

TACTICAL



AS103

IDENTITY AND PRIVILEGE ABUSE

Your agents authenticate to things. Most organisations cannot say as whom.

CYBER SECURITY THAT STOPS HACKERS

// 01 // WHAT IT IS

AN AGENT IS A PRINCIPAL, NOT A FEATURE

It holds credentials, carries permissions and reaches systems. Every one of those is an identity decision that somebody made, or failed to make.

HOLDS CREDENTIALS

Keys, tokens and secrets sit with the agent, not with a person.

CARRIES PERMISSIONS

Entitlements accumulate as the agent is wired into more systems.

REACHES SYSTEMS

Each reach is an identity decision made, or failed to be made.

// 02 // HOW IT HAPPENS

SHARED KEYS. INHERITED PERMISSIONS. SERVICE ACCOUNTS NOBODY OWNS.

The agent is given the access of the person or the system it was built beside, because that was the fastest way to make it work.

// THE THREE SHORTCUTS

01

SHARED KEYS

02

INHERITED PERMISSIONS

03UNOWNED SERVICE
ACCOUNTS

// 03 // THE MEASURED PROBLEM

ATTRIBUTION FAILS FIRST

26%

VERY CONFIDENT THEY COULD PROVE AN AGENT
CAUSED AN INCIDENT

87%

AGREE CREDENTIALLED AGENTS ARE A GREATER
INSIDER THREAT THAN EMPLOYEES

Arkose Labs, 300 enterprise leaders, fielded February 2026. North America, Europe and Asia-Pacific only, no African respondents.

// 04 // WHY SOUTH AFRICA

ACCOUNTABILITY IS THE LEGAL TEST

POPIA

PROCESSING DUTY

POPIA requires accountability for how personal information is processed.

KING V

GOVERNANCE DUTY

King V requires organisations to demonstrate clear accountability for decisions, actions, outputs and outcomes, with human oversight and override proportionate to risk.

King V took effect for financial years beginning on or after 1 January 2026.

// 05 // THE POINT

YOU CANNOT DEMONSTRATE ACCOUNTABILITY FOR AN ACTION YOU CANNOT ATTRIBUTE

Attribution is not an incident response capability. It is a design decision, made before the incident, when the identity was issued or not issued.

WHAT IT IS NOT

AN IR CAPABILITY

No investigation recovers an identity that was never issued.

WHAT IT IS

A DESIGN DECISION

Made before the incident, when the identity was issued or not issued.

// 06 // THREE QUESTIONS FOR MONDAY

THREE QUESTIONS FOR MONDAY

-
- 01** DOES EVERY AGENT HAVE ITS OWN IDENTITY, SEPARATE FROM A PERSON OR A SERVICE?
 - 02** WHO REVIEWS AGENT PERMISSIONS, AND ON WHAT CYCLE?
 - 03** COULD WE PROVE WHICH AGENT TOOK AN ACTION, SIX MONTHS LATER?
-

GIVE EVERY AGENT A NAME BEFORE YOU NEED TO PROVE WHAT IT DID.

WE DO NOT RUN SCANS. WE DEPLOY OPERATORS.

// THE NEXT STEP

A THIRTY MINUTE DISCUSSION.

A no-obligation discussion to understand your requirement and to provide guidance on how NEWORDER can assist. No deployment, no commitment.

BOOK DISCUSSION →

EMAIL INFO@NEWORDERGROUP.NET • WEB WWW.NEWORDERGROUP.NET

NEXT: ASIO4 AGENTIC SUPPLY CHAIN