INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 06:51 UTC

Talos 2025 Year in Review: Five Structural Weaknesses Attackers Exploited Most, and What Defenders Can Do Now

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0092
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	IAM platforms, PAM systems, VPNs, Active Directory Domain Controllers, application delivery controllers (ADCs), firewalls, PHP frameworks, Apache Log4j (Log4Shell), Adobe ColdFusion, network management platforms, with elevated exposure on end-of-life systems
Published	2026-04-28T13:23:20+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Cisco Talos' 2025 Year in Review identifies five structural weaknesses that attackers exploited systematically across the full year: identity and authentication abuse, unpatched and end-of-life systems, network edge device compromise, Active Directory exploitation, and AI-assisted attack scaling. Device compromise rose 178% year over year, and nearly 40% of the most targeted vulnerabilities affected products that vendors no longer support. The report signals that attacker advantages are increasingly structural, not situational, meaning organizations that have deferred identity hygiene, patch cycles, and edge device hardening are now carrying compounding risk across all five vectors simultaneously.

Technical Analysis

Talos' annual synthesis draws from incident response engagements, telemetry, and threat intelligence collected across 2025, and the picture it assembles is one of converging structural failures rather than isolated exploitation events.

The first and most pervasive weakness is identity and authentication abuse. Attackers targeting IAM and PAM platforms used credential stuffing, MFA bypass techniques (T1621, MFA fatigue and push-bombing), and session token theft (T1539) to circumvent authentication without ever touching a vulnerability. Valid account abuse (T1078) and authentication mechanism modification (T1556, T1556.006) appeared consistently across ransomware and state-sponsored intrusions alike, reinforcing that authentication controls, not just perimeter

defenses, are the primary battleground.

The second weakness is the unpatched and end-of-life system problem, which Talos frames as an industry-wide governance failure rather than a technical oversight. Nearly 40% of the top 100 most targeted vulnerabilities affected EOL products. Log4Shell (CVE-2021-44228) and Adobe ColdFusion vulnerabilities, some more than a decade old, remained active exploitation targets throughout 2025. Exploitation of public-facing applications (T1190) mapped consistently to CWE-1104 (use of unmaintained third-party components) and CWE-1395 (use of weak or broken cryptographic primitives), indicating that the exposure is not merely about missing patches but about inherited technical debt that defenders cannot patch their way out of.

The third weakness is trust-broker compromise. VPNs, application delivery controllers, and firewalls, devices that sit at the intersection of trusted and untrusted networks, were systematically targeted for persistent access. External remote services (T1133) provided initial footholds; exploitation of privilege escalation weaknesses (T1068) extended attacker reach once inside. Because these devices often lack EDR coverage and generate logs that security teams underinspect, dwell times in this vector tend to be extended.

The fourth weakness is Active Directory abuse. Once inside, attackers consistently turned to AD as the path of least resistance for lateral movement and privilege escalation. Domain policy modification (T1484), credential dumping (T1003), and remote service exploitation (T1021) formed a recurring post-exploitation chain. The persistence of this pattern reflects a broader problem: AD environments accumulate misconfigurations, legacy trusts, and over-provisioned accounts over years, and few organizations have continuous AD posture monitoring in place.

The fifth weakness is AI-assisted attack scaling. Talos documents attacker use of AI to accelerate reconnaissance (T1595, T1589), generate targeted phishing content (T1566), and automate exploitation chain assembly. The practical effect is compression of the time between initial access and lateral movement, reducing the window defenders have to detect and respond. This is not a speculative future threat; Talos observed it operationally across 2025 engagements.

Across all five vectors, Talos notes that behavioral anomalies remain detectable by well-tuned defenses. The core defensive gap is not sensor coverage, it is the absence of tuned behavioral baselines, which means attacker activity blends into noise rather than generating actionable alerts.

Action Checklist

1. Step 1: Assess exposure, audit your environment for end-of-life systems across all five affected categories: IAM/PAM platforms, VPNs, ADCs, firewalls, and application frameworks including PHP, Log4j-dependent services, and ColdFusion instances. Prioritize internet-facing and network-edge assets.
2. Step 2: Review controls, verify MFA implementation quality (not just MFA presence): confirm push-bombing protections are active, session token lifetimes are enforced, and PAM solutions log and alert on privileged session anomalies. Confirm EDR coverage extends to network edge devices or compensating log monitoring is in place.
3. Step 3: Update threat model, incorporate all five Talos-identified vectors as active threat scenarios in your threat register. Map them to your current control inventory against MITRE ATT&CK techniques T1078, T1621, T1539, T1190, T1484, T1003, T1133, and T1595. Flag gaps where no detective control exists.
4. Step 4: Communicate findings, brief leadership on the 178% device compromise increase and the EOL system finding. Frame the EOL issue as governance risk, not technical debt: if 40% of targeted

vulnerabilities affect unsupported products, any EOL system your organization runs is a documented attacker priority.

5. Step 5: Monitor developments, subscribe to Cisco Talos threat intelligence feeds for follow-on disclosures and sector-specific findings related to the threat vectors described in this report.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if any Talos-published IOC matches observed network traffic or log entries, if an EOL network edge device (VPN, ADC, firewall) shows evidence of unauthorized access, or if Active Directory replication metadata indicates DCSync activity (T1003.006) — any of these conditions indicate a likely active compromise requiring breach notification assessment under applicable regulatory frameworks (HIPAA, PCI-DSS, state breach notification laws).
Recovery Notes	Following containment of any compromise linked to the Talos-identified vectors, prioritize rebuilding affected identity infrastructure (PAM, IAM, AD) from known-good baselines rather than attempting in-place remediation — session tokens, Kerberos tickets (including Golden/Silver Ticket artifacts), and OAuth tokens issued during the compromise window must be invalidated wholesale via a krbtgt double-reset for AD environments and full OAuth token revocation for IAM platforms. Monitor rebuilt systems for at least 30 days post-recovery using enhanced logging at the DEBUG level on PAM platforms, and watch specifically for T1078 (Valid Account) re-use, T1484 (Domain Policy Modification) attempts, and any reconnection to Talos-disclosed C2 infrastructure. EOL systems that cannot be patched must remain isolated from production network segments post-recovery until a formal decommission or compensating control decision is documented and approved.
Forensic Artifacts	Active Directory replication metadata — run `repadmin /showrepl` and audit Event ID 4662 (object access with DS-Replication-Get-Changes-All permission) on Domain Controllers to detect DCSync (T1003.006) credential theft that Talos identified as a top AD exploitation technique | PAM platform privileged session logs — export full session recordings and command audit trails for all sessions initiated in the 90 days prior to detection, focusing on sessions accessing Domain Controllers, firewall management interfaces, and VPN admin consoles — these are the lateral movement paths Talos documented in AD exploitation chains | Web server access logs on ColdFusion and PHP application servers — search for URI patterns consistent with deserialization exploitation (`/CFIDE/administrator/`, `/flex2gateway/`, `%{${`) and Log4Shell JNDI payloads (`${jndi:ldap://`, `${jndi:rmi://`) with source IPs and response codes preserved for timeline reconstruction | Network edge device (VPN/ADC/firewall) configuration change logs — extract all configuration changes (Cisco ASA: `show archive log config all`, Palo Alto: configuration audit log) for the prior 90 days to identify backdoor accounts, policy weakening, or rogue admin sessions consistent with the 178% device compromise increase Talos reported | Windows Security Event Log Event ID 4776 (NTLM credential validation) and Event ID 4771 (Kerberos pre-auth failure) on Domain Controllers — high volumes of these events from a single source IP or against multiple accounts indicate credential stuffing or password spray attacks against AD, the identity abuse vector Talos ranked as the top structural weakness of 2025

Per-Action IR Details

Step 1: Assess exposure — audit your environment for end-of-life systems across all five affected categories: IAM/PAM platforms, VPNs, ADCs, firewalls, and application frameworks including PHP, Log4j-dependent

services, and ColdFusion instances. Prioritize internet-facing and network-edge assets.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and reducing attack surface before incidents occur

Controls: NIST SI-2 (Flaw Remediation) — identify and correct EOL systems that cannot receive patches, NIST RA-3 (Risk Assessment) — assess risk of running unsupported IAM/PAM, VPN, ADC, and firewall platforms, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — enumerate all assets including network-edge devices and application frameworks, CIS 2.2 (Ensure Authorized Software is Currently Supported) — flag Log4j-dependent services, Adobe ColdFusion, and PHP frameworks running unsupported versions, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — scope vulnerability scanning to include EOL network edge devices that scanners often skip

Compensating: Run `nmap -sV --script=banner -p 443,8443,80,8080,22,23 ` against your perimeter to fingerprint VPN gateways, ADCs, and firewalls and identify product versions. Cross-reference output against CISA's Known Exploited Vulnerabilities (KEV) catalog using a local copy and `grep`. For Log4j exposure, use the free Huntress Log4Shell Vulnerability Tester or run `find / -name 'log4j*.jar' -o -name 'log4j*.war'` on Linux hosts; on Windows use `Get-ChildItem -Recurse -Filter 'log4j*.jar'`. For ColdFusion, query HTTP response headers for `X-Powered-By: ColdFusion` or check `C:\ColdFusion\cfusion\logs\` for version strings.

Evidence: Before modifying any system, capture: (1) current firewall and VPN firmware version strings from admin console or SNMP OID 1.3.6.1.2.1.1.1.0 (sysDescr); (2) ColdFusion administrator logs at `{cf_root}/cfusion/logs/application.log` and `server.log` for evidence of pre-existing exploitation; (3) Log4j JNDI lookup attempts in Java application logs — search for `${jndi:` string patterns in any `.log` file; (4) PAM platform audit logs showing recent privileged session creation, particularly any sessions initiated from external IP ranges; (5) network flow data (NetFlow/IPFIX) from edge devices showing unusual outbound connections on TCP 1389, 389, or 636 (LDAP/LDAPS) which indicate active Log4Shell exploitation.

Step 2: Review controls — verify MFA implementation quality (not just MFA presence): confirm push-bombing protections are active, session token lifetimes are enforced, and PAM solutions log and alert on privileged session anomalies. Confirm EDR coverage extends to network edge devices or compensating log monitoring is in place.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring detective and preventive controls are functional before adversary activity occurs; aligns with CSF PR and DE functions

Controls: NIST IR-4 (Incident Handling) — validate that PAM alerting on privileged session anomalies feeds the incident handling capability, NIST SI-4 (System Monitoring) — confirm monitoring coverage extends to VPN concentrators, ADCs, and firewalls where EDR agents cannot be deployed, NIST IA-5 (Authenticator Management) — enforce session token lifetimes and MFA push-bombing protections on IAM/PAM platforms targeted in the Talos findings, CIS 6.3 (Require MFA for Externally-Exposed Applications) — validate push-fatigue protections (number matching, geographic context) are enabled, not just MFA enrollment, CIS 6.5 (Require MFA for Administrative Access) — confirm PAM-gated administrative sessions require MFA at privilege elevation, not only at initial login, CIS 8.2 (Collect Audit Logs) — verify syslog forwarding is active from VPN gateways, firewalls, and ADCs to a central log store

Compensating: For MFA push-bombing detection without enterprise IAM tooling: enable number-matching in Microsoft Authenticator (Entra ID free tier) or use TOTP-based MFA (Google Authenticator, FreeOTP) which is immune to push-bombing by design. For PAM session monitoring on a budget, deploy Sysmon (config minimum: EventID 1 process create, EventID 3 network connect, EventID 10 process access) on PAM jump hosts and forward via WEF (Windows Event Forwarding) to a central Windows Event Collector. For network edge devices without EDR, configure syslog-ng or rsyslog to receive device logs and write a simple `grep`/`awk` cron job alerting on authentication failure bursts: `awk '/Failed|authentication failure/{count[$4]++} END{for(ip in count) if(count[ip]>10) print ip, count[ip]}' /var/log/syslog`.

Evidence: Before tuning controls, baseline and preserve: (1) Azure AD / Entra ID sign-in logs (MFA result field, conditional access outcome, IP address) — export via `Get-MgAuditLogSignIn` for the prior 30 days to establish normal MFA approval rates and detect historical push-bombing attempts; (2) PAM platform session recordings index —

note any sessions with anomalous duration, unusual target systems, or off-hours timing consistent with T1078 (Valid Accounts) abuse; (3) VPN authentication logs showing successful logins from IP ranges not matching established user baselines — on Cisco ASA review `%ASA-6-113015` and `%ASA-6-113019` syslog messages; (4) Active Directory Security Event Log (Event ID 4768 — Kerberos TGT request, Event ID 4769 — service ticket request) on Domain Controllers to identify credential abuse predating the control review.

Step 3: Update threat model — incorporate all five Talos-identified vectors as active threat scenarios in your threat register. Map them to your current control inventory against MITRE ATT&CK techniques T1078, T1621, T1539, T1190, T1484, T1003, T1133, and T1595.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: using threat intelligence to shape IR plans and detection priorities; aligns with CSF ID.RA (Risk Assessment) and DE.AE-07 (CTI integration into adverse event analysis)

Controls: NIST RA-3 (Risk Assessment) — update risk register entries for identity abuse (T1078, T1621), network edge exploitation (T1190, T1133), and AD attacks (T1484, T1003) based on Talos prevalence data, NIST IR-8 (Incident Response Plan) — revise IR plan scenarios to include the five Talos structural weaknesses as named threat scenarios with specific playbook triggers, NIST SI-5 (Security Alerts, Advisories, and Directives) — formally process the Talos 2025 Year in Review as a threat intelligence input requiring control gap analysis, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate T1190 (Exploit Public-Facing Application) targeting EOL ADCs, firewalls, and ColdFusion into vuln prioritization criteria, CIS 7.2 (Establish and Maintain a Remediation Process) — assign remediation priority to control gaps identified in the ATT&CK mapping, particularly where no detective control exists for T1484 (Domain Policy Modification) or T1003 (OS Credential Dumping)

Compensating: Use the free MITRE ATT&CK Navigator (browser-based, no installation) to create a layer mapping your existing detective controls against T1078, T1621, T1539, T1190, T1484, T1003, T1133, and T1595 — color-code red for no coverage, yellow for partial, green for covered. Export the layer as JSON for your threat register. For Sigma rule coverage gaps, search the public Sigma rule repository (`github.com/SigmaHQ/sigma`) for rules targeting each technique — e.g., `rules/windows/builtin/security/win_security_dcsync.yml` covers T1003.006 (DCSync), and `rules/network/cisco/` covers edge device anomalies.

Evidence: Before updating the threat model, pull current-state evidence to establish a baseline: (1) Windows Security Event Log — query for Event ID 4742 (computer account changed) and Event ID 4662 (directory service object access with replication rights) on DCs to determine if T1003.006 (DCSync) has been attempted; (2) Group Policy change audit logs — Event ID 5136 (directory service object modified) filtered on `groupPolicyContainer` objects to detect T1484 (Domain Policy Modification) in the prior 90 days; (3) Windows Security Event Log Event ID 4964 (special groups logon) and Event ID 4672 (special privileges assigned) to surface T1078 (Valid Account) privilege escalation; (4) VPN and firewall logs for T1133 (External Remote Services) — extract all successful authentications from IP reputation feeds and flag any from Tor exit nodes, bulletproof hosting ASNs, or anonymizers.

Step 4: Communicate findings — brief leadership on the 178% device compromise increase and the EOL system finding. Frame the EOL issue as governance risk, not technical debt: if 40% of targeted vulnerabilities affect unsupported products, any EOL system your organization runs is a documented attacker priority.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, communicating systemic risk to leadership to drive policy and resource decisions; aligns with CSF GV.OC (Organizational Context)

Controls: NIST IR-6 (Incident Reporting) — extend reporting obligations to proactive risk communication: leadership must be informed of material threat intelligence findings like the Talos 178% device compromise increase before an incident occurs, NIST IR-8 (Incident Response Plan) — EOL system risk must be documented in the IR plan as a known environmental constraint affecting containment and eradication options, NIST SI-2 (Flaw Remediation) — the 40% EOL vulnerability targeting statistic is a direct input to the flaw remediation program; unsupported systems are unfixable by definition and require compensating control or decommission decisions, CIS 7.2 (Establish and Maintain a Remediation Process) — EOL systems with no patch path must be escalated to leadership as requiring either compensating controls or formal decommission timelines per the remediation process

Compensating: For teams without a formal risk register tool: create a one-page EOL Risk Register in a spreadsheet listing each EOL asset, its internet-facing status, the CVEs actively targeting its product family (pulled from CISA KEV), and the business owner. Attach the Talos statistic (40% of targeted vulns affect EOL products) as a cited source. Present as a risk acceptance decision requiring leadership signature — this documents due diligence and creates accountability for the decommission/compensate decision. Use CISA's free Cyber Hygiene (CyHy) scanning service for external attack surface validation to support the briefing with objective data.

Evidence: Supporting data for the leadership brief that must be preserved as documented evidence: (1) CISA KEV catalog entries — download the current KEV JSON feed (`https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) and filter for CVEs affecting your specific EOL products to produce a count of actively exploited vulnerabilities you cannot patch; (2) Asset inventory export showing EOL systems with their last-seen network activity timestamps — confirming they are active, not dormant; (3) Vulnerability scanner output (even from free tools like OpenVAS or Greenbone Community Edition) showing CVSS scores against EOL assets — this quantifies the risk in terms leadership can act on; (4) Network flow records showing inbound connection attempts to EOL network edge devices from external IP ranges — demonstrating active adversary interest, not hypothetical risk.

Step 5: Monitor developments — track the full Talos 2025 Year in Review report for published IOCs, additional campaign details, and sector-specific findings. Subscribe to Cisco Talos threat intelligence feeds for follow-on disclosures tied to the campaigns described in this report.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: integrating external threat intelligence into ongoing monitoring; aligns with DE.AE-07 (CTI integrated into adverse event analysis) and DE.CM-01 (network monitoring for adverse events)

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — formally subscribe to Cisco Talos intelligence feeds as an external organization providing security alerts and advisories, NIST IR-5 (Incident Monitoring) — incorporate Talos-published IOCs (IP ranges, domains, file hashes associated with identity abuse and edge device compromise campaigns) into active monitoring queries, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — update log review procedures to query for Talos-disclosed IOCs across VPN, firewall, AD, and IAM log sources as new indicators are published, CIS 8.2 (Collect Audit Logs) — ensure log collection scope covers the sources where Talos-identified campaign activity would appear: DC Security logs, VPN auth logs, ADC access logs, and IAM platform audit trails

Compensating: Subscribe to Cisco Talos free intelligence feeds: the Talos IP Blacklist (`https://talosintelligence.com/documents/ip-blacklist`) updates daily and can be ingested into pfSense, iptables, or Windows Firewall via scheduled script. Use `curl` + `cron` to pull the feed daily and pipe into a local blocklist. For IOC matching without a SIEM, deploy osquery with the `osquery-defense-kit` pack and write a simple query against `process_open_sockets` to flag connections to Talos-listed IPs. For file-based IOCs (hashes), update ClamAV signatures with community databases including the `MalwarePatrol` feed (free tier available) and run scheduled scans on web-facing servers hosting PHP, ColdFusion, or Log4j-dependent applications. Create a free account on VirusTotal to bulk-check any new hashes Talos publishes.

Evidence: Evidence to collect and preserve as Talos publishes follow-on IOCs: (1) DNS query logs from your resolver (bind query log or Windows DNS debug logging — enable via `dnscmd /config /logLevel 0x8100`) to retroactively hunt Talos-disclosed C2 domains against historical queries, identifying beaconing that predates your subscription to the feed; (2) Proxy/firewall logs for HTTP/S connections matching Talos-published URI patterns associated with identity abuse campaigns — specifically look for POST requests to `/api/` endpoints on IAM/PAM platforms from unusual source IPs; (3) NetFlow or firewall session logs for connections to Talos-disclosed C2 IP ranges, preserved for at least 90 days to support retroactive hunt when new IOCs are released; (4) Windows Security Event Log Event ID 4624 (successful logon) Type 3 (network) and Type 10 (remote interactive) from Domain Controllers — retain for 180 days to support retroactive correlation when Talos publishes actor-attributed IP indicators from the 2025 campaigns.

Detection Guidance

Talos' findings map to several high-value detection opportunities across the five vectors.

For identity and authentication abuse: monitor authentication logs for MFA push fatigue patterns (multiple push requests in short succession from a single account), impossible travel events, and session token reuse from new or anomalous IP ranges. Alert on PAM session initiations outside business hours or from unexpected source addresses. Review for T1556 and T1556.006 indicators, specifically, modifications to authentication provider configurations or conditional access policies.

For EOL system exploitation: query your asset inventory against published EOL dates for all network-facing systems. Cross-reference with vulnerability scan results for CVEs affecting Log4j (CVE-2021-44228 and related), Adobe ColdFusion, and PHP frameworks. Prioritize assets with no available vendor patch path, these require compensating controls or isolation.

For trust-broker compromise: establish baseline traffic profiles for all VPNs, ADCs, and firewalls. Alert on configuration changes, unexpected authentication attempts, and outbound connections to non-standard destinations from these devices. Review for T1133 patterns, authentication to external remote services from internal service accounts.

For Active Directory abuse: enable and baseline AD audit logging, focusing on Group Policy Object modifications (T1484), Kerberoastable account queries, NTDS.dit access attempts (T1003), and new trust relationship creation. Tools like BloodHound CE should be run on a recurring schedule (monthly or quarterly) and results baselined for AD attack path change detection.

For AI-assisted reconnaissance: monitor for high-volume, structured reconnaissance patterns (T1595) that suggest automation, port scanning cadence, subdomain enumeration bursts, or LinkedIn scraping activity. These precede the phishing (T1566) and exploitation phases and represent an early-warning opportunity that is often ignored.

Log sources to prioritize: identity provider authentication logs, PAM session logs, VPN/firewall authentication and configuration change logs, Windows Security Event Log (event IDs 4624, 4625, 4648, 4672, 4768, 4769, 4776), and Active Directory replication logs.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Cisco Talos 2025 Year in Review report for published indicators`	C2 infrastructure details, payload hashes, and campaign-specific IOCs are documented in the full Talos 2025 Year in Review report. The source article URL provided does not surface specific indicator values; retrieve directly from the Talos report PDF at the source URL listed.	LOW

Framework Mappings

MITRE-ATTACK

- **T1484** — Domain or Tenant Policy Modification
- **T1621** — Multi-Factor Authentication Request Generation

- **T1190** — Exploit Public-Facing Application
- **T1098.005** — Device Registration
- **T1539** — Steal Web Session Cookie
- **T1021** — Remote Services
- **T1003** — OS Credential Dumping
- **T1589** — Gather Victim Identity Information
- **T1566** — Phishing
- **T1569.002** — Service Execution
- **T1550.001** — Application Access Token
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process
- **T1595** — Active Scanning
- **T1556.006** — Multi-Factor Authentication
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-20** — Use of External Systems
- **AC-2** — Account Management
- **SA-4** — Acquisition Process
- **SA-9** — External System Services
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan

- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A06:2021** — Vulnerable and Outdated Components
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.4** — Establish and Manage an Inventory of Third-Party Software Components
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1484	Domain or Tenant Policy Modification	Defense-Evasion

Technique ID	Technique Name	Tactic
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1098.005	Device Registration	Persistence
T1539	Steal Web Session Cookie	Credential-Access
T1021	Remote Services	Lateral-Movement
T1003	OS Credential Dumping	Credential-Access
T1589	Gather Victim Identity Information	Reconnaissance
T1566	Phishing	Initial-Access
T1569.002	Service Execution	Execution
T1550.001	Application Access Token	Defense-Evasion
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1595	Active Scanning	Reconnaissance
T1556.006	Multi-Factor Authentication	Credential-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/five-defender-priorities-from-th...	T3
[PDF] 2025	https://storage.ghost.io/c/af/a0/afa04ee3-414f-4481-8d23-7e7c146f19...	T3
Top 14 Network Security Risks Impacting Businesses Today	https://www.sentinelone.com/cybersecurity-101/cybersecurity/network...	T3
New Eldorado Ransomware Targets Multiple Sectors with Advanced ...	https://www.varutra.com/ctp/threatpost/postDetails/New-Eldorado-Ran...	T3
Palo Alto Networks Security Advisories	https://security.paloaltonetworks.com/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-29 06:51 UTC by TJS Security Command Center