DATA SHEET

Vulnerability Assessment and Penetration Testing Services

Uncover Hidden Vulnerabilities, Before Attackers Do.

Strengthen Your Security with Proactive Real-World Testing

Cybercriminals increasingly target African organisations, knowing that security investment often lags behind digital growth. The average cost of a data breach in Africa now exceeds $2.5 million but yet a professional VAPT engagement costs a fraction of that. A single undetected vulnerability can give an attacker everything they need to compromise your operations, damage your reputation and disrupt the services your customers depend on. The question is not whether you can afford to test - it is whether you can afford not to.

ProComm Technologies delivers certified, intelligence-led Vulnerability Assessment and Penetration Testing services that find real risk before attackers do. Our certified experts simulate real-world attacks across your entire environment, using cutting-edge tools and ethical hacking methodologies scoped to your business context so every investment is targeted, proportionate and measurable.

What We Deliver

Real Attack Simulations	Comprehensive Risk Assessment	Actionable Remediation Plan	Compliance Confidence
Emulating real adversary techniques to test your true resilience.	Identifying vulnerabilities across every system, application and environment.	Clear, prioritised steps ordered by risk level and ease of fix.	Documented evidence aligned with PCI DSS, ISO 27001, NIST and other frameworks.

With ProComm Technologies, you gain more than a report. You gain a trusted security partner that turns your security spend into measurable risk reduction. We help you protect revenue, satisfy regulators and give leadership the confidence that your organisation is genuinely defended.

Key Service Features

Our VAPT service is built on certified expertise, proven methodology and a genuine commitment to your security outcomes. Every feature is designed to maximise your return on security investment, from scoping through to remediation confirmation.

Certified Expert Team

All assessments conducted by certified experts with deep offensive and defensive security expertise.

Adversary-Simulated Testing

We replicate the tools and tactics of real threat actors to give you an accurate picture of your true risk exposure.

Minimal Business Disruption

Flexible scheduling including out-of-hours testing windows ensures zero impact on your daily operations.

Actionable Risk-Scored Reporting

Every finding is manually verified, severity-scored and paired with clear remediation guidance for your environment.

Compliance Confidence

Documented evidence to support PCI DSS, ISO 27001, NIST and other regulatory requirements your organisation must meet.

Free Post-Remediation Retest

We retest all critical and high-severity findings after remediation at no extra cost, giving you independent confirmation that vulnerabilities are genuinely closed, not just marked fixed.

Services Overview

Our certified consultants deliver intelligence-led testing across every layer of your technology environment. Each assessment is scoped to your specific needs and conducted safely within agreed boundaries to ensure no disruption to your operations.

Infrastructure Security

Internal Network Testing

Our Internal Network Penetration Testing service evaluates your internal systems from the perspective of a malicious insider or compromised device. We assess your Active Directory environment, lateral movement paths, credential theft vectors and privilege escalation opportunities to determine how far an attacker could move once inside your network. The findings give your leadership team a clear understanding of internal exposure and the controls needed to contain a breach.

External Network Testing

Our External Network Penetration Testing service evaluates all internet-facing systems from an attacker's external perspective. We identify vulnerabilities in your network perimeter, public-facing services, firewalls, VPN endpoints and DMZ systems by simulating techniques used by real-world threat actors. The findings provide a clear picture of your external exposure and specific recommendations to strengthen your perimeter defences.

Wi-Fi Security Testing

Our Wi-Fi Security Assessment evaluates the security of your wireless network infrastructure. We examine configuration settings, encryption protocols and authentication systems to identify weaknesses. Testing covers rogue access point detection, evil-twin attack scenarios, client isolation gaps and guest network segmentation issues to ensure your wireless infrastructure is not an unmonitored entry point into your organisation.

OT and ICS Security Testing

Our Operational Technology and Industrial Control Systems Security Testing evaluates cyber-physical risks in your industrial environments. We assess PLCs, SCADA systems and related protocols for vulnerabilities that could allow an attacker to disrupt operations or compromise safety systems. All testing is conducted within carefully agreed parameters to ensure live production environments remain fully operational throughout the engagement.

Application Security

Web Application Testing

Our Web Application Security Assessment provides a thorough evaluation of your web-based applications against the most dangerous attack vectors. We examine front-end interfaces, back-end systems, authentication mechanisms, session management and data handling processes to identify weaknesses that could expose sensitive information or enable unauthorised access. Testing follows industry-recognised frameworks to ensure coverage of all known vulnerability classes.

Mobile Application Testing

Our Mobile Application Security Assessment evaluates the security of your iOS and Android applications. We examine the application architecture, data storage mechanisms, communication channels, server-side integrations and the risk of sensitive information being exposed through insecure coding practices. By identifying platform-specific vulnerabilities, we protect your customers' personal data and the integrity of your mobile services.

API Security Testing

Our API Security Testing service evaluates the security of your application interfaces covering REST and GraphQL APIs. We test for authentication and authorisation weaknesses, improper data exposure, rate limiting failures and access control issues that could allow an attacker to access or manipulate sensitive data. Our findings provide your development teams with clear, prioritised guidance to harden your API layer.

AI and LLM Security Testing

Our AI and Large Language Model Security Testing provides specialist assessment of AI-powered applications. We test for prompt injection vulnerabilities, model data leakage, insecure plugin chain configurations and adversarial input manipulation. As organisations adopt AI tools and platforms, this assessment ensures your AI adoption does not introduce new attack surfaces or expose sensitive information through unexpected model behaviours.

Cloud Security

Cloud Security Assessment

Our Cloud Security Assessment evaluates the security posture of your cloud infrastructure across leading platforms including AWS, Azure and Google Cloud. We assess identity and access management configurations, storage permissions, network security controls, serverless function security and container orchestration environments for misconfiguration and privilege escalation risks. The assessment also covers CI/CD pipeline exposure and cross-account trust relationships to map your complete cloud attack surface. As organisations move more workloads to the cloud, securing these environments against misconfiguration has become one of the most critical aspects of a comprehensive security programme.

Social Engineering

Social Engineering Assessment

Our Social Engineering Assessment evaluates the human-layer defences of your organisation against targeted manipulation and deception. We design and execute tailored phishing campaigns, vishing exercises and pretexting scenarios based on real threat actor techniques. The assessment measures the effectiveness of your security awareness programme and the resilience of your staff to social manipulation tactics. Findings are accompanied by targeted recommendations to strengthen your human-layer defences and improve security behaviours across your workforce.

Physical Security Assessment

Our Physical Security Assessment evaluates the safeguards protecting your premises, server rooms, data centres and critical physical assets. Our consultants test access control systems, CCTV coverage, tailgating vulnerabilities, badge cloning risks and the real-world effectiveness of your physical security policies and procedures. Physical access to your facilities can bypass even the most sophisticated digital controls, making this a critical component of a comprehensive security programme. The findings help you close physical gaps that could allow direct, undetected access to your infrastructure.

Other Assessments and Reviews

Secure Code Review

Our Secure Code Review provides manual and automated static analysis of your application source code to identify security defects before they reach your production environment. Our consultants examine code for injection flaws, insecure cryptographic implementations, hardcoded credentials, improper error handling and insecure dependencies that runtime testing alone is unlikely to detect. Addressing vulnerabilities at the code level reduces the cost of remediation and builds security into your development process from the ground up.

Configuration and Hardening Review

Our Configuration and Hardening Review evaluates the security settings of your systems, network devices, databases and cloud environments against recognised security standards and hardening best practices. Misconfigurations are among the most common root causes of security incidents, yet also among the most preventable. Our consultants provide a clear, prioritised list of hardening actions that reduce your attack surface and bring your environments in line with accepted security baselines.

Security Architecture Review

Our Security Architecture Review provides a strategic evaluation of your organisation's security design, identifying structural weaknesses, single points of failure and alignment gaps with leading security frameworks. Our consultants assess network segmentation, identity and access management design, encryption strategies and the overall resilience of your controls as an interconnected system. This review examines how your controls work together and whether they are positioned to detect and contain a determined attacker.

Deliverables

- A full technical findings report detailing all identified vulnerabilities, evidence of exploitation and prioritised step-by-step remediation guidance.
- An executive summary providing a non-technical overview of findings and recommended actions, formatted for board and leadership review.
- A live debrief session with your team to walk through key findings, answer questions and agree next steps on the remediation roadmap.

The ProComm 6-Phase Methodology

Our structured, intelligence-driven methodology ensures every engagement is controlled, thorough and aligned to your business environment and risk tolerance.

01 **Scoping and Pre-Engagement**

We agree the objectives, boundaries and rules of engagement with your team. Formal written authorisation is obtained before any testing begins, tailored to your environment and business risk tolerance.

02 **Reconnaissance and Intelligence**

We gather open-source intelligence and map your attack surface to build a complete picture of your environment, identifying systems, technologies and potential entry points before active testing begins.

03 **Scanning and Vulnerability Analysis**

Automated and manual scanning identifies open services, software versions and configuration weaknesses. All findings are verified and cross-referenced with known vulnerability databases and current threat intelligence.

04 **Risk Prioritisation and Threat Modelling**

Findings are mapped to business impact and likelihood of exploitation, ensuring your remediation effort is focused on the vulnerabilities that pose the greatest risk to your organisation first.

05 **Attack Execution**

Controlled, safe exploitation of identified vulnerabilities demonstrates real-world impact, including lateral movement and privilege escalation scenarios, all conducted within agreed testing boundaries.

06 **Reporting and Advisory**

We deliver an executive summary, full technical report, risk-scored vulnerability register and prioritised remediation roadmap, followed by a live debrief session with your key stakeholders.

The 3 Testing Approaches

Not all penetration tests are created equal. The type of assessment you choose significantly impacts the results, costs and insights you gain. The three most common approaches are White Box, Black Box and Grey Box. They differ in how much information is shared with testers before they begin. At ProComm, we help our clients select the right method based on business objectives, risk appetite, compliance needs and budget. For organisations new to VAPT, even a focused assessment typically costs less than one day of downtime from a ransomware attack, making it one of the highest-return security investments available.

Black Box Test

Penetrating the system with no prior knowledge of your environment, simulating a real external attacker who has the same limited information they would realistically have about your organisation.

Grey Box Test

Penetrating the system with limited knowledge, representing a compromised insider or a partially informed attacker. This is the most common real-world scenario and typically the most revealing approach.

White Box Test

The tester has full access to system details and source code, working collaboratively with your technical team to achieve the most thorough, deep and comprehensive coverage of all potential vulnerabilities.

About ProComm

ProComm Technologies is Zambia's leading cybersecurity consultancy, delivering specialist Vulnerability Assessment and Penetration Testing services to organisations across finance, government, mining, telecommunications, manufacturing and critical infrastructure. We understand that African businesses operate in a unique environment with rapid digital adoption, growing regulatory expectations and increasing attacker interest and we deliver enterprise-grade security testing built for that reality. ProComm is a CREST Pathway organisation, reflecting our commitment to internationally recognised standards in penetration testing and cybersecurity assurance.

Many African organisations view cybersecurity as a cost rather than a business enabler, until an incident forces the conversation. Our mission is to change that. We deliver assessments that go beyond compliance tick-boxes, providing genuine risk insight that protects revenue, preserves customer trust and reduces the likelihood of a costly breach. Every engagement is led by a certified expert with real-world adversary knowledge and a direct commitment to your outcomes.

At ProComm, we believe security testing should leave your organisation stronger and better positioned, not just assessed. Every engagement concludes with a clear remediation roadmap, a live debrief with your team and a free retest of all critical findings to confirm every vulnerability has been fully resolved. We are your long-term security partner, invested in your growth and not a one-time vendor.

Why Choose ProComm?

Leading Cybersecurity Firm

CREST Pathway penetration testing firm, combining certified expertise with intelligence-led adversary simulation tailored to the regional threat landscape.

Cross-Sector Experience

Proven across finance, government, telecommunications, mining, manufacturing and critical infrastructure ,we understand the risks your sector faces in Africa's evolving threat environment.

Actionable, Not Just Academic

Every finding comes with clear, prioritised remediation guidance your team can act on immediately, maximising the value of every dollar invested in security.

Intelligence-Led Assessments

Every engagement is built on real threat intelligence, not automated scans alone so that you spend remediation budget where it matters most.

No Impact on Your Operations

Flexible testing windows and carefully controlled protocols ensure zero disruption to your business.

Long-Term Partnership

Security is not a once-off exercise. We stay engaged through remediation, retest and ongoing advisory, building your organisation's resilience over time, not just on paper.

Our Penetration Testing Credentials

CEH
Certified Ethical Hacker - Practical

CISSP
Certified Information Systems Security Professional

CISM
Certified Information Security Manager

CRTA
Certified Red Team Analyst

ISO 27001
ISO 27001 Lead Auditor

CREST PATHWAY

Ready to Assess Your Security Posture?

Speak to a certified ProComm expert today.

+260 973 728 698 | security@procomm.cloud | www.procomm.cloud