



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 24 | 31 May – 7 June 2026

THREAT LEVEL: HIGH

CSIR/CHPC Lengau supercomputer forced offline 4 June (SSH credential breach, POPIA s.22 initiated). ROOTBOY publicly released full 1.2 TB Standard Bank dataset (~1 June, EWN confirmed cards at \$350/bundle). Central JHB TVET POPIA enforcement notice sets internal-disclosure precedent. NETSCOUT confirms SA #1 globally for DDoS against banking/insurance/IT. Cisco SD-WAN takes its 7th 0-day of 2026 (no patch). Citrix NetScaler CVSS 9.8 mass exploit. Patch Tuesday 9 June: Exchange OWA permanent patch + OpenSSL HIGH/CRITICAL update expected. SA ransomware count FLAT at 111; Black X ANC claim UNVERIFIED.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W24 | Classification: TLP:WHITE

Published Monday 8 June 2026

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. SA Cyber Incidents & Breaches
- 4. Global Incidents with SA Relevance
- 5. Threat Actors
- 6. Critical Vulnerabilities & CISA KEV
- 7. Ransomware Landscape
- 8. OSINT Exposure & Attack Surface
- 9. Regulatory & Compliance
- 10. Weekly Threat Hunt & IOCs
- 11. Recommendations
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged from W21–W23) — Week 24 (31 May–7 June 2026)

Story 1 — CSIR/CHPC Lengau Supercomputer Forced Offline: South Africa's national flagship supercomputer, the CHPC Lengau system at CSIR, was forced offline on 4 June after unauthorised access to user credentials and SSH keys was detected in late May. POPIA section 22 notification has been initiated. No exfiltration of research datasets has been confirmed; attribution remains open. Lengau hosts research workloads for SA universities, the Department of Science and Innovation, and partner institutions — making this both a credential-theft incident and a strategic-research-target compromise. This is the highest-profile public-sector breach of 2026 to date.¹

Story 2 — Standard Bank 1.2 TB Dataset Publicly Released + NETSCOUT SA DDoS #1 Globally: ROOTBOY escalated from quiet extortion to mass disclosure, publicly releasing the full 1.2 TB Standard Bank dataset around 1 June. EWN's dark-web investigation confirmed SA bank cards trading at roughly \$350 per bundle. Separately, NETSCOUT confirmed on 3 June that SA holds the **#1 global rank for DDoS attacks against commercial banking, insurance, and IT services** — quantitatively anchoring the W22 Black Matter ISP wave as part of a sustained campaign.²³

Story 3 — Patch Tuesday 9 June: Exchange OWA Permanent Patch + OpenSSL HIGH/CRITICAL Expected: The KEV deadline for Exchange OWA CVE-2026-42897 passed on 29 May (W23) with no permanent patch; EEMS Mitigation M2 remains the only protection. The 9 June Patch Tuesday is forecast to deliver the permanent fix. OpenSSL pre-announced a security update for 9 June at undisclosed HIGH/CRITICAL severity. Cisco SD-WAN took its **seventh exploited zero-day of 2026** (CVE-2026-20245) with no patch and no workaround. Citrix NetScaler CVE-2026-3055 (CVSS 9.8) is under thousands of daily exploit attempts globally.⁴⁵

KPI Dashboard

Metric	Current (W24)	Prior (W23)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged	FLAT
SA ransomware.live victims (total)	111	111	0 new W24	FLAT
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W23)	FLAT	FLAT
Black X ANC claim (2 Jun)	UNVERIFIED (3 compromised users per HudsonRock)	N/A	NEW W24	UP
CISA KEV additions (W24)	~3-4 (SolarWinds Serv-U + others)	~8 (W23)	Lighter week	DOWN
Confirmed SA breach -- Lengau supercomputer	YES -- CSIR/CHPC offline 4 Jun (credential/SSH breach)	No comparable (W23)	NEW W24	UP
Standard Bank 1.2 TB -- status	PUBLICLY RELEASED ~1 Jun; EWN confirmed \$350/bundle	Developing (W23)	ESCALATED	UP
SA DDoS global rank (NETSCOUT)	#1 globally -- banking, insurance, IT services (confirmed 3 Jun)	Not formally ranked	CONFIRMED W24	UP
Exchange OWA permanent patch	NO permanent patch; EEMS M2 only; expected PT 9 Jun	NO (W23)	APPROACHING	FLAT
Cisco SD-WAN 0-days (2026 total)	7 (CVE-2026-20245 -- NO patch, no workaround)	6 (W23)	NEW W24	UP
POPIA enforcement notice (Central TVET)	ISSUED 1 Jun -- inadvertent internal disclosure precedent	None W23	NEW	UP
Patch Tuesday next	9 June 2026	--	Exchange OWA perm patch + OpenSSL expected	FLAT

W24 KEY FRAMING: W24 is defined by three compounding breach events at the highest-profile target level: the national supercomputer (Lengau/CSIR), the country's largest bank (Standard Bank full data release), and a precedent-setting regulatory enforcement action (Central JHB TVET). The FLAT ransomware count (111) again masks real threat activity. The dominant operational driver shifts to 9 June Patch Tuesday — Exchange OWA permanent patch and OpenSSL HIGH/CRITICAL update must be the primary change-window focus for every SA organisation this week.

TOP 3 ACTIONS THIS WEEK

1. PATCH TUESDAY 9 JUNE -- PRIMARY CHANGE WINDOW: Pre-stage Exchange OWA permanent patch (CVE-2026-42897); pre-stage OpenSSL HIGH/CRITICAL update; deploy full Windows June security rollup. Hold business calls scheduled for that window if possible. Run Exchange Health Checker (aka.ms/ExchangeHealthChecker) now to confirm EEMS M2 is active as interim protection. This is the single highest-priority action for the week.

2. CISCO SD-WAN CVE-2026-20245 (7th 0-DAY, NO PATCH): Collect admin-tech logs from all SD-WAN edges immediately; restrict netadmin access to out-of-band only; monitor for configuration drift pushed to edge devices; prepare for emergency patch when Cisco ships. Mandiant confirmed exploitation results in configuration changes to edge devices. Compounded by still-active UAT-8616 exploitation of CVE-2026-20182.

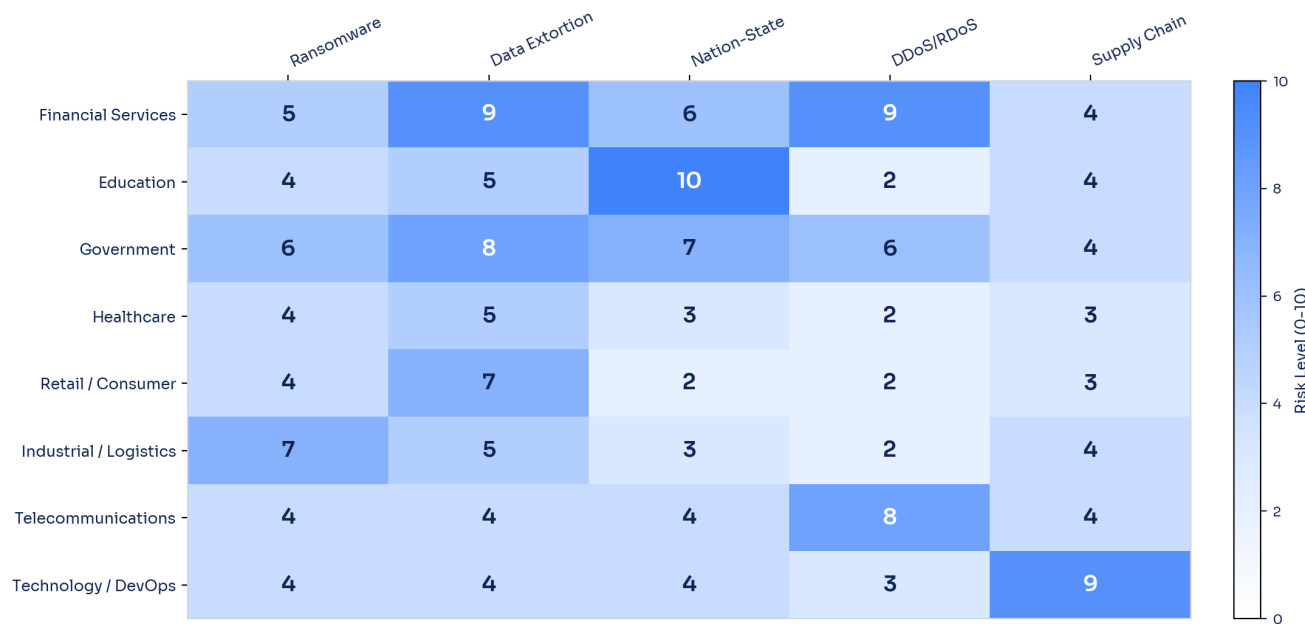
3. CITRIX NETSCALER CVE-2026-3055 (CVSS 9.8, MASS EXPLOIT): Identify any NetScaler instance configured as SAML IDP; patch to 13.1-62.23 or 14.1-60.58 immediately; review SAML assertion logs for anomalies. Fortinet confirms thousands of daily attack attempts globally. SA banking and enterprise SSO/VDI stacks are directly in scope.

1. The Citizen -- Cybersecurity breach forces SA supercomputer offline (4 June 2026) — <https://www.citizen.co.za/rekord/news-headlines/2026/06/04/cybersecurity-breach-forces-sas-supercomputer-offline/>
2. ITWeb -- security weekly roundup (1 June 2026) / ROOTBOY Standard Bank release — <https://www.itweb.co.za/>
3. NETSCOUT DDoS Threat Intelligence Report H1 2026 (3 June 2026) — <https://www.netscout.com/>
4. Help Net Security -- June 2026 Patch Tuesday forecast (5 June 2026) — <https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>
5. Help Net Security -- Cisco SD-WAN CVE-2026-20245 zero-day exploited (5 June 2026) — <https://www.helpnetsecurity.com/2026/06/05/cisco-sd-wan-cve-2026-20245-0-day-exploited/>

2. THREAT LANDSCAPE HEATMAP

The heatmap maps eight South African sectors against five threat categories, rated 0–10 based on confirmed incidents, active threat actor campaigns, and vulnerability exposure during Week 24 (31 May–7 June 2026). **Education** spikes to 10 on Nation-State following the confirmed CSIR/CHPC Lengau supercomputer breach (SSH credential theft). **Financial Services** rises to 9 on Data Extortion (Standard Bank 1.2 TB publicly released; EWN confirmed \$350/bundle) and 9 on DDoS/RDoS (NETSCOUT SA #1 globally against banking). **Technology/DevOps** rises to 9 on Supply Chain following Cisco SD-WAN's 7th zero-day and Citrix NetScaler mass exploit. **Telecommunications** rises to 8 on DDoS/RDoS (NETSCOUT confirms IT services sector in top SA DDoS targets).

SA THREAT LANDSCAPE HEATMAP | W24 (31 May – 7 June 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting period, (b) active threat actor campaigns targeting the sector, (c) vulnerability exposure, and (d) regulatory scrutiny. **Critical (9–10)** = active exploitation or confirmed breach; **High (7–8)** = credible active threat; **Medium (4–6)** = elevated baseline risk; **Low (1–3)** = standard risk posture.

3. SA CYBER INCIDENTS & BREACHES

Week 24 (31 May–7 June 2026): Zero new ransomware.live listings (SA tally holds at 111). Dominant stories: (1) CSIR/CHPC Lengau supercomputer forced offline (4 June — confirmed credential/SSH breach); (2) Standard Bank 1.2 TB dataset publicly released by ROOTBOY (~1 June); (3) Central JHB TVET POPIA enforcement notice sets internal-disclosure precedent (1 June); (4) NETSCOUT confirms SA #1 globally for DDoS against banking/insurance/IT (3 June); (5) SABS executive disciplinary hearings begin (Lynx attribution confirmed); (6) Black X claims ANC compromise (2 June — UNVERIFIED).⁶

3.1 INC-2026-W24-01 — CSIR/CHPC Lengau Supercomputer Breach [CONFIRMED]

Sector	Public Sector / Academic Research (CSIR / DSI)
Date	4 June 2026 (forced offline); access detected late May
Actor	Unknown -- no group has claimed attribution
Compromise	User credentials and SSH keys; no confirmed research-data exfiltration
Regulatory	POPIA section 22 notification process initiated; investigation ongoing
Affected	SA universities, Department of Science and Innovation, partner institutions
Strategic context	Lengau hosts research workloads for national science infrastructure -- strategic-research-target profile
Confidence	CONFIRMED -- system offline; POPIA notification initiated

The CHPC Lengau system is South Africa's national flagship high-performance computing cluster, supporting research workloads for SA universities, the Department of Science and Innovation, and partner institutions. The breach — involving user credentials and SSH keys — forced Lengau offline on 4 June. POPIA section 22 notification has been initiated; no exfiltration of research datasets has been confirmed at time of publication. Attribution is open with no group claiming responsibility. The strategic-research-target profile makes this analytically significant beyond the credential incident itself: compromise of SSH keys to a national HPC facility creates persistent access risk to research data across the entire user community.¹

3.2 INC-2026-W24-02 — Standard Bank / ROOTBOY -- Full 1.2 TB Dataset Publicly Released [CONFIRMED]

Actor	ROOTBOY (criminal extortion/data leak operator)
Escalation date	~1 June 2026 (public release event)
Prior status	W21-W23: quiet extortion / selective disclosure
Dataset	1.2 TB cumulative; includes account data and card-linked details
Dark-web pricing	SA bank cards at ~\$350 per bundle (EWN dark-web investigation confirmed)
Bank response	IR continuing; no new Standard Bank public statement W24
Confidence	CONFIRMED (release event); financial-impact assessment in progress

ROOTBOY's escalation from quiet extortion (W21-W23) to public mass disclosure marks a significant shift in the group's operational posture. EWN's dark-web investigation confirmed SA bank cards trading at approximately \$350 per bundle. ITWeb's 1 June weekly roundup confirmed the release event. The financial-sector SOC community should subscribe to dark-web bundle telemetry and initiate targeted client notification for high-volume Standard Bank corporate customers. Fraud-prevention thresholds should be reviewed given the confirmed card-bundle data now in circulation.²⁷

3.3 INC-2026-W24-03 — Central JHB TVET College -- POPIA Enforcement Notice [CONFIRMED PRECEDENT]

Authority	Information Regulator of South Africa
Date	1 June 2026
Breach type	Staff criminal-background-check data inadvertently shared internally with unauthorised employees
POPIA violations found	Accountability, further processing limits, security safeguards, s.22 notification failure, IO registration failure
Orders	Register Information Officer within 31 days; implement POPIA compliance framework; staff training; remediation report
Consequence	Non-compliance = criminal offence
Precedent value	Inadvertent internal disclosure now treated as a notifiable security compromise under POPIA
Confidence	CONFIRMED -- enforcement notice publicly issued

This enforcement notice is analytically significant beyond the specific institution. It establishes that inadvertent internal sharing of sensitive staff data — not just external breach or exfiltration — constitutes a notifiable security compromise under POPIA. Every SA HR function, payroll department, and compliance team should review internal data-sharing practices for staff vetting, background-check, and criminal-check workflows. Failure to register an Information Officer (IO) was explicitly cited as a violation — organisations that have not completed IO registration are now at direct enforcement risk.⁸

3.4 INC-2026-W24-04 — NETSCOUT -- SA #1 Globally for DDoS Against Banking, Insurance, IT Services [CONFIRMED]

Source	NETSCOUT DDoS Threat Intelligence Report H1 2026 (published 3 June 2026)
Finding	SA holds #1 global rank by sector-specific DDoS volume: commercial banking, insurance, and IT services
Context	Re-grounds W22 Black Matter ISP wave as part of a longer-running campaign (not an isolated event)
Attack type	Extortion-linked, multi-vector DDoS targeting SA hosting/ISP/connectivity and financial sector
SA relevance	Quantitative validation for sector board cyber-risk reviews; changes risk-modelling basis from anecdotal to measured
Confidence	CONFIRMED (vendor intelligence report)

The NETSCOUT H1 2026 report provides the first quantitative benchmark placing SA at the top of the global DDoS target ranking by sector. This changes the analytical basis for SA financial-sector DDoS risk from anecdotal ("we see DDoS attacks") to measured ("we are the #1 global target by volume in our sector"). Financial services CISOs should use this data to support board-level investment in DDoS scrubbing capacity, upstream mitigation agreements, and sector-coordinated incident response with SARB/FSCA.³

3.5 INC-2026-W24-05 — SABS Executive Disciplinary Hearings -- Lynx Ransomware Attribution Confirmed [CONFIRMED]

DTIC commenced disciplinary proceedings against two suspended SABS acting CEOs in the first week of June. Lynx Ransomware has been formally attributed to the November 2024 SABS attack. The charge basis explicitly references failure to implement SSA and Auditor-General cybersecurity recommendations dating back to 2022. This creates a material C-suite accountability precedent: documented failure to act on cybersecurity recommendations now forms the basis for criminal/disciplinary proceedings. SA boards and executives who have received and not acted on AGSA cybersecurity findings should treat this as a direct precedent applicable to their own governance posture.⁹

3.6 INC-2026-W24-06 — Black X Claims ANC Compromise (2 June) [UNVERIFIED]

Actor	Black X (ransomware group)
Claim date	2 June 2026 -- listed anc1912.org.za on Black X leak site
Claimed attack date	August 2025
Telemetry check	HudsonRock infostealer telemetry: only 3 compromised users (low-volume or stale claim)
ANC response	No response to date
Distinction	Distinct from W21 Black Ax UNVERIFIED carryover -- different group, different claim
Confidence	UNVERIFIED

The Black X claim against the ANC follows a pattern of ransomware groups using high-profile political organisations for visibility. The HudsonRock telemetry showing only 3 compromised users is a strong signal that this claim is either stale, low-volume, or fabricated for reputational impact. Until the ANC issues a statement or independent corroboration emerges, this should be treated as UNVERIFIED and tracked separately from the distinct W21 Black Ax claim which also remains unconfirmed.

3.7 Ongoing / Continuation Incidents (W24 Status)

Incident	W24 Status
Pick n Pay / Bottles	Regulatory loop closed -- IR + NCC publicly engaged; PnP formally initiated POPIA s.22 notification.
SA2000 / STORMOUS	CORRECTION -- SA2000 is a Canadian company; no SA nexus (previously flagged in error).
Webworm SA university	No new W24 victims; IOC takedowns executed.
Oday Syndicate / XL Africa	Group active (Bulgaria + Brazil W24); XL Africa still listed; no new Africa victims.
The Gentlemen / Storm-2697	20+ global victims posted 4 June; no new SA victims.
Polmed 1.7M / 214 GB	Still DEVELOPING; no statement.
SANBS / KillSec	STILL UNVERIFIED.
ANC "Black Ax" (W21)	STILL UNVERIFIED -- distinct from W24 Black X claim.
Telkom claim (W23)	STILL DENIED by Telkom.
#OpSouthAfrica Week 3	Nullsec Nigeria, 404 Crew, Infernalis active 4-5 Jun; no new verified victim acknowledgements.

6. ITWeb Security Summit Johannesburg 2026 (2-4 June) -- programme and coverage — <https://www.itweb.co.za/event/itweb-security-summit-2026/>
7. EWN dark-web investigation -- SA bank cards trading at \$350/bundle (June 2026) — <https://ewn.co.za/>
8. ITWeb -- TVET college in POPIA breach over employee data exposure (1 June 2026) — <https://www.itweb.co.za/article/tvet-college-in-popia-breach-over-employee-data-exposure/8OKdWqDX3VdqbnQ>
9. Daily Maverick / ITWeb -- SABS executive disciplinary hearings begin (June 2026) — <https://www.dailymaverick.co.za/>

4. GLOBAL INCIDENTS WITH SA RELEVANCE

TA4922 (China-linked) Phishing Expands to SA -- Proofpoint (W24 intel)

Proofpoint confirmed financially motivated China-linked actor TA4922 (ValleyRAT / Atlas RAT toolkit) expanded targeting to SA in March–April 2026. Tool family overlaps with prior China-aligned crimeware; financial motivation rather than espionage. No named SA victim yet. SA financial services and commercial enterprises should be alert to ValleyRAT / Atlas RAT IOCs in phishing campaigns.¹⁰

GroundUp / AGSA: SITA 5,014 CVEs Across 30+ SA Government Departments (3 June)

A GroundUp investigation (3 June) documented 5,014 CVEs and 125 critical vulnerabilities across 30+ SA government departments served by SITA — including ProxyLogon-class Exchange issues and a 2006–vintage flaw still exposed. SITA publicly disputed the findings ("systems secure"). AGSA referenced the same governance gaps to a parliamentary committee within the same week. This directly contradicts SITA's prior denial of #OpSouthAfrica claims (W23). SA government SOCs should treat the GroundUp inventory as a baseline for remediation prioritisation.¹¹

The Gentlemen / Storm-2697 -- 20+ Global Victims Posted 4 June; No New SA Victims

Storm-2697 ("The Gentlemen") continues its global campaign. 20+ new victims were posted to the leak site on 4 June. No new SA victims were identified in W24, but the Sunspray Food Solutions (SA) attribution from W23 remains. Self-propagating Go-based ransomware with 21 lateral-movement techniques.¹²

Nightspire Ransomware -- First Mutual Holdings (Zimbabwe) Posted 5 June

Nightspire posted First Mutual Holdings (Zimbabwe) on 5 June — the nearest SADC victim in W24. No direct SA victims from Nightspire, but the SADC regional footprint warrants monitoring. SA insurance-sector CISOs should review Nightspire TTPs.¹³

Screening Serpens / UNC1549 (Iran APT) -- Expanding Beyond Middle East (CYFIRMA W24)

CYFIRMA "Threat Actor in Focus" W24 profiled Screening Serpens / UNC1549 (Iran-aligned) expanding targeting beyond the Middle East using AppDomainManager hijacking technique. No confirmed SA targets at time of publication. SA organisations with Middle East business exposure should review UNC1549 IOCs.¹⁴

US EO on AI Innovation and Cybersecurity (2 June)

A Trump Executive Order on 2 June directed CISA to issue Binding Operational Directives within 30 days for AI-enabled federal cyber defence; established a voluntary AI Cybersecurity Clearinghouse; defined "covered frontier model" classification; and directed AG to prioritise AI-assisted cybercrime prosecutions. SA organisations with US operations should monitor resulting CISA BOD activity for compliance implications.¹⁵

10. Proofpoint -- TA4922 (China-linked) ValleyRAT/Atlas RAT SA targeting (W24) — <https://www.proofpoint.com/>

11. GroundUp -- SITA says its systems secure; we looked (3 June 2026) — <https://groundup.org.za/article/sita-says-its-systems-secure-we-looked-this-what-we-found/>

12. Microsoft Threat Intelligence -- Storm-2697 / The Gentlemen (ongoing) — <https://www.microsoft.com/security/blog/>

13. Leak-site tracker -- Nightspire First Mutual Holdings (Zimbabwe) (5 June 2026) — <https://www.ransomware.live/>

14. CYFIRMA -- Screening Serpens / UNC1549 threat actor profile (W24) — <https://www.cyfirma.com/news/>

15. White House -- EO on AI Innovation and Cybersecurity (2 June 2026) — <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>

5. THREAT ACTORS

5.1 ROOTBOY — Standard Bank 1.2 TB Public Release (~1 June)

ROOTBOY escalated from W21-W23 quiet extortion to full public data release around 1 June 2026. The complete 1.2 TB Standard Bank dataset entered the open domain. EWN's dark-web investigation confirmed SA bank cards trading at approximately \$350 per bundle. This moves the Standard Bank incident from an active IR engagement to a widespread financial-sector fraud risk. Financial services SOC teams should initiate dark-web bundle telemetry subscriptions and targeted corporate client notification programmes.²⁷

5.2 Lynx Ransomware — SABS Attribution Confirmed; C-Suite Accountability Precedent

Lynx Ransomware has been formally attributed to the November 2024 SABS attack as part of the DTIC disciplinary proceedings against two suspended SABS acting CEOs. The charge basis explicitly references failure to implement SSA and Auditor-General cybersecurity recommendations from 2022. This is the first SA case where documented failure to act on cybersecurity governance recommendations has formed the basis for C-suite disciplinary proceedings. Every SA board and executive that has received AGSA cybersecurity findings and not acted on them should review their governance posture in light of this precedent.⁹

5.3 Black X — ANC Claim 2 June (UNVERIFIED; Distinct from W21 Black Ax)

Black X listed anc1912.org.za on 2 June 2026, claiming an August 2025 attack. HudsonRock infostealer telemetry shows only 3 compromised users — a very low-volume signal consistent with a stale or fabricated claim. This is analytically distinct from the W21 "Black Ax" unverified carryover; both remain unconfirmed. Monitor Black X leak site for additional activity; treat current claim as UNVERIFIED pending corroboration.

5.4 Threat Actor Summary — W24

Actor	Type	Notable W24 Activity	Source
ROOTBOY	Criminal	Publicly released full Standard Bank 1.2 TB dataset ~1 Jun; EWN confirmed SA cards at ~\$350/bundle	ITWeb, EWN
TA4922 (China-linked)	Fin. crimeware	Proofpoint confirmed SA-targeting expansion Mar-Apr 2026; ValleyRAT / Atlas RAT toolkit	Proofpoint
Lynx	Ransomware	Formally attributed to Nov 2024 SABS attack; SABS exec hearings begin first week of June	DTIC, Daily Maverick
Webworm (China APT)	State espionage	No new Africa victims W24; IOC takedowns executed; W23 SA university compromise stands	ESET
Oday Syndicate	Ransomware	New victims Bulgaria + Brazil this week; no new Africa; XL Africa Group still listed	Cyble
The Gentlemen / Storm-2697	RaaS	20+ global victims posted 4 June; no new SA	Microsoft
Nightspire	Ransomware	First Mutual Holdings (Zimbabwe) posted 5 Jun -- nearest SADC victim W24	Leak-site tracker
Screening Serpens / UNC1549	Iran APT	CYFIRMA W24 profile; expanding beyond Middle East; AppDomainManager hijacking; no confirmed SA	CYFIRMA
Nullsec Nigeria / 404 Crew / Infernalis	Hacktivist	#OpSouthAfrica Week 3 reaffirmed claims 4-5 Jun; no new verified victim acknowledgements	Multiple
SideWinder (suspected India)	APT	Africa nuclear + Djibouti/Egypt maritime escalation continuing from W23	WhoisXML
Lazarus (DPRK)	State-aligned	Operation DangerousPassword retrospective continues (axios npm)	ESET
Black X	Ransomware	Claimed ANC 2 Jun -- UNVERIFIED (HudsonRock telemetry shows only 3 compromised users)	Black X leak site

5.5 Notable Industry Intelligence Actions (W24)

NETSCOUT H1 2026 Report: SA confirmed #1 globally for DDoS attacks against commercial banking, insurance, and IT services sectors. Quantifies the W22 Black Matter ISP wave as part of a longer-running coordinated campaign rather than an isolated event. This report provides the most authoritative data to date on SA's DDoS threat posture.³

GroundUp SITA investigation (3 June): 5,014 CVEs and 125 critical vulnerabilities across 30+ SA government departments. AGSA simultaneously referenced the same governance gaps in a parliamentary committee. SITA's "systems secure" denial directly contradicts the GroundUp technical findings, which include ProxyLogon-class Exchange issues and a 2006-vintage flaw still exposed.¹¹

10. Proofpoint -- TA4922 China-linked actor SA expansion (W24) — <https://www.proofpoint.com/>

11. GroundUp -- SITA CVE investigation (3 June 2026) —

<https://groundup.org.za/article/sita-says-its-systems-secure-we-looked-this-what-we-found/>

12. Microsoft -- Storm-2697 / The Gentlemen ongoing advisory — <https://www.microsoft.com/security/blog/>

13. Ransomware.live -- Nightspire / First Mutual Holdings listing — <https://www.ransomware.live/>

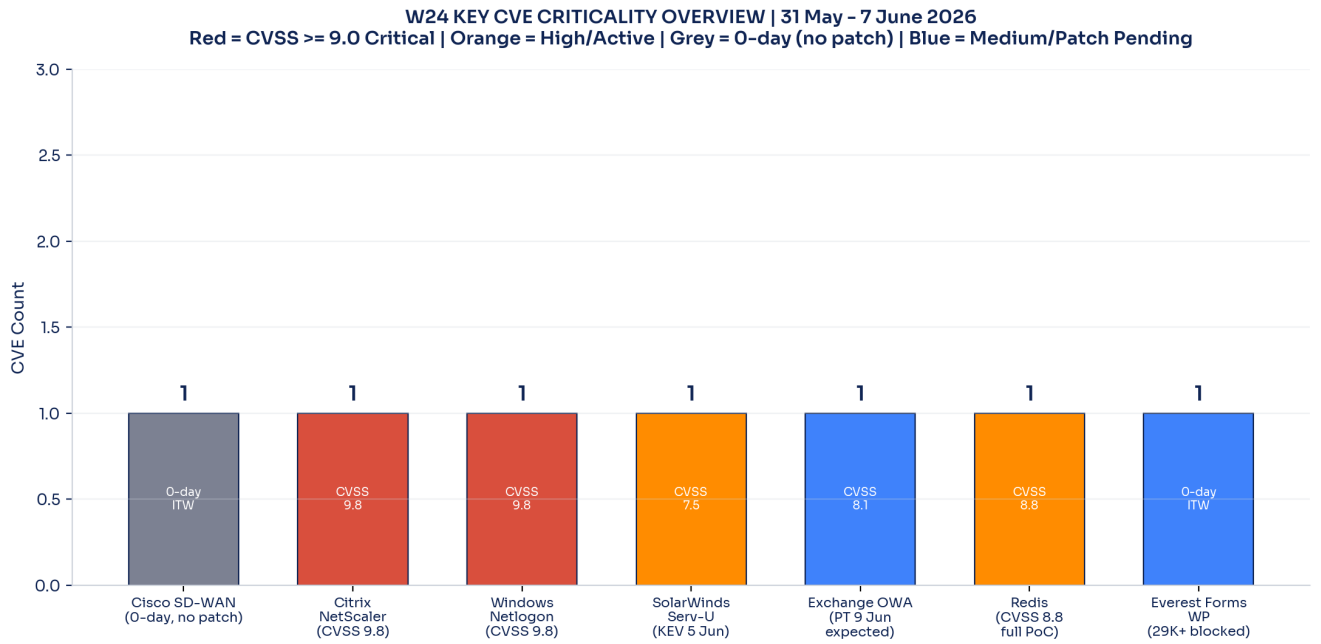
14. CYFIRMA -- Screening Serpens UNC1549 W24 profile — <https://www.cyfirma.com/news/>

6. CRITICAL VULNERABILITIES & CISA KEV

CISA KEV activity was lighter than W23 but operationally critical. **SolarWinds Serv-U CVE-2026-28318** (KEV added 5 June, federal deadline 19 June) is the only fresh active-deadline item in SA-relevant stacks. **Cisco SD-WAN took its seventh exploited zero-day of 2026** (CVE-2026-20245) with no patch and no workaround. **Citrix NetScaler CVE-2026-3055** (CVSS 9.8) is under thousands of daily exploit attempts globally. **Patch Tuesday 9 June** is the primary operational focus: Exchange OWA permanent patch and

OpenSSL HIGH/CRITICAL update both expected.⁴⁵¹⁶

W24 Key CVE Criticality Overview — (7 Tracked, 9 June Patch Tuesday Critical)



W24 CISA KEV / Critical CVE Tracking (31 May–7 June 2026)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-20245	Cisco / SD-WAN (all editions)	n/a	0-day RCE	NO PATCH	Cisco 7th SD-WAN 0-day 2026; Mandiant ITW; config push to edge devices; chain with CVE-2026-20182
CVE-2026-3055	Citrix / NetScaler (SAML IDP)	9.8	Unauth RCE	Patch NOW	Fortinet: thousands/day attacks; patch 13.1-62.23 / 14.1-60.58; SA banking/SSO in scope
CVE-2026-28318	SolarWinds / Serv-U	7.5	Unauth DoS	19 Jun 2026	KEV 5 Jun; crafted POST Content-Encoding:deflate; patch 15.5.4 HF1
CVE-2026-42897	Microsoft / Exchange OWA (2016, 2019, SE)	8.1	XSS/Spoofing	29 May PASSED	NO permanent patch; EEMS M2 only; perm fix EXPECTED PT 9 Jun
CVE-2026-41089	Microsoft / Windows Netlogon	9.8	0-click RCE (DC)	Apply 12 May PT	Belgium CCB active–exploit warning; rotate krbtgt if DCs exposed 12 May–1 Jun
OpenSSL pre-announce	OpenSSL (all versions)	HIGH/CRITICAL	TBD	9 Jun release	Severity undisclosed; inventory containerised + static deployments now
CVE-2026-23479	Redis 7.2.0–8.6.2	8.8	Use-after-free RCE	Patched May	Full 3-stage public PoC (AI-discovered); self-hosted urgent; Redis Cloud patched
CVE-2026-3300	Everest Forms Pro WP Plugin	n/a	PHP code injection	Patch 1.9.13	Wordfence: 29,300+ blocked attempts; unauthenticated eval() injection
CVE-2026-45247	Mirasvit Cache Warmer (Magento)	n/a	RCE	6 Jun PASSED	KEV deadline 6 Jun PASSED; audit all Magento/Adobe Commerce shops
CVE-2026-0257	Palo Alto / PAN-OS GlobalProtect	9.3	Auth bypass	19 Jun 2026	KEV 29 May (W23); ITW continuing; new IOCs from Vultr + Dromatics tracked
CVE-2026-34926	Trend Micro / Apex One (on-prem)	8.4	Directory traversal	4 Jun PASSED	KEV 26 May; federal compliance audit phase; AV update channel poisoning

Pattern note: W24 introduces a "7th zero-day" pattern for Cisco SD-WAN: seven exploited zero-days in a single product line across one calendar year is analytically unprecedented. Organisations dependent on Cisco SD-WAN for WAN edge infrastructure should begin formal architecture reviews for zero-day exposure reduction, including air-gapped management plane options and vendor diversification planning.

6.1 Cisco SD-WAN CVE-2026-20245 (0-day, No Patch, ACTIVE) -- 7th Exploited SD-WAN 0-day of 2026

Authenticated netadmin attackers (credential obtainable by chaining CVE-2026-20182) can execute root commands via crafted file upload. Mandiant reporting confirmed Cisco observed exploitation resulting in configuration changes pushed to edge devices. No patch and no workaround are available. SA relevance is CRITICAL: SD-WAN is deployed across SA telcos/ISPs and large enterprise WAN edges. Immediate mitigation: collect admin-tech logs from all SD-WAN edges before any upgrade attempt; restrict netadmin access to out-of-band management only; monitor for configuration drift.⁵

6.2 Prior KEV Status -- W23 Carryover Deadlines (W24 Status)

CVE	Status W24
PAN-OS GlobalProtect CVE-2026-0257 (CVSS 9.3)	KEV deadline 19 Jun UPCOMING; ITW continuing; new IOCs/IPs from Vultr + Dromatics tracked W24
Trend Micro Apex One CVE-2026-34926 (8.4)	KEV deadline 4 Jun PASSED -- federal compliance audit phase; verify patch status
Oracle ORDS CVE-2026-46840 (10.0)	June CSPU follow-up; additional advisories expected; treat as urgent if not patched
Supply chain triple (DAEMON / @tanstack / Nx Console)	KEV deadline 10 Jun UPCOMING -- developer toolchain audit still required
Linux kernel pair (Copy Fail / ssh-keysign-pwn)	Public PoC + Metasploit available -- patch + reboot all exposed systems
Ghost CMS CVE-2026-26980	700+ sites compromised -- ClickFix campaign ongoing; visitors at risk regardless of internal stack
Mirasvit Cache Warmer CVE-2026-45247	KEV deadline 6 Jun PASSED -- audit all Magento/Adobe Commerce deployments
FortiClient EMS CVE-2026-35616	EKZ Infostealer campaign continuing; verify patches 7.4.5/7.4.6/7.4.7

EXCHANGE OWA CVE-2026-42897 -- PERMANENT PATCH EXPECTED PATCH TUESDAY 9 JUNE

Status: KEV deadline 29 May 2026 PASSED. EEMS Mitigation ID M2 is the ONLY available protection. Permanent patch forecast for 9 June Patch Tuesday (Help Net Security Patch Tuesday preview, 5 June).

Pre-stage now: Run Exchange Health Checker (aka.ms/ExchangeHealthChecker) to confirm M2 is active. Pre-stage the 9 June change window. Block SVG and active-attachment rendering as additional precaution.

EEMS M2 limitations: OWA Print Calendar, inline images in OWA, OWA Light (?layout=light) broken; IE/Edge IE-mode users remain unprotected by M2. Document breakage with users.

After 9 June PT: Apply permanent patch; remove M2 mitigation only after patch is confirmed applied and Health Checker shows healthy state.

6.3 SolarWinds Serv-U CVE-2026-28318 (KEV 5 June, Deadline 19 June)

Unauthenticated DoS crash via crafted POST request with Content-Encoding: deflate header. CISA confirmed active exploitation and added to KEV on 5 June with federal deadline 19 June. Patch: Serv-U 15.5.4 HF1 (available now). SA relevance is HIGH: SolarWinds is present in SA public-sector and large enterprise IT-ops stacks. Audit all external Serv-U exposure immediately; patch ahead of the 19 June federal deadline.¹⁶

4. Help Net Security -- June 2026 Patch Tuesday forecast (5 June 2026) —

<https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>

5. Help Net Security -- Cisco SD-WAN CVE-2026-20245 0-day exploited (5 June 2026) —

<https://www.helpnetsecurity.com/2026/06/05/cisco-sd-wan-cve-2026-20245-0-day-exploited/>

16. BleepingComputer -- CISA: hackers now exploit SolarWinds Serv-U flaw (5 June 2026) —

<https://www.bleepingcomputer.com/news/security/cisa-hackers-now-exploit-solarwinds-serv-u-flaw-to-crash-servers/>

17. SecurityWeek -- Critical Windows Netlogon vulnerability in attackers crosshairs —

<https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs/>

18. Cyware daily threat brief -- Citrix NetScaler CVE-2026-3055 (1 June 2026) —

<https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-june-01-2026>

19. Threat Modeling -- vulnerability intelligence report (4 June 2026) —

<https://threat-modeling.com/vulnerability-intelligence-report-june-4-2026/>

20. OffSec -- Redis CVE-2026-23479 full public exploit chain released —

<https://radar.offsec.com/threat/a-two-year-old-rce-bug-in-redis-was-just-made-publ-b15cdac8>

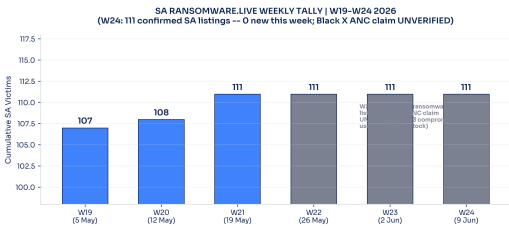
21. Loginsoft weekly report -- Everest Forms Pro + Mirasvit vulnerabilities weaponised —

<https://www.loginsoft.com/reports/weekly/resurfaced-vulnerabilities-weaponized-workflows-and-exposed-operations-define-the-week>

7. RANSOMWARE LANDSCAPE

SA ransomware.live victim count remains at **111 cumulative (FLAT)** for W24, with **zero new listings** on the ransomware.live tracker during 31 May–7 June 2026. The only new claim against a SA entity — Black X's listing of the ANC on 2 June — is assessed as UNVERIFIED based on HudsonRock infostealer telemetry showing only 3 compromised users, which is inconsistent with a meaningful breach of a national political organisation with tens of thousands of members.²²

SA Contextualisation: The FLAT count is now a three-week streak (W22, W23, and W24 all FLAT at 111). This should not be interpreted as a reduction in ransomware risk. The Standard Bank 1.2 TB public release (W24) demonstrates that the criminal ecosystem is active and escalating against SA targets outside the ransomware.live tracking mechanism. The SABS/Lynx precedent demonstrates that ransomware consequences continue to play out through regulatory and governance channels long after the initial incident.



End W23 baseline	111 confirmed SA listings
New W24 listings (31 May – 7 Jun)	0 confirmed on ransomware.live
End W24 count	111 (FLAT)
Black X ANC claim (2 Jun)	UNVERIFIED (HudsonRock: 3 compromised users only)
Nearest SADC victim W24	Nightspire / First Mutual Holdings (Zimbabwe) -- posted 5 Jun
Threat level driver (non-ransomware.live)	Standard Bank 1.2 TB publicly released; CSIR/CHPC Lengau breach

22. Ransomware.live -- South Africa country map (W24) — <https://www.ransomware.live/map/ZA>

8. OSINT EXPOSURE & ATTACK SURFACE

CSIR/CHPC Lengau SSH key exposure -- sector-wide academic IR sweep required

The confirmed SSH key compromise at Lengau creates downstream exposure risk for every user community member who may have reused SSH credentials across their own institution's infrastructure. SA research and academic institutions should immediately audit SSH key reuse, revoke and regenerate keys for any user with a Lengau account, and hunt for lateral movement indicators in university and DSI networks.¹

Standard Bank 1.2 TB public release -- financial sector fraud monitoring

With 1.2 TB of Standard Bank data now in the open domain, the immediate risk is large-scale card fraud from the \$350/bundle market. SA financial sector fraud operations should: subscribe to dark-web bundle telemetry; increase transaction monitoring thresholds for Standard Bank corporate account patterns; initiate targeted client notification for high-volume customers. EWN investigation confirmed specific bundle pricing.²⁷

SITA 5,014 CVE inventory -- SA government attack surface baseline

The GroundUp/AGSA documented 5,014 CVEs across 30+ SA government departments include ProxyLogon-class Exchange issues and a 2006-vintage flaw. SITA's denial does not diminish the documented exposure. SA government IT operations should treat the GroundUp CVE inventory as a baseline for remediation prioritisation. The presence of ProxyLogon-class Exchange CVEs suggests potential persistent access channels for threat actors.¹¹

Cisco SD-WAN 0-day (CVE-2026-20245) -- no patch, admin-tech log collection urgent

With no patch and no workaround available, the only immediate defensive action is: collect admin-tech logs from all SD-WAN edges; restrict netadmin access to out-of-band-only; monitor for configuration drift pushed to edge devices. Mandiant confirmed exploitation results in configuration changes to edge devices, which could introduce routing changes, traffic interception, or backdoor persistence.⁵

Citrix NetScaler CVE-2026-3055 -- SAML IDP instances at immediate risk

Any NetScaler deployed as SAML Identity Provider is at immediate risk from thousands of daily attack attempts. Identify all SAML IDP NetScaler instances in SA banking, enterprise SSO, and VDI stacks. Patch to 13.1-62.23 or 14.1-60.58 immediately. Review SAML assertion logs for anomalies (unexpected attribute assertions, anomalous session lifetimes, assertion replay patterns).¹⁸

POPIA enforcement expansion -- internal disclosure now notifiable

Central JHB TVET enforcement notice establishes that inadvertent internal sharing of sensitive staff data constitutes a notifiable security compromise. SA HR functions should immediately review criminal background check data handling workflows, staff vetting data sharing practices, and Information Officer registration status. The precedent is directly applicable to any organisation processing sensitive staff data internally.⁸

9. REGULATORY & COMPLIANCE

SA Cabinet Withdraws Draft National AI Policy (3 June)

The SA Cabinet formally withdrew the Draft National AI Policy on 3 June following the DCDT AI-hallucinated-references scandal. Three new DDGs have been appointed; the revised policy targets November 2026 for Cabinet approval. The public comment window for the original draft is effectively closed. SA organisations deploying AI should continue their comment preparation but adjust to the revised November 2026 target. Note: EU AI Act Article 4 literacy obligations for 2 August 2026 are unaffected by SA policy delays — EU-operating SA organisations remain in scope.²³

PASA Dissolved -- SARB Acquires 50% Stake in PayInc (5 June)

PASA (Payments Association of South Africa) was dissolved after 30+ years, with SARB taking a 50% stake in PayInc (formerly BankservAfrica). Functions transfer to PayInc; transition date pending. SA payment-system participants should monitor SARB/PayInc communications for operational transition timelines. PASA membership obligations and payment-system compliance frameworks will require review under the new governance structure.²⁴

FICA ss.30, 54, 55, 70 Effective 1 July 2026 -- Cash Conveyance Criminalisation

The FICA cash/bearer instrument conveyance reporting sections (ss.30, 54, 55, 70) were gazetted for effect from 1 July 2026. This completes SA's pre-FATF Mutual Evaluation compliance posture. From 1 July, failure to report cash conveyance above prescribed thresholds becomes a criminal offence. SA accountable institutions must brief finance and legal teams immediately. The convergence of B15-2026 (AML/CFT), FICA ss.30/54/55/70, and crypto exchange-control updates creates a tight Q3 board-level compliance window.²⁵

SARB/FSCA Joint Statement -- Crypto Not Legal Tender; Rand-Backed Stablecoin Assessment

SARB and FSCA confirmed on 29 May/2 June: crypto and stablecoins excluded from NPS Act; foreign stablecoins excluded as domestic payment instruments (dollarisation risk); IFWG to assess rand-backed stablecoins by late 2026; SARB regulatory sandbox active; FIC Directive 9 (travel rule) in full force. SA crypto exchanges and digital asset service providers should review their NPS Act classification and prepare for IFWG rand-backed stablecoin assessment process.²⁶

Other W24 Regulatory Developments

- **ITWeb Security Summit Johannesburg (2-4 June):** 21st edition; ~1,000 attendees; SA CISO panel (FirstRand, Telkom, Transnet, Foschini) on regulatory compliance as board-investment lever; CSIR Dr Jabu Mtsweni skills collaboration; Huawei Cloud 5 AI security upgrades for Sub-Saharan Africa; BBC/Joe Tidy on teenage hacking gangs.⁶
- **EU CSA2 / NIS2 package (9 June TTE Council):** CSA2 in EP/Council negotiation; 7% global turnover penalties; ENISA budget +75%; high-risk ICT supplier designation; ransomware disclosure; 36-month phase-out for telcos with high-risk components. Final text expected 2027+. SA technology exporters to EU should track high-risk ICT supplier designation criteria.²⁷
- **EU AI Act -- 2 August 2026 AI Literacy Deadline UNCHANGED:** Article 4 literacy obligations unaffected by Digital Omnibus deferrals; all EU-operating SA organisations in scope. Deadline is 47 days from publication of this report.²⁷
- **UK DUAA complaints duty live 19 June 2026 (active in 12 days from 8 June publication):** Internal data-protection complaints process mandatory; 30-day acknowledgement; ICO 2-week countdown reminders active.²⁸
- **Canada Bill C-8 -- Critical Cyber Systems Protection Act:** Passed Senate 5 June; mandatory cyber framework for critical infrastructure; supplier-ban powers; monetary penalties; awaiting Royal Assent. SA organisations with Canadian critical infrastructure partnerships should monitor Royal Assent timeline.²⁹

Compliance Deadlines — W24 Forward View

Date	Item	Owner
9 Jun 2026	Patch Tuesday -- Exchange OWA permanent patch EXPECTED + OpenSSL HIGH/CRITICAL	IT
10 Jun 2026	CISA KEV: Supply chain triple (DAEMON/TanStack/Nx) deadline	IT
19 Jun 2026	CISA KEV: SolarWinds Serv-U CVE-2026-28318 federal deadline	IT
19 Jun 2026	CISA KEV: PAN-OS GlobalProtect CVE-2026-0257 deadline	IT
19 Jun 2026	UK DUAA complaints-handling statutory duty active	Compliance
1 Jul 2026	FICA ss.30/54/55/70 cash conveyance criminalisation effective	Compliance
2 Aug 2026	EU AI Act Art. 4 literacy obligations (unchanged)	Compliance
2 Aug 2026	EU AI Act Art. 50 transparency obligations (chatbot disclosure)	Compliance
Late 2026	SARB/IFWG rand-backed stablecoin assessment	Finance/Legal
Nov 2026	SA revised AI Policy Cabinet approval target	Compliance
2 Dec 2026	EU AI Act watermarking/deepfake marking	Compliance

23. SANews -- Cabinet approves withdrawal of AI Policy (3 June 2026) —

<https://www.sanews.gov.za/south-africa/cabinet-approves-withdrawal-ai-policy>

24. Condia -- SA dissolves PASA; PayInc and SARB co-own (5 June 2026) —

<https://thecondia.com/south-africa-dissolves-pasa-payinc-sarb/>

25. SA Legal Academy -- FICA more sections in force soon (1 July 2026) —

<https://legalacademy.co.za/news/read/financial-intelligence-centre-act-more-sections-in-force-soon>

26. CryptoNews -- SARB/FSCA joint statement on crypto and stablecoins — <https://cryptonews.net/news/legal/32951895/>

27. ISC2 -- EU CSA2/NIS2 updates proposals (June 2026) —

<https://www.isc2.org/insights/2026/06/eu-csa2-nis2-updates-proposals-and-the-isc2-response>

28. Mishcon -- UK DUAA complaints process 19 June 2026 —

<https://www.mishcon.com/news/is-your-data-protection-complaints-process-ready-for-19-june-2026>

29. Jurist -- Canada Bill C-8 passed Senate (5 June 2026) —

<https://www.jurist.org/news/2026/06/canada-parliament-passes-cybersecurity-bill-amid-privacy-concerns/>

10. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W24. Two P1 missions address the 9 June Patch Tuesday pre-staging (Exchange OWA + OpenSSL) and Cisco SD-WAN 0-day log collection. Two P2 missions address Citrix NetScaler SAML IDP exploitation and CSIR/Lengau SSH key reuse across SA academic networks. Two P2 missions address Standard Bank dark-web fraud monitoring and the Windows Netlogon CVSS 9.8 DC patch audit. Two P3 missions address POPIA enforcement readiness and Black X / ANC claim monitoring.

TH-2026-W24-01 — Patch Tuesday 9 June Pre-Staging (Exchange OWA + OpenSSL + Full Rollup)**P1 — CRITICAL: PT 9 June; Exchange OWA perm patch + OpenSSL HIGH/CRITICAL both expected**

Hypothesis: Exchange OWA CVE-2026-42897 KEV deadline passed 29 May with no permanent patch; EEMS M2 is the only protection. 9 June PT is forecast to deliver the permanent fix plus an OpenSSL HIGH/CRITICAL update. Organisations not pre-staged face post-PT emergency change management pressure.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts via Exchange OWA session).

IOCs: Anomalous OWA URL patterns with script payloads; unexpected OWA logon-cookie reuse from new IPs or geolocations; Exchange Health Checker EEMS M2 not listed as active.

Data Sources: Exchange Health Checker output, Exchange IIS logs (OWA paths), Exchange audit log, Azure AD sign-in logs for Exchange-authenticated sessions.

Detection Guidance: Pre-stage: confirm EEMS M2 active (Exchange Health Checker); block SVG / active-attachment rendering; schedule 9 June change window. Post-PT: apply Exchange OWA permanent patch; apply OpenSSL update across all instances including containerised/static deployments; verify Health Checker shows healthy. Alert on OWA logon-cookie reuse from new geolocations until patch confirmed.

TH-2026-W24-02 — Cisco SD-WAN CVE-2026-20245 (0-day, No Patch) -- Admin-Tech Log Collection**P1 — CRITICAL: 0-day; no patch; Mandiant ITW; config changes on edge devices**

Hypothesis: Cisco SD-WAN CVE-2026-20245 is actively exploited with no patch and no workaround. Mandiant confirmed exploitation results in configuration changes pushed to edge devices. Any SA telco or enterprise SD-WAN edge may already be compromised.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1562.004 (Impair Defenses: Disable or Modify System Firewall), T1565 (Data Manipulation for routing changes).

IOCs: Unexpected SD-WAN configuration changes; new policy entries pushed to edge devices from unexpected management sources; admin-tech log entries showing file upload attempts; credentials used outside normal netadmin windows.

Data Sources: SD-WAN admin-tech logs, vManage audit logs, edge device configuration change history, management-plane access logs.

Detection Guidance: Immediately collect admin-tech logs from all SD-WAN edges before any upgrade attempt. Restrict netadmin access to out-of-band management only. Alert on any SD-WAN policy change or configuration push from unexpected source IPs. Compare current edge device configuration against known-good baseline. Chain: if CVE-2026-20182 credentials were exposed, treat CVE-2026-20245 as a confirmed active exploit chain.

TH-2026-W24-03 — Citrix NetScaler CVE-2026-3055 SAML IDP Exploitation Hunt**P2 — HIGH: CVSS 9.8; thousands/day attacks; SA banking/SSO/VDI in scope**

Hypothesis: Citrix NetScaler CVE-2026-3055 (CVSS 9.8) is under thousands of daily attack attempts globally against SAML IDP deployments. SA banking and enterprise SSO/VDI environments are directly in scope.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts via SAML assertion forgery), T1550.001 (Use Alternate Authentication Material).

IOCs: Anomalous SAML assertion patterns (unexpected attributes, anomalous session lifetimes, assertion replay); NetScaler management plane access from unexpected IPs; POST requests to /saml/login or equivalent SAML endpoints from scanning/exploit IPs.

Data Sources: NetScaler syslog, SAML assertion logs, ADC management audit logs, WAF/perimeter logs for NetScaler-exposed endpoints.

Detection Guidance: Identify all NetScaler instances configured as SAML IDP. Patch to 13.1-62.23 or 14.1-60.58 immediately. Review SAML assertion logs for anomalies. Alert on POST requests to SAML endpoints from non-enumerated source IPs. If management plane was exposed: treat as compromised pending full config review.

TH-2026-W24-04 — CSIR/Lengau SSH Key Reuse -- SA Academic/Research Network Sweep	P2 — HIGH: CSIR/CHPC Lengau breach CONFIRMED 4 June; SSH key reuse risk across SA academic sector
Hypothesis: The Lengau supercomputer breach involved SSH key theft. Users of Lengau include SA universities, DSI staff, and partner institutions. SSH key reuse across those institutions creates lateral movement risk even after Lengau itself is taken offline. MITRE ATT&CK: T1021.004 (Remote Services: SSH), T1098.004 (Account Manipulation: SSH Authorized Keys), T1078 (Valid Accounts). IOCs: SSH logins using keys associated with Lengau user accounts; new authorised_keys entries on academic institution servers; anomalous SSH sessions from CSIR/DSI IP ranges or unfamiliar source IPs. Data Sources: SSH authentication logs on academic institution servers, CSIR/DSI network logs, university SIEM for SSH session anomalies. Detection Guidance: Contact CSIR/CHPC for list of compromised user account identifiers (if available under POPIA). Audit authorised_keys files on all university-managed servers for keys matching Lengau user patterns. Hunt for new SSH sessions from unexpected source IPs. Rotate all SSH keys for any account with Lengau access as a precautionary measure.	
TH-2026-W24-05 — Standard Bank Dark-Web Fraud Monitoring -- \$350/Bundle Alert	P2 — HIGH: 1.2 TB publicly released ~1 Jun; confirmed \$350/bundle pricing
Hypothesis: ROOTBOY has publicly released the full 1.2 TB Standard Bank dataset. EWN confirmed SA bank cards trading at ~\$350 per bundle. Fraud actors are now actively monetising this data through card-not-present transactions, account takeover, and credential-stuffing. MITRE ATT&CK: T1110.004 (Credential Stuffing), T1539 (Steal Web Session Cookie), T1650 (Acquire Access). IOCs: Standard Bank card details appearing in dark-web bundle telemetry; credential-stuffing patterns against Standard Bank customer portals; card-not-present transactions from unusual geolocations for Standard Bank accounts. Data Sources: Dark-web intelligence feeds, fraud operations telemetry, Standard Bank customer authentication logs, card transaction monitoring systems. Detection Guidance: Subscribe to dark-web bundle telemetry monitoring for Standard Bank-pattern data. Increase transaction monitoring thresholds for Standard Bank corporate account patterns. Initiate targeted notification for high-volume Standard Bank corporate customers. Alert on authentication attempts using email/partial-card combinations consistent with the leaked dataset pattern.	
TH-2026-W24-06 — Windows Netlogon CVE-2026-41089 (CVSS 9.8) -- DC Patch Compliance Audit	P2 — HIGH: CVSS 9.8; Belgium CCB active-exploit warning; every AD estate in SA in scope
Hypothesis: CVE-2026-41089 is a 0-click unauthenticated RCE against domain controllers via stack overflow. Belgium CCB issued an active-exploitation warning. The 12 May Patch Tuesday patch applies; any unpatched DC since 12 May is at active risk. MITRE ATT&CK: T1210 (Exploitation of Remote Services), T1078.002 (Valid Accounts: Domain Accounts), T1557 (Adversary-in-the-Middle for DC compromise). IOCs: Unexpected Netlogon service crashes or restarts; anomalous LDAP/Netlogon traffic patterns; new domain admin accounts created without standard provisioning process; krbtgt password changes not associated with routine rotation. Data Sources: DC event logs (System, Security), Netlogon service logs, AD audit logs, SIEM for Netlogon traffic anomalies. Detection Guidance: Audit all DCs for 12 May Patch Tuesday compliance. If any DC was unpatched between 12 May and 1 June (per CCB exploitation window), rotate krbtgt immediately. Alert on Netlogon service anomalies. Review new domain admin account creation events in the post-12 May window.	

TH-2026-W24-07 — POPIA Enforcement Readiness -- Internal Disclosure Assessment	P3 — MONITORING: Enforcement notice 1 Jun; internal-disclosure-as-notifiable-compromise precedent
Hypothesis: Central JHB TVET enforcement notice establishes that inadvertent internal sharing of sensitive staff data constitutes a notifiable security compromise under POPIA. SA organisations with inadequate internal data-sharing controls are now at direct enforcement risk. MITRE ATT&CK: Not applicable (governance/compliance hunt). IOCs: Internal data-sharing incidents involving criminal-background-check data, HR data, staff vetting records; failed IO registration; absence of documented data-sharing agreements for sensitive HR workflows. Data Sources: HR data-sharing workflow documentation, Information Officer registration records, internal incident log for inadvertent disclosure events. Detection Guidance: Review all internal data-sharing workflows for staff criminal-background-check, vetting, and HR data. Verify Information Officer is registered with the Information Regulator. Confirm internal POPIA breach notification triggers cover inadvertent internal disclosure (not just external breach). Document findings for board reporting.	
TH-2026-W24-08 — Black X / ANC Claim -- Dark-Web Monitoring and Attribution Assessment	P3 — MONITORING: UNVERIFIED; HudsonRock shows only 3 compromised users
Hypothesis: Black X listed anc1912.org.za on 2 June claiming an August 2025 attack. HudsonRock telemetry shows only 3 compromised users -- consistent with stale or low-volume claim. Until ANC responds or corroboration emerges, treat as UNVERIFIED. MITRE ATT&CK: T1078 (Valid Accounts via stolen credentials), T1110.004 (Credential Stuffing). IOCs: ANC domain data appearing on Black X leak site; ANC employee credentials in infostealer feeds; HudsonRock telemetry exceeding the initial 3-user baseline. Data Sources: Black X leak site monitoring, HudsonRock infostealer telemetry, dark-web intelligence feeds, ANC public communications. Detection Guidance: Monitor Black X leak site for data publication (escalates UNVERIFIED to CONFIRMED). Monitor HudsonRock and infostealer feeds for ANC domain credential spikes. Track ANC public communications for breach acknowledgement. Maintain distinction from W21 Black Ax claim (different group, different claim, both unconfirmed).	

IOC Master Table — W24

Indicator	Type	Attribution	Hunt ID
CSIR/CHPC Lengau user credentials + SSH keys	Credential/SSH	Lengau supercomputer breach (4 Jun CONFIRMED)	TH-2026-W24-04
Standard Bank card bundles (~\$350/bundle)	Financial data	ROOTBOY Standard Bank 1.2 TB release (~1 Jun)	TH-2026-W24-05
CVE-2026-20245 (Cisco SD-WAN admin-tech logs)	CVE/O-day	Cisco 7th SD-WAN O-day 2026; Mandiant ITW; no patch	TH-2026-W24-02
CVE-2026-3055 (Citrix NetScaler SAML IDP)	CVE	CVSS 9.8; mass exploit (thousands/day); Fortinet confirmed	TH-2026-W24-03
CVE-2026-28318 (SolarWinds Serv-U)	CVE	KEV 5 Jun; federal deadline 19 Jun; patch 15.5.4 HF1	N/A
CVE-2026-42897 (Exchange OWA)	CVE	KEV 29 May PASSED; no perm patch; expected PT 9 Jun	TH-2026-W24-01
CVE-2026-41089 (Windows Netlogon CVSS 9.8)	CVE	Belgium CCB active-exploit warning; 12 May PT patch	TH-2026-W24-06
OpenSSL HIGH/CRITICAL pre-announce	Software	Pre-announced 9 Jun; severity undisclosed; all deployments	TH-2026-W24-01
anc1912.org.za (Black X claim)	Domain	Black X UNVERIFIED claim (2 Jun); 3 users per HudsonRock	TH-2026-W24-08
Vultr ASN (AS20473) + Dromatics IPs	ASN/IP	PAN-OS CVE-2026-0257 exploit source (Rapid7 MDR W23)	N/A (W23 carryover)

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Patch Tuesday 9 June -- primary change-window event (Exchange OWA permanent patch + OpenSSL HIGH/CRITICAL):** Pre-stage Exchange OWA permanent patch for CVE-2026-42897; pre-stage OpenSSL HIGH/CRITICAL update across all instances including containerised and static deployments; deploy full Windows June security rollout. Hold business calls scheduled for that window. Run Exchange Health Checker (aka.ms/ExchangeHealthChecker) now to confirm EEMS M2 is active. After PT, apply permanent patch and remove M2 mitigation only after confirmed healthy state.
- **2. Cisco SD-WAN CVE-2026-20245 (O-day, no patch):** Collect admin-tech logs from all SD-WAN edges immediately; restrict netadmin access to out-of-band-only; monitor for configuration drift; compare current edge configuration against known-good baseline. Prepare emergency patch response window for when Cisco ships a fix. If CVE-2026-20182 credentials were exposed, treat the chain as an active compromise scenario.
- **3. Citrix NetScaler CVE-2026-3055 (CVSS 9.8):** Identify all NetScaler instances configured as SAML IDP in SA banking, SSO, and VDI environments. Patch to 13.1-62.23 or 14.1-60.58 immediately. Review SAML assertion logs for anomalies. Alert on POST requests to SAML endpoints from non-enumerated source IPs.
- **4. SolarWinds Serv-U CVE-2026-28318 (KEV deadline 19 June):** Apply Serv-U 15.5.4 HF1 immediately. Audit all external Serv-U exposure. Add to your 9 June change-window batch if not done before.
- **5. CSIR/Lengau SSH key reuse sweep -- SA academic sector:** Contact CSIR/CHPC for affected user identifiers if available under POPIA. Audit authorised_keys files on university-managed servers. Rotate all SSH keys for accounts with Lengau access as a precautionary measure. Hunt for anomalous SSH sessions from unexpected source IPs in academic network environments.
- **6. POPIA enforcement readiness (Central TVET precedent):** Review all internal data-sharing workflows for criminal-background-check, HR, and staff vetting data. Verify Information Officer

registration with the Information Regulator. Confirm that internal POPIA breach notification triggers cover inadvertent internal disclosure (not just external exfiltration). This precedent is applicable to every SA HR function.

▪ **7. Windows Netlogon CVE-2026-41089 (CVSS 9.8) -- DC patch audit:** Audit all domain controllers for 12 May Patch Tuesday compliance. If any DC was unpatched between 12 May and 1 June, rotate krbtgt immediately. Alert on Netlogon service anomalies and new domain admin account creation in the post-12 May window.

Short-Term (Next 30 Days)

- Standard Bank dataset public release: financial-sector SOC subscription to dark-web bundle telemetry; targeted client notification for high-volume Standard Bank corporate customers; review fraud-prevention thresholds for card-pattern data now in open domain.
- SITA 5,014 CVE inventory: SA government SOC posture review against GroundUp baseline; ProxyLogon Exchange remediation prioritised; 2006-vintage flaw identification and emergency patch.
- FICA 1 July readiness: SA accountable institutions to brief finance and legal teams on cash conveyance reporting criminalisation; brief operations teams on new reporting obligations.
- Supply chain triple (DAEMON/TanStack/Nx) KEV deadline 10 June: complete developer toolchain audit; rotate all developer credentials and API keys where exposure confirmed.
- PAN-OS GlobalProtect CVE-2026-0257 KEV deadline 19 June: complete patch programme for all PAN-OS 10.2/11.x/12.x and Prisma Access deployments.
- PAIA annual report (2024/25) due via IR eServices by 30 June 2026.
- FATF Mutual Evaluation prep: convergence of B15-2026 (AML/CFT) + FICA ss.30/54/55/70 + crypto exchange-control updates creates tight Q3 board-level compliance window.

Strategic (Next Quarter)

- Lengau supercomputer impact: SA research/academic IR sweep for SSH key reuse and credential overlap with the affected Lengau user base; coordinate via CSIR and SA universities. Establish a cross-institutional SSH key hygiene programme with annual rotation requirements.
- Cisco SD-WAN zero-day programme: seven exploited zero-days in a single product line in one calendar year is analytically unprecedented. SA organisations dependent on Cisco SD-WAN should initiate formal architecture reviews for zero-day exposure reduction, including air-gapped management plane options and vendor diversification planning.
- POPIA enforcement trajectory: the Central TVET precedent signals that the Information Regulator is extending enforcement scope from external breach to inadvertent internal disclosure. SA privacy officers should expect this precedent to be applied broadly. Implement comprehensive internal data-sharing workflow audits covering all sensitive staff and customer data categories.
- SABS/Lynx C-suite accountability model: the first confirmed C-suite disciplinary proceedings tied to documented failure to act on cybersecurity governance recommendations will be cited by boards, auditors, and regulators in SA. All executives with documented AGSA cybersecurity findings should treat SABS as a direct precedent and initiate immediate compliance remediation.
- SA AI Policy reset (3 June withdrawal): prepare comments cycle for revised draft (November 2026 target); align with EU AI Act Article 4 literacy obligations due 2 August 2026 for cross-border-operating SA organisations.

12. OSINT SOURCES CONSULTED

The following open-source intelligence sources were consulted in the preparation of this report. All sources are TLP:WHITE and publicly accessible.

1. The Citizen -- Cybersecurity breach forces SA supercomputer offline (4 June 2026) — <https://www.citizen.co.za/rekord/news-headlines/2026/06/04/cybersecurity-breach-forces-sas-supercomputer-offline/>
2. ITWeb -- security weekly roundup (1 June 2026) / ROOTBOY Standard Bank release — <https://www.itweb.co.za/>
3. NETSCOUT DDoS Threat Intelligence Report H1 2026 (3 June 2026) — <https://www.netscout.com/>
4. Help Net Security -- June 2026 Patch Tuesday forecast (5 June 2026) — <https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>
5. Help Net Security -- Cisco SD-WAN CVE-2026-20245 zero-day exploited (5 June 2026) — <https://www.helpnetsecurity.com/2026/06/05/cisco-sd-wan-cve-2026-20245-0-day-exploited/>
6. ITWeb Security Summit Johannesburg 2026 -- programme (2-4 June) — <https://www.itweb.co.za/event/itweb-security-summit-2026/>
7. EWN dark-web investigation -- SA bank cards trading at \$350/bundle (June 2026) — <https://ewn.co.za/>
8. ITWeb -- TVET college in POPIA breach over employee data exposure (1 June 2026) — <https://www.itweb.co.za/article/tvet-college-in-popia-breach-over-employee-data-exposure/8OKdWqDX3VdqbnzQ>
9. Daily Maverick / ITWeb -- SABS executive disciplinary hearings begin (June 2026) — <https://www.dailymaverick.co.za/>
10. Proofpoint -- TA4922 China-linked actor SA targeting expansion (W24) — <https://www.proofpoint.com/>
11. GroundUp -- SITA says its systems secure; we looked (3 June 2026) — <https://groundup.org.za/article/sita-says-its-systems-secure-we-looked-this-what-we-found/>
12. Microsoft Security Blog -- Storm-2697 / The Gentlemen ongoing (4 June 2026) — <https://www.microsoft.com/security/blog/>
13. Ransomware.live -- Nightspire / First Mutual Holdings Zimbabwe (5 June 2026) — <https://www.ransomware.live/>
14. CYFIRMA -- Screening Serpens / UNC1549 threat actor profile W24 — <https://www.cyfirma.com/news/>
15. White House -- EO on AI Innovation and Cybersecurity (2 June 2026) — <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>
16. BleepingComputer -- CISA: hackers now exploit SolarWinds Serv-U (5 June 2026) — <https://www.bleepingcomputer.com/news/security/cisa-hackers-now-exploit-solarwinds-serv-u-flaw-to-crash-servers/>
17. SecurityWeek -- Critical Windows Netlogon vulnerability in attackers crosshairs — <https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs/>
18. Cyware daily threat brief -- Citrix NetScaler CVE-2026-3055 (1 June 2026) — <https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-june-01-2026>
19. Threat Modeling -- vulnerability intelligence report (4 June 2026) — <https://threat-modeling.com/vulnerability-intelligence-report-june-4-2026/>
20. OffSeq -- Redis CVE-2026-23479 full public exploit chain released — <https://radar.offseq.com/threat/a-two-year-old-rce-bug-in-redis-was-just-made-publ-b15cdac8>
21. Loginsoft weekly report -- Everest Forms Pro + Mirasvit vulnerabilities weaponised — <https://www.loginsoft.com/reports/weekly/resurfaced-vulnerabilities-weaponized-workflows-and-exposed-operations-define-the-week>
22. Ransomware.live -- South Africa country map (W24) — <https://www.ransomware.live/map/ZA>
23. SANews -- Cabinet approves withdrawal of AI Policy (3 June 2026) — <https://www.sanews.gov.za/south-africa/cabinet-approves-withdrawal-ai-policy>
24. Condia -- SA dissolves PASA; PayInc and SARB co-own (5 June 2026) — <https://thecondia.com/south-africa-dissolves-pasa-payinc-sarb/>
25. SA Legal Academy -- FICA more sections in force soon (1 July 2026) — <https://legalacademy.co.za/news/read/financial-intelligence-centre-act-more-sections-in-force-soon>
26. CryptoNews -- SARB/FSCA joint statement on crypto and stablecoins — <https://cryptonews.net/news/legal/32951895/>
27. ISC2 -- EU CSA2/NIS2 updates proposals (June 2026) — <https://www.isc2.org/insights/2026/06/eu-csa2-nis2-updates-proposals-and-the-isc2-response>
28. Mishcon -- UK DUAA complaints process 19 June 2026 — <https://www.mishcon.com/news/is-your-data-protection-complaints-process-ready-for-19-june-2026>
29. Jurist -- Canada Bill C-8 passed Senate (5 June 2026) — <https://www.jurist.org/news/2026/06/canada-parliament-passes-cybersecurity-bill-amid-privacy-concerns/>
30. CISA KEV Catalog -- Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
31. Ransomware.live -- South Africa country map — <https://www.ransomware.live/map/ZA>
32. CYFIRMA -- Weekly Intelligence Report W24 (Screening Serpens / TA4922) — <https://www.cyfirma.com/news/>
33. Tenable -- Cisco SD-WAN UAT-8616 ongoing exploitation FAQ — <https://www.tenable.com/blog/faq-about-the-continued-exploitation-of-cisco-catalyst-sd-wan-vulnerabilities-uat-8616>
34. ITWeb -- SA cybersecurity statistics 2026 YoY context — <https://www.itweb.co.za/>
35. AGSA -- Parliamentary committee reference to SITA CVE governance gaps (W24) — <https://www.agsa.co.za/>

This report is classified TLP:WHITE. It may be distributed without restriction. Information sourced from publicly available OSINT. No classified or restricted sources were used. Prepared by Digital Progression | dpcyber.co.za | DP-CTI-2026-W24 | Published Monday 8 June 2026