Solutions

THE OFFENSIVE SECURITY PLAYBOOK

A Comprehensive Report on Offensive Security and Continuous Threat Exposure Management

security@spurt.solutions

Table of Content

Introduction

Vulnerabilities Persist - Threats Evolve Rapidly

Overview

- Organisations face an escalating threat landscape where sophisticated cyberattacks exploit vulnerabilities in IT systems, including on-premises applications, cloud infrastructure, and emerging AI technologies.

- Without standardised, authorised offensive security testing, such as red teaming, penetration testing, and vulnerability assessments, organisations risk undetected weaknesses and operational disruptions.

- The absence of clear protocols for ethical hacking ("whitehat exercises") often leads to unauthorised tests and inconsistent scoping, which undermines security postures.

- This guide addresses these challenges by providing a standardised framework to ensure all offensive security activities are conducted with documented scope, explicit authorisation, and rollback plans, achieving **100%** compliance while proactively mitigating risks across diverse environments.

Organisations in Africa endure about **3,325** cyberattacks per week, **72%** above the global average of **1,938**.

In Sub-Saharan Africa, Kaspersky detected **42.4 million** web attacks and **95.6** million on-device attacks in H1 2025 alone,

Cybercrime has cost Africa over **$3 billion** since 2019, equating to roughly **$3 billion** annually.

SCOPE & DEFINITIONS

This report is relevant to the offensive security testing of an organisation's IT systems, which includes:

- Internal and external applications (whether on-premises or hosted in the cloud).
- Cloud infrastructure (such as AWS, Azure, GCP, encompassing IaaS, PaaS, SaaS, and FaaS models).
- Third-party integrated applications or services.
- Hybrid environments that blend on-premises and cloud configurations.

- **Vulnerability Assessment:** Systematic, often automated, scanning to detect weaknesses.
- **Whitehat Exercises:** Ethical hacking activities (e.g., pentests, bug bounties) conducted by authorised internal or external testers.
- **Purple Teaming:** Collaborative red and blue team exercises to improve detection and response.

Out of Scope:
Employee personal devices, unless explicitly included in test scope (e.g., for social engineering simulations).

- **Red Teaming:** Simulating real-world adversarial attacks to test systems, processes, and personnel, often using frameworks like MITRE ATT&CK.
- **Penetration Testing (Pentest)**: Authorised testing to identify vulnerabilities in specific systems, with a defined scope (black-box, white-box, or grey-box).

The following steps outline the process for effectively implementing offensive security within your organisation

Solutions

01

Mandatory Authorisation

No offensive security testing (e.g., network scanning, exploitation attempts) may occur without explicit written approval from:

- Legal Counsel: To ensure compliance with applicable laws **(e.g., GDPR, HIPAA, CFAA).**
- Executive Leadership: Senior management **(e.g., CISO, CTO, CEO)** to align with organisational risk tolerance.

02

Unauthorised Testing

Prohibited for both internal and external testers. Unauthorised actions may result in disciplinary measures or legal consequences.

03

Approval process

Submit test requests via a ticketing system (e.g., Jira, ServiceNow) with proposed scope, objectives, and timeline. Legal review confirms compliance (recommended: 1-3 business days).

Executive sign-off validates risk acceptance (recommended: 1-3 business days).

04

Responsible Disclosure

Encourage reporting of vulnerabilities observed during normal system use (e.g., via bug reporting channels) without active exploitation unless authorised.

Whitehat Exercise Requirements

Solutions

Scope Documentation: Each exercise must define:

Systems in scope (e.g., IP ranges, APIs, cloud services like AWS RDS or Lambda).
Exclusions (e.g., production systems during peak hours).
Test types (e.g., web app pentest, cloud configuration audit, social engineering).

Authorisation:

Documented in a Rules of Engagement (RoE) form, specifying permissions, contacts, escalation paths, and test boundaries.

Rollback Plans: Include:

- Pre-test backups of systems, configurations, and data.
- Procedures to restore services (e.g., revert VM snapshots, clear test artefacts).

Contingency plan:

In case of unexpected service disruption, an incident response and disaster recovery plan is in place

Execution Guidelines:

- **Test Types**

Web Apps and APIs: Test for injection flaws, authentication issues, or business logic errors.

Cloud Environments: Audit misconfigurations (e.g., public S3 buckets, overly permissive IAM roles).

AI/LLM Testing: Assess risks like data poisoning, prompt injection, or model misuse.

Social Engineering: Conduct phishing simulations to raise awareness, followed by targeted training based on response gaps.

Execution Guidelines:

- **Frequency**

Vulnerability assessments: Weekly or continuous using automated tools (e.g., Nessus, OpenVAS).

Penetration tests: Quarterly for critical systems.

Red teaming: Continuous or scheduled to simulate advanced threats.

Testing Calendar:

Schedule tests to minimise business impact (e.g., off-hours for production systems).

Stay ahead of emerging threats by conducting Responsible Disclosures and Bug Bounties

Channels

Establish platforms for vulnerabilities reporting or responsible disclosure.

Classification

Categorise findings by severity (e.g., using CVSS):
Critical/High: Remediate within 24-48 hours.
Medium: Remediate within 7 days.
Low/Informational: Remediate within 30 days.

Reward

Offer bounties for external researchers, scaled by severity (defined in a separate bounty policy).

Median time To Resolve (MTTR)

Track and optimise remediation timelines for efficiency.

Organisations that remediate high-severity vulnerabilities within **3 days** can reduce breach risks by up to **90%,** compared to months-long patching delays that leave systems exposed to active exploits

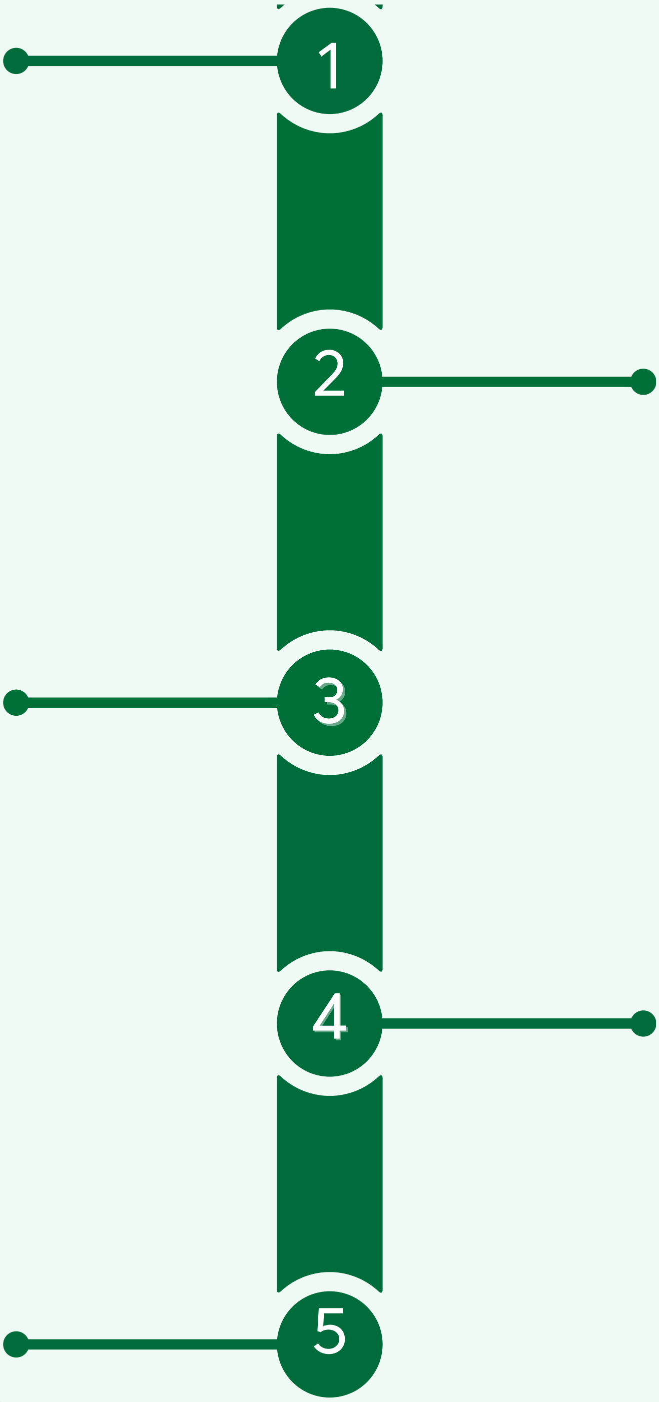
Cloud and Hybrid Environment Considerations

80% of cloud permissions are unused, which expands attack surfaces.

CHALLENGES	STRATEGIES
Cloud models (PaaS, SaaS, FaaS) limit infrastructure control, requiring focus on configurations and identities. Hybrid setups (on-premises + cloud) introduce risks like misconfigured trust boundaries (e.g., cloud-connected VPNs) or unmonitored service accounts.	• Continuously audit cloud configurations using tools like AWS Config, Security Hub or Audit Manager. • Test identity systems (e.g., IAM, SSO) for overly permissive roles. • Simulate multi-environment attacks to validate controls across on-premises and cloud assets. • Secure CI/CD pipelines to prevent exposed secrets or misconfigured workflows.

Ad-hoc testing should be replaced with systematic, high-fidelity threat simulations

Standardised frameworks and methodologies are critical for ensuring that offensive security testing is systematic, repeatable, and aligned with industry best practices, providing structured approaches to simulate real-world threats, assess vulnerabilities, and measure the effectiveness of remediation.



1

MITRE "ATT&CK"

Provides a blueprint for mapping the TTPS of specific adversaries to determine if you're vulnerable to their attack.(e.g. APT 29)

2

CTEM (Continous Threat Exposure Managment)

Support ongoing assessment and remediation

3

OWASP (Testing Guide)

Guides web app and API Testing

4

NIST SP 800-115

Offers structured pentest methodology

5

PTES/CREST

Standards for penetration testing execution

The Offensive Security Process follows a disciplined lifecycle that ensures all security assessments are controlled, impactful, and results-driven

1.Map Architecture: Document applications, infrastructure, and cloud services.

2.Assemble Team: Internal red team or vetted and skilled third-party vendors.

3.Define Tests:

- Black-Box: No prior knowledge, mimicking external attackers.
- White-Box: Full access to code/configurations for in-depth testing.
- Grey-Box: Partial knowledge, balancing realism and efficiency.

4.Create Testing Calendar: Schedule to avoid disruptions (e.g., evenings for production systems).

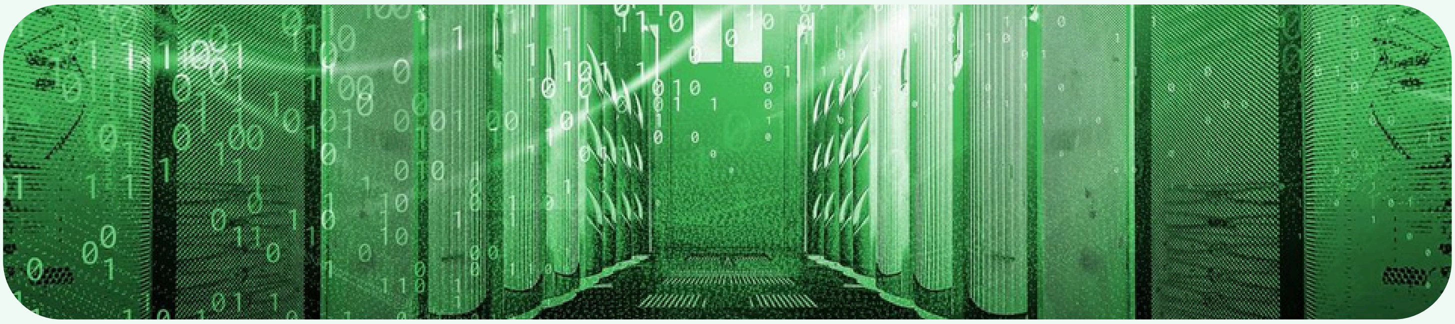
5.Execute Tests: Adhere to RoE, log all actions, and monitor for unintended impacts.

6.Rollback: Implement pre-defined restoration plans.

7.Report: Produce detailed reports with:

- Vulnerability details and proof-of-concept (PoC).
- Risk ratings and business impact.
- Remediation recommendations.

Retest: Verify fixes within defined SLAs.



Outsourcing Best Practices

- **Vendor Selection:** Engage certified providers with clear contracts.
- **Scope Clarity:** Define in-scope/out-of-scope assets, execution windows (e.g., off-hours), and confidentiality requirements (NDAs).
- **Phases:** Pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, reporting.

Integration and Automation

It takes more than 20 minutes of manual effort to detect, prioritise, and remediate one vulnerability, contributing to why **83%** of high-severity vulnerabilities remain unpatched in many organisations.

- Integrate findings into developer tools (e.g., Jira, GitHub Issues) for streamlined remediation.
- Use tools like Wazuh to monitor and correlate test-related alerts.
- Track MTTR, test coverage, and compliance (aim for 100% documented exercises).
- Implement gamified training (e.g., capture-the-flag challenges, phishing quizzes) to engage employees.

AI and Emerging Threats

AI/LLM Testing:
Test for risks like data poisoning, model inversion, or adversarial inputs.

Red Teaming AI:
Simulate attacks to extract sensitive data or manipulate outputs.

Proactive Approach:
Move beyond compliance checkboxes to comprehensive coverage of digital and AI-driven assets.

Governance and Compliance

Executive Support → Secure leadership buy-in to align testing with business goals.

Legal Oversight → Conduct reviews to ensure alignment with regulatory requirements.

Audit → Conduct quarterly reviews to verify 100% compliance with scope, authorisation, and rollback requirements

Backup → Regularly test data retrieval and recovery processes.

Governance and Compliance

Draft and publish this policy, securing legal and executive approval.	Develop RoE and scope templates for reuse.	Establish a testing calendar and SLAs.	Set up responsible disclosure channels (e.g., bug bounty platforms).	Integrate with SIEM tools for monitoring.	Train staff on policy adherence and ethical hacking principles.
✓	✓	✓	✓	✓	✓

Metrics for Success

Policy published and accessible (e.g., via public website, GitHub, or industry forums)	100% of whitehat exercises have documented scope, authorisation, and rollback plans.	MTTR for critical vulnerabilities < 48 hours.	Quarterly pentests and continuous red teaming implemented without disruptions.

Offensive Security is now a Big Deal in Africa

Africa's data and privacy ecosystem is growing rapidly and Startups, in particular, sit at the heart of this digital evolution. Whether a startup collects, stores, analyses, or processes personal data from users in Nigeria, South Africa, Kenya or the wider African region, it must stay up to date with emerging regulatory requirements.

Despite differences in structure or terminology, all three provides mechanisms for offensive security processes

Nigeria: NDPA and the GAID Framework

The Nigeria Data Protection Commission (NDPC) now mandates technical evidence of security via the GAID 2025. For major data controllers, annual audits are insufficient without verifiable vulnerability assessments. Under the NDPA, high-risk processing requires a Data Protection Impact Assessment (DPIA). In 2026, the NDPC expects these DPIAs to include offensive simulations to prove that "integrity and confidentiality" are functional realities, not just policy. Failure to demonstrate these proactive measures has already resulted in significant fines for "negligent" organisations.

South Africa: POPIA and the Reasonable Measures Standard

South Africa's Information Regulator aggressively enforces Section 19 of POPIA, which demands "appropriate, reasonable technical measures." As of 2025, the Regulator treats the absence of regular Red Teaming as evidence of negligence during breach investigations. With the new mandatory digital reporting portal, organisations must disclose their preventive actions; failure to produce a recent offensive security report can lead to the maximum **R10 million** fine.

Kenya: DPA and Compliance Audit Regulations

The Office of the Data Protection Commissioner (ODPC) has been empowered to conduct special audits focusing on system integrity. For Kenya's tech sector, offensive security is now a prerequisite for legal cross-border data transfers. Firms must demonstrate that their architecture can withstand sophisticated threats via incident response testing. Proactive hacking of one's own systems is now the standard proof required to satisfy Kenyan regulators that data is truly protected.

References

MITRE ATT&CK Framework
MITRE. (n.d.). MITRE ATT&CK. https://attack.mitre.org

OWASP Testing Guide
OWASP Foundation. (2025). OWASP Web Security Testing Guide. https://owasp.org/www-project-web-security-testing-guide/

NIST SP 800-115
National Institute of Standards and Technology. (2006). Technical guide to information security testing and assessment (NIST Special Publication 800-115). https://csrc.nist.gov/pubs/sp/800/115/final

World Bank Group
World Bank Group. (2024). P178769: Implementation status and results report (No. 099092324164536687). https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf

Indusface
Indusface. (n.d.). Key cybersecurity statistics. https://www.indusface.com/blog/key-cybersecurity-statistics/

IBM
IBM Security. (n.d.). New report finds businesses introducing security risk in cloud environments. https://www.ibm.com/think/x-force/new-report-finds-businesses-introducing-security-risk-cloud-environments

Industrial Cyber
Industrial Cyber. (n.d.). Businesses and manufacturing bear brunt of 36% ransomware spike as government and healthcare see declines. https://industrialcyber.co/reports/businesses-and-manufacturing-bear-brunt-of-36-ransomware-spike-as-government-and-healthcare-see-declines/

LTP Solicitors. (2025) Data protection laws in Africa explained: NDPA (Nigeria), POPIA (South Africa), GDPR for startups. https://ltpsolicitors.com.ng/data-protection-laws-in-africa-explained-ndpa-nigeria-popiasouth-africa-gdpr-for-startups/

Market Data Forecast.(2025) Africa cyber security market. https://www.marketdataforecast.com/market-reports/africa-cyber-security-market

Commence your Offensive Security Journey Today!

Cyber threats evolve daily, but your organisation can stay ahead. Contact us today!

Don’t wait for a malicious actor to find the gaps in your logic. Our Offensive Security Service provides more than just a scan; we deliver a rigorous "Red Team" simulation specifically calibrated for the African digital landscape. We identify the vulnerabilities that automated tools miss. Protect your user data, satisfy your compliance requirements, and help you build a platform that investors can trust.

Not sure where your perimeter is weakest? Let’s start with a high-level vulnerability briefing tailored to your organisation.
Schedule a 15-Minute Security Briefing with our Information Security team today!

✉ security@spurt.solutions