INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 06:50 UTC

ShinyHunters Vishing-to-Salesforce Chain Hits ADT: SSO Compromise Pattern Signals Broader Enterprise Risk

DATA BREACH | **HIGH** | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0101
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ADT Inc. (Okta SSO, Salesforce CRM)
Published	2026-04-24T18:53:14
Discovery Source	Rss

Executive Summary

ADT confirmed a data breach on April 20, 2026, in which the ShinyHunters extortion group socially engineered an employee into surrendering Okta SSO credentials via a voice phishing call, then used that access to exfiltrate data from approximately 10 million customer records stored in Salesforce. The core failure is architectural: a single compromised credential bypassed authentication controls across ADT's entire connected SaaS estate. Any enterprise relying on password-plus-SMS MFA across Okta, Microsoft Entra ID, or Google Workspace SSO faces the same structural exposure today.

Technical Analysis

Attack chain: ShinyHunters conducted a vishing call targeting an ADT employee, socially engineering disclosure of Okta SSO credentials (MITRE T1598.004, T1566.004). The actor authenticated to Okta using the stolen credentials (T1078, T1078.004), harvested the active SSO session token (T1539, T1550.001), and pivoted laterally into ADT's Salesforce CRM without triggering per-application authentication challenges (T1213, T1530). Customer data was exfiltrated to an external location (T1537). Extortion followed (T1657). No CVE is associated; the failure is procedural and architectural. Applicable CWEs: CWE-287 (Improper Authentication, SSO credential compromise via social engineering), CWE-306 (Missing Authentication for Critical Function, absence of phishing-resistant MFA enforcement at the SSO layer), CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor, resulting customer data exfiltration). There is no software patch. Remediation requires enforcing phishing-resistant MFA (FIDO2/WebAuthn passkeys or hardware security keys such as YubiKey) at the IdP layer and restricting SaaS application access to compliant, phishing-resistant

authentication methods only. Standard TOTP and SMS-based MFA do not mitigate this attack vector; they are bypassable via real-time phishing and vishing interception. Source: BleepingComputer (T3), April 2026.

Action Checklist

1. Containment: Audit immediately all active Okta (or Entra ID / Google Workspace) SSO sessions for anomalous access patterns: logins from new geographies, new devices, or outside business hours within the past 30 days. Revoke suspicious sessions and reset credentials for affected accounts. Identify all SaaS applications (including Salesforce) connected to your IdP and determine which were accessible via the suspect session.
2. Detection: Query your IdP logs for: (1) authentication events followed within minutes by access to a new or rarely accessed SaaS application; (2) successful logins where MFA method was SMS or TOTP rather than FIDO2/hardware key; (3) large-volume Salesforce API queries or exports outside normal user behavior. In Okta, review System Log for 'user.session.start' events paired with 'app.oauth2.token.grant' events to connected apps. In Salesforce, audit Setup > Login History and Data Export logs for bulk record access.
3. Eradication: Enforce phishing-resistant MFA (FIDO2/WebAuthn passkeys or FIDO2 hardware security keys) as the required authenticator for all IdP logins. In Okta: configure an Authentication Policy requiring 'Hardware Protected' or 'WebAuthn' factor; remove SMS and voice call authenticators from high-privilege user profiles. Disable or restrict legacy authentication protocols (BasicAuth, IMAP) that bypass MFA entirely. Do not treat TOTP as equivalent mitigation, it is interceptable via real-time vishing.
4. Recovery: Validate that no unauthorized OAuth tokens or API keys were issued to external applications during the compromise window. Rotate all Salesforce Connected App credentials and Okta API tokens provisioned within the suspect timeframe. Confirm phishing-resistant MFA enrollment for 100% of IdP users before restoring full SaaS access. Monitor Salesforce and IdP logs at elevated frequency for 30 days post-remediation.
5. Post-Incident: Conduct a SaaS blast radius analysis: map every application connected to your IdP and document what data each can access with a valid SSO session. Implement Okta or Entra ID Conditional Access policies restricting SaaS access to managed, compliant devices. Establish vishing-specific awareness training emphasizing that no internal helpdesk or vendor will ask for SSO credentials or MFA codes verbally. Review break-glass account procedures to ensure emergency admin access does not bypass phishing-resistant MFA requirements.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if Okta System Log or Salesforce Event Log Files confirm any bulk export of records containing PII (names, addresses, account numbers) for 10M+ customers, as this triggers mandatory breach notification obligations under applicable state data breach notification laws (e.g., CCPA, SHIELD Act) and potentially SEC material disclosure requirements for public companies; escalate to IR retainer or MSSP if internal team cannot revoke all active Okta sessions and connected OAuth tokens within 2 hours of detection.

Recovery Notes	Before restoring full Salesforce access to any user, verify FIDO2 enrollment is confirmed in Okta for that user's account and that their session was issued post-eradication under the new Authentication Policy enforcing hardware-protected factors. Monitor Salesforce Event Log Files daily for EventType 'ReportExport', 'ApiTotalUsage', and 'Login' for a minimum of 30 days post-remediation, baselining normal API call volume and flagging any query returning more than 1,000 records from Contact, Account, or custom PII-holding objects. Retain all Okta System Log exports and Salesforce Event Log Files from the breach window for a minimum of 12 months in immutable storage to support regulatory investigations, cyber insurance claims, and any litigation initiated by affected customers.
Forensic Artifacts	Okta System Log (Admin > Reports > System Log): primary forensic record of the vishing-to-SSO chain — contains 'user.session.start' event with the compromised employee's sessionId, client IP, geolocation, device fingerprint, and 'authenticationContext.credentialType' field confirming SMS or TOTP factor was used (the vished OTP); cross-reference sessionId across all subsequent 'app.oauth2.token.grant' events to map every Salesforce Connected App and SaaS application that received a delegated token during the ShinyHunters session. | Salesforce Event Log Files — EventType 'ReportExport' and 'ApiTotalUsage' (Setup > Event Log Files, or REST API: /services/data/v59.0/query?q=SELECT+Id,+EventType,+LogDate+FROM+EventLogFile+WHERE+EventType='ReportExport'): quantifies the actual exfiltration volume — each ReportExport record contains the report name, the number of rows exported, and the user/API client that triggered the export, directly evidencing the 10M record exfiltration scope attributed to ShinyHunters. | Salesforce Setup Audit Trail (Setup > View Setup Audit History, exportable as CSV): records any Connected App registrations, OAuth policy changes, permission set grants, or profile modifications made during the compromised session — ShinyHunters commonly registers a new Connected App or modifies an existing one to establish OAuth persistence that survives session revocation and password reset. | Okta API Token Creation Log (Okta System Log filtered to eventType 'system.api_token.create'): identifies any API tokens created during the compromised session that function as persistence backdoors independent of the user's password or MFA enrollment — these survive session revocation and must be explicitly inventoried and revoked as part of eradication. | Salesforce Login History (Setup > Login History, SOQL: SELECT LoginTime, UserId, LoginType, SourceIp, Application, Status FROM LoginHistory WHERE LoginTime > [breach_start] ORDER BY LoginTime ASC): establishes the exact timestamp the ShinyHunters-controlled Okta session authenticated into Salesforce via SSO, the source IP used for Salesforce access (may differ from the Okta authentication IP if a proxy or VPN was used post-credential theft), and the specific Salesforce application context (API vs. UI) that facilitated bulk record access.

Per-Action IR Details

Containment — Immediately audit all active Okta (or Entra ID / Google Workspace) SSO sessions for anomalous access patterns: logins from new geographies, new devices, or outside business hours within the past 30 days. Revoke suspicious sessions and reset credentials for affected accounts. Identify all SaaS applications (including Salesforce) connected to your IdP and determine which were accessible via the suspect session.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: short-term containment to limit damage scope before eradication

Controls: NIST IR-4 (Incident Handling) — execute containment as part of the incident handling capability, NIST AC-2 (Account Management) — review and revoke anomalous active sessions tied to compromised Okta account, NIST AC-17 (Remote Access) — identify and terminate SSO sessions initiated outside authorized access patterns, CIS 5.3

(Disable Dormant Accounts) — extend logic to revoke sessions showing no legitimate activity post-credential compromise, CIS 6.2 (Establish an Access Revoking Process) — execute documented revocation process for the vished employee account and any accounts the session touched

Compensating: Without enterprise SIEM: use Okta's free System Log export (Admin > Reports > System Log) filtered to the past 30 days, export as CSV, and parse with PowerShell: Import-Csv okta_syslog.csv | Where-Object { $_.eventType -eq 'user.session.start' } | Sort-Object city,device | Export-Csv suspicious_sessions.csv. Cross-reference resulting IPs against the employee's known work locations using ipinfo.io CLI (free tier). Manually force-expire all sessions for the compromised account via Okta Admin > Directory > People > [user] > More Actions > Clear User Sessions.

Evidence: BEFORE revoking sessions, capture: (1) Okta System Log entries showing the exact 'user.session.start' event for the vished employee — record sessionId, client IP, geolocation, device fingerprint, and userAgent string; (2) the full list of 'app.oauth2.token.grant' events issued during that sessionId to map every Salesforce Connected App and other SaaS app that received an OAuth token; (3) Salesforce Login History (Setup > Login History) showing the SSO-authenticated login correlated to the Okta session timestamp — capture LoginType field confirming 'SSO' and SourceIp; (4) screenshot or export of Okta's connected application list showing blast radius before any revocation action removes the audit trail.

Detection — Query your IdP logs for: (1) authentication events followed within minutes by access to a new or rarely accessed SaaS application; (2) successful logins where MFA method was SMS or TOTP rather than FIDO2/hardware key; (3) large-volume Salesforce API queries or exports outside normal user behavior. In Okta, review System Log for 'user.session.start' events paired with 'app.oauth2.token.grant' events to connected apps. In Salesforce, audit Setup > Login History and Data Export logs for bulk record access.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to establish attack timeline and scope of ShinyHunters lateral movement from Okta into Salesforce

Controls: NIST SI-4 (System Monitoring) — monitor Okta and Salesforce telemetry for indicators consistent with SSO credential abuse and bulk data exfiltration, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — analyze Okta System Log and Salesforce Login History for anomalous authentication and data access events, NIST AU-2 (Event Logging) — confirm that Okta System Log retention and Salesforce event log file (ELF) generation were enabled and capturing the required event types during the compromise window, NIST IR-5 (Incident Monitoring) — track and document all identified anomalous Okta and Salesforce events as incident records, CIS 8.2 (Collect Audit Logs) — verify Okta System Log and Salesforce Event Log Files were enabled and ingested before the breach window

Compensating: Without SIEM: download Okta System Log via API (GET /api/v1/logs?since=2026-03-22&until=2026-04-20&filter=eventType+eq+%22user.session.start%22) using curl with your Okta API token, pipe to jq to extract sessionId, actor, client.geographicalContext, and authenticationContext.credentialType. Flag any credentialType of 'PASSWORD_IWA', 'SMS', or 'TOTP'. For Salesforce: enable Event Monitoring (available on Enterprise/Unlimited without additional cost for Login and API event types), then query via SOQL: SELECT LoginTime, UserId, LoginType, SourceIp, Application FROM LoginHistory WHERE LoginTime > 2026-03-22T00:00:00Z AND LoginType = 'Remote Access 2.0'. For bulk export detection, query EventLogFile object filtering on EventType = 'Report' or 'API' and sort by RecordCount descending.

Evidence: BEFORE concluding detection scope: (1) Okta System Log events with eventType 'user.authentication.auth_via_mfa' — capture the 'factor' field value to confirm whether SMS/TOTP (phishable) was used rather than FIDO2, establishing that the vishing call succeeded in harvesting a usable OTP; (2) Okta 'app.oauth2.token.grant.implicit' or 'app.oauth2.as.token.grant' log entries correlated to the compromised sessionId — these identify every Salesforce Connected App that received a delegated token; (3) Salesforce Event Log Files for EventType = 'ReportExport' and 'ApiTotalUsage' during the breach window — these will show the specific report names exported and API call volume consistent with 10M record exfiltration; (4) Salesforce Setup Audit Trail (Setup > View Setup Audit History) for any Connected App permission changes or profile modifications made during the session; (5) network flow logs or proxy logs showing data volume egress from Salesforce API endpoints (*.salesforce.com) correlated to the session timestamps.

Eradication — Enforce phishing-resistant MFA (FIDO2/WebAuthn passkeys or FIDO2 hardware security keys) as the required authenticator for all IdP logins. In Okta: configure an Authentication Policy requiring 'Hardware Protected' or 'WebAuthn' factor; remove SMS and voice call authenticators from high-privilege user profiles. Disable or restrict legacy authentication protocols (BasicAuth, IMAP) that bypass MFA entirely. Do not treat TOTP as equivalent mitigation — it is interceptable via real-time vishing.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the exploited authentication weakness (SMS/TOTP MFA) that enabled ShinyHunters to complete the vishing-to-SSO chain and eliminate the attack vector, not merely the compromised session

Controls: NIST IA-5 (Authenticator Management) — replace phishable SMS/TOTP authenticators with FIDO2/WebAuthn hardware-bound credentials for all Okta users, NIST IA-2(6) (Identification and Authentication — Multi-Factor Authentication to Privileged Accounts — Access to Non-Privileged Accounts) — enforce phishing-resistant MFA at the IdP layer covering all Salesforce-connected sessions, NIST SI-2 (Flaw Remediation) — treat the SMS/TOTP authentication policy as a configuration flaw enabling this breach and remediate by policy enforcement, not just credential reset, NIST AC-3 (Access Enforcement) — enforce Okta Authentication Policy rules that deny session establishment unless FIDO2 factor is satisfied, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce phishing-resistant MFA specifically on Okta as the externally-exposed authentication gateway to Salesforce and all connected SaaS, CIS 6.5 (Require MFA for Administrative Access) — prioritize FIDO2 enforcement for Okta administrator accounts and Salesforce System Administrator profiles before general user rollout

Compensating: For orgs without budget for hardware keys: deploy passkeys using platform authenticators (Windows Hello, Apple Touch ID/Face ID) as a zero-cost FIDO2 option — enroll via Okta's built-in WebAuthn enrollment flow (Security > Authenticators > Add Authenticator > FIDO2 WebAuthn). For legacy protocol blocking: in Okta, navigate to Security > API > Trusted Origins and remove any origins permitting BasicAuth; use Okta's Network Zone policy to block authentication requests not originating from managed device IP ranges. Run this Okta API query to identify all users still enrolled with SMS as their only MFA factor: GET /api/v1/users?filter=status+eq+%22ACTIVE%22, then for each userId GET /api/v1/users/{id}/factors and flag any without a FIDO2 factor type.

Evidence: BEFORE reconfiguring Okta Authentication Policies: (1) export the current Okta Authentication Policy ruleset (Admin > Security > Authentication Policies) as a screenshot or API export — GET /api/v1/policies?type=ACCESS_POLICY — to document the pre-breach policy state that permitted SMS/TOTP; this establishes the configuration gap for post-incident reporting and any regulatory notification; (2) export the full list of Okta users enrolled with SMS or voice call authenticators only (no FIDO2 factor) — this defines the population of accounts that remain vulnerable to the same vishing technique; (3) document Salesforce Connected App OAuth scopes active during the breach window before any revocation, capturing what data permissions were delegatable via a single SSO token.

Recovery — Validate that no unauthorized OAuth tokens or API keys were issued to external applications during the compromise window. Rotate all Salesforce Connected App credentials and Okta API tokens provisioned within the suspect timeframe. Confirm phishing-resistant MFA enrollment for 100% of IdP users before restoring full SaaS access. Monitor Salesforce and IdP logs at elevated frequency for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore Okta and Salesforce to a verified-clean state, confirm FIDO2 enrollment completeness, and establish elevated monitoring to detect any persistence mechanisms left by ShinyHunters during the compromise window

Controls: NIST IR-4 (Incident Handling) — execute the recovery phase of the incident handling lifecycle including system restoration and verification, NIST IA-3 (Device Identification and Authentication) — validate that all Okta API tokens and Salesforce Connected App credentials issued during the breach window are rotated and re-authorized only to verified applications, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of Salesforce Connected App configurations and Okta application assignments to confirm no unauthorized integrations were added during the breach, NIST AU-11 (Audit Record Retention) — ensure Okta System Log and Salesforce Event Log Files for the full compromise window are preserved and retained before log rotation could purge them, CIS 7.2 (Establish

and Maintain a Remediation Process) — follow documented remediation process to verify token rotation completeness and confirm no residual ShinyHunters access paths remain, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — audit all Okta service accounts and Salesforce integration user accounts to confirm none were created or modified during the compromise window

Compensating: Without automated token lifecycle tooling: query Okta API for all active API tokens — GET /api/v1/api-tokens — and revoke any created between the breach start date and eradication completion: DELETE /api/v1/api-tokens/{id}. For Salesforce: navigate to Setup > Connected Apps OAuth Usage, sort by 'Last Used Date', and identify any Connected App that had token activity during the breach window; revoke via 'Revoke All Tokens' for each suspect app. Verify FIDO2 enrollment completeness with: GET /api/v1/users?filter=status+eq+%22ACTIVE%22 piped through a factor-type check script, producing a CSV of any user still missing a FIDO2 factor — block their Okta sessions until enrollment is confirmed.

Evidence: BEFORE restoring full SaaS access: (1) Okta System Log entries for 'system.api_token.create' events during the compromise window — any API token created by the compromised session represents a persistence backdoor that survives password reset; (2) Salesforce Setup Audit Trail entries for 'Connected App' and 'Remote Site Settings' changes during the breach window — ShinyHunters may have registered a new Connected App to maintain OAuth access independently of the SSO session; (3) Salesforce Event Log Files for EventType = 'InstalledPackage' or 'SetupAudit' showing any new package installations or permission set grants made during the compromise window; (4) Okta application assignment logs for any new app-to-user assignments made under the compromised session that would persist after session revocation.

Post-Incident — Conduct a SaaS blast radius analysis: map every application connected to your IdP and document what data each can access with a valid SSO session. Implement Okta or Entra ID Conditional Access policies restricting SaaS access to managed, compliant devices. Establish vishing-specific awareness training emphasizing that no internal helpdesk or vendor will ask for SSO credentials or MFA codes verbally. Review break-glass account procedures to ensure emergency admin access does not bypass phishing-resistant MFA requirements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned analysis to close the architectural gap that allowed a single vished Okta credential to expose 10M Salesforce records, and to harden against the ShinyHunters SSO-chaining technique for future campaigns

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to include SaaS blast radius analysis as a standard post-incident deliverable, NIST IR-8 (Incident Response Plan) — revise IR plan to incorporate vishing as an explicit attack vector with Okta SSO-chaining as a scenario, informed by this ADT breach pattern, NIST RA-3 (Risk Assessment) — document the SaaS blast radius map as a risk assessment artifact identifying the aggregate data exposure risk from a single compromised IdP credential, NIST AC-20 (Use of External Systems) — enforce Conditional Access device compliance requirements as a control on external SaaS access via Okta, NIST AT-2 (Literacy Training and Awareness) — implement vishing-specific training module addressing the ShinyHunters social engineering pattern: caller impersonation, urgency tactics, and verbal MFA code harvesting, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — include Okta Conditional Access and device trust policies in the secure configuration baseline, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — integrate SaaS IdP configuration review (authentication policies, connected app scopes, legacy protocol status) into recurring vulnerability management cadence

Compensating: For blast radius analysis without commercial SaaS discovery tooling: query Okta API for all active application integrations — GET /api/v1/apps?filter=status+eq+%22ACTIVE%22 — and for each app, retrieve assigned groups and users — GET /api/v1/apps/{id}/users. Map each app to its data classification using the app's OAuth scopes (visible in the app's 'Sign On' tab) to estimate exposure tier. For device trust without Okta Device Trust licensing: implement Okta Sign-On Policy network zone restrictions (Security > Networks) to limit SSO access to corporate IP ranges as a compensating control while device trust is deployed. For vishing training on zero budget: use CISA's free phishing guidance (CISA Phishing Guidance, September 2023) and build a tabletop exercise scenario directly modeled on the ShinyHunters ADT vishing call pattern — caller claims to be IT helpdesk, requests Okta password and SMS OTP to 'verify identity before a system migration.'

Evidence: For lessons-learned documentation: (1) Okta System Log export for the full breach window preserved in immutable storage (S3 with Object Lock, or equivalent) before Okta's default 90-day log retention window expires — this is the primary forensic record of the ShinyHunters session chain; (2) the SaaS blast radius map produced during this step, documenting which Salesforce objects and fields were accessible via the OAuth scopes granted to the compromised session — quantifies the maximum possible exfiltration scope for regulatory breach notification purposes; (3) Okta Authentication Policy configuration snapshot (pre- and post-remediation) documenting the specific policy gap (SMS/TOTP permitted) that enabled the attack — required for any regulatory or cyber insurance disclosure; (4) Salesforce Data Export logs and Report Export event log entries from the breach window establishing the actual records accessed versus the theoretical maximum, to bound the notification population for state breach notification law compliance.

Detection Guidance

IdP log queries (Okta System Log): filter for 'user.session.start' events where 'authenticationContext.credentialType' is not 'FIDO2' or 'HardwareProtectedKey'; cross-reference with subsequent 'app.oauth2.token.grant' events to Salesforce or other connected SaaS apps within the same session. Flag any session where a new device fingerprint or unrecognized IP authenticated successfully. Salesforce: audit Setup > Login History for logins tied to SSO that accessed Reports, Data Export, or bulk API endpoints (e.g., Bulk API 2.0 job creation events in the Event Log File). Behavioral indicators: a single user account accessing multiple connected SaaS applications in rapid succession after an IdP login, particularly outside normal working hours or from an IP not associated with corporate egress. No confirmed public IOCs (IPs, domains, hashes) have been released for this incident as of the latest available public disclosures. Do not treat absence of IOCs as absence of risk, this attack pattern relies on legitimate credentials, not malware.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none confirmed`	No public IOCs have been released for this incident as of April 2026. ShinyHunters operations rely on legitimate credentials rather than persistent malware infrastructure, which limits traditional IOC-based detection utility.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1598.004** — Spearphishing Voice
- **T1566.004** — Spearphishing Voice
- **T1537** — Transfer Data to Cloud Account
- **T1550.001** — Application Access Token
- **T1213** — Data from Information Repositories

- **T1078.004** — Cloud Accounts
- **T1539** — Steal Web Session Cookie
- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1598.004	Spearphishing Voice	Reconnaissance
T1566.004	Spearphishing Voice	Initial-Access
T1537	Transfer Data to Cloud Account	Exfiltration
T1550.001	Application Access Token	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1078.004	Cloud Accounts	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/adt-confirms-data-br...	T3
ADT confirms data breach after ShinyHunters leak threat	https://techloghub.com/blog/adt-confirms-data-breach-after-shinyhun...	T3
Okta SSO Accounts Targeted by Sophisticated Vishing ... - Rescana	https://www.rescana.com/post/okta-sso-accounts-targeted-by-sophisti...	T3
Okta SSO accounts targeted in vishing-based data theft attacks	https://www.bleepingcomputer.com/news/security/okta-sso-accounts-ta...	T3
Reco Security Labs: Okta Authentication Vulnerability	https://www.reco.ai/blog/okta-authentication-vulnerability-highligh...	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-25 06:50 UTC by TJS Security Command Center