



— INDEPENDENT SECURITY ASSESSMENT

CYBERSECURITY ASSURANCE

**Know where security can fail.
Fix what matters first.**

Independent cybersecurity assessment and authorised testing that connects material exposure to prioritised, accountable action.

INDEPENDENT / EVIDENCE-LED / DEFENSIBLE

forensics@siftcon.africa | +27 10 979 0010

siftcon.africa

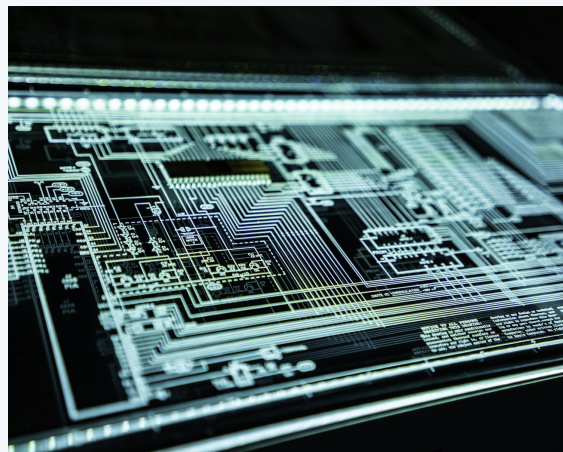


THE OBJECTIVE

ASSURANCE MUST EXPLAIN RISK, NOT ONLY LIST WEAKNESSES.

A technical finding becomes useful when decision-makers understand the asset affected, credible attack path, potential impact and control response required.

SIFTCON combines authorised technical testing with risk and governance context to focus attention on the weaknesses that matter most and the actions most likely to reduce exposure.



ASSESSMENT COVERAGE

EXTERNAL ATTACK SURFACE

Internet-facing assets, exposed services, domains and reachable entry points.

IDENTITY & ACCESS

Authentication, privilege, account lifecycle and pathways to elevated control.

APPLICATIONS & INTERFACES

Web applications, APIs, integrations and critical workflow assumptions.

INFRASTRUCTURE & CLOUD

Configuration, segmentation, hardening, workload and administrative control.

DETECTION & RESPONSE

Whether material activity can be recognised, escalated and contained.

GOVERNANCE & DEPENDENCIES

Ownership, assurance evidence, third parties and residual-risk decisions.

CORE CAPABILITIES

TEST EXPOSURE, CONTROLS AND REMEDIATION AS ONE SYSTEM.

The programme is shaped around the environment, threat context, critical services and required level of confidence.

01 SECURITY POSTURE ASSESSMENT

Establish a risk-based view of exposure, critical assets, safeguards and material control gaps.

02 VULNERABILITY ASSESSMENT

Identify and validate technical weaknesses across authorised infrastructure, applications and configurations.

03 PENETRATION TESTING

Test credible attack paths within agreed rules to demonstrate practical impact and control performance.

04 APPLICATION & INFRASTRUCTURE REVIEW

Assess security design, configuration, access, exposed services and defensive controls.

05 CONTROL-EFFECTIVENESS ASSURANCE

Examine whether governance, preventative, detective and response controls operate as intended.

06 REMEDIATION & VALIDATION

Prioritise corrective action, clarify ownership and retest completed work to confirm risk reduction.

ENGAGEMENT METHOD

MAINTAIN CONTROL FROM SCOPE THROUGH RETEST.



CONTROLLED TESTING

AUTHORISED SCOPE. DEFINED SAFETY. TRACEABLE RESULTS.

Objectives, permitted techniques, exclusions, contacts and stop conditions are agreed before testing begins. Formal compliance or third-party reliance requirements are addressed explicitly in the mandate.

WHAT YOU RECEIVE

- Evidence-led assessment of material security exposure
- Risk-ranked technical findings with practical implications
- Prioritised remediation roadmap with accountable ownership
- Retest evidence confirming whether exposure was reduced

— TARGET OUTCOMES

ONE VIEW OF PRIORITY FOR TECHNICAL TEAMS AND LEADERS.

01 VERIFIED EXPOSURE

An evidence-led view of where security can fail and credible impact.

02 RISK-BASED PRIORITIES

Findings ranked by context, exploitability, criticality and controls.

03 DECISION-READY ASSURANCE

Technical results translated into implications, ownership and action.

04 VALIDATED PROGRESS

Retesting confirms actual risk reduction rather than reported completion.

WHO RELIES ON THE WORK

01

Financial, healthcare & regulated industries

02

Government departments, SOEs & institutions

03

Organisations managing critical information

04

Audit & regulatory-readiness teams



SIFTCON
Empowering Insights

STRENGTHEN SECURITY CONFIDENCE

START WITH THE SYSTEMS AND EXPOSURE THAT MATTER MOST.

We can help define the right assessment scope, testing approach and route from finding to verified remediation.

START A CONFIDENTIAL DISCUSSION

EMAIL

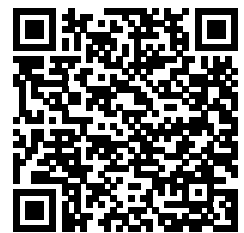
forensics@siftcon.africa

PHONE

+27 10 979 0010

WEB

siftcon.africa



Explore the service online

Northgate Office Park, 14 Aureole Avenue, Gauteng, South Africa, 2188

Security testing is performed only within an agreed, authorised scope and defined rules of engagement.