TACTICAL NEW ORDER
MANAGED CYBER PROTECTION

OFFENSIVE SECURITY / 2026

SKILLED PENETRATION TESTING + RED TEAM

ADVERSARY-ALIGNED / HUMAN-DRIVEN / NOT AUTOMATED

Adversary-aligned offensive security delivered by experienced human operators, not automated scanners. Industry-recognised frameworks blended with proprietary techniques refined across Africa, Europe, and the Middle East. Every finding manually discovered, validated, and exploited.

01 // NETWORK	02 // APPLICATION	03 // CLOUD	04 // HUMAN	05 // ADVERSARY
External + Internal	Web + API + Mobile	AWS + Azure + GCP	Phishing + Social	MITRE ATT&CK Sim

CYBER SECURITY THAT STOPS HACKERS

// THE PROBLEM

> **AMATEURS HAVE TOOLS. PROFESSIONALS HAVE PEOPLE.**

01 WHY MOST PEN-TESTS FAIL

// SCANNER OUTPUT IS NOT A PEN-TEST

Every organisation depends on technology that is directly exposed to adversaries — networks connected to the internet, applications handling customer data, APIs powering integrations, and cloud infrastructure running critical operations. A single vulnerability can lead to breaches costing millions, ransomware that halts operations for weeks, and credential theft that enables long-term persistent access.

The penetration testing market is flooded with providers who run automated scanners, repackage the output as a consulting report, and call it a penetration test. These engagements produce volumes of theoretical findings ranked by CVSS scores — but they do not tell you what an actual attacker can achieve in your environment.

// NEWORDER OPERATES DIFFERENTLY

200+ Page scanner reports are not penetration tests.	**100%** Human-validated findings on every NEWORDER engagement.	**4** Offensive frameworks blended into one methodology.

> **A VULNERABILITY LIST TELLS YOU WHAT MIGHT BE WRONG. A NEWORDER ENGAGEMENT PROVES WHAT AN ATTACKER CAN ACTUALLY DO.**

02 WHAT WE TEST. HOW WE TEST IT.

// PEN-TESTING CAPABILITY

A structured seven-phase lifecycle based on PTES, enhanced with OWASP, NIST SP 800-115, and MITRE ATT&CK. Coverage across every layer of digital infrastructure.

// 01 NETWORK **External infrastructure** Internet-facing perimeter. Footprinting, manual exploitation, and validation of firewall, IDS, IPS, and WAF defences.	// 02 NETWORK **Internal infrastructure** "Zero to Hero" engagement. Active Directory, segmentation, lateral movement. Unprivileged foothold to Domain Admin.	// 03 APP **Web application** Manual interception beyond OWASP Top 10. Business logic flaws, race conditions, SSRF, deserialisation, session attacks.	// 04 APP **API security** REST, GraphQL, SOAP. BOLA, mass assignment, rate limit abuse, excessive data exposure, function-level abuse.
// 05 CLOUD **Cloud penetration** AWS, Azure, GCP. IAM misconfiguration, public storage, container and serverless weaknesses, privilege escalation.	// 06 APP **Mobile application** iOS and Android against OWASP Mobile Top 10. Decompilation, traffic interception, hardcoded secrets, pinning bypass.	// 07 NETWORK **Wireless assessment** Rogue access points, WPA2 and WPA3 weaknesses, evil twin attacks, segmentation between wireless and wired.	// 08 HUMAN **Social engineering** Targeted phishing, pretexting, human-factor exercises. Customised scenarios mirroring real adversary techniques.

// OPERATING FRAMEWORKS

PTES Penetration Testing Execution Standard	**OWASP** Application Security Testing Guide	**NIST 800-115** Technical Information Testing	**MITRE ATT&CK** Adversary Tactics + Techniques

03 TACTICAL METHODOLOGY. MEASURABLE OUTCOMES.

// SIX OPERATING PRINCIPLES

Six operating principles that separate a NEWORDER engagement from a commodity scan. Every principle is enforced on every engagement, regardless of scope or sector.

01 MANUAL-FIRST METHODOLOGY

Every finding is discovered and validated by human operators using real-world exploitation techniques. Automated tools assist with coverage. Human expertise drives the engagement.

02 POLYMETHODOLOGIST APPROACH

No single framework covers everything. We blend the lifecycle of PTES, the application depth of OWASP, the rigour of NIST SP 800-115, and the adversary realism of MITRE ATT&CK.

03 TACTICAL REPORTING

Two distinct deliverables on every engagement. Executive summary for leadership in business language. Technical report for security and development teams with evidence and reproduction steps.

04 PROVEN ATTACK PATH

We do not just identify that a vulnerability exists. We prove what an attacker can achieve with it. Demonstrated exploitation. Actual access. Real data reached. Concrete business impact.

05 ZERO OPERATIONAL DISRUPTION

Coordinated planning around operational needs. Controlled techniques. Emergency procedures established before testing begins. If unexpected issues arise, we halt and communicate.

06 REGULATORY COMPLIANCE

Direct support for POPIA, GDPR, PCI DSS Requirement 11.3, ISO 27001 Annex A.18, CIS Controls v8.1 Control 18, and SOC 2. Documentation that auditors and regulators accept.

// SEVEN-PHASE ENGAGEMENT LIFECYCLE

PTES-aligned. Every phase documented and signed off before the next begins.

01	02	03	04	05	06	07
SCOPING	INTEL	MODELLING	EXPLOIT	PIVOT	REPORT	DEBRIEF

04 WAR-GAMING AGAINST YOUR DEFENCES

// RED TEAM OPERATIONS

Penetration testing finds what is broken. Red Team operations test whether your people, processes, and technology can detect and stop a real adversary before they achieve their objective.

CRITERIA	PENETRATION TEST	RED TEAM OPERATION
SCOPE	Defined network, app, or system	**Entire org: people, process, tech**
OBJECTIVE	Identify max vulnerabilities in scope	**Achieve goal-based outcome covertly**
AWARENESS	IT and security team aware of testing	**Only a small trusted group knows**
TECHNIQUES	Technical exploitation in scope	**Phishing, physical, social, technical**
DURATION	One to three weeks typical	**Four to eight weeks of patient ops**
DELIVERABLE	Vulnerability report with severity	**Attack narrative + detection gap analysis**
FRAMEWORK	PTES, OWASP, NIST SP 800-115	**MITRE ATT&CK adversary simulation**

> **THE QUESTION YOUR BOARD SHOULD BE ASKING IS NOT "DO WE HAVE VULNERABILITIES?" — IT IS "CAN WE DETECT AND STOP A REAL ATTACKER?"**

// TYPICAL ENGAGEMENT OBJECTIVES

CROWN JEWELS
Reach a defined high-value asset undetected.

EXEC ACCESS
Compromise the CEO inbox or board materials.

EXFILTRATION
Demonstrate covert removal of regulated data.

IMPACT SIM
Prove ransomware deployment capability safely.

05 EVIDENCE. NOT ASSUMPTIONS.

// RED TEAM DELIVERABLES

Every Red Team engagement closes with a complete operational record: what was achieved, what your defences detected, where they failed, and what to fix in priority order.

01 ATTACK NARRATIVE

Chronological account of the operation from reconnaissance to objective completion. Written for leadership in non-technical language.

02 MITRE ATT&CK MAP

Every technique used during the engagement mapped to ATT&CK tactics: reconnaissance, initial access, persistence, privilege escalation, exfiltration, impact.

03 DETECTION GAP ANALYSIS

What your controls detected. What they missed. At which stage of the attack chain detection failed. Specific recommendations for closing the gaps.

04 RESPONSE EFFECTIVENESS

Response times, escalation procedures, containment actions, and communication effectiveness. Whether your incident response works under real-world conditions.

05 STRATEGIC RECOMMENDATIONS

Prioritised by impact. Control improvements, detection rules, process changes, training needs, and architectural changes needed to defend against demonstrated techniques.

06 EXECUTIVE DEBRIEF

Face-to-face board-level presentation. Business risk, clearly communicated. No CVSS scores. No technical jargon. What was achieved, what it would cost in a real attack.

06 WHY NEWORDER OUTPERFORMS

// THE TACTICAL ADVANTAGE

A head-to-head comparison against the typical approach taken by commodity testing providers. Eight points where we operate differently — and why it matters to you.

CRITERIA	MOST PROVIDERS	NEWORDER
OPERATOR MODEL	Junior analysts running scanner suites with limited oversight.	**Senior offensive operators with field experience across Africa, Europe, and the Middle East.**
FINDING VALIDATION	Raw scanner output exported to PDF without human verification.	**Every finding manually discovered, validated, and exploited by a human operator.**
METHODOLOGY	Single-framework checklist, usually OWASP or PTES alone.	**Polymethodologist blend of PTES, OWASP, NIST SP 800-115, and MITRE ATT&CK.**
ATTACK PATH PROOF	Severity scores assigned in isolation. No demonstrated impact.	**Chained exploitation. Real access. Real data reached. Concrete business impact.**
REPORTING DEPTH	200-page automated dump. Volume mistaken for value.	**Two-tier deliverable: executive narrative for leadership, technical evidence for engineers.**
ADVERSARY REALISM	Generic test cases recycled across every client.	**Adversary Path Engineering customised to your industry, geography, and threat profile.**
BUSINESS LOGIC	Skipped or noted as out of scope.	**Custom workflows, race conditions, and authorisation logic tested manually on every job.**
OPERATIONAL DISCIPLINE	Best-effort coordination, ad-hoc emergency procedures.	**ISO 27001 and ISO 9001 certified delivery. Pre-engagement rules of engagement on every job.**

// NEWORDER PILLARS

ADVERSARY PATH ENGINEERING	HUMAN VALIDATION AT SCALE	OUTCOME OVER OUTPUT	SPEED TO INSIGHT	INTEGRATED EXECUTION

// GET ASSESSED

CAN YOUR BUSINESS AFFORD TO BE HACKED?

Test what an adversary can really do. Contact NEWORDER for a no-obligation discussion about your offensive security requirements.

// DIGITAL

WEB newordergroup.net
LINKEDIN linkedin.com/company/neworder

MAIL info@newordergroup.net

// ACCREDITATION

ISO 27001 INFO SECURITY

ISO 9001 QUALITY MGMT

GET ASSESSED →

DOMINATE AIR. LAND. WATER. CYBERSPACE.