



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 21 | 10 May – 17 May 2026

THREAT LEVEL: HIGH

Canvas/Instructure ransom paid 11 May -- SA tally 108 to 111 (+3 W21 net: SANBS/KillSec UNVERIFIED, Merensky Timber/BlackSuit, Sew Treat/BlackSuit). Cisco SD-WAN CVE-2026-20182 (CVSS 10.0) KEV deadline 17 May (now overdue if unpatched). Exchange OWA CVE-2026-42897 ITW zero-day (14 May, no permanent patch -- EEMS mitigation only). Patch Tuesday 12 May: 120-138 CVEs, ZERO zero-days at release (first clean Patch Tuesday in months). Defender RedSun + UnDefend STILL UNPATCHED.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W21 | Classification: TLP:WHITE

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary**
- 2. Threat Landscape Heatmap**
- 3. SA Cyber Incidents & Breaches**
- 4. Nation-State: APT28 & Glowworm / APT41**
- 5. Active Threat Campaigns**
- 6. Critical Vulnerabilities & CISA KEV**
- 7. Threat Actor Profiles & Ransomware Activity**
- 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 W20) — Week 21 (10–17 May 2026) delivered three new SA ransomware–tracker listings, a CVSS 10.0 KEV deadline (17 May), and an actively exploited Exchange OWA zero-day with no permanent patch. On **11 May**, Canvas/Instructure confirmed that **ShinyHunters' ransom was paid** (est. ~US\$10M), averting the threatened data publication but leaving downstream phishing risk live across 5 SA tertiary institutions. On **12 May**, **SANBS (South African National Blood Service)** appeared on KillSec’s leak portal -- this claim is **UNVERIFIED** and SANBS has not issued a public statement. **Merensky Timber** (13 May) and **Sew Treat** (16 May) were both listed by **BlackSuit**, taking the SA cumulative tally from 108 to **111**. Patch Tuesday 12 May delivered 120–138 CVEs with **zero zero-days at release** -- the first clean Patch Tuesday in months -- but **Defender RedSun + UnDefend remain unpatched** through the cycle. CVE-2026-42897 (Exchange OWA XSS/spoofing) became actively exploited on **14 May** with only an EEMS mitigation available. CVE-2026-20182 (Cisco Catalyst SD-WAN, CVSS 10.0) is KEV-listed with a deadline of **17 May** -- any unpatched estate is now in active-exploitation crosshair.¹

KPI Dashboard

Metric	Current (W21)	Baseline / Prior	Change	Direction
SA threat level	HIGH	HIGH (W20)	Unchanged	FLAT
New SA ransomware.live victims (this week)	3 (SANBS* / KillSec, Merensky Timber / BlackSuit, Sew Treat / BlackSuit)	1 (Standard Bank/PrinzEugen W20)	+3 gross	UP
Cumulative SA ransomware.live victims	111 (*SANBS unverified)	108	+3 net	UP
New CISA KEV entries (W21 scope)	3 (Cisco SD-WAN 10.0, Exchange OWA 8.1, Ivanti EPMM 9.8)	4 (W20)	+3 new	UP
Active SA breach investigations	7 (Canvas resolved, Standard Bank, Polmed, CGCSA, Adumo, FlySafair, SANBS*)	5	+2 new	UP
Patch Tuesday May 2026 zero-days at release	0 (first clean Patch Tuesday in months)	2+ prior cycles	IMPROVED	DOWN
SA-relevant unpatched zero-days	3 (RedSun, UnDefend, Exchange OWA no perm patch)	2 (W20)	+1 (Exchange OWA)	UP
Cisco Catalyst SD-WAN KEV deadline	17 May (CVSS 10.0)	N/A	NEW W21 CRITICAL	UP
Canvas ransom payment / downstream risk	Ransom paid 11 May; data NOT published; phishing risk LIVE	Active deadline W20	RESOLVED (payment) but downstream risk	FLAT
SANBS / KillSec listing	UNVERIFIED -- 12 May; no SANBS statement	N/A	NEW W21 (unverified)	UP
BlackSuit SA double-hit	Merensky Timber (13 May) + Sew Treat (16 May)	N/A	NEW W21	UP

W21 KEY FRAMING: *SANBS UNVERIFIED: The KillSec SANBS listing (12 May) is treated as unverified pending an official SANBS statement. Healthcare-supply-chain criticality (national blood supply) makes this the highest-concern unverified claim of the week. SA tally is stated as 111 with this caveat explicit. The Cisco SD-WAN CVE-2026-20182 (CVSS 10.0, auth bypass/RCE on SD-WAN controller) KEV deadline of 17 May has now passed -- any SA organisation running Cisco Catalyst SD-WAN that has not patched or implemented compensating controls is in active-exploitation crosshair. Exchange OWA CVE-2026-42897 has no permanent patch; the EEMS mitigation must be applied immediately.

TOP 3 ACTIONS THIS WEEK

- 1. PATCH Cisco Catalyst SD-WAN CVE-2026-20182 IMMEDIATELY (KEV deadline 17 May -- CVSS 10.0):** Authentication bypass / RCE on vManage / vBond / vSmart SD-WAN controllers. CVSS 10.0 -- the highest possible score. The KEV deadline of 17 May has now passed; any SA organisation running Cisco Catalyst SD-WAN that has not patched or implemented compensating controls must do so without further delay. Detection: vManage authentication-bypass attempts; unusual config pushes; new admin accounts on SD-WAN controller. MITRE: T1190, T1133.
- 2. APPLY Exchange OWA EEMS mitigation for CVE-2026-42897 (no permanent patch yet -- KEV due 29 May):** Exchange OWA XSS/spoofing zero-day actively exploited since 14 May. Microsoft has published EEMS (Exchange Emergency Mitigation Service) mitigation only -- no permanent patch. Apply EEMS immediately. Detection: anomalous OWA URL patterns; OWA logon-cookie reuse from new IPs; account takeover indicators in Exchange logs. MITRE: T1190, T1078, T1059.007.
- 3. DEPLOY Patch Tuesday May 2026 across Windows estate (Netlogon CVSS 9.8, DNS Client CVSS 9.8, Dynamics 365 CVSS 9.9):** Despite zero ITW zero-days at release, the May 2026 Patch Tuesday carries three critical RCE CVEs that must be prioritised: CVE-2026-41089 (Netlogon RCE, SYSTEM on Domain Controllers), CVE-2026-41096 (DNS Client RCE), CVE-2026-42898 (Dynamics 365 On-Prem RCE). Also patch Ivanti EPMM CVE-2026-1281 (KEV due ~27 May) and FortiAuthenticator CVE-2026-44277 (unauthenticated RCE).

Critical Findings:

- **Canvas/Instructure ransom paid 11 May -- downstream risk LIVE:** ShinyHunters ransom (est. ~US\$10M) paid one day before deadline. "Shred logs" provided but unverifiable. 8,809 institutions covered including 5 SA tertiaries: Wits, Stadio, Milpark, Invictus, SPARK Schools. Data not published, but affiliate-retained copies of .ac.za emails and course data create live phishing risk. FBI PSA 15 May warns of ongoing ShinyHunters extortion campaigns. Polmed data is NOT covered by this settlement.²
- **SANBS / KillSec listing 12 May -- UNVERIFIED, HIGH CONCERN:** South African National Blood Service appeared on KillSec's leak portal on 12 May 2026. No SANBS public statement as of 17 May. Healthcare-supply-chain criticality is extreme (national blood supply). Treat as unverified but warrant-monitor pending confirmation. SA tally stated as 111 includes this entry with explicit caveat.³
- **BlackSuit double-hit SA industrials (Merensky Timber 13 May, Sew Treat 16 May):** Two SA mid-sized industrial companies listed by BlackSuit (Royal/Conti lineage) within 4 days, suggesting a targeted campaign against SA industrial sector. Forestry (Merensky Timber) and textile/apparel (Sew Treat) sectors now in scope.³
- **FlySafair chat-API exposure confirmed POPIA breach (6 May incident, 15 May Pinsent Masons analysis):** Chat API vulnerability exposed customer names, emails, and IPs during 6 May birthday sale. Acknowledged by FlySafair; reported to Information Regulator; customers notified. Pinsent Masons POPIA compliance analysis published 15 May.⁴
- **ANC "Black Ax" leak claim 15 May -- UNVERIFIED:** TikTok-sourced claim of ANC database compromise ~15 May. ITWeb coverage published. Attribution and data authenticity unverified. IR involvement likely if substantiated.⁵
- **Patch Tuesday 12 May -- ZERO ITW zero-days at release (first clean in months):** 120-138 total CVEs, 17-30 critical. First Patch Tuesday in months with no zero-days at release. Microsoft attributed larger volume to AI-driven internal vulnerability discovery. Critical fixes: Netlogon RCE (9.8), DNS Client RCE (9.8), Dynamics 365 On-Prem RCE (9.9). Defender RedSun + UnDefend NOT addressed.⁶
- **Exchange OWA CVE-2026-42897 ITW zero-day 14 May -- no permanent patch:** Exchange OWA XSS/spoofing (CVSS 8.1) disclosed 14 May. Actively exploited in the wild. CISA KEV-listed 15 May (due 29 May). No permanent patch -- EEMS mitigation only. SA Exchange on-premises deployments must apply EEMS immediately.⁶
- **Cisco SD-WAN CVE-2026-20182 CVSS 10.0 -- KEV deadline 17 May (now past):** Authentication bypass/RCE on Cisco Catalyst SD-WAN Controller (vManage / vBond / vSmart). CVSS 10.0. KEV

deadline 17 May 2026 has passed; SA enterprises running unpatched Cisco Catalyst SD-WAN are in active-exploitation crosshair.⁷

W21 KEY INSIGHT: CANVAS RANSOM PAID -- DOWNSTREAM PHISHING RISK WINDOW OPENS

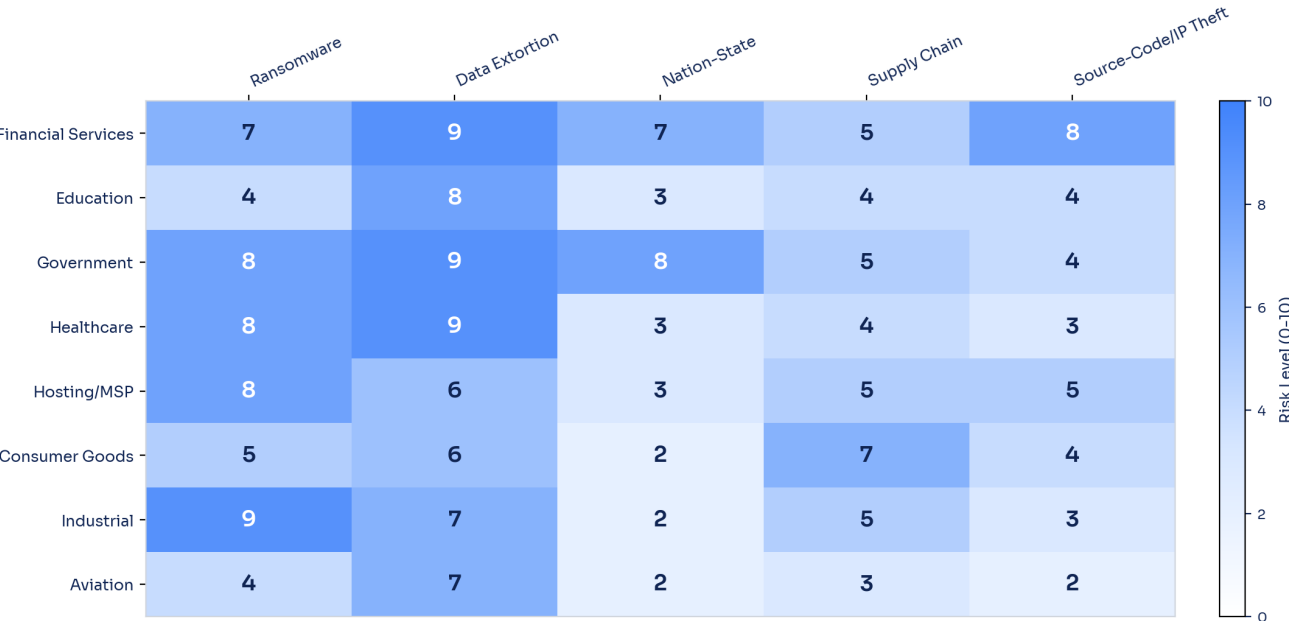
The Canvas/Instructure ransom payment on 11 May 2026 resolves the immediate data-publication threat but opens a multi-week phishing exploitation window. ShinyHunters and their affiliates retain harvested .ac.za email addresses, Canvas course IDs, instructor names, and assignment titles -- exactly the data needed to craft believable academic phishing lures. FBI PSA 15 May confirms ongoing ShinyHunters extortion campaigns globally. SA tertiary security and communications teams at Wits, Stadio, Milpark, Invictus, and SPARK Schools should brief students and staff on Canvas-themed phishing campaigns immediately. Hunt mission TH-2026-W21-01 provides the detection playbook.²

1. Digital Progression — SA CTI Report W21 Compiled Briefing — <https://dpcyber.co.za>
2. FBI IC3 — ShinyHunters PSA 15 May 2026 — <https://www.ic3.gov/>
3. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>
4. Pinsent Masons — FlySafair POPIA compliance analysis (15 May 2026) — <https://www.pinsentmasons.com/>
5. ITWeb — ANC Black Ax leak coverage — <https://www.itweb.co.za/>
6. Microsoft MSRC — May 2026 Security Update Guide — <https://msrc.microsoft.com/update-guide/releaseNote/2026-May>
7. CISA KEV Catalog — CVE-2026-20182 Cisco Catalyst SD-WAN — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

2. THREAT LANDSCAPE HEATMAP

The heatmap below maps eight key South African sectors against five threat categories, rated 0–10 based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 21. **Financial Services** remains elevated (Standard Bank/PrinzEugen ongoing; APT28 SAMA watch). **Healthcare** spikes UP to 8/9 driven by SANBS/KillSec (UNVERIFIED, but healthcare-supply-chain criticality is extreme) and Polmed ongoing. **Industrial** spikes to 9 on Ransomware following BlackSuit's double-hit (Merensky Timber + Sew Treat) within 4 days. **Education** stabilises slightly (Canvas ransom paid) but downstream phishing risk remains. **Hosting/MSP** elevated by cPanel ongoing and FortiAuthenticator CVE-2026-44277. **Aviation** enters the heatmap on Data Extortion (7) driven by the FlySafair chat-API POPIA exposure.

SA THREAT LANDSCAPE HEATMAP | W21 (10 May - 17 May 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 21 (10–17 May 2026) brought three new SA ransomware-tracker listings taking the cumulative tally from 108 to **111** (SANBS unverified). Eight active incident tracks are maintained: INC-2026-W21-01 through -08. Three new DLS listings appeared: SANBS/KillSec (12 May, UNVERIFIED), Merensky Timber/BlackSuit (13 May), and Sew Treat/BlackSuit (16 May). Canvas/Instructure resolved via ransom payment (11 May) but downstream phishing risk is live.³

3.1 INC-2026-W21-01 — Canvas/Instructure / ShinyHunters [RESOLVED via ransom -- downstream risk LIVE]

Organisation	Instructure (Canvas LMS) -- 8,809 institutions globally including 5 SA tertiaries: Wits, Stadio, Milpark, Invictus, SPARK Schools
Sector	Education / EdTech
Threat Actor	ShinyHunters (UNC6240)
Date	Ransom paid 11 May 2026 (one day before deadline); "shred logs" provided
Data	Scope: 3.65 TB, 275M records, 8,809 institutions globally. SA: .ac.za emails, course IDs, instructor names, assignment titles, Canvas API/OAuth data
Ransom	Approximately US\$10M (unconfirmed); paid 11 May
Data Published	NOT published as threatened -- but shred logs are unverifiable
Status	RESOLVED (ransom) -- downstream phishing risk LIVE. Affiliate-retained copies of .ac.za emails and Canvas data persist. FBI PSA 15 May confirms ongoing ShinyHunters campaigns.
SA Significance	Canvas-themed phishing campaigns leveraging harvested .ac.za addresses and course data are expected in coming weeks. Polmed data is NOT covered by this settlement -- ShinyHunters retains that separately.
Sources	FBI IC3 PSA 15 May 2026; BlackFog April 2026 report; ransomware.live

The ransom payment on 11 May 2026 averted the threatened public data release and represents a major operational closure for ShinyHunters. However, the "shred logs" provided as proof of destruction are unverifiable, and cybersecurity experts widely note that affiliate-retained copies of data are standard practice. The specific risk for SA tertiary institutions is targeted academic phishing: ShinyHunters and their affiliates hold .ac.za email addresses, Canvas course structures, instructor names, and assignment data that can be weaponised for convincing credential-harvest campaigns targeting students and staff. Security teams should brief student and staff populations immediately. Polmed data is explicitly NOT part of this settlement -- ShinyHunters retains the 1.7M record / 214 GB Polmed dataset separately.²

3.2 INC-2026-W21-02 — Standard Bank Group / PrinzEugen (ROOTBOY) [ONGOING]

Organisation	Standard Bank Group (JSE: SBK)
Sector	Financial Services / Banking
Threat Actor	PrinzEugen (ROOTBOY operation)
Date	ransomware.live formal listing: 4 May 2026 (ongoing); W21: daily dumps continuing
Data	1.2 TB, 154,333,668 SQL rows claimed: PII, ID documents, credit cards (no CVV), SAP records, SharePoint/OneDrive/Power Apps/Oracle SQL
Demand	1 BTC (~R1.2M) -- refused
Status	CONFIRMED ONGOING -- full 154M-row / 1.2 TB dataset presumed near-complete. No new bank statement, SARB, or IR announcement in W21 window.
SA Significance	Credential-stuffing, SIM-swap, and identity-fraud risk elevated for all SA organisations with Standard Bank workforce relationships. IR enforcement posture maintains public tracker evidence.
Sources	ransomware.live; ITWeb; Standard Bank newsroom

PrinzEugen continues daily dumps into W21 with the 1.2 TB dataset believed to be near-complete. No new official statements from Standard Bank, SARB, or the Information Regulator were identified during the 10–17 May window. The 1 BTC ransom demand continues to be refused. The formal ransomware.live indexing (4 May) remains visible globally and continues to serve as the IR's public-evidence anchor for its fact-finding process.³

3.3 INC-2026-W21-03 — Polmed / ShinyHunters [OPEN -- NOT covered by Canvas ransom]

Organisation	Police Medical Aid Scheme (Polmed)
Sector	Healthcare / Law Enforcement
Threat Actor	ShinyHunters (UNC6240)
Date	Ongoing; W21: no new data release; forensic probe continues
Data	1.7M records, 68,000 active SAPS officers, 214 GB -- undercover designations, PTSD codes, home addresses, command structure roles
Status	CONFIRMED ACTIVE -- R67M emergency response ongoing. CRITICAL: NOT covered by Instructure ransom deal. ShinyHunters retains this data separately.
SA Significance	NATIONAL SECURITY -- undercover officer designations and home addresses create surveillance/targeting risk. Data being monetised in IAB channels.
Sources	ITWeb; Integrity360; allAfrica; Information Regulator

The Polmed breach remains critically open. The Canvas/Instructure ransom payment (11 May) explicitly does NOT cover the Polmed dataset -- ShinyHunters retains the 1.7M record / 214 GB / 68,000 SAPS officer dataset separately and it was not part of the Instructure negotiation. No new data release was identified during the W21 window, but the data continues to circulate in IAB channels. The R67M emergency response and parallel regulatory probes (IR, SAPS, Council for Medical Schemes) remain active.

3.4 INC-2026-W21-04 — CGCSA / Stormous [STALE -- no W21 activity]

Organisation	Consumer Goods Council of South Africa (CGCSA)
Sector	Industry Body / Retail Supply Chain
Threat Actor	Stormous (STMX_GhostLocker partner)
Date	Listed 3 May; 20 GB published W20; no W21 activity
Status	STALE -- 20 GB published in W20; no new W21 data release or CGCSA statement
SA Significance	GS1 South Africa SharePoint, Sage 200 Evolution backups, Unilever/Nestle/L'Oreal partner data remain at risk of further publication.
Sources	HookPhish; RedPacket Security; ransomware.live

3.5 INC-2026-W21-05 — Adumo (Lesaka) [STALE -- no W21 update]

Organisation	Adumo (Lesaka Technologies subsidiary, Nasdaq: LSAK)
Sector	Fintech / Payments Processing
Threat Actor	Unknown dark web forum seller
Date	Surfaced ~17 Apr; W21 no movement
Data	14 GB, 15,546 files: InnerEDGE Docker images, C# POS source, EMV kernel source, PAX firmware
Status	W21 STALE -- dark-web listing from April; no update from Lesaka/Adumo; patient-adversary risk horizon 6-18 months
Sources	Techmoonshot; MEXC/Crypto.news; LaunchBase Africa

3.6 INC-2026-W21-06 — City of Ekurhuleni R2bn Billing Fraud [ONGOING -- W21 media coverage]

Organisation	City of Ekurhuleni (Metropolitan Municipality, Gauteng)
Sector	Government / Municipal
Threat Actor	Unknown (Wi-Fi-based intrusion; suspected insider-assisted)
Date	Intrusion period: 2023-2024; disclosed SCOPA 6 May 2026; W21: post-SCOPA media coverage 10-13 May
Status	ONGOING -- SIU referrals and arrests pre-date W21; no new W21 arrests identified; CIO suspended
SA Significance	Post-SCOPA media coverage continued through 10-13 May. W21 no new arrests or SIU findings; monitoring posture.
Sources	Parliament of South Africa SCOPA hearing 6 May; ITWeb; MyBroadband

3.7 INC-2026-W21-07 — FlySafair Chat API Exposure [NEW, CONFIRMED -- POPIA breach]

Organisation	FlySafair (Safair Operations, low-cost carrier)
Sector	Aviation / Transport
Threat Actor	N/A (vulnerability exposure during high-traffic event)
Date	6 May 2026 (birthday sale high-traffic event); Pinsent Masons POPIA analysis 15 May
Data	Customer names, email addresses, and IP addresses exposed via chat API vulnerability during 6 May birthday sale
Status	CONFIRMED NEW -- acknowledged by FlySafair; reported to Information Regulator; customers notified. POPIA s.22 notification obligations met.
SA Significance	POPIA compliance signal -- rapid notification and IR reporting is the correct response model. Pinsent Masons analysis 15 May highlights API-security obligations under POPIA for aviation-sector operators.
Sources	FlySafair statement; Pinsent Masons (pinsentmasons.com) 15 May 2026; Information Regulator

The FlySafair chat API exposure (6 May 2026) is notable as a compliant breach response: FlySafair acknowledged the incident, notified the Information Regulator, and informed affected customers, all within the POPIA s.22 timeframe requirements. Pinsent Masons published a detailed POPIA compliance analysis on 15 May highlighting the API-security obligations applicable to aviation-sector operators processing customer data. This incident serves as a positive reference model for breach-response compliance.⁴

3.8 INC-2026-W21-08 — ANC "Black Ax" Leak Claim [NEW, UNVERIFIED]

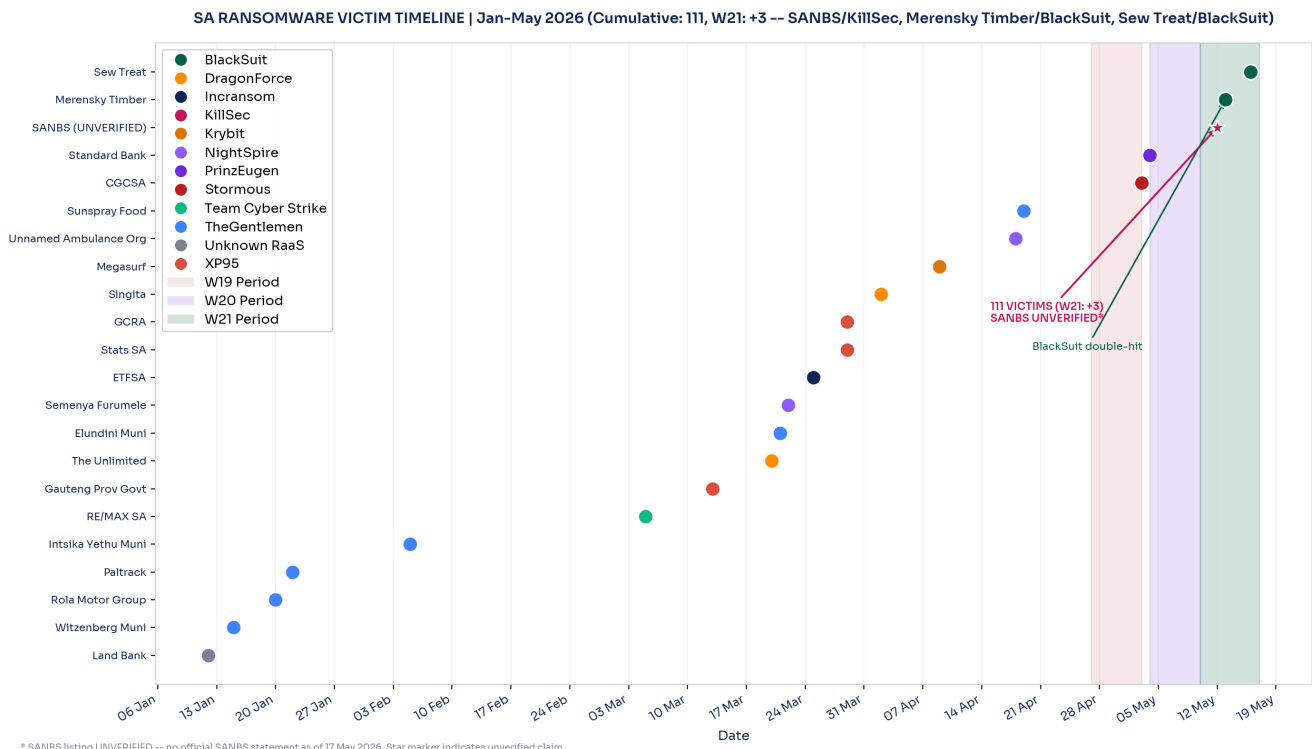
Organisation	African National Congress (ANC)
Sector	Political Party / Government-adjacent
Threat Actor	"Black Ax" (attribution unverified)
Date	Claim surfaced approximately 15 May 2026 via TikTok; ITWeb coverage published
Status	UNVERIFIED -- TikTok-sourced claim. Attribution and data authenticity unverified. No ANC or IR statement.
SA Significance	If substantiated: contains ANC member PII, operational data, political correspondence. IR involvement likely. Political-party data attracts nation-state and hacktivist interest.
Sources	ITWeb (itweb.co.za) -- ANC Black Ax coverage ~15 May 2026

Three New ransomware.live Listings -- W21

Three new SA-affecting DLS listings appeared during the 10–17 May 2026 window, taking the SA cumulative tally from 108 to 111. All are tracked on ransomware.live.

Date	Organisation	Sector	Threat Actor	Status	SA Significance
12 May 2026	SANBS (South African National Blood Service)	Healthcare -- Blood Supply Chain	KillSec	UNVERIFIED -- no SANBS statement	CRITICAL if confirmed: national blood supply logistics, hospital integrations, donor PII
13 May 2026	Merensky Timber	Industrial -- Forestry/Timber	BlackSuit	CONFIRMED (DLS listing)	Part of BlackSuit's W21 SA industrial campaign (2 hits in 4 days)
16 May 2026	Sew Treat	Industrial -- Textile/Apparel	BlackSuit	CONFIRMED (DLS listing)	Part of BlackSuit's W21 SA industrial campaign; second consecutive hit

SA Ransomware Victim Timeline — Jan-May 2026 (Cumulative: 111 -- *SANBS unverified)



Note: SANBS listing is marked with a star (*) indicator to denote UNVERIFIED status. No official SANBS statement has been issued as of 17 May 2026. Tally of 111 includes this entry with explicit caveat.

8. ransomware.live — South Africa Recent Victims (W21 additions) — <https://www.ransomware.live/recentvictims>

9. BlackFog — State of Ransomware (monthly tracking) — <https://www.blackfog.com/>

10. Pinsent Masons — FlySafair POPIA analysis (15 May 2026) — <https://www.pinsentmasons.com/>

4. NATION-STATE: APT28 & GLOWWORM / APT41

W21 nation-state activity is characterised by carry-over campaigns rather than new SA-specific disclosures. **APT28 (Russia GRU)** continues Windows Shell NTLM zero-click campaigns with SAMA banking-sector watch (Fyntralink flag 7 May, no W21 update); the CVE-2026-32202 KEV deadline closed on 12 May. **Glowworm / APT41-linked (China-nexus)** continues compromising African government departments via ToolShell (CVE-2025-53770); no new W21 SA-specific intelligence but carry-over watch remains. **MuddyWater (Iran)** Operation Olalampo MENA is ongoing.¹¹¹²

APT28 — Windows Shell NTLM Campaigns; SAMA Watch

Attribution	APT28 (Fancy Bear) — Russia GRU Unit 26165 / 74455. Also tracked as Sofacy, STRONTIUM, UAC-0001.
SA Status	Fyntralink flagged SAMA bank-sector targeting expansion 7 May; no new W21 SA-specific update. CVE-2026-32202 KEV deadline closed 12 May.
Primary Weapon	CVE-2026-32202 — Windows Shell NTLM zero-click hash theft via LNK/library-ms files. KEV deadline 12 May 2026 (closed). May 2026 Patch Tuesday addresses this.
TTPs	Zero-click NTLM hash capture via malicious .lnk and .library-ms files. Hash relay / Pass-the-Hash for lateral movement. No user interaction required.
Detection	Block outbound SMB (445/139) and WebDAV at perimeter; block .lnk and .library-ms email attachments; Sysmon EID 11 for .lnk files in user-writable paths; outbound NTLM auth to non-corporate IPs.
SA Action	SA banks: verify May 2026 Patch Tuesday deployment. Extend APT28 IOC coverage via threat intel feeds.

Glowworm / APT41-linked — African Government Departments (carry-over)

Attribution	Glowworm (APT41-linked, China-nexus). Also tracked via MSTIC as Storm-0744.
SA Status	Confirmed compromising African government departments via ToolShell (CVE-2025-53770). No new W21 SA-specific intelligence. Carry-over watch posture.
Primary Weapon	ToolShell (CVE-2025-53770) — SharePoint-based web shell deployment.
Tooling	Zingdoor (C2 implant), ShadowPad (modular backdoor), KrustyLoader (staged loader).
TTPs	T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1059 (Command Scripting).
SA Action	SA orgs with African government MOUs / data-share: maintain ToolShell IOC hunt posture. Hunt mission TH-2026-W21-09 (carry-over).

MuddyWater — Operation Olalampo (MENA, ongoing)

MuddyWater (Iran, Ministry of Intelligence) continues Operation Olalampo across MENA. No confirmed SA target in W21; watch-list posture for SA organisations with MENA exposure. TTPs include spear-phishing, LOLBins, and custom C2 infrastructure.¹¹

11. Fyntralink — Threat Intelligence (APT28/MuddyWater/Glowworm) — <https://www.fyntralink.com/>
12. CISA KEV Catalog — CVE-2026-32202 Windows Shell NTLM — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

5. ACTIVE THREAT CAMPAIGNS

5.1 ShinyHunters — Canvas Ransom Paid; Phishing Window Open

ShinyHunters' Canvas/Instructure ransom was paid on 11 May 2026 (est. ~US\$10M), closing the immediate data-publication threat but opening a phishing exploitation window. Affiliate-retained .ac.za emails, Canvas course IDs, and instructor data are expected to fuel targeted academic phishing campaigns in the coming weeks. FBI PSA 15 May 2026 confirms ongoing ShinyHunters global extortion campaigns. Polmed data (1.7M records, 214 GB, 68K SAPS officers) is explicitly NOT covered and remains in ShinyHunters' possession.²⁹

5.2 KillSec — SANBS Listing (UNVERIFIED, Healthcare-Supply-Chain Risk)

KillSec listed SANBS (South African National Blood Service) on its DLS on 12 May 2026. This claim is **UNVERIFIED** as of 17 May -- SANBS has not issued a public statement. KillSec operates a double-extortion playbook typical of lower-tier data-extortion crews. If confirmed, the healthcare-supply-chain implications are severe: SANBS coordinates the national blood supply for SA hospitals. SA security teams and SANBS contacts should monitor the KillSec portal and SANBS-domain credential activity.³⁹

5.3 BlackSuit — SA Industrial Double-Hit (Merensky Timber + Sew Treat)

BlackSuit (Royal/Conti lineage RaaS) listed two SA mid-sized industrial companies within 4 days: **Merensky Timber** (forestry/timber, 13 May) and **Sew Treat** (textile/apparel, 16 May). This double-hit pattern in a compressed timeframe suggests a targeted SA industrial campaign rather than opportunistic selection. BlackSuit uses Cobalt Strike beaoning for C2, RClone/MEGA for exfiltration, and standard RaaS deployment methods. SA industrial-sector organisations should review BlackSuit IOCs and build incident-response plans for RaaS-style attacks.³⁹

5.4 PrinzEugen / ROOTBOY — Standard Bank Daily Dumps Continuing

PrinzEugen continues daily dumps of Standard Bank data into W21. The 1.2 TB / 154M+ row dataset is believed near-complete. The 1 BTC ransom demand remains refused. No new official statements from Standard Bank, SARB, or the Information Regulator were identified. The IR's fact-finding process continues with the public ransomware.live indexing as evidence anchor.³

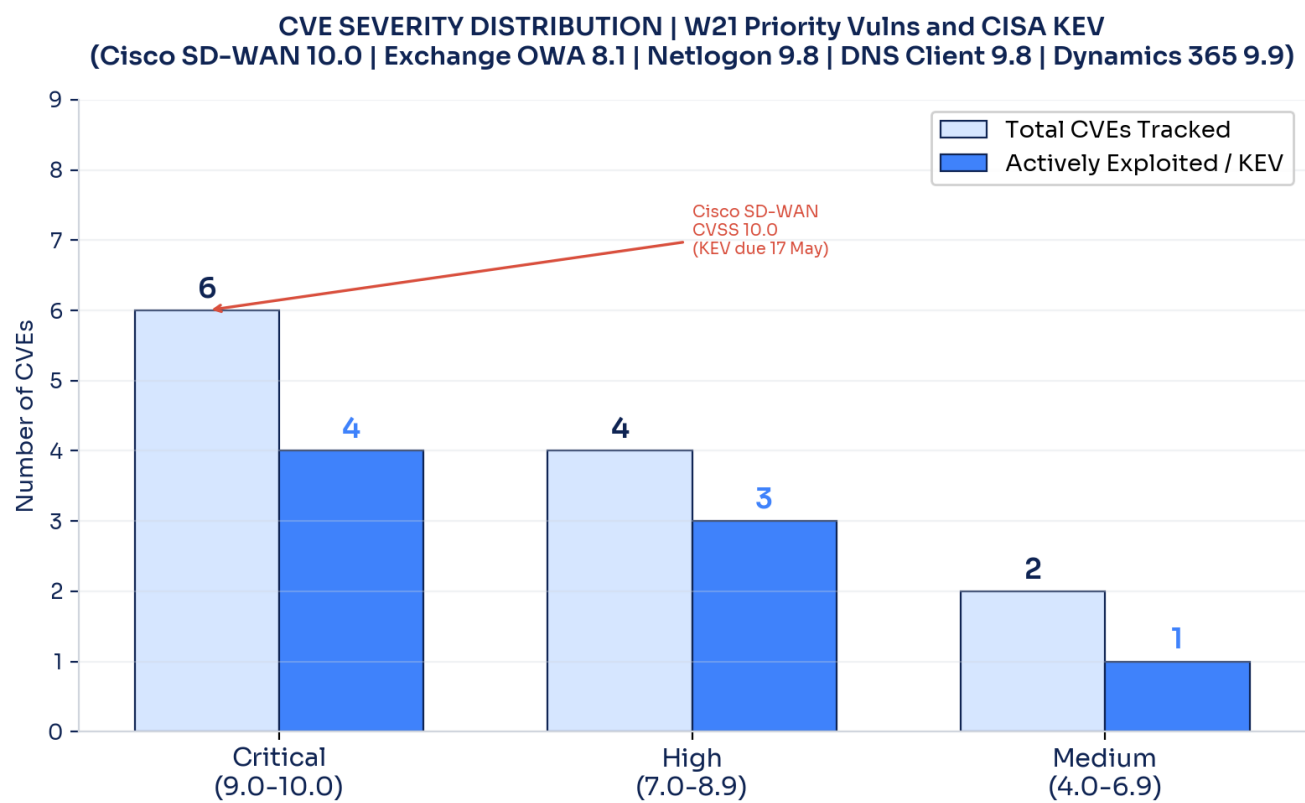
5.5 Storm-1175 — ConnectWise ScreenConnect KEV Deadline Closed 12 May

The CISA KEV deadline for ConnectWise ScreenConnect CVE-2024-1708 closed on 12 May 2026. SA organisations still unpatched after the deadline are in CISA non-compliance and active-exploitation crosshair via Storm-1175 (Medusa ransomware affiliate). No confirmed SA target W21 was identified, but unpatched defenders remain at highest risk.¹²

13. BlackFog — April/May 2026 Ransomware Report — <https://www.blackfog.com/>

14. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>

6. CRITICAL VULNERABILITIES & CISA KEV



Week 21 brought **3 new CISA KEV additions**: Cisco Catalyst SD-WAN CVE-2026-20182 (CVSS 10.0, KEV due 17 May), Microsoft Exchange OWA CVE-2026-42897 (CVSS 8.1, actively exploited zero-day 14 May, KEV due 29 May), and Ivanti EPMM CVE-2026-1281 (CVSS 9.8, re-confirmed, KEV due ~27 May). Patch Tuesday 12 May delivered 120-138 CVEs with **zero ITW zero-days at release** -- a first in recent memory -- including critical RCEs: Netlogon (9.8), DNS Client (9.8), Dynamics 365 On-Prem (9.9). **Microsoft Defender RedSun + UnDefend remain STILL UNPATCHED** through the May cycle -- 7+ weeks unpatched.⁷¹⁵

New CISA KEV Additions — W21 (10-17 May 2026)

CVE ID	Vendor/Product	CVSS	Class	Ransomware?	KEV Deadline
CVE-2026-20182	Cisco Catalyst SD-WAN Controller	10.0	Auth Bypass / RCE	Unknown	17 May 2026
CVE-2026-42897	Microsoft Exchange OWA (XSS/spoofing ITW zero-day)	8.1	XSS / Spoofing (ITW)	Unknown	29 May 2026
CVE-2026-1281	Ivanti EPMM (Pre-auth RCE re-confirmed)	9.8	Pre-auth RCE	Unknown	~27 May 2026

Patch Tuesday May 2026 (12 May) — 120-138 CVEs, Zero Zero-Days at Release

CVE ID	Vendor/Product	CVSS	Class	Ransomware?	KEV Deadline
CVE-2026-41089	Microsoft Netlogon RCE	9.8	RCE (SYSTEM on Domain Controllers)	Unknown	Deploy immediately
CVE-2026-41096	Microsoft DNS Client RCE	9.8	RCE	Unknown	Deploy immediately
CVE-2026-42898	Microsoft Dynamics 365 On-Prem RCE	9.9	RCE	Unknown	Deploy immediately

Patch Tuesday Notes: 120–138 total CVEs (17–30 critical). Microsoft attributed the larger volume to AI-driven internal vulnerability discovery. Zero ITW zero-days at release -- first clean Patch Tuesday in months. Defender RedSun + UnDefend NOT addressed this cycle -- 7+ weeks unpatched.

UNPATCHED ZERO-DAYS — Microsoft Defender RedSun + UnDefend: STILL UNPATCHED (7+ weeks): RedSun abuses Defender cloud rollback to disable signature updates. UnDefend denial-of-services Defender entirely. Both have NO patch available through the May cycle. Detection-only posture required. Hunt for RedSun.exe / UnDefend.exe / FunnyApp.exe in user folders; Qualys QID 92382; alert on Defender service status anomalies and signature update failures. Deploy compensating EDR controls and consider third-party EDR overlay.

Top Priority CVE Details — W21

CVE-2026-20182 — Cisco Catalyst SD-WAN Controller — CVSS 10.0 — P1 PATCH NOW (KEV deadline 17 May, now past)

Authentication bypass / Remote Code Execution on Cisco Catalyst SD-WAN Controller (vManage / vBond / vSmart). CVSS 10.0 -- the maximum possible severity score. The KEV deadline of 17 May has passed; any SA organisation running Cisco Catalyst SD-WAN that has not yet patched or implemented compensating controls must do so without further delay. Detection: vManage / vBond / vSmart authentication-bypass attempts; unusual config pushes from unexpected sources; new admin accounts on SD-WAN controller; anomalous traffic patterns on SD-WAN management plane. MITRE: T1190, T1133. Hunt mission TH-2026-W21-03.⁷

CVE-2026-42897 — Microsoft Exchange OWA — CVSS 8.1 — P1 APPLY EEMS NOW (no permanent patch; KEV 29 May)

XSS / Spoofing zero-day in Microsoft Exchange OWA, actively exploited in the wild since 14 May 2026. CISA KEV-listed 15 May (due 29 May). **No permanent patch available** -- Microsoft has published an EEMS (Exchange Emergency Mitigation Service) mitigation only. SA organisations running Exchange on-premises must apply the EEMS mitigation immediately. Detection: anomalous OWA URL patterns containing script payloads; unexpected OWA logon-cookie reuse from new IPs; account takeover indicators in Exchange logs; Exchange IIS logs showing anomalous GET/POST to OWA paths. MITRE: T1190, T1078, T1059.007. Hunt mission TH-2026-W21-02.¹⁵

CVE-2026-1281 — Ivanti EPMM Pre-Auth RCE — CVSS 9.8 — P1 PATCH (KEV ~27 May)

Pre-authentication Remote Code Execution in Ivanti Endpoint Manager Mobile (EPMM). CVSS 9.8. KEV deadline approximately 27 May 2026. SA enterprises managing mobile devices via Ivanti EPMM must patch by ~27 May. This is a re-confirmation of a known vulnerability class in Ivanti EPMM (consistent with CVE-2026-6973 KEV from W20). Patch immediately; restrict EPMM admin interface to VPN/OOB.⁷

CVE-2026-41089 — Microsoft Netlogon RCE — CVSS 9.8 — P1 (Patch Tuesday May 2026)

Remote Code Execution on Domain Controllers via Netlogon. CVSS 9.8, SYSTEM privilege on DCs. Patch via Patch Tuesday May 2026. Detection: anomalous Netlogon authentication patterns; unexpected schema/replication activity; Domain Admin account creations without change management tickets. MITRE: T1210, T1078.002. Hunt mission TH-2026-W21-04.¹⁵

CVE-2026-41940 — cPanel — SA HOSTING-PROVIDER ESPIONAGE TARGETING (IOCs active)

Ctrl-Alt-Intel confirmed 2 May that an unattributed espionage actor (not pure ransomware) interactively targeted SA MSPs and hosting providers. IOCs: **.sorry extension files** on hosted volumes; root password reset to **123Qwe123C**; session files containing **hasroot=1** in `/var/cpanel/sessions/raw/`. Any unpatched cPanel/WHM since February 2026 should be assumed potentially compromised. Espionage TTPs -- not just ransomware deployment. Hunt mission TH-2026-W21-07.¹⁶

CVE-2026-44277 — FortiAuthenticator Unauthenticated RCE — CRITICAL

Unauthenticated Remote Code Execution in FortiAuthenticator -- the dominant MFA/authentication stack for SA enterprise. CVSS critical. Patch immediately. Detection: unexpected FortiAuth admin sessions; new admin accounts created; config drift; bypass attempts to /api/v2/* endpoints. MITRE: T1190, T1556. Hunt mission TH-2026-W21-06.¹⁷

RedSun + UnDefend — MS Defender — STILL UNPATCHED — PI DETECTION ONLY (7+ weeks)

Two of the W17 Microsoft Defender zero-day trio remain unpatched 7+ weeks on through the May Patch Tuesday cycle. **RedSun** abuses Defender's cloud rollback mechanism to silently disable signature updates. **UnDefend** achieves a full denial-of-service against the Defender service. No patch available. Deploy compensating EDR rules; consider third-party EDR overlay. Hunt for RedSun.exe, UnDefend.exe, FunnyApp.exe in user-writable directories. Use Qualys QID 92382. Alert on mpcmdrun.exe -SignatureUpdate failures.¹⁵

Carry-Over KEV Deadlines Closed During W21

- **PAN-OS CVE-2026-0300 (9 May):** Captive Portal RCE -- deadline closed. Anyone unpatched = in CISA non-compliance.
- **Ivanti EPMM CVE-2026-6973 (10 May):** Auth Bypass -- deadline closed.
- **LiteLLM CVE-2026-42208 (11 May):** RCE in BerriAI LiteLLM -- deadline closed.
- **ConnectWise ScreenConnect CVE-2024-1708 (12 May):** Path traversal RCE -- deadline closed. Storm-1175/Medusa exploitation ongoing.
- **Windows Shell NTLM CVE-2026-32202 (12 May):** APT28 NTLM zero-click -- deadline closed. May 2026 Patch Tuesday addresses.
- **Linux Kernel CVE-2026-31431 (15 May):** LPE "Copy Fail" -- deadline closed.

15. Microsoft MSRC — May 2026 Security Update Guide — <https://msrc.microsoft.com/update-guide/releaseNote/2026-May>

16. Ctrl-Alt-Intel — cPanel SA wave (2 May 2026) — <https://ctrl-alt-intel.com/>

17. Fortinet PSIRT — FortiAuthenticator CVE-2026-44277 — <https://www.fortiguard.com/psirt>

7. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

SA Ransomware Victim Count: 111 as of end W21 (108 to 111, +3 net, SANBS unverified). Three new SA ransomware.live listings in W21: SANBS/KillSec (UNVERIFIED), Merensky Timber/BlackSuit, and Sew Treat/BlackSuit. The global landscape continues at the elevated 150–200 victims/week tempo. BlackSuit's double-hit in the SA industrial sector (2 in 4 days) is the defining W21 ransomware story.¹³¹⁴

Active SA-Relevant Threat Actor Summary — W21

Actor	Type	SA Victims/Status	W21 Activity	Primary TTPs
ShinyHunters	Data Extortion / EaaS	Canvas RESOLVED (ransom paid 11 May); Polmed ongoing (NOT covered)	Downstream phishing risk LIVE; FBI PSA 15 May; global campaigns continuing	Vishing to Okta FastPass; SaaS pivoting; T1528
KillSec	Data Extortion / double-extortion	SANBS (12 May, UNVERIFIED)	UNVERIFIED listing -- healthcare-supply-chain concern; no SANBS statement	Double-extortion DLS; lower-tier crew TTPs
BlackSuit	RaaS (Royal/Conti lineage)	Merensky Timber (13 May) + Sew Treat (16 May)	ACTIVE -- SA industrial double-hit; targeted campaign suspected	Cobalt Strike C2; RClone/MEGA exfil; T1486
PrinzEugen / ROOTBOY	Data Extortion (single operator)	Standard Bank (ongoing)	ACTIVE -- 154M rows / 1.2TB; daily dumps; ransom refused	SharePoint/OneDrive/Power Apps/Oracle SQL movement
Stormous	Extortion / hacktivist-hybrid	CGCSA (W19, stale W21)	STALE -- no W21 new activity; CGCSA 20 GB published W20	CRM/SharePoint/Sage 200 access
Storm-1175	Criminal (RaaS affiliate)	No confirmed SA target W21	KEV deadline closed 12 May -- unpatched SA orgs at risk	ConnectWise RMM abuse; Medusa ransomware deployment
APT28	Nation-State (Russia GRU)	SAMA financial-sector watch (7 May flag)	ONGOING -- CVE-2026-32202 KEV deadline closed 12 May; campaign continues	LNK/library-ms NTLM hash theft; Pass-the-Hash
Glowworm / APT41	Nation-State (China-nexus)	African govt depts (SA partners at risk)	ONGOING -- ToolShell CVE-2025-53770; Zingdoor/ShadowPad	Web shell; SharePoint exploitation; T1505.003
MuddyWater	Nation-State (Iran)	No confirmed SA target W21	ONGOING -- Operation Olalampo MENA	Spear-phish; LOLBins; custom C2
Unknown (cPanel espionage)	Espionage actor	SA MSPs / hosting providers (confirmed targeted)	ACTIVE -- espionage TTPs; IOCs: .sorry files, hasroot=1 sessions	cPanel CVE-2026-41940; interactive espionage TTPs
IAB market	Initial Access Broker	SA credential market still flooded	ELEVATED -- watch BreachForums replacements / XSS.ac / RAMP	R100/set credentials; SA server access listings

ShinyHunters — CANVAS RESOLVED (ransom paid); Polmed OPEN; phishing LIVE

The Canvas/Instructure ransom payment (11 May, est. ~US\$10M) closes the most acute SA threat of W20–W21. However, ShinyHunters retains two critical SA datasets: (1) .ac.za email/course data for phishing exploitation, and (2) the Polmed 1.7M record / 214 GB / 68K SAPS officer dataset (explicitly NOT covered by the Instructure deal). FBI PSA 15 May 2026 confirms ongoing ShinyHunters global extortion campaigns. Hunt mission TH-2026-W21-01 covers Canvas phishing detection.²

KillSec — SANBS LISTING UNVERIFIED (12 May)

KillSec listed SANBS on 12 May 2026 with no response from SANBS as of 17 May. KillSec is a lower-tier data-extortion group with a standard double-extortion playbook. If the SANBS listing is genuine, the healthcare-supply-chain implications are severe: SANBS coordinates the national blood supply. SA security teams and healthcare sector contacts should monitor the KillSec portal and SANBS-domain credential sightings on IAB markets. Hunt mission TH-2026-W21-08.³

BlackSuit — SA INDUSTRIAL DOUBLE-HIT (Merensky Timber + Sew Treat)

BlackSuit (Royal/Conti lineage RaaS) listed two SA industrial companies -- Merensky Timber (forestry, 13 May) and Sew Treat (textile/apparel, 16 May) -- within 4 days. This concentrated tempo suggests a targeted SA industrial campaign. BlackSuit uses Cobalt Strike beaconing, RClone/MEGA exfiltration, and standard double-extortion playbook. SA mid-sized industrials should review BlackSuit IOCs (T1486 ransomware behaviour, Cobalt Strike C2 patterns). Hunt mission TH-2026-W21-09.³

PrinzEugen / ROOTBOY — STANDARD BANK DAILY DUMPS ONGOING

PrinzEugen continues daily dumps of Standard Bank data into W21. 154M rows, 1.2 TB. No new victims identified. No official Standard Bank, SARB, or IR statements in W21 window. The ransom (1 BTC) remains refused. The IR's fact-finding maintains the public ransomware.live indexing as evidence anchor. SA organisations with Standard Bank workforce relationships face elevated credential-stuffing risk.³

APT28 — NTLM CAMPAIGNS ONGOING; SAMA WATCH

APT28 continues Windows Shell NTLM zero-click campaigns. The CVE-2026-32202 KEV deadline closed 12 May -- SA banks should have applied May 2026 Patch Tuesday. No new W21 SA-specific attribution. SAMA banking-sector watch posture maintained. SA banks: verify May Patch Tuesday deployment; extend APT28 IOC coverage.¹¹

Unknown espionage actor — cPanel SA HOSTING-PROVIDER TARGETING (ONGOING)

The interactive espionage targeting of SA MSPs and hosting providers via cPanel CVE-2026-41940 (Ctrl-Alt-Intel 2 May) continues. This is espionage-focused, not pure ransomware. IOCs: .sorry extension files; root password 123Qwe123C; hasroot=1 session files in /var/cpanel/sessions/raw/. Any SA cPanel/WHM instance unpatched since February 2026 should be assumed potentially compromised. Hunt mission TH-2026-W21-07.¹⁶

IAB Market — SA CREDENTIAL MARKET STILL FLOODED

The SA IAB market remains highly active. Credentials available at R100/set. SANBS domain credential sightings should be monitored on IAB markets if the KillSec listing proves genuine. Watch BreachForums replacements / XSS.ac / RAMP for fresh SA-listing turnover. Polmed data continues to circulate.

Q1 2026 Global Ransomware Landscape (Context)

Metric	Value
Q1 2026 victims (GuidePoint / ZeroFox)	2,622 / 2,059
Weekly tempo	150-200 (the new normal)
March 2026 monthly	808 victims, 65 active groups
US share of victims	51%
Africa share	Under 5%
Top 3 by Q1 victims	Qilin (361), Akira (197), TheGentlemen (192)
Most active April 2026 (BlackFog)	ShinyHunters (15 incidents)
W21 SA new victims	3 (SANBS/KillSec UNVERIFIED, Merensky Timber/BlackSuit, Sew Treat/BlackSuit)

18. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>

19. BlackFog — April 2026 State of Ransomware — <https://www.blackfog.com/>

8. OSINT EXPOSURE & ATTACK SURFACE

Canvas/Instructure ransom paid 11 May -- 5 SA tertiaries; phishing risk LIVE

ShinyHunters' Canvas/Instructure ransom paid 11 May. "Shred logs" unverifiable. Downstream phishing risk is live across Wits, Stadio, Milpark, Invictus, SPARK Schools. SA tertiary security teams: rotate Canvas API tokens, tag external mail referencing Canvas course data, brief student/staff comms teams. Hunt mission TH-2026-W21-01.²

SANBS / KillSec listing 12 May -- UNVERIFIED, healthcare-supply-chain concern

South African National Blood Service appeared on KillSec's DLS 12 May. No SANBS statement as of 17 May. SANBS-domain credential sightings on IAB markets should be monitored. Healthcare sector contacts should reach out to SANBS security team. Hunt mission TH-2026-W21-08.³

BlackSuit double-hit: Merensky Timber (13 May) + Sew Treat (16 May)

Two SA mid-sized industrials listed by BlackSuit within 4 days. Targeted SA industrial campaign suspected. SA industrial-sector organisations: review BlackSuit IOCs (Cobalt Strike beacon, RClone/MEGA exfil patterns); build RaaS incident-response plan. Hunt mission TH-2026-W21-09.³

FlySafair chat-API POPIA exposure (6 May incident, 15 May Pinsent Masons analysis)

FlySafair acknowledged chat-API exposure of customer names, emails, IPs (6 May birthday sale). Reported to Information Regulator; customers notified. Pinsent Masons POPIA analysis 15 May highlights API security obligations for aviation-sector data processors. Positive compliance model for breach-response.⁴

ANC "Black Ax" leak claim 15 May -- UNVERIFIED

TikTok-sourced claim of ANC database compromise ~15 May. ITWeb coverage published. Attribution and data authenticity unverified. If substantiated: IR involvement likely; nation-state and hacktivist interest probable.⁵

Patch Tuesday 12 May -- zero ITW zero-days; Netlogon + DNS Client + Dynamics 365 critical RCEs

First clean Patch Tuesday in months. Critical RCEs that must be prioritised: Netlogon (9.8), DNS Client (9.8), Dynamics 365 On-Prem (9.9). Defender RedSun + UnDefend NOT addressed (7+ weeks unpatched). Deploy May 2026 Patch Tuesday across entire Windows estate this week.¹⁵

Exchange OWA CVE-2026-42897 ITW zero-day 14 May -- no permanent patch

Exchange OWA zero-day (XSS/spoofing, CVSS 8.1) actively exploited since 14 May. CISA KEV due 29 May. Apply EEMS mitigation immediately. No permanent patch available. Monitor Exchange IIS logs and OWA session anomalies. Hunt mission TH-2026-W21-02.¹⁵

Cisco SD-WAN CVE-2026-20182 CVSS 10.0 -- KEV deadline 17 May (past)

CVSS 10.0 auth bypass/RCE on Cisco Catalyst SD-WAN Controller. KEV deadline 17 May 2026 has now passed. Any SA organisation running unpatched Cisco SD-WAN is in active-exploitation crosshair. Patch or implement compensating controls immediately. Hunt mission TH-2026-W21-03.⁷

20. Surfshark — Q1 2026 SA data breach research — <https://surfshark.com/research/>

21. ITWeb — ANC Black Ax coverage (15 May 2026) — <https://www.itweb.co.za/>

9. REGULATORY & COMPLIANCE

Information Regulator — APP Portfolio Committee (5 May); Health Data Regs Gap (12 May)

IR APP Portfolio Committee 5 May (W21 detail): The Information Regulator presented its 2025/26 Annual Performance Plan to Parliament's Portfolio Committee. **2,898 breach notifications in 2025/26** (+40% year-on-year). PAIA compliance across public bodies only 33%. Gated-access Code of Conduct and cross-border Guidance Note both on track. Faster enforcement signals noted. IR is litigating 4 enforcement matters in parallel. This data underpins the imperative for SA organisations to maintain robust breach-notification readiness.^{22,23}

POPIA Health Data Regulations -- compliance gap (12 May reporting): Legal press reported 12 May that employers are widely non-compliant with the POPIA Health Data Processing Regulations. **No grace period applies.** Immediate enforcement risk. Any SA employer processing employee health data must conduct an immediate compliance review. SANBS listing (UNVERIFIED) elevates this further if confirmed.²²

Surfshark Q1 2026 SA Data: 70 in 100 South Africans breach-affected; credentials at R100/set; SA ranked 42nd globally, 2nd in Africa. These figures contextualise the credential-exposure baseline that attackers are exploiting via IAB markets.²⁰

Protected Disclosures Bill — 14 May civil society comment deadline: Civil society requested extension for the Protected Disclosures Bill. Direct relevance to whistleblower/cybercrime reporting in SA. No decision announced in W21 window.

SA Draft AI Policy — comment open to 10 June 2026: New gazette (replacing the withdrawn 2025 policy) proposes 7 AI governance bodies with POPIA as cornerstone. Comments open to 10 June 2026. SA organisations deploying AI systems should engage with this policy process.²⁴

ANC "Black Ax" breach claim (15 May): Unverified claim of ANC database compromise. IR involvement likely if substantiated. See Section 3.8.

Global Regulatory with SA Impact

EU AI Act Omnibus agreed 7 May 2026: High-risk Annex III deadline moved to **2 December 2027** (from 2 August 2026); watermarking enforcement moved to **2 December 2026**. SA AI/tech exporters to the EU gain additional runway for high-risk system compliance but watermarking remains on near-term horizon.²⁵

NIS2 first audit deadline 30 June 2026 (no extension): Fixed for pre-2025 in-scope entities. SA organisations with EU operations should complete NIS2 gap assessments immediately -- 6 weeks remaining.²⁶

UK Cyber Security Bill progressing: Higher penalties than NIS2; MSPs added as a new regulated category. SA MSPs with UK clients should track progress.²⁶

Verizon DBIR 2026 Webinar 19 May (17:00 SAST): Generative AI-augmented attacks and credential theft themes. SOC teams should register. Key SA data: credentials R100/set on dark web; 90% of SA breaches with identity weakness.²⁷

Compliance Deadlines Table — W21 (Next 8 Weeks)

Deadline	Item	Jurisdiction
17 May 2026 (now past)	KEV: Cisco Catalyst SD-WAN CVE-2026-20182 (CVSS 10.0)	US federal (advisory globally)
19 May 2026	Verizon DBIR 2026 SA Webinar (17:00 SAST)	SA
27 May 2026	KEV: Ivanti EPMM CVE-2026-1281 (~27 May)	US federal (advisory globally)
29 May 2026	KEV: Exchange OWA CVE-2026-42897 (EEMS mitigation only)	US federal (advisory globally)
10 June 2026	SA Draft AI Policy comment deadline	SA
30 June 2026	NIS2 first audit deadline (no extension)	EU (SA orgs in scope)
~July 2026	NCC registration opens (CPA Amendment Regs)	SA
2 December 2026	EU AI Act watermarking enforcement	EU (SA orgs in scope)
2 December 2027	EU AI Act high-risk Annex III enforcement (extended)	EU (SA orgs in scope)

22. Information Regulator South Africa — Media Statements — <https://infoeregulator.org.za/media-statements/>

23. Werksmans — IR APP 2025/26 Portfolio Committee coverage — <https://www.werksmans.com/>

24. DCDT — SA Draft AI Policy (open to 10 June 2026) — <https://www.gov.za/>

25. European Commission — EU AI Act Omnibus (7 May 2026) — <https://ec.europa.eu/>

26. D3 Security — NIS2 SOC Audit Readiness 2026 — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>

27. Verizon DBIR 2026 — Data Breach Investigations Report — <https://www.verizon.com/business/resources/reports/dbir/>

10. WEEKLY THREAT HUNT & IOCs

Nine hunt missions are active for W21: 4 P1 missions (Canvas phishing readiness, Exchange OWA zero-day, Cisco SD-WAN CVSS 10.0, Netlogon DC RCE) address the most acute exploitation risks. 4 P2 missions (DNS Client + Dynamics 365 RCE chain, FortiAuthenticator unauthenticated RCE, cPanel IOC hunt, SANBS/KillSec verification) address high-severity but less immediately time-critical vectors. 1 P3 mission (BlackSuit SA industrial watch) provides ongoing monitoring.

TH-2026-W21-01 — Canvas/Instructure Phishing-Readiness for SA Tertiaries

P1 — CRITICAL: Phishing window opened by ransom payment

Hypothesis: Ransom paid 11 May but affiliate-retained .ac.za email addresses and Canvas course data (Wits, Stadio, Milpark, Invictus, SPARK) remain exploitable for targeted academic phishing. Canvas-themed credential-harvest campaigns are expected in the coming weeks.

MITRE ATT&CK: T1566 (Phishing), T1078.004 (Cloud Accounts), T1528 (Steal Application Access Token).

IOCs: Inbound emails to .ac.za domains referencing Canvas course IDs / instructor names / assignment titles; lookalike domains (canvas-*, instructure-*); credential-harvest pages mimicking Canvas SSO.

Data Sources: Email security gateway (MTA logs, attachment hashes), DNS sinkholing for Canvas lookalike domains, Canvas audit log, OAuth token grant log, SIEM correlation.

Detection Guidance: Rotate Canvas API tokens for Wits, Stadio, Milpark, Invictus, SPARK. Tag external mail referencing Canvas. Brief student/staff comms teams on Canvas-themed phishing. Hunt for anomalous Canvas OAuth token grants and /api/v1/users/* access.

TH-2026-W21-02 — Exchange OWA CVE-2026-42897 ITW Exploitation**P1 — CRITICAL: ITW**
zero-day; no permanent patch

Hypothesis: Exchange OWA XSS/spoofing zero-day actively exploited in the wild since 14 May. No permanent patch. EEMS mitigation is the only defence. Organisations that have not applied EEMS are actively exposed.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1059.007 (JavaScript).

IOCs: Anomalous OWA URL patterns containing script payloads; unexpected OWA logon-cookie reuse from new IPs; account takeover indicators in Exchange logs.

Data Sources: Exchange IIS logs (OWA paths), Exchange audit log, SIEM correlation, IdP/Azure AD sign-in logs for Exchange-authenticated sessions.

Detection Guidance: Apply EEMS mitigation immediately. Monitor Exchange IIS logs for anomalous OWA GET/POST patterns. Alert on OWA logon-cookie reuse from new geolocations. Review account takeover indicators (new forwarding rules, new delegates, anomalous mailbox access).

TH-2026-W21-03 — Cisco Catalyst SD-WAN CVE-2026-20182 (CVSS 10.0)**P1 — CRITICAL: CVSS 10.0;**
KEV deadline 17 May (past)

Hypothesis: CVSS 10.0 auth bypass/RCE on Cisco Catalyst SD-WAN controllers (vManage / vBond / vSmart). KEV deadline 17 May has now passed. Any unpatched SA SD-WAN deployment is in active-exploitation crosshair.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1133 (External Remote Services).

IOCs: vManage / vBond / vSmart authentication-bypass attempts from external IPs; unusual config pushes; new admin accounts created on SD-WAN controller; SD-WAN version below patched release.

Data Sources: Cisco SD-WAN vManage audit logs, SD-WAN controller NetFlow, SIEM, perimeter firewall logs for SD-WAN management ports.

Detection Guidance: Patch Cisco SD-WAN immediately. Restrict vManage admin interface to OOB/management-only access. Audit all admin accounts created in last 7 days. Review SD-WAN config for unexpected changes.

TH-2026-W21-04 — Netlogon CVE-2026-41089 RCE on Domain Controllers**P1 — CRITICAL: CVSS 9.8**
SYSTEM on DCs

Hypothesis: Netlogon RCE (CVSS 9.8) via Patch Tuesday 12 May. SYSTEM privilege on Domain Controllers. Unpatched DCs are the highest-value target for ransomware operators seeking to encrypt the domain.

MITRE ATT&CK: T1210 (Exploitation of Remote Services), T1078.002 (Domain Accounts).

IOCs: Anomalous Netlogon authentication traffic; unexpected replication activity; Domain Admin account creations without change management records.

Data Sources: Windows Security log (EID 4624/4625/4768/4769), Netlogon debug logs, Active Directory replication logs, SIEM domain controller baseline.

Detection Guidance: Apply May 2026 Patch Tuesday to all Domain Controllers immediately. Alert on anomalous Netlogon authentication from non-DC sources. Monitor Domain Admin group membership changes.

TH-2026-W21-05 — DNS Client CVE-2026-41096 + Dynamics 365 CVE-2026-42898**P2 — HIGH: Critical RCE**
chain potential

Hypothesis: DNS Client RCE (9.8) and Dynamics 365 On-Prem RCE (9.9) from May 2026 Patch Tuesday. RCE chain potential if combined with lateral movement. SA Dynamics 365 On-Prem deployments are highest risk.

MITRE ATT&CK: T1210 (Exploitation of Remote Services), T1190 (Exploit Public-Facing App).

IOCs: Malformed DNS responses from non-corporate resolvers; unusual outbound resolver behaviour; Dynamics 365 on-prem unexpected POSTs to /api/data/* endpoints.

Data Sources: DNS query logs, DNS resolver logs, Dynamics 365 IIS logs, SIEM.

Detection Guidance: Apply May 2026 Patch Tuesday. Restrict Dynamics 365 On-Prem to internal/VPN access. Monitor DNS resolver anomalies. Alert on unexpected Dynamics 365 API calls.

TH-2026-W21-06 — FortiAuthenticator CVE-2026-44277 Unauthenticated RCE

**P2 — HIGH: Dominant SA
MFA stack; unauthenticated
RCE**

Hypothesis: Unauthenticated RCE on FortiAuthenticator -- the dominant MFA stack in SA enterprise. Compromise of FortiAuth gives attacker control over authentication bypass for all FortiGate-integrated systems.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1556 (Modify Authentication Process).

IOCs: Unexpected FortiAuth admin sessions from non-management IPs; new admin accounts created; FortiAuth config drift; bypass attempts to /api/v2/* endpoints.

Data Sources: FortiAuth admin audit log, FortiAuth API access log, syslog from FortiAuth, perimeter NetFlow to FortiAuth management ports.

Detection Guidance: Patch FortiAuthenticator immediately. Restrict FortiAuth admin interface to OOB/management VLAN. Audit all admin accounts created in last 30 days. Review API access logs for /api/v2/* anomalies.

TH-2026-W21-07 — cPanel CVE-2026-41940 IOC Hunt (SA Hosting/MSP)

**P2 — HIGH: SA-specific
confirmed espionage
targeting**

Hypothesis: Espionage actor interactively targeted SA MSPs/hosting providers via cPanel CVE-2026-41940. Any unpatched cPanel/WHM since February 2026 may be compromised. Specific IOC set: .sorry extension files, root password 123Qwe123C, hasroot=1 session files.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1098 (Account Manipulation), T1505.003 (Web Shell).

IOCs: .sorry extension files on hosted volumes; root password reset to 123Qwe123C; session files with hasroot=1 in /var/cpanel/sessions/raw/; cpsrvd/whostmgrd anomalous child processes.

Data Sources: cPanel audit log (/var/cpanel/logs/), SSH auth log, /var/cpanel/sessions/raw/ review, shared-hosting volume file scan, cPanel API token audit.

Detection Guidance: Patch cPanel. Scan /var/cpanel/sessions/raw/ for hasroot=1 entries. Check root password against 123Qwe123C hash. Scan hosted volumes for .sorry extension. Audit new cPanel API tokens and SSH keys added after February 2026.

TH-2026-W21-08 — SANBS / KillSec Data-Exposure Verification

**P2 — HIGH: Healthcare
supply chain; UNVERIFIED
but critical**

Hypothesis: If SANBS listing is genuine, expect downstream impact on blood-supply logistics, hospital integrations, and donor PII. Early verification and containment is critical given healthcare-supply-chain implications.

MITRE ATT&CK: T1567 (Exfiltration Over Web Service), T1078 (Valid Accounts).

IOCs: KillSec leak portal SANBS entries; SANBS-domain credential sightings on IAB markets (XSS.ac, BreachForums replacements, RAMP); lookalike-domain registrations mimicking SANBS.

Data Sources: Open-source monitoring of KillSec leak portal, dark-web monitoring feeds (SANBS domain), domain registrar alerts for sanbs-* lookalikes, SANBS IT security team contact.

Detection Guidance: Monitor KillSec portal for SANBS data publication. Check dark-web intelligence feeds for SANBS credential sightings. Contact SANBS security team directly if engaged. Alert on lookalike-domain registrations.

TH-2026-W21-09 — BlackSuit SA Industrial-Sector Watch

P3 — MONITOR: Targeted SA industrial campaign pattern

Hypothesis: Two SA mid-sized industrials listed by BlackSuit in 4 days (Merensky Timber, Sew Treat) suggests a targeted SA industrial campaign. Cobalt Strike beaconing and RClone/MEGA exfiltration are BlackSuit’s standard TTPs.

MITRE ATT&CK: T1486 (Data Encrypted for Impact), T1567.002 (Exfiltration to Cloud Storage), T1059.001 (PowerShell).

IOCs: BlackSuit IOCs: Cobalt Strike C2 beaconing patterns; RClone exfiltration to MEGA/cloud storage; T1486 ransomware behaviour on file servers; encryption of backup infrastructure.

Data Sources: EDR (Cobalt Strike beacon detection), perimeter NetFlow (MEGA/cloud exfil patterns), SIEM for ransomware behaviour signatures, backup system integrity monitoring.

Detection Guidance: Distribute BlackSuit IOC signatures to EDR. Alert on RClone to MEGA from corporate endpoints. Monitor backup infrastructure for encryption. Build BlackSuit-specific incident-response playbook for SA industrial sector.

Hunt Mission Summary Checklist — W21

Hunt ID	Hypothesis (Short)	Priority	Key Data Sources	Status
TH-2026-W21-01	Canvas phishing-readiness for SA tertiaries	P1 — CRITICAL	Email gw, Canvas audit, OAuth logs	Not Started
TH-2026-W21-02	Exchange OWA CVE-2026-42897 (ITW zero-day)	P1 — CRITICAL	Exchange IIS logs, IdP sign-in logs	Not Started
TH-2026-W21-03	Cisco SD-WAN CVE-2026-20182 (CVSS 10.0)	P1 — CRITICAL	vManage audit, SD-WAN NetFlow	Not Started
TH-2026-W21-04	Netlogon CVE-2026-41089 RCE on DCs	P1 — CRITICAL	Windows Security log, AD replication	Not Started
TH-2026-W21-05	DNS Client + Dynamics 365 RCE chain	P2 — HIGH	DNS logs, Dynamics 365 IIS logs	Not Started
TH-2026-W21-06	FortiAuthenticator CVE-2026-44277	P2 — HIGH	FortiAuth audit, API access logs	Not Started
TH-2026-W21-07	cPanel CVE-2026-41940 IOC hunt (SA hosting)	P2 — HIGH	cPanel audit, /var/cpanel/sessions/raw/	Not Started
TH-2026-W21-08	SANBS / KillSec verification + healthcare SC	P2 — HIGH	Dark-web monitoring, KillSec portal	Not Started
TH-2026-W21-09	BlackSuit SA industrial-sector watch	P3 — MONITOR	EDR (Cobalt Strike), NetFlow, SIEM	Not Started

IOC Master Table — W21

Indicator	Type	Attribution	Hunt ID
canvas-* / instructure-* lookalike domains	Domain pattern	Post-Canvas-ransom ShinyHunters phishing	TH-2026-W21-01
Canvas /api/v1/users/* anomalous access	API endpoint	ShinyHunters Canvas residual exploitation	TH-2026-W21-01
CVE-2026-42897 (Exchange OWA XSS/spoofing)	CVE	Exchange OWA ITW zero-day; KEV 29 May	TH-2026-W21-02
Anomalous OWA URL patterns with script payloads	URI pattern	Exchange OWA exploitation indicator	TH-2026-W21-02
CVE-2026-20182 (Cisco SD-WAN auth bypass/RCE)	CVE	Cisco SD-WAN; CVSS 10.0; KEV 17 May past	TH-2026-W21-03
vManage admin account created without change mgmt	User anomaly	SD-WAN post-exploitation persistence	TH-2026-W21-03
CVE-2026-41089 (Netlogon RCE SYSTEM on DC)	CVE	Patch Tuesday May 2026; CVSS 9.8	TH-2026-W21-04
CVE-2026-44277 (FortiAuthenticator unauthenticated RCE)	CVE	FortiAuth dominant SA MFA stack	TH-2026-W21-06
.sorry extension files on hosted volumes	File extension	cPanel CVE-2026-41940 SA espionage wave	TH-2026-W21-07
Root password 123Qwe123C on cPanel hosts	Credential pattern	cPanel CVE-2026-41940 IOC	TH-2026-W21-07
hasroot=1 in /var/cpanel/sessions/raw/	File content pattern	cPanel CVE-2026-41940 session IOC	TH-2026-W21-07
KillSec SANBS DLS listing (12 May)	Threat actor claim	KillSec SANBS (UNVERIFIED)	TH-2026-W21-08
SANBS-domain credentials on IAB markets	Credential sighting	Post-SANBS-listing credential risk	TH-2026-W21-08
BlackSuit Cobalt Strike C2 beacon patterns	Network behaviour	BlackSuit SA industrial campaign	TH-2026-W21-09
RCIone exfiltration to MEGA from SA industrial endpoints	Network pattern	BlackSuit exfiltration TTP	TH-2026-W21-09
UnDefend.exe / FunnyApp.exe / RedSun.exe	Filename	MS Defender zero-day (still unpatched)	N/A — Detection only
CVE-2026-1281 (Ivanti EPMM Pre-auth RCE)	CVE	Ivanti EPMM; KEV ~27 May	N/A — Patch

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Patch Cisco Catalyst SD-WAN CVE-2026-20182 IMMEDIATELY (KEV deadline 17 May has now passed -- CVSS 10.0):** Apply vendor patch or implement compensating controls on all vManage / vBond / vSmart controllers. Audit admin accounts created in last 7 days. Restrict SD-WAN management to OOB/management-only access.
- **2. Apply Exchange OWA EEMS mitigation for CVE-2026-42897 (no permanent patch; KEV 29 May):** EEMS is the ONLY available mitigation. Apply immediately to all Exchange on-premises deployments. Monitor OWA IIS logs for exploitation indicators.
- **3. Deploy Patch Tuesday May 2026 across Windows estate (Netlogon 9.8, DNS Client 9.8, Dynamics 365 9.9):** Three critical RCE CVEs require immediate attention. Prioritise Domain Controllers (Netlogon), DNS servers, and Dynamics 365 On-Prem. Patch FortiAuthenticator CVE-2026-44277 concurrently.

- **4. Patch FortiAuthenticator CVE-2026-44277 (unauthenticated RCE):** Dominant SA MFA stack. Restrict FortiAuth admin interface to OOB/management VLAN. Audit new admin accounts.
- **5. Sweep cPanel IOCs -- .sorry files, hasroot=1 sessions, root password 123Qwe123C:** Patch cPanel CVE-2026-41940. Scan /var/cpanel/sessions/raw/ for hasroot=1 entries. Check root password hashes. Any unpatched cPanel/WHM since February 2026 = assume compromised.
- **6. Rotate Canvas/Instructure API tokens and brief SA tertiaries on Canvas-themed phishing (post-ransom):** Wits, Stadio, Milpark, Invictus, SPARK Schools. Rotate API tokens, OAuth secrets, and SSO credentials. Brief student/staff comms teams on expected Canvas-themed phishing campaigns.
- **7. Monitor SANBS / KillSec situation; reach out to SANBS contacts if engaged:** UNVERIFIED but healthcare-supply-chain criticality is extreme. Monitor KillSec portal and SANBS-domain IAB activity. Alert SANBS security team if your organisation has a relationship.
- **8. Patch Ivanti EPMME CVE-2026-1281 (KEV due approximately 27 May):** Pre-auth RCE. Restrict EPMME admin interface to VPN/OOB. Audit MDM enrolments and admin-role grants.

Short-Term (Next 30 Days)

- Defender RedSun/UnDefend STILL UNPATCHED (7+ weeks) -- deploy compensating EDR controls; consider third-party EDR overlay; monitor for RedSun.exe / UnDefend.exe / FunnyApp.exe.
- Verizon DBIR SA webinar 19 May (17:00 SAST) -- SOC team to attend. Credentials R100/set; 90% of SA breaches with identity weakness; 30% third-party involvement.
- NIS2 first audit prep (30 June deadline) for SA orgs with EU operations: 6 weeks remaining; complete gap assessment immediately.
- POPIA Health Data Regs compliance review for any SA org processing employee health data -- no grace period; immediate enforcement risk.
- Submit comments on SA Draft AI Policy by 10 June 2026.
- Industrial-sector incident-prep for BlackSuit-style campaigns: build RaaS incident-response playbook for SA industrial organisations.
- Healthcare-sector hardening if SANBS confirms breach: blood-supply-chain dependencies audit for SA hospitals and healthcare providers.

Strategic (Next Quarter)

- Identity-first defence — DBIR 2026 shows 90% of SA breaches have identity weakness; Patch Tuesday Netlogon RCE elevates identity-plane criticality. MFA maturity, IdP hardening, and privileged-account management are the highest-leverage controls.
- Third-party supply-chain risk programme — Canvas/Instructure (8,809 institutions), cPanel-hosted services, and SD-WAN providers all generated W21 incidents. Extend vendor risk programme to include these dependency classes.
- POPIA breach-notification readiness — IR 2,898 notifications in 2025/26 (+40% YoY) with faster enforcement signals. Incident-notification runbooks and IR e-portal registration are non-negotiable.
- EU AI Act watermarking readiness (2 December 2026) for SA AI exporters — Omnibus moved high-risk deadline to 2027, but watermarking remains on 2026 horizon. Start gap assessment for relevant systems.

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. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>

2. CISA KEV Catalog — Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

3. Microsoft MSRC — May 2026 Security Update Guide — <https://msrc.microsoft.com/update-guide/releaseNote/2026-May>
4. Ctrl-Alt-Intel — cPanel SA hosting-provider wave (2 May 2026) — <https://ctrl-alt-intel.com/>
5. Information Regulator South Africa — Media Statements — <https://infoeregulator.org.za/media-statements/>
6. Werksmans — IR APP Portfolio Committee 2025/26 coverage — <https://www.werksmans.com/>
7. Pinsent Masons — FlySafair POPIA compliance analysis (15 May 2026) — <https://www.pinsentmasons.com/>
8. ITWeb — ANC Black Ax leak coverage (15 May 2026) — <https://www.itweb.co.za/>
9. FBI IC3 — ShinyHunters PSA (15 May 2026) — <https://www.ic3.gov/>
10. Verizon DBIR 2026 — Data Breach Investigations Report — <https://www.verizon.com/business/resources/reports/dbir/>
11. Surfshark — Q1 2026 SA data breach research — <https://surfshark.com/research/>
12. HookPhish — Ransomware and threat actor tracking — <https://www.hookphish.com/>
13. RedPacket Security — Daily threat intelligence — <https://www.redpacketsecurity.com/>
14. BlackFog — State of Ransomware (monthly reports) — <https://www.blackfog.com/>
15. Fortinet PSIRT — FortiAuthenticator CVE-2026-44277 — <https://www.fortiguard.com/psirt>
16. Cisco PSIRT — SD-WAN CVE-2026-20182 advisory — <https://sec.cloudapps.cisco.com/security/center/publicationListing.x>
17. Ivanti — Security Advisories (EPM CVE-2026-1281) — <https://www.ivanti.com/blog/topics/security-advisory>
18. Fyntralink — Threat Intelligence (APT28 / MuddyWater) — <https://www.fyntralink.com/>
19. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>
20. ZeroFox — ShinyHunters TTPs — <https://www.zerofox.com/>
21. BleepingComputer — MS Defender RedSun / UnDefend coverage — <https://www.bleepingcomputer.com/>
22. ITWeb — SA cyber incident coverage (W21) — <https://www.itweb.co.za/>
23. Parliament of South Africa — Portfolio Committee records — <https://www.parliament.gov.za/>
24. TechCentral — SA cyber incident coverage — <https://techcentral.co.za/>
25. Standard Bank — Official newsroom (data incident updates) — <https://www.standardbank.co.za/southafrica/news-and-media/newsroom>
26. D3 Security — NIS2 SOC Audit Readiness 2026 — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>
27. Mayet Law — POPIA enforcement 2026 developments — <https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/>
28. Check Point Research — Q1 2026 attack volume baseline — <https://research.checkpoint.com/>
29. SABRIC — Annual Crime Statistics Report 2024 — <https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>
30. Xcitium ThreatLabs — BlackSuit Ransomware Profile — <https://threatlabsnews.xcitium.com/>
31. GuidePoint Security — GRIT Q1 2026 Ransomware Report — <https://www.guidepointsecurity.com/>
32. DataBreaches.net — SA breach analysis — <https://databreaches.net/>
33. allAfrica — Polmed breach coverage — <https://allafrica.com/>
34. UpGuard — SA Data Breach tracking 2026 — <https://www.upguard.com/>
35. Censys — SA threat exposure tracking — <https://censys.com/>
36. Daily Maverick — SA cyber landscape W21 — <https://www.dailymaverick.co.za/>
37. Integrity360 — Polmed breach technical analysis — <https://www.integrity360.com/>
38. IT-Online — Surfshark Q1 2026 SA data (8 May 2026) — <https://it-online.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-W21