INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 14:02 UTC

Cloud Breach Reality Check: Industry Data Reveals Detection and Response Gaps Across 94% of Organizations

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0246
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cloud environments broadly (multi-cloud and hybrid); enterprise security operations teams
Discovery Source	Rss:T1 Threatintel

Executive Summary

A CrowdStrike-sponsored survey of enterprise security teams finds that 94% of organizations have suffered cloud intrusions resulting in data exposure or exfiltration, pointing to systemic failure across the industry rather than isolated incidents. Three structural breakdowns drive this figure: insufficient telemetry coverage across cloud environments, alert volumes that overwhelm triage capacity, and fragmented tooling that creates blind spots between cloud workload protection and SOC workflows. The findings signal that cloud adoption has outpaced the detection and response infrastructure organizations built to protect it, and the gap is actively being exploited.

Technical Analysis

The survey data, while sponsored by CrowdStrike and carrying the vendor bias that entails, describes failure patterns consistent with independent guidance from NIST SP 800-53 control families AU (audit and accountability) and SI (system and information integrity), as well as CISA cloud security advisories. The three structural failure modes map cleanly to known weaknesses in enterprise cloud security programs.

The first failure mode, visibility gaps in cloud telemetry, reflects endemic problems with logging coverage across multi-cloud and hybrid environments. Organizations routinely lack unified audit log pipelines across IaaS, PaaS, and SaaS layers, leaving detection engineering teams without the event data needed to build effective detection rules. MITRE ATT&CK techniques T1619 (Cloud Storage Object Discovery), T1580 (Cloud Infrastructure Discovery), and T1613 (Container and Resource Discovery) describe adversary reconnaissance that succeeds precisely when this telemetry is absent.

The second failure mode, alert overload causing triage inefficiency, is a consequence of both the scale of cloud environments and the misconfigured or over-permissive alerting policies common in CSPM deployments. When SOC analysts receive thousands of low-fidelity alerts daily, genuinely malicious activity embedded in the noise misses detection. This directly enables techniques like T1078 (Valid Accounts) and T1078.004 (Cloud Accounts), where adversaries operating through legitimate credentials generate activity that blends with normal user behavior. Prolonged mean-time-to-detect figures in the survey are a direct output of this dynamic.

The third failure mode, fragmented tooling, creates seams between cloud workload protection platforms, CSPM tools, and SOC SIEM and SOAR workflows. When these systems do not share context, analysts cannot correlate a cloud misconfiguration event with a subsequent access event and an exfiltration attempt. Techniques T1537 (Transfer Data to Cloud Account) and T1530 (Data from Cloud Storage) represent the exfiltration end of kill chains that were likely detectable earlier if telemetry integration existed.

The CWE mappings reinforce this chain: CWE-284 (improper access control) enables initial intrusion through misconfigured IAM or over-permissive roles; CWE-778 (insufficient logging) ensures the intrusion proceeds undetected; and CWE-200 (exposure of sensitive information) captures the outcome when exfiltration completes. Technique T1552.005 (Cloud Instance Metadata API) and T1562.008 (Impair Defenses: Disable Cloud Logs) show adversaries actively harvesting cloud credentials and suppressing logging to extend their dwell time. T1190 (Exploit Public-Facing Application) represents a common initial access vector into cloud-hosted workloads.

The vendor interest in these findings warrants scrutiny. CrowdStrike sells Cloud Detection and Response tooling, and survey-derived statistics are a well-established marketing instrument. However, the structural issues described are independently corroborated. NIST SP 800-53 Rev. 5 AU and SI control deficiencies in cloud environments are a recurring finding in federal assessments, and CISA has issued multiple advisories specifically addressing cloud logging gaps and misconfigurations. The 94% figure should be read as directionally credible but not treated as a precise population statistic.

Action Checklist

1. Step 1: Assess cloud telemetry coverage, audit which cloud services, accounts, and regions are generating logs, and identify gaps where no logging pipeline exists. Cross-reference against NIST AU-2 (Event Logging) requirements and verify that log collection covers IaaS control plane, workload runtime, and data access events.
2. Step 2: Audit cloud logging configurations for adversarial tampering or suppression, check for disabled CloudTrail trails, suppressed audit logs, or missing log sink configurations consistent with T1562.008 (Impair Defenses: Disable Cloud Logs). Align with NIST AU-9 (Protection of Audit Information) to ensure logs are write-protected and stored outside the environment being monitored.
3. Step 3: Review IAM and access control posture, enumerate over-permissive roles, unused high-privilege accounts, and cloud instance metadata API exposure consistent with T1078, T1078.004, and T1552.005. Apply NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to reduce the attack surface available to adversaries using valid credentials.
4. Step 4: Evaluate alert triage capacity and CSPM integration, measure current alert volume against analyst capacity, identify rules generating high false-positive rates, and assess whether CSPM findings are correlated with SIEM events. Apply NIST SI-4 (System Monitoring) principles to prioritize signal-to-noise improvements over raw alert volume.

5. Step 5: Map detection coverage to cloud ATT&CK techniques, run a gap analysis against T1580, T1619, T1613, T1537, T1530, and T1190 to determine which techniques have no active detection rule. Document gaps as accepted risk or assign remediation owners with target dates.

6. Step 6: Communicate findings to leadership, brief CISOs and relevant business unit leaders on the specific cloud services, accounts, and data types with no telemetry coverage, framed as concrete business risk rather than a generic cloud security concern.

7. Step 7: Monitor for follow-on guidance, track CISA cloud security advisories and NIST SP 800-53 implementation guidance updates for cloud-specific control enhancements. If CrowdStrike publishes the full CDR survey report, review it for additional operational metrics, but apply the same vendor-bias scrutiny to any statistics or product recommendations.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if Steps 1-2 reveal active CloudTrail suppression, unexplained IAM privilege escalation events, or confirmed data-plane access to sensitive S3 buckets or cloud databases without corresponding business-justified access records — any of these conditions indicates an in-progress or completed breach requiring breach notification assessment under GDPR Article 33, HIPAA §164.412, or applicable state privacy law.
Recovery Notes	After telemetry gaps are remediated and IAM posture is hardened, re-run the full CloudTrail and CSPM audit cycle against all accounts and regions to confirm logging is active and tamper-protected before declaring the environment stable. Establish a 90-day enhanced monitoring period during which CloudWatch alarms are configured for all IAM privilege escalation events, CloudTrail configuration changes, and S3 bucket policy modifications, with alerts routed directly to the SOC queue rather than standard ticketing. Retain all CloudTrail logs, VPC Flow Logs, and CSPM findings from the incident assessment period for a minimum of 12 months to support any delayed regulatory inquiry or cyber insurance claim.
Forensic Artifacts	CloudTrail management event logs filtered for StopLogging, DeleteTrail, UpdateTrail, and PutEventSelectors API calls — these are the primary indicators of adversarial log suppression preceding data access or exfiltration in cloud intrusions of this type | AWS IAM credential report and STS AssumeRole history for the 90 days preceding the audit — persistent valid credential abuse (T1078.004) leaves no malware artifacts and is recoverable only from these logs before credentials are rotated | S3 server access logs and CloudTrail data-plane events (GetObject, PutObject, DeleteObject) for buckets containing sensitive data — exfiltration via T1530 (Data from Cloud Storage) produces access patterns with anomalous source IPs, unusual access volumes, or access from non-standard IAM principals | VPC Flow Logs for unusual egress to non-organizational IP ranges correlated with S3 presigned URL generation events — T1537 (Transfer Data to Cloud Account) often involves staging data to adversary-controlled cloud storage, producing large outbound flows to AWS, GCP, or Azure IP ranges not in the organization's own footprint | EC2 instance metadata service (IMDS) access logs from application-level logging (where IMDSv2 is not enforced) or CloudTrail `ec2:GetInstanceMetadataToken` events — credential theft via SSRF to the metadata API (T1552.005) is recoverable only from these sources before the instance is terminated or reimaged

Per-Action IR Details

Step 1: Assess cloud telemetry coverage — audit which cloud services, accounts, and regions are generating logs, and identify gaps where no logging pipeline exists. Cross-reference against NIST AU-2 (Event Logging) requirements and verify that log collection covers IaaS control plane, workload runtime, and data access events.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing logging and monitoring infrastructure prior to incident detection

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a SIEM: use AWS CLI `aws cloudtrail describe-trails --include-shadow-trails` and `aws cloudtrail get-trail-status` across all regions to enumerate disabled or misconfigured trails; use `aws config get-compliance-summary-by-config-rule` to surface Config rules not reporting. For GCP, run `gcloud logging sinks list --project=PROJECT_ID` to identify projects with no export sink. Pipe results to a CSV and diff against your asset inventory to identify gaps. A two-person team can execute this across a mid-size environment in one shift using a simple bash loop over account/project lists.

Evidence: This is a preparation/audit step that does not alter live system state. No volatile capture is required before execution. However, document the current state of all CloudTrail trail configurations (trail ARNs, S3 bucket targets, multi-region status, log file validation enabled/disabled) and GCP/Azure equivalent log sink configurations before making any changes, so the pre-audit baseline is preserved as a forensic reference if a concurrent intrusion is later discovered.

Step 2: Audit cloud logging configurations for adversarial tampering or suppression — check for disabled CloudTrail trails, suppressed audit logs, or missing log sink configurations consistent with T1562.008 (Impair Defenses: Disable Cloud Logs). Align with NIST AU-9 (Protection of Audit Information) to ensure logs are write-protected and stored outside the environment being monitored.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Identifying indicators of adversarial log suppression as precursors to or evidence of active intrusion

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without a SIEM, query CloudTrail management events directly: `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=StopLogging --region us-east-1` repeated across all regions. Also query for `DeleteTrail`, `UpdateTrail`, `PutEventSelectors` (narrowing event selectors is a soft suppression technique), and `DeleteBucket` against the CloudTrail S3 target. For GCP, run `gcloud logging logs list` and compare against expected audit log categories. Cross-reference IAM event history for `iam.serviceAccounts.actAs` grants made within 24 hours of any log suppression event — this pairing is a high-confidence indicator of adversarial access.

Evidence: Before making any configuration changes to re-enable logging: capture the current trail status output (`aws cloudtrail get-trail-status --name TRAIL_NAME`) and the raw CloudTrail management event history for the 30-day window prior to audit (export via `aws cloudtrail lookup-events` or S3 bucket copy). Preserve S3 access logs for the CloudTrail bucket itself to determine whether logs were exfiltrated or deleted before suppression. These artifacts establish the adversary's timeline and whether a gap in log coverage was exploited to conceal lateral movement or data access events.

Step 3: Review IAM and access control posture — enumerate over-permissive roles, unused high-privilege accounts, and cloud instance metadata API exposure consistent with T1078, T1078.004, and T1552.005. Apply NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to reduce the attack surface available to adversaries using valid credentials.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Enumerating valid credential abuse indicators and over-permissive access as preconditions for cloud intrusion

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Use AWS IAM Access Analyzer (`aws accessanalyzer list-findings`) to surface roles with external or cross-account trust. Run `aws iam generate-credential-report` and parse LastUsedDate for all keys older than 90 days with no use — these are candidate compromised-but-quiet credentials. For IMDS exposure, query `aws ec2 describe-instances` filtering on `MetadataOptions.HttpTokens=optional` (IMDSv1 enabled) — these instances are vulnerable to SSRF-to-metadata credential theft. A two-person team can script this enumeration in Python using boto3 and produce a risk-ranked spreadsheet in one shift.

Evidence: This step involves reviewing but not yet revoking credentials, so live credential state is still intact. Before any subsequent revocation action: export the full CloudTrail event history for `AssumeRole`, `GetSessionToken`, `sts:AssumeRoleWithWebIdentity`, and `ec2:GetInstanceMetadataToken` for the past 90 days to establish a baseline of legitimate vs. anomalous credential use. Capture currently active STS sessions via `aws sts get-caller-identity` from all federated and assumed-role contexts before any rotation, as active session tokens will be invalidated and unrecoverable after revocation.

Step 4: Evaluate alert triage capacity and CSPM integration — measure current alert volume against analyst capacity, identify rules generating high false-positive rates, and assess whether CSPM findings are correlated with SIEM events. Apply NIST SI-4 (System Monitoring) principles to prioritize signal-to-noise improvements over raw alert volume.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Building sustainable detection and triage capacity as a prerequisite for effective cloud incident response

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

Compensating: Without a commercial SIEM or CSPM, deploy Sigma rules mapped to cloud ATT&CK techniques against CloudTrail logs ingested into an open-source stack (OpenSearch or Elastic SIEM free tier). Use the SigmaHQ cloud ruleset (`pySigma` with the AWS backend) to convert Sigma rules directly to CloudWatch Insights queries at no cost. For CSPM gap coverage, run Prowler (`prowler aws --compliance nist_800_53_revision_5`) which produces finding-level output with NIST control mappings — a two-person team can integrate this into a weekly cron job and review findings in a shared spreadsheet to simulate CSPM triage without a commercial tool.

Evidence: This step does not alter live system state. Before tuning or disabling any detection rules, export the current alert history (minimum 30 days) from the SIEM or CSPM in raw form, including rule name, triggering event, disposition (true positive / false positive / no action), and analyst handling time. This baseline documents pre-tuning detection state and is required if a post-incident review later questions whether a suppressed rule would have caught an active intrusion.

Step 5: Map detection coverage to cloud ATT&CK techniques — run a gap analysis against T1580, T1619, T1613, T1537, T1530, and T1190 to determine which techniques have no active detection rule. Document gaps as accepted risk or assign remediation owners with target dates.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Systematic detection engineering to ensure coverage of known cloud adversary techniques before incidents occur

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Use the MITRE ATT&CK Navigator (free, browser-based) to load the Cloud matrix and color-code techniques by detection status. For each uncovered technique, search the SigmaHQ repository for existing community rules (e.g., `aws_cloudtrail_resource_discovery.yml` for T1580 cloud infrastructure discovery, `aws_s3_data_exfiltration.yml` for T1537/T1530). Convert applicable Sigma rules to CloudWatch Insights queries using pySigma and deploy via CloudFormation or a simple CLI script. A two-person team can complete a gap analysis and deploy initial compensating rules for the six named techniques in two to three days using these free resources.

Evidence: This is a planning and engineering step that does not alter live system state. Document the pre-gap-analysis detection inventory as a dated artifact — including rule names, last-modified dates, and mapped

techniques — so that a future post-incident review can determine whether a gap that allowed an intrusion was known, accepted, or unidentified at the time of the incident. This record is critical for regulatory and insurance purposes if a breach later occurs through an undocumented coverage gap.

Step 6: Communicate findings to leadership — brief CISOs and relevant business unit leaders on the specific cloud services, accounts, and data types with no telemetry coverage, framed as concrete business risk rather than a generic cloud security concern.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Translating technical findings into organizational risk communication and driving structural improvements based on lessons learned

Controls: NIST AC-1 (Policy And Procedures)

Compensating: For teams without a formal GRC platform, produce a one-page risk register in a shared spreadsheet: columns for cloud service, account/project ID, data classification of assets in that environment, current telemetry status (covered / partial / blind), and estimated business impact if that environment is breached without detection. Tie each blind spot to a concrete dollar or regulatory exposure (e.g., 'S3 bucket X contains customer PII with no CloudTrail data-plane logging — a breach here triggers GDPR Article 33 72-hour notification'). This framing converts a technical audit finding into a board-level risk decision.

Evidence: No live system state is altered by this step. Ensure that all supporting evidence used in the leadership brief — telemetry gap reports, IAM findings, CloudTrail configuration exports — has been preserved as immutable artifacts (e.g., exported to a read-only S3 bucket with Object Lock enabled or an offline storage location) before the brief, in case the brief triggers an investigation or regulatory inquiry that requires documentation of the security posture at a specific point in time.

Step 7: Monitor for follow-on guidance — track CISA cloud security advisories and NIST SP 800-53 implementation guidance updates for cloud-specific control enhancements, and watch for CrowdStrike's full CDR survey report publication for additional operational metrics.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Integrating external threat intelligence and updated guidance into ongoing security posture improvement

Controls: NIST AU-13 (Monitoring For Information Disclosure)

Compensating: Subscribe to CISA advisories via the free CISA email notification service (us-cert.cisa.gov/forms/email-registration) and RSS feed. For NIST publication updates, monitor the NIST Computer Security Resource Center publications feed (csrc.nist.gov/publications/search). Create a free RSS aggregator workflow (e.g., using n8n self-hosted or a simple Python feedparser cron job) that filters for keywords 'cloud,' 'AWS,' 'Azure,' 'GCP,' 'IAM,' and 'CloudTrail' and delivers a daily digest to a team email or Slack channel — executable by a two-person team with no licensing cost.

Evidence: This step does not alter live system state and requires no volatile evidence capture. Maintain a timestamped log of advisory publications reviewed and actions taken in response — this constitutes the organization's documented threat intelligence consumption record and supports audit evidence for NIST AU-6 (Audit Record Review, Analysis, and Reporting) compliance.

Detection Guidance

Detection focus for this threat pattern should concentrate on three behavioral clusters drawn directly from the MITRE techniques referenced.

Cloud reconnaissance: Hunt for API calls consistent with T1580 (Cloud Infrastructure Discovery), T1619 (Cloud Storage Object Discovery), and T1613 (Container and Resource Discovery). Specifically, look for high-volume or automated Describe*, List*, and Get* API calls in AWS CloudTrail, Azure Activity Log, or GCP Audit Logs originating from identities that do not normally perform infrastructure enumeration. Unusual enumeration from

service accounts or from identities that authenticated for the first time from an unfamiliar IP or geography warrants immediate investigation.

Credential abuse and metadata API access: Alert on access to cloud instance metadata endpoints (169.254.169.254 or equivalent) from processes or identities outside expected operational baselines, consistent with T1552.005. Flag authentication events matching T1078 and T1078.004 where a valid account is used outside normal working hours, from an unrecognized source IP, or following a failed MFA challenge. NIST AU-2 and AU-6 controls require logging and reviewing exactly these event types.

Log suppression activity: Per T1562.008, alert on any API call that disables, deletes, or modifies audit trail configurations, log sinks, or diagnostic settings. In AWS, watch for StopLogging, DeleteTrail, or PutEventSelectors calls that reduce scope. In Azure, watch for deletion of diagnostic settings or modification of Log Analytics workspace retention policies. These should be treated as high-priority alerts, not low-fidelity noise, per NIST AU-9.

Exfiltration patterns: For T1537 (Transfer Data to Cloud Account) and T1530 (Data from Cloud Storage), baseline normal data egress volumes per bucket, container, or storage account, then alert on deviations. Look for GetObject or equivalent calls at volumes inconsistent with application behavior, particularly where the destination account or IP is external or newly observed. Cross-reference with CIS 8.2 (Collect Audit Logs) to verify storage access logging is enabled on all buckets and containers.

Log gap auditing: Periodically query your SIEM for cloud accounts, regions, or services generating no log data. Absence of logs is itself a detection signal. Map gaps against CIS 1.1 (Enterprise Asset Inventory) to ensure all cloud assets are represented in the logging pipeline.

Framework Mappings

MITRE-ATTACK

- **T1580** — Cloud Infrastructure Discovery
- **T1619** — Cloud Storage Object Discovery
- **T1613** — Container and Resource Discovery
- **T1078** — Valid Accounts
- **T1552.005** — Cloud Instance Metadata API
- **T1190** — Exploit Public-Facing Application
- **T1537** — Transfer Data to Cloud Account
- **T1078.004** — Cloud Accounts
- **T1562.008** — Disable or Modify Cloud Logs
- **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
- **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-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SI-4** — System Monitoring

OWASP-TOP10-2021

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

HIPAA-SECURITY

- **164.312(a)(1)** — 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
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **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
T1580	Cloud Infrastructure Discovery	Discovery
T1619	Cloud Storage Object Discovery	Discovery
T1613	Container and Resource Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1552.005	Cloud Instance Metadata API	Credential-Access

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1537	Transfer Data to Cloud Account	Exfiltration
T1078.004	Cloud Accounts	Defense-Evasion
T1562.008	Disable or Modify Cloud Logs	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-state-of-cdr-sur...	T3
CrowdStrike Falcon® Cloud Security: Modern Security From Code to ...	https://www.crowdstrike.com/en-us/platform/cloud-security/	T3
CrowdStrike Falcon Cloud Security Adds Application Context to ...	https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-cloud-sec...	T3
Protect AI Development with Falcon Cloud Security | CrowdStrike	https://www.crowdstrike.com/en-us/blog/protect-ai-development-with-...	T3
Falcon Cloud Security - Proactive Security - YouTube	https://www.youtube.com/watch?v=Eo_EGl7VKfo	T3

Generated 2026-06-22 14:02 UTC by TJS Security Command Center