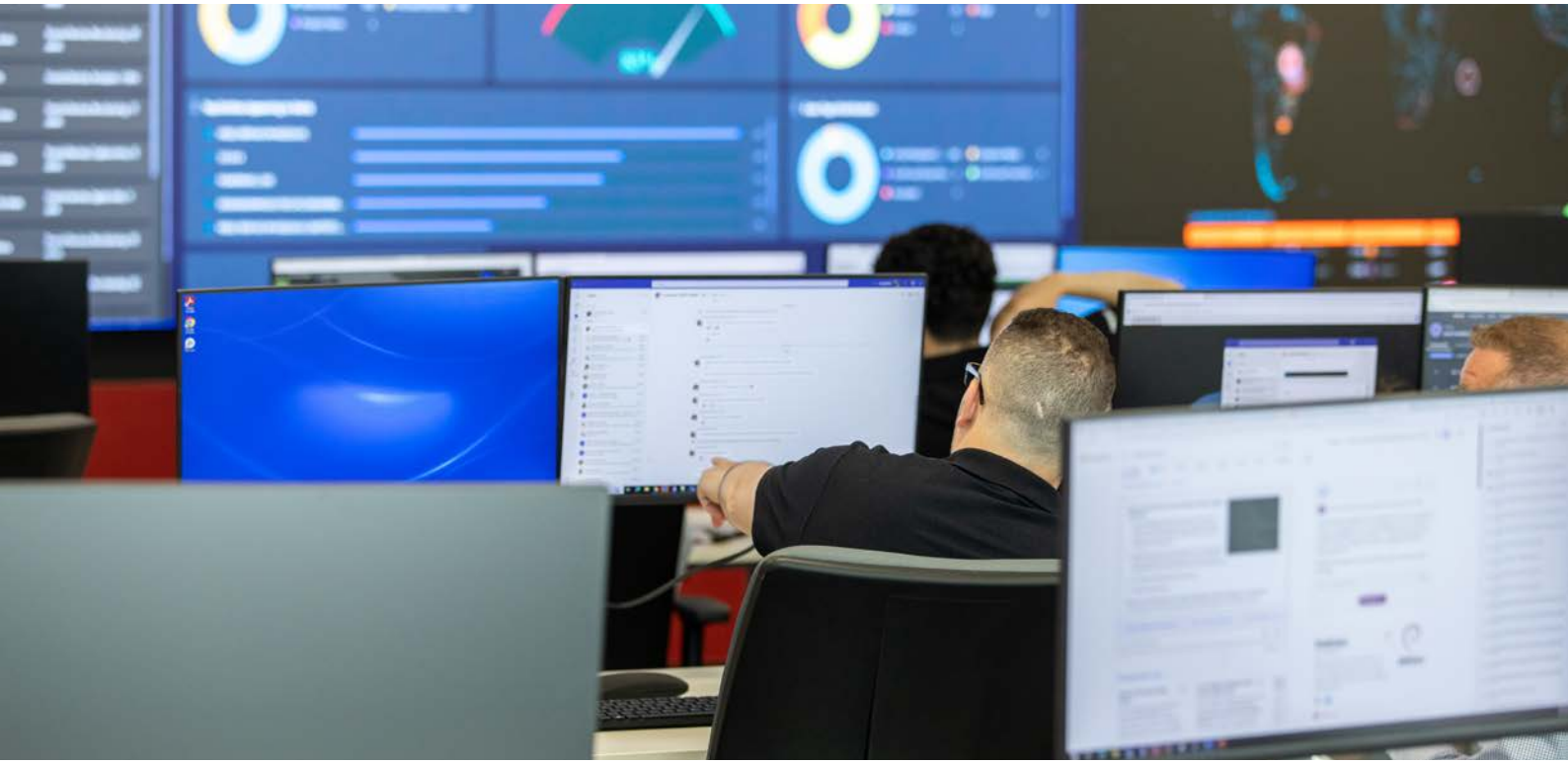
Integrity360's Penetration Testing as a Service (PTaaS) is a comprehensive solution engineered to deliver security testing as a fully managed, continuous service. Our PTaaS model is built around the core principle of delivering expert-led testing with all the flexibility, visibility, and governance today's businesses demand.

Clients start their journey with a service planning kick-off workshop, facilitated by a dedicated Technical Test Lead, who remains with them throughout the subscription period. This ensures continuity, expert guidance, and an alignment of testing activities to organisational goals.

The service is underpinned by a SaaS-based interface that enables seamless communication, subscription management, test scheduling, and access to findings in real time. **Customers can schedule tests via an intuitive portal, access detailed dashboards, and monitor remediation progress through integrations with downstream ticketing systems such as Jira and ServiceNow.**

PTaaS includes standard retests to verify successful remediation, and any unused test allowances can be carried over between months—offering unmatched operational flexibility. Should additional capacity be required, clients can purchase extra test days on demand.

Regular governance calls keep your security strategy on track, allowing for periodic review, planning, and optimisation. All findings are mapped to business assets to help prioritise actions that reduce real-world risk.



From start to finish, PTaaS is designed to reduce overhead, streamline processes, and strengthen your security posture with consistent, expert-led testing. With Integrity360, you gain more than a service—you gain a security partner committed to long-term resilience and assurance.

Core features include:

- **Dedicated Technical Test Lead:** Support and guidance around the entire testing programme from an experienced testing professional throughout the entire subscription
- **Real-time dashboards:** View findings by severity, asset, and remediation status
- **Automated ticketing integration:** Push vulnerability remediation actions downstream ticketing systems such as Jira or ServiceNow
- **Asset-based findings:** Link exposures to affected systems for accurate resolution
- **Retesting included:** Validate remediations without consuming your test day allowance
- **Vulnerability scans:** Complimentary scans for ongoing exposure management
- **Governance and reporting:** Regular reviews of performance, findings, and plans
- **Phishing awareness tests:** Included in high-tier subscriptions

What makes it different?

PTaaS from Integrity360 is built to solve the shortcomings of traditional pen testing engagements. While legacy models often result in fragmented security efforts, delayed remediation, and static PDF reports, PTaaS offers a living, integrated service designed for modern cyber challenges.

Key differentiators include:

- **Continuous testing approach:** Unlike once-a-year engagements, PTaaS supports continuous assessment aligned with your release cycles and infrastructure changes.
- **Self-service flexibility:** Schedule tests on your terms through an intuitive portal, cutting down on delays and paperwork.
- **Integrated remediation workflows:** Findings are automatically fed into your existing ticketing systems for efficient resolution.
- **Expert oversight:** A designated TTL ensures the service delivers value aligned with your goals, offering strategic input and governance.
- **Data-driven insights:** Consolidated dashboards provide visibility across tests, assets, and remediation activities—ideal for compliance and audit readiness.
- **Operational efficiency:** Reduce testing overhead, eliminate repetitive scoping meetings, and maintain momentum with complimentary retests and vulnerability scans.

This isn't just a pen test—it's a service engineered to strengthen your entire security posture. It's time to move from periodic testing to continuous assurance.

The Integrity360 PTaaS Portal

The Integrity360 PTaaS Portal is an essential tool for organisations looking to manage their security exposures efficiently. Designed to provide real-time insights into vulnerabilities identified during Cyber Security Testing, the portal offers:

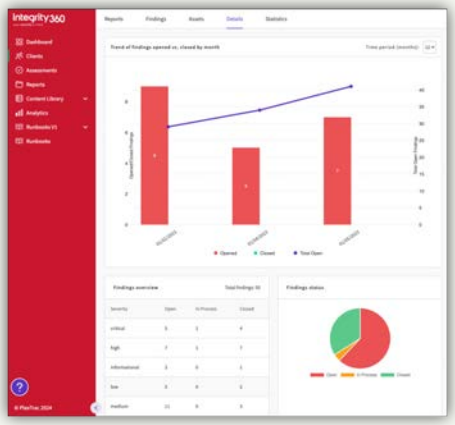
- **Test Scheduling:** Request your specific tests via the convenient online scheduler.
- **Centralised vulnerability management:** All findings from vulnerability assessments and penetration tests are stored in one place, ensuring easy access and tracking.
- **Detailed risk ratings:** Each vulnerability is assigned a risk score, helping organisations prioritise remediation efforts based on severity and exploitability.
- **Remediation tracking:** Monitor the status of identified vulnerabilities, track progress on remediation actions, and ensure issues are resolved effectively.
- **Exploit evidence & Technical guidance:** Findings include step-by-step reproduction details and recommended mitigation strategies, ensuring clear and actionable insights.
- **Compliance support:** The portal assists in meeting regulatory requirements by maintaining a historical record of vulnerability assessments, remediation efforts, and security improvements.
- **Secure client access:** Each organisation receives dedicated access to their own vulnerability reports, with strict permission controls to maintain confidentiality.
- **24/7 availability:** The portal is accessible at any time, allowing security teams to review findings and implement fixes as needed.

By leveraging the Integrity360 PTaaS Portal, organisations can proactively address security exposures, streamline remediation efforts, and continuously improve their cyber security posture.

The PTaaS portal powers the service and is the one stop shop for keeping track of test planning, scheduling, results, findings, assets, remediation tracking, reports, and dashboards.

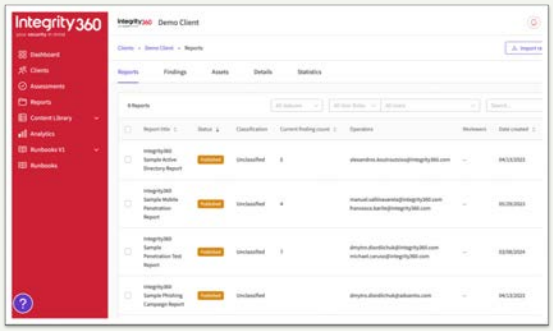
Through the portal, clients will receive comprehensive reporting on the security issues discovered in the targeted applications and infrastructure. Features of the portal include:

- Online Dashboard, available 24x7
- Complete visibility of findings and trends
- Ability to drill down into any detail
- All reports and vulnerabilities in one place
- Remediation tracker with the history of remediation
- Vulnerabilities assignment
- Assets inventory
- Email notifications
- Ability to schedule engagements



Client Access

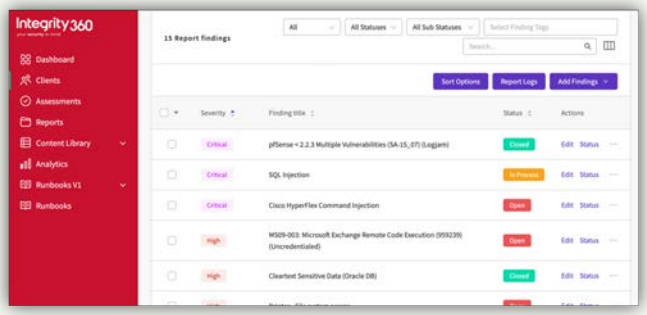
- Each client has dedicated, secure space
- Clients can have several tenants in the console to represent different business units or sub organisations
- 24/7 online access is provided to up to 3 users as standard



Online Reporting details

Each finding is assigned a risk rating and includes evidence that the stated flaws exist, as well as examples and best practices that developers can use to identify and resolve the stated issue.

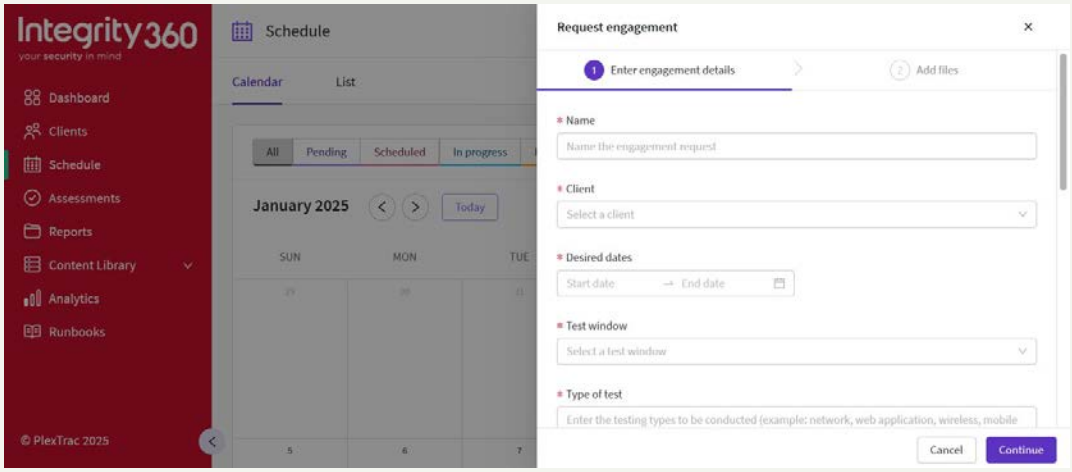
- Title
- Risk score
- Remediation status
- Exploitation status
- Technical description
- Steps to reproduce and evidence of exploitation
- Remediation actions and references



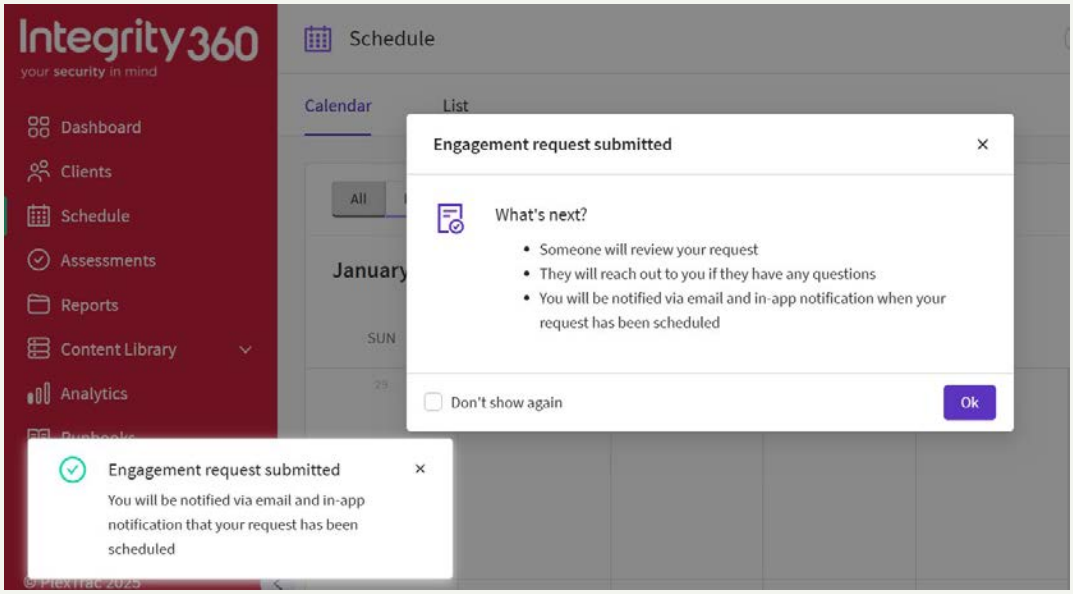
Test request scheduling

Customers can request their pen testing activities via the scheduling interface.

Scheduling:



Submission confirmation



Through the power of the Integrity360 Penetration Testing as a Service portal, clients are provided with maximum visibility and control of their penetration testing activities.

Why Integrity360 for Penetration Testing as a Service?

Choosing the right partner for Penetration Testing as a Service (PTaaS) is critical to maintaining a strong, responsive cyber security posture. At Integrity360, we go beyond one-off engagements to deliver continuous, expert-led testing aligned to your evolving needs—backed by real-world experience and industry-leading certifications.

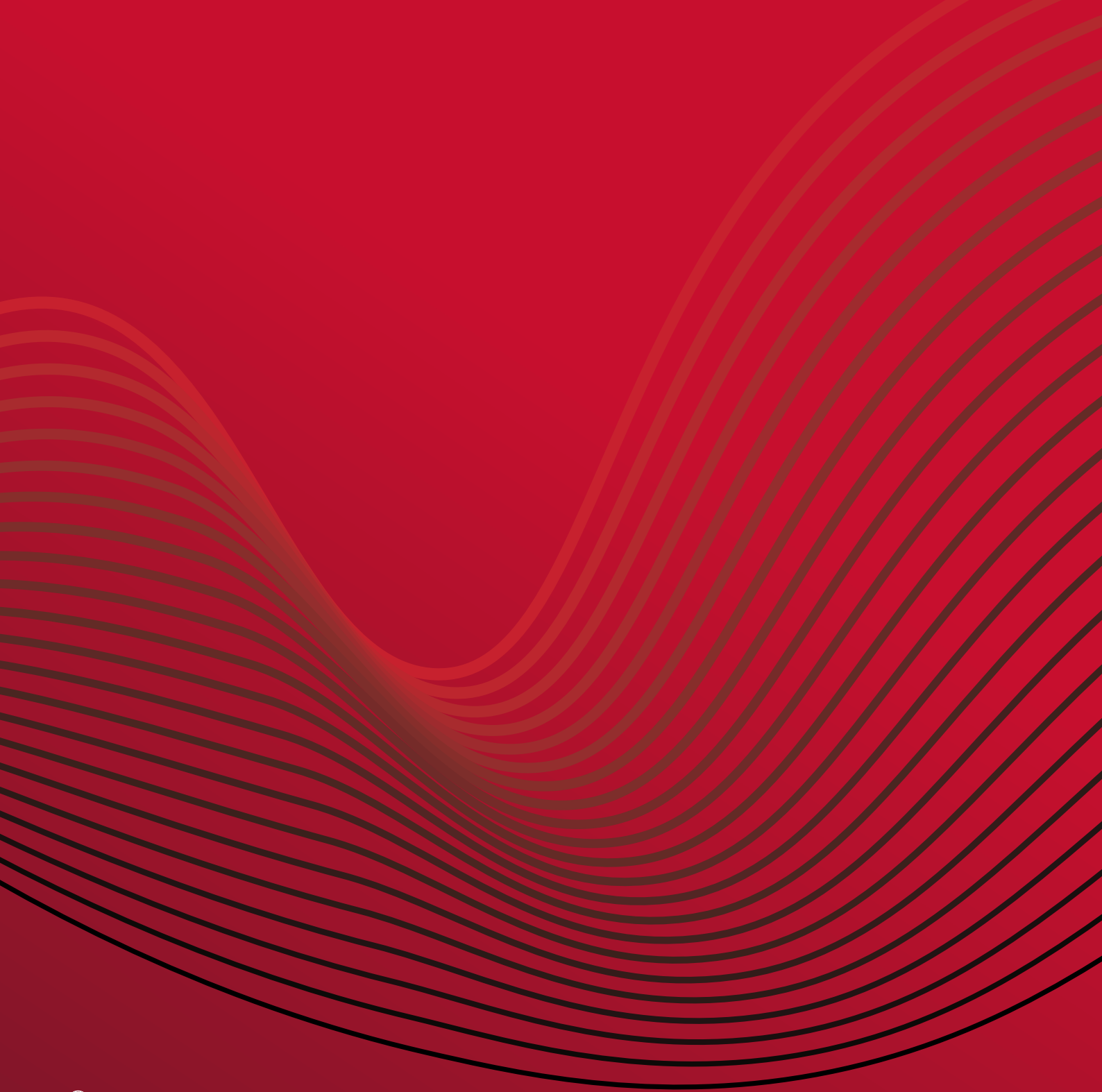
Our PTaaS model is powered by a team of over 30 seasoned penetration testers, accredited across OSCP, OSCE, CREST, GIAC, CISSP, and EC-Council, and CREST. We adopt a expert-first testing approach that identifies complex, real-world exposures that automated tools can overlook—delivering insights that matter.

Every year, we conduct more than 500 penetration tests for organisations of all sizes, covering internal and external infrastructure, web and mobile applications, cloud platforms, APIs, Active Directory, and more.

What makes our PTaaS stand out?

- Dedicated Technical Leads ensuring strategic alignment and consistency
- Secure SaaS portal with 24/7 access to test results, dashboards, and remediation workflows
- Bi-directional ticketing integration with tools like Jira and ServiceNow
- Retests included as standard, with flexible scheduling
- Clear, risk-prioritised reports designed for both technical and executive audiences
- Post-test support to validate remediation and advise on risk reduction
- Global reach with in-region experts across the UK, Ireland, Europe, Africa, and the Caribbean

At Integrity360, PTaaS isn't just about testing—it's about building a long-term partnership in cyber resilience. We help you uncover exposures, track improvements, and continuously strengthen your defences.



integrity360.com

info@integrity360.com

Dublin, Ireland
+353 1 293 4027

Ludwigsburg, Germany
+49 7141 48799 80

Sofia, Bulgaria
+359 2 491 0110

Cape Town, South Africa
+27 21 100 3774

London, UK
+44 2033 9734 14

Madrid, Spain
+34 910 767 092

Stockholm, Sweden
+46 8 514 832 00

Johannesburg, South Africa
+27 860 625 673

Kyiv, Ukraine
+38 504 701 125

Paris, France
+33 1848 0070 0

Zurich, Switzerland
+41 4442 1333 6

Vilnius, Lithuania

Rome, Italy