INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:11 UTC

Cloud Security's Measurement Problem: Why 94% Breach Rates Persist Despite Growing Investment

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0323
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Multi-cloud enterprise environments (AWS, Azure, Google Cloud); organizations using cloud workload protection platforms broadly; CrowdStrike Falcon Cloud Security referenced as survey sponsor
Discovery Source	Rss:T1 Threatintel

Executive Summary

A CrowdStrike-commissioned survey reports that 94% of enterprise organizations experienced cloud intrusions resulting in data exposure or exfiltration, with 73% unable to consistently detect cloud-based threats, findings that, if directionally accurate, describe a systemic detection failure across multi-cloud environments. The survey identifies three converging failure patterns: coverage gaps in workload visibility, alert fatigue consuming the majority of triage capacity, and tool fragmentation slowing containment. These findings align with a reported 37% year-over-year increase in cloud-conscious intrusions attributed to CrowdStrike's 2026 Global Threat Report, though all specific statistics originate from a single vendor-commissioned source and have not been independently corroborated; treat all figures as vendor-reported data pending independent validation.

Technical Analysis

The CrowdStrike State of CDR survey, conducted among enterprise security teams, identifies cloud detection and response as a discipline lagging significantly behind cloud adoption. Three structural failure modes are described.

First, workload visibility gaps: organizations operating across AWS, Azure, and Google Cloud report incomplete sensor or agent coverage across cloud workloads, leaving portions of the attack surface unmonitored. MITRE ATT&CK techniques T1580 (Cloud Infrastructure Discovery), T1526 (Cloud Service Discovery), and T1619 (Cloud Storage Object Discovery) map directly to the adversarial reconnaissance that exploits these blind spots,

attackers enumerate what defenders cannot see.

Second, alert fatigue: the survey reports approximately 77% of analyst triage time consumed by false positives. This is a documented operational problem across the industry, not unique to cloud environments, but the cloud context amplifies it because cloud telemetry volumes and ephemeral workload churn generate signal noise at scale that on-premises tooling was not designed to handle.

Third, tool fragmentation: disconnected point solutions delay containment. When detection occurs in one platform and response requires action in another, the handoff introduces latency. Against threat actors executing cloud-conscious intrusions, a term CrowdStrike uses to describe adversaries who understand and exploit cloud-native permission models and APIs, containment delays translate directly to expanded blast radius.

The 37% year-over-year increase in cloud-conscious intrusions is attributed to CrowdStrike's 2026 Global Threat Report. Threat actor categories named are eCrime adversaries and state-nexus actors, no specific named groups or APT designations are attributed in the source material. Techniques T1078 (Valid Accounts), T1087.004 (Account Discovery: Cloud Account), T1530 (Data from Cloud Storage), T1190 (Exploit Public-Facing Application), and T1110 (Brute Force) represent the access and collection patterns most associated with cloud intrusion campaigns in the broader threat intelligence record.

Important source caveat: all specific statistics in this story, 94%, 73%, 77%, 37%, originate from CrowdStrike-owned content. The survey was commissioned by CrowdStrike, and all five source URLs resolve to CrowdStrike blog properties. No independent third-party corroboration of these figures was identified in the provided source set. The directional finding, that cloud detection coverage is materially incomplete across the enterprise market, is well-supported by corroborating industry patterns, but the specific figures should be treated as vendor-reported data pending independent validation.

Action Checklist

1. Step 1: Assess coverage, inventory all cloud workloads across AWS, Azure, and Google Cloud and verify that detection tooling (EDR/CDR agents, API-based monitoring) covers each workload type; document gaps explicitly rather than assuming coverage
2. Step 2: Audit cloud account visibility, cross-reference your cloud account inventory against your identity provider; unknown or unmonitored accounts map directly to T1078 (Valid Accounts) and T1087.004 (Cloud Account Discovery) exposure; apply NIST AC-2 (Account Management) and CIS 5.1 (Establish and Maintain an Inventory of Accounts)
3. Step 3: Reduce false positive load, review detection rule tuning for cloud workloads; alert fatigue at scale is an operational control failure; prioritize high-fidelity detections for T1530 (Data from Cloud Storage), bulk downloads, unusual geographic access, and T1190 (Exploit Public-Facing Application), scanning patterns, error-rate spikes; reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for cadence and scope
4. Step 4: Enforce least privilege on cloud IAM, review and tighten cloud IAM role assignments; apply NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts); adversaries exploiting T1562.001 (Impair Defenses: Disable or Modify Tools) frequently require elevated permissions acquired through over-provisioned roles
5. Step 5: Require MFA on all cloud management interfaces, externally exposed cloud consoles and APIs are primary entry points for T1110 (Brute Force) and T1078 (Valid Accounts) campaigns; enforce per CIS

6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access); apply D3-MFA countermeasure

6. Step 6: Map tool handoff latency, document the detection-to-containment workflow across your cloud security stack; identify where platform boundaries introduce manual steps; consolidation or integration at these boundaries directly addresses the tool fragmentation failure mode described in the survey

7. Step 7: Update threat model, add cloud-conscious intrusion patterns (cloud API abuse, storage enumeration, IAM privilege escalation) to your threat register, referencing eCrime and state-nexus actor categories per the CrowdStrike 2026 Global Threat Report; note these are aggregate categories, not named groups

8. Step 8: Brief leadership, present cloud detection gap findings to CISO and relevant business stakeholders with specific coverage metrics from your own environment, not vendor survey figures; frame around data exposure risk tied to T1530 (Data from Cloud Storage) given direct revenue and regulatory implications

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal if Step 2 account audit reveals IAM principals with no IdP match that have made data-plane API calls (s3:GetObject, storage.objects.get, blob read) against sensitive buckets or storage accounts within the prior 90-day CloudTrail/Activity Log window, as this constitutes probable unauthorized data access triggering breach notification assessment under GDPR Article 33, HIPAA §164.412, or applicable state privacy statutes.
Recovery Notes	After IAM tightening (Step 4) and MFA enforcement (Step 5), verify recovery by running a full CloudTrail and Azure Activity Log review for the 24 hours post-enforcement to confirm no residual non-MFA console authentications and no API calls from roles whose permissions were revoked — unexpected continued activity indicates a missed identity or a persisted access key that must be rotated before the environment is considered contained. Monitor cloud storage access logs (S3 Server Access Logging, Azure Blob Storage diagnostic logs, GCP Cloud Storage audit logs) for anomalous bulk-read patterns for a minimum of 30 days post-remediation, as adversaries who achieved pre-remediation access may have staged data for delayed exfiltration. Validate that all detection gaps documented in Step 1 have been closed by re-running the workload inventory cross-reference against active log feeds and confirming zero-gap coverage before returning affected cloud environments to normal operational status.

Forensic Artifacts	AWS CloudTrail management and data-plane event logs (S3:GetObject, AssumeRole, ConsoleLogin, CreateAccessKey) for the prior 90 days — the primary source for reconstructing cloud API abuse and IAM privilege escalation chains in multi-cloud intrusions of this type | Azure Active Directory Sign-In Logs and Azure Activity Log filtered for OAuth token issuance events, role assignment changes, and storage account access operations — required to identify Valid Accounts abuse and lateral movement between Azure services | GCP Cloud Audit Logs (Admin Activity and Data Access logs) for IAM policy changes, service account key creation, and Cloud Storage object list/read operations — key artifacts for detecting storage enumeration and over-provisioned service account exploitation | Cloud provider IAM credential reports (AWS `aws iam get-credential-report`, Azure AD `az ad user list` with lastSignInDateTime, GCP service account key age via `gcloud iam service-accounts keys list`) — establish which credentials existed, when they were last used, and whether any were created by an adversary during the intrusion window | Cloud storage server-access logs for S3 (enabled separately from CloudTrail), Azure Blob diagnostic logs, and GCP Cloud Storage data access audit logs — these capture individual object-level GET/LIST operations that CloudTrail management logs may not fully record, and are the definitive source for confirming or ruling out data exfiltration consistent with T1530 (Data from Cloud Storage)

Per-Action IR Details

Step 1: Assess coverage — inventory all cloud workloads across AWS, Azure, and Google Cloud and verify that detection tooling (EDR/CDR agents, API-based monitoring) covers each workload type; document gaps explicitly rather than assuming coverage

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability, tools, and visibility prerequisites before incidents occur

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Run AWS CLI `aws ec2 describe-instances --query 'Reservations[*].Instances[*].[InstanceId,Tags]'`, Azure CLI `az vm list --output table`, and GCP `gcloud compute instances list` to enumerate workloads; cross-reference against osquery `SELECT * FROM running_services` on reachable hosts; document each workload's monitoring status in a spreadsheet, flagging any without an active EDR/CDR agent or API log feed.

Evidence: Before acting on gaps, capture current CloudTrail, Azure Activity Log, and GCP Audit Log exports for the prior 90 days — these establish a baseline of what has and has not been logged; gaps in log continuity are themselves forensic evidence of unmonitored windows during which cloud intrusions (matching the 94% survey finding) may have occurred without detection.

Step 2: Audit cloud account visibility — cross-reference your cloud account inventory against your identity provider; unknown or unmonitored accounts map directly to T1078 (Valid Accounts) and T1087.004 (Cloud Account Discovery) exposure; apply NIST AC-2 (Account Management) and CIS 5.1 (Establish and Maintain an Inventory of Accounts)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Identify indicators of compromise through log and identity correlation

Controls: NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: In AWS, run `aws iam get-credential-report` and `aws iam list-users` to export all IAM users and last-activity timestamps; in Azure, use `az ad user list --output table` and cross-reference against Azure AD Sign-In Logs filtered for accounts with no sign-in in 45+ days; in GCP, use `gcloud iam service-accounts list`; compare all three outputs against your authoritative IdP user list (Okta, AD) and flag any account present in cloud but absent in IdP as a

Valid Account exposure risk.

Evidence: Before disabling or removing any suspicious account, capture: AWS CloudTrail `LookupEvents` filtered for the account's IAM principal to document all API calls made; Azure AD Sign-In Logs for the account's authentication history including IP, user-agent, and MFA status; GCP Cloud Audit Logs for the service account's resource access history — these are volatile in the sense that account deletion destroys the association between identity and activity.

Step 3: Reduce false positive load — review detection rule tuning for cloud workloads; alert fatigue at scale is an operational control failure; prioritize high-fidelity detections for T1530 (Data from Cloud Storage) and T1190 (Exploit Public-Facing Application); reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for cadence and scope

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Tune detection capability and establish sustainable triage processes before incidents occur

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging)

Compensating: Deploy Sigma rules mapped to cloud storage enumeration (e.g., rules detecting `s3:ListBuckets`, `s3:GetObject` in bulk, or Azure Blob `List` operations from anomalous principals); use `grep` or `jq` against exported CloudTrail JSON to baseline normal GetObject rates per principal, then set threshold alerts manually; suppress rules generating more than 20 false positives per analyst per shift and document the suppression rationale — alert fatigue is identified in this survey as the primary reason 73% of organizations miss cloud threats.

Evidence: No live-state alteration occurs in this step; capture current alert volume metrics and false-positive rates per rule before tuning to establish a pre/post baseline — this documents the operational control failure for post-incident review and regulatory reporting if a breach is later confirmed.

Step 4: Enforce least privilege on cloud IAM — review and tighten cloud IAM role assignments; apply NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts); adversaries exploiting T1562.001 (Impair Defenses: Disable or Modify Tools) frequently require elevated permissions acquired through over-provisioned roles

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Reduce attacker capability and limit blast radius by restricting privilege pathways

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use AWS IAM Access Analyzer to export unused permissions per role (`aws accessanalyzer list-findings`) and generate a least-privilege policy recommendation; in Azure, use the Azure AD Access Review feature or `az role assignment list --all` to identify accounts with Owner/Contributor at subscription scope without justification; in GCP, run `gcloud projects get-iam-policy` and flag any principal with `roles/owner` or `roles/editor` not tied to a break-glass account.

Evidence: Before revoking or modifying any IAM role or policy, capture: the current full IAM policy document (`aws iam get-policy-version`, `az role definition show`, `gcloud iam roles describe`) and all recent API calls made under that role via CloudTrail/Activity Log for the prior 30 days — role revocation on a compromised identity destroys the attacker's access but also the live session artifacts showing what they did; capture active sessions via `aws iam list-roles --query` and note any assumed-role sessions still active.

Step 5: Require MFA on all cloud management interfaces — externally exposed cloud consoles and APIs are primary entry points for T1110 (Brute Force) and T1078 (Valid Accounts) campaigns; enforce per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access); apply D3-MFA countermeasure

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Implement controls that deny adversary re-entry and reduce active exposure surface

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-17 (Remote Access)

Compensating: In AWS, enforce MFA via IAM policy condition `aws:MultiFactorAuthPresent: true` on all console and sensitive API actions; use AWS Config rule `mfa-enabled-for-iam-console-access` (free, built-in) to continuously audit compliance; in Azure, enable Conditional Access policies requiring MFA for all users accessing the Azure portal — for teams without Azure AD P1/P2, use Security Defaults as a free baseline; in GCP, enforce MFA through Google Workspace organizational policy `requireTotpMfaEnrollment`.

Evidence: Before enforcing MFA policies that will terminate existing non-MFA sessions, capture: AWS CloudTrail `ConsoleLogin` events for the prior 30 days filtered for `additionalEventData.MFAUsed: No` to identify accounts that have authenticated without MFA — these represent the exact Valid Accounts and Brute Force exposure described in the survey; also capture Azure AD Sign-In Logs filtered for `authenticationRequirement: singleFactorAuthentication` to document the pre-enforcement exposure window.

Step 6: Map tool handoff latency — document the detection-to-containment workflow across your cloud security stack; identify where platform boundaries introduce manual steps; consolidation or integration at these boundaries directly addresses the tool fragmentation failure mode described in the survey

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Document IR workflows and identify process gaps that degrade response time

Compensating: Conduct a tabletop walkthrough of a simulated cloud storage exfiltration (S3 bucket mass-download by an anomalous IAM principal): time each handoff from CloudTrail alert → SIEM ingestion → analyst triage → containment action; document each manual step and its average latency; for teams without a SIEM, use AWS EventBridge + Lambda or Azure Logic Apps (both free-tier eligible) to automate the alert-to-ticket creation step and reduce the first manual handoff.

Evidence: No volatile live-state alteration in this step; preserve the current workflow documentation and any prior incident tickets as a baseline showing pre-improvement detection-to-containment times — this directly supports the post-incident lessons learned phase (NIST 800-61r3 §4) and quantifies the tool fragmentation impact identified in the survey.

Step 7: Update threat model — add cloud-conscious intrusion patterns (cloud API abuse, storage enumeration, IAM privilege escalation) to your threat register, referencing eCrime and state-nexus actor categories per the CrowdStrike 2026 Global Threat Report; note these are aggregate categories, not named groups

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Use lessons learned and threat intelligence to improve detection and update risk posture

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Update your threat register (even a spreadsheet) to include the three cloud-specific attack patterns from this survey — workload coverage gaps exploited for initial access, IAM over-provisioning enabling privilege escalation, and storage enumeration for data exfiltration; map each to the MITRE ATT&CK Cloud matrix tactics (Initial Access, Privilege Escalation, Exfiltration) in your documentation as narrative context, not as controls; subscribe to CISA Known Exploited Vulnerabilities catalog RSS feed and CrowdStrike Adversary Intelligence free tier for ongoing eCrime and state-nexus actor updates relevant to multi-cloud environments.

Evidence: No live-state alteration; before finalizing threat model updates, export your current detection coverage map (which rules exist, which ATT&CK techniques they address) to document the pre-update gap — this establishes an auditable record showing when your organization became aware of cloud-specific intrusion patterns and what actions were taken, which is relevant to regulatory breach notification timelines if a prior undetected intrusion is later discovered.

Step 8: Brief leadership — present cloud detection gap findings to CISO and relevant business stakeholders with specific coverage metrics from your own environment, not vendor survey figures; frame around data

exposure risk tied to T1530 (Data from Cloud Storage) given direct revenue and regulatory implications

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Communicate findings, drive investment decisions, and improve organizational risk posture through leadership engagement

Controls: NIST AC-1 (Policy And Procedures)

Compensating: Prepare a one-page coverage metric report using data from Steps 1–3: number of unmonitored workloads (raw count and percentage), number of accounts without MFA (from Step 5 evidence captures), and alert false-positive rate before tuning (from Step 3); translate data exposure risk into regulatory language — GDPR Article 33 (72-hour breach notification), HIPAA §164.412 (breach notification), or applicable state privacy law — to frame the detection gap as a compliance liability rather than a purely technical gap; use your own environment's numbers, not the 94%/73% survey figures.

Evidence: No volatile live-state alteration; the evidence for this step is the aggregated output from Steps 1–7 — coverage gap documentation, account audit results, MFA compliance data, and workflow latency measurements — compiled before the leadership briefing to ensure metrics reflect the environment's actual state at a specific point in time rather than a shifting operational baseline.

Detection Guidance

No specific IOCs (hashes, IPs, domains) were published in the provided source material for this story. Detection focus should be behavioral and architectural.

Cloud account and identity telemetry: Monitor for T1087.004 (Cloud Account Discovery), enumeration of IAM roles, service accounts, and permission boundaries via cloud-native APIs (AWS IAM list-*, Azure Graph API queries, GCP IAM list calls). Anomalous enumeration volume or enumeration by non-automated identities warrants triage. Apply NIST AU-2 (Event Logging) to ensure these API calls are captured in CloudTrail, Azure Monitor, or GCP Audit Logs.

Storage access patterns: Hunt for T1530 (Data from Cloud Storage), bulk GET or download operations against S3 buckets, Azure Blob Storage, or GCP Cloud Storage by identities that do not routinely access those objects. Time-of-day anomalies and geographic outliers in storage access logs are productive hunt hypotheses. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for review cadence.

Defense impairment: Alert on T1562.001 (Impair Defenses: Disable or Modify Tools), API calls that disable logging (e.g., CloudTrail StopLogging, Azure Diagnostic Settings deletion, GCP Log Sink deletion). These are high-fidelity indicators of active adversary presence and should trigger immediate escalation. Apply D3-SFA (System File Analysis) principles to configuration and logging state monitoring.

Cloud service discovery: Monitor for T1526 (Cloud Service Discovery) and T1538 (Cloud Service Dashboard), unusual queries to cloud management APIs enumerating running services, regions, or resource inventories by non-infrastructure identities.

Public-facing application access: Review WAF and load balancer logs for T1190 (Exploit Public-Facing Application) patterns, scanning, error-rate spikes, and unusual request patterns against externally exposed cloud workloads.

Account hardening gaps to audit: Verify that all cloud IAM accounts comply with CIS 5.2 (Use Unique Passwords) and CIS 5.3 (Disable Dormant Accounts, accounts inactive beyond 45 days). Dormant cloud service accounts are a persistent and frequently exploited access vector.

D3FEND countermeasures applicable to this threat profile: D3-UAP (User Account Permissions), D3-CRO (Credential Rotation), D3-LAM (Local Account Monitoring extended to cloud account monitoring), D3-MFA

(Multi-factor Authentication).

Framework Mappings

MITRE-ATTACK

- **T1087.004** — Cloud Account
- **T1526** — Cloud Service Discovery
- **T1562.001** — Disable or Modify Tools
- **T1580** — Cloud Infrastructure Discovery
- **T1538** — Cloud Service Dashboard
- **T1619** — Cloud Storage Object Discovery
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1190** — Exploit Public-Facing Application
- **T1110** — Brute Force

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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-7** — Unsuccessful Logon Attempts
- **AC-3** — Access Enforcement
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1087.004	Cloud Account	Discovery
T1526	Cloud Service Discovery	Discovery
T1562.001	Disable or Modify Tools	Defense-Evasion
T1580	Cloud Infrastructure Discovery	Discovery
T1538	Cloud Service Dashboard	Discovery
T1619	Cloud Storage Object Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T1110	Brute Force	Credential-Access

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-state-of-cdr-sur...	T1
CrowdStrike	https://www.crowdstrike.com/en-us/blog/crowdstrike-expands-real-tim...	T1
CrowdStrike	https://www.crowdstrike.com/en-us/blog/key-findings-crowdstrike-202...	T1
CrowdStrike	https://www.crowdstrike.com/en-us/blog/crowdstrike-named-leader-202...	T1
What's New in Falcon Cloud Security - CrowdStrike	https://www.crowdstrike.com/en-us/blog/new-in-falcon-cloud-security...	T1

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 2026-07-06 15:11 UTC by TJS Security Command Center