

AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Audit Appendix: Evidence by Finding

Week 2 of 6: Audit (appendix) · prepared for Tidepost, Inc.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

January 15, 2026 · AWS Security, Compliance & Governance Audit: The Hardening (six weeks)

SAMPLE DELIVERABLE

This is a sample deliverable. Tidepost, Inc. is a fictional company: its people, products, users, accounts, investors, and figures are invented for this sample, and any resemblance to a real company, person, product, or publication is coincidental. AWS prices are list prices from the AWS Price List API retrieved on October 13, 2026, and from the public AWS Price List bulk API on October 18, 2026.

Contents

How to use this appendix	3
Critical findings	4
C-1: Root user with two active access keys and no MFA	4
C-2: tp-media-originals public-read, and location metadata on 61% of images	5
C-3: tp-exports public with listing on: 104,318 user records	5
C-4: RDS PostgreSQL publicly accessible from 0.0.0.0/0	6
C-5: OpenSearch domain with a public endpoint and an open access policy	6
C-6: Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	7
C-7: Seven IAM users with administrator access and long-lived keys, two of them departed	8
C-8: Database password and a third-party API key in the repository and in launch template user data	8
C-9: No CloudTrail trail	9
C-10: A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	10
High findings	10
H-1: RDS and EBS volumes unencrypted at rest	10
H-2: IMDSv1 on every instance	11
H-3: No MFA on any of the 16 IAM users with a console password	11
H-4: SSH open to the internet on 18 instances	12
H-5: Account-level S3 Block Public Access off	12
H-6: GuardDuty, Inspector, and Security Hub off in both Regions	13
H-7: Redis without AUTH, TLS, or automatic backups	13
H-8: SageMaker notebooks with direct internet access and root access	14
H-9: EKS endpoint public, with every developer mapped to cluster administrator	14
H-10: No web application firewall on the two public load balancers	14
H-11: Two customer-managed KMS keys whose policies allow any identity in the account	15
H-12: No deletion pipeline for removed posts' media	15
H-13: Moderation Lambda functions share one execution role with s3:* and sagemaker:*	16
H-14: CI on 400-day-old access keys instead of OIDC federation	16
Medium findings	17
M-1: No VPC flow logs	17
M-2: The default security group allows all traffic between members, and 9 instances use it	17
M-3: Secrets in the environment variables of 9 Lambda functions	17

M-4: AWS Config not recording in either Region	18
M-5: 11 buckets accept requests over plain HTTP	18
M-6: 14 buckets use SSE-S3 where the data class needs customer-managed keys	19
M-7: Server access logging off on 7 buckets	19
M-8: 11 access keys unused for more than 90 days	19
M-9: No IAM Access Analyzer.....	20
M-10: SageMaker endpoints and training jobs without customer-managed volume keys	20
M-11: No alarms on root sign-in, unauthorized API calls, or IAM changes, and PostgreSQL logs not exported	20
M-12: Public IPv4 addresses on 14 private-tier instances	21
M-13: CloudFront accepts TLS 1.0 from viewers	21
M-14: Four vendor cross-account roles without an external ID	22
M-15: Session Manager sessions not logged	22
Low findings	22
L-1: 41 unused security groups, 18 with blank descriptions.....	22
L-2: Three DNS records point at released Elastic IP addresses.....	23
L-3: Billing and operations alternate contacts are the founders' personal addresses	23
L-4: Bucket names disclose internal project names.....	23
L-5: Two public ECR repositories	24
L-6: Two unused IAM roles trust an account no one at Tidepost can identify	24
L-7: No DMARC policy on the company domain	24
L-8: Deletion protection off on 6 DynamoDB tables	25

How to use this appendix

This appendix is the evidence behind the audit report's findings register. The audit report says what is wrong, who can reach it, what to do, and by when. This document holds the rest: for each of the 47 findings, under the same ID, what was read, how, and what it showed, with the checks that failed, the SOC 2 criteria the finding touches, and where the plan stands on January 15, 2026.

- **Find a finding by its ID.** The findings are in the register's order within each severity: 10 Critical, 14 High, 15 Medium, and 8 Low.
- **"Read-only through the SecurityAudit and ViewOnlyAccess managed policies"** means the audit role described in the week-one scan. It reads configuration and cannot change anything or read stored data.

- **Requests from outside the account** are the few places a finding needed proof that an exposure is real. Each was one request, nothing was kept beyond a count or a status code, and none used the audit role. The week-one scan lists them.
- **The checks** are controls from the scan. Each shows the failed resources at week one, on January 5, 2026. A finding with no check was found by reading configuration or code that no control covers.
- **Status** is where the finding stood on January 15, 2026, and the plan lists the dated steps still to come. The audit report explains the four states and who closes what.

Critical findings

10 Critical findings.

C-1: Root user with two active access keys and no MFA

Critical. Root user of tp-prod. **Owner:** Kofi Brandvold. **SOC 2:** CC6.1. **Status on January 15:** In progress; next January 29.

What was read

- iam get-account-summary (AccountAccessKeysPresent 2, AccountMFAEnabled 0) and the credential report, read-only through the SecurityAudit and ViewOnlyAccess managed policies
- one key sits in a GitHub Actions secret and one in a deploy script on the CTO's laptop

What the checks showed: IAM. 4 (IAM root user access key should not exist) failed on 2 resources; IAM. 6 (Hardware MFA should be enabled for the root user) failed on 1 resource; IAM. 9 (MFA should be enabled for the root user) failed on 1 resource.

Who can reach it: One stolen credential or one application bug. **What they do:** Uses either root access key, from the GitHub Actions secret or the deploy script on a laptop. **What they reach:** Everything in the account, with no policy able to limit it, including billing and closing the account.

Plan

- Done January 6, Tidepost on notice: Both root access keys deleted after the pipeline and the script moved to roles; two FIDO2 keys registered
- Planned January 29, Foundation: Root credentials removed from the member account under centralized root access after the January 28 join; root tasks run through sts:AssumeRoot

C-2: tp-media-originals public-read, and location metadata on 61% of images

Critical. S3 bucket tp-media-originals. **Owner:** Amara Delacroix. **SOC 2:** CC6.6. **Status on January 15:** Closed January 14.

What was read

- s3 get-bucket-policy-status (IsPublic true) and an unauthenticated HEAD request on 20 sampled keys
- EXIF GPS tags read on a random sample of 1,000 image objects, 610 of them carrying coordinates
- nothing was copied out of the bucket

What the checks showed: S3.2 (S3 buckets should prohibit public read access) failed on 2 resources; S3.8 (S3 buckets should have block public access settings enabled) failed on 17 resources.

Who can reach it: Anyone on the internet. **What they do:** Lists and downloads originals from the public bucket with no credentials. **What they reach:** Every original upload, and on 61% of images the GPS coordinates of where the contributor stood (9.8 million originals).

Plan

- Done January 6, Tidepost on notice: Block Public Access turned on and CloudFront origin access control put in front of the bucket; originals answer only a short-lived signed URL from the API, and every other reader gets renditions
- Done January 14, Hardening: Location metadata stripped from 9,800,000 image originals by an S3 Batch Operations job that ran January 7 to 14

C-3: tp-exports public with listing on: 104,318 user records

Critical. S3 bucket tp-exports. **Owner:** Lior Haddad. **Status on January 15:** Closed January 6.

What was read

- Unauthenticated list-objects-v2 returned the key list
- the file's line count (104,318 data rows) came from a streamed read and no record was kept or printed
- the bucket has no server access logging

What the checks showed: S3.2 (S3 buckets should prohibit public read access) failed on 2 resources.

Who can reach it: Anyone on the internet. **What they do:** Lists the bucket with no credentials and downloads the export. **What they reach:** The 104,318 user records in the marketing export.

Plan

- Done January 6, Tidepost on notice: Closed within the hour; the CSV deleted after counsel copied it. With no access logs, exposure could not be ruled out; counsel was told, and the decision on notification is Tidepost's (Vantalect records only that counsel was told)

C-4: RDS PostgreSQL publicly accessible from 0.0.0.0/0

Critical. RDS for PostgreSQL 13 production writer. **Owner:** Kofi Brandvold. **SOC 2:** CC6.6. **Status on January 15:** Acceptance proposed, to March 22.

What was read

- rds describe-db-instances (PubliclyAccessible true) and the security group (5432 from 0.0.0.0/0), read-only through the SecurityAudit and ViewOnlyAccess managed policies
- a TCP handshake from outside the account reached the listener and no login was attempted

What the checks showed: RDS . 2 (RDS DB instances should prohibit public access) failed on 2 resources.

Who can reach it: One stolen credential or one application bug. **What they do:** Connects to the database listener from anywhere and tries the password, which C-8 had left in the repository.

What they reach: The production database: every user, post, and moderation record.

Proposed written acceptance, to be signed by Dev Raman: PubliclyAccessible stays true until the new encrypted private instance replaces this one at the March 22 cutover; until then the security group admits only the BI vendor's four published ranges and TLS is required.

Plan

- Done January 7, Hardening: Security group restricted to the BI vendor's four published ranges and TLS required; the staging copy's security group restricted the same day

C-5: OpenSearch domain with a public endpoint and an open access policy

Critical. OpenSearch domain tp-search (2.13). **Owner:** Marcus Oyelaran. **SOC 2:** CC6.6. **Status on January 15:** Planned January 21.

What was read

- opensearch describe-domain (no VPCOptions)

- access policy Principal * with es:*), read-only through the SecurityAudit and ViewOnlyAccess managed policies
- an unauthenticated GET / returned the cluster banner and no index was read

What the checks showed: 0pensearch.2 (OpenSearch domains should not be publicly accessible) failed on 1 resource.

Who can reach it: Anyone on the internet. **What they do:** Sends requests to the open search endpoint; the access policy allows every action to every caller. **What they reach:** Read, change, or delete of every search index.

Plan

- Planned January 21, Hardening: Domain moved into the VPC with fine-grained access control and a restrictive access policy

C-6: Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess

Critical. Link-preview service on the web tier. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.3. **Status on January 15:** Closed January 8.

What was read

- Static review of the link-preview handler (no URL allowlist, follows redirects) and of the instance profile (AdministratorAccess attached)
- IMDS HttpTokens optional on the tier. No exploit was run

What the checks showed: IAM. 1 (IAM policies should not allow full '*' administrative privileges) failed on 4 resources.

Who can reach it: One stolen credential or one application bug. **What they do:** Gives the link-preview service a URL that reaches the instance metadata service and takes the role's temporary credentials. **What they reach:** Administrator access to the whole account, with the keys of an instance role.

Plan

- Done January 8, Hardening: Allowlisted egress proxy and URL validation added; IMDSv2 required on the tier; the role cut to 14 actions

C-7: Seven IAM users with administrator access and long-lived keys, two of them departed

Critical. Seven IAM users in tp-prod. **Owner:** Sasha Ilyin. **SOC 2:** CC6.2. **Status on January 15:** In progress; next January 26.

What was read

- The credential report and list-attached-user-policies, read-only through the SecurityAudit and ViewOnlyAccess managed policies
- the two departed users' keys were last used between 60 and 140 days earlier (HR roster compared by Sasha Ilyin)

What the checks showed: IAM. 1 (IAM policies should not allow full '*' administrative privileges) failed on 4 resources; IAM. 2 (IAM users should not have IAM policies attached) failed on 16 resources.

Who can reach it: One stolen credential or one application bug. **What they do:** Uses a long-lived administrator key, including the keys of the two people who had left. **What they reach:** Administrator access, and the keys never expire.

Plan

- Done January 6, Tidepost on notice: The two departed users' passwords and keys deleted, and the users with them
- Planned January 26, Hardening: The 14 current staff provisioned into IAM Identity Center over SCIM, by group (Identity Center connected January 23)
- Planned January 28, Hardening: Permission sets assigned to tp-prod the day it joined the organization: the 5 remaining administrators and the 9 other people with console access sign in through Identity Center
- Planned February 10, Foundation: The five IAM users deleted after the policy set that denies new IAM users and keys reached Prod on February 5

C-8: Database password and a third-party API key in the repository and in launch template user data

Critical. The backend repository and launch template versions. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.1. **Status on January 15:** Closed January 9.

What was read

- A secret-pattern scan of the default branch and 90 days of history, and describe-launch-template-versions user data
- matches were counted and no value was printed

What the checks showed: nothing; no control in the 50 covers it.

Who can reach it: A foothold inside the account. **What they do:** Reads the repository or a launch template's user data, as any engineer or contractor with access can. **What they reach:** The production database password and a third-party API key.

Plan

- Done January 9, Hardening: Both secrets rotated into Secrets Manager and read at runtime, and user data cleaned; the history rewrite was declined because rotation closes the exposure

C-9: No CloudTrail trail

Critical. CloudTrail in tp-prod. **Owner:** Sasha Ilyin. **SOC 2:** CC7.1. **Status on January 15:** In progress; next January 28.

What was read

- cloudtrail describe-trails returned none and lookup-events reaches only 90 days of management events, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: CloudTrail.1 (CloudTrail should be enabled and configured with at least one multi-Region trail) failed on 1 resource; CloudTrail.2 (CloudTrail should have encryption at rest enabled) failed on 1 resource; CloudTrail.4 (CloudTrail log file validation should be enabled) failed on 1 resource.

Who can reach it: Not an entry point: it removes the evidence. **What they do:** Nothing: it is the missing record. **What they reach:** A compromise through any other finding would leave no trail past the 90 days of management events AWS keeps.

Plan

- Done January 6, Hardening: An account trail created, multi-Region, writing to a locked bucket
- Planned January 28, Foundation: Replaced by the organization trail into tp-log-archive when the account joined

C-10: A forgotten g5.12xlarge with SSH open and a Jupyter server without a token

Critical. EC2 instance (g5.12xlarge) in tp-prod. **Owner:** Yuki Sorensen. **Status on January 15:** Closed January 6.

What was read

- ec2 describe-instances (running since September 2025)
- security group open to 0.0.0.0/0 on 22 and 8888), read-only through the SecurityAudit and ViewOnlyAccess managed policies
- a status-code request to the Jupyter API returned 200 with no token

What the checks showed: EC2 . 13 (Security groups should not allow ingress from 0.0.0.0/0 to port 22) failed on 6 resources; EC2 . 19 (Security groups should not allow unrestricted access to high-risk ports) failed on 3 resources.

Who can reach it: Anyone on the internet. **What they do:** Runs code on a GPU server through the Jupyter server, which asks for no token, with SSH also open. **What they reach:** Four GPUs to mine on, and whatever the instance's role and network can reach.

Plan

- Done January 6, Tidepost on notice: Snapshotted for the record and terminated. No indicators in its shell history, processes, or packages; with no flow logs, compromise could not be ruled out, and counsel was told. The cost engagement does not count this instance

High findings

14 High findings.

H-1: RDS and EBS volumes unencrypted at rest

High. RDS production writer and 58 of 61 EBS volumes. **Owner:** Kofi Brandvold. **Status on January 15:** Deferral proposed, to March 22.

What was read

- rds describe-db-instances (StorageEncrypted false), ec2 describe-volumes (Encrypted false on 58 of 61), and get-ebs-encryption-by-default (false), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: RDS. 3 (RDS DB instances should have encryption at rest enabled) failed on 2 resources; EC2. 7 (EBS default encryption should be enabled) failed on 2 resources.

Proposed dated deferral, to be signed by Dev Raman: the production database cannot be encrypted in place; the new encrypted PostgreSQL 16 instance replaces it at the March 22 cutover.

Plan

- Planned January 21, Hardening: EBS default encryption turned on in both Regions
- Planned January 27, Hardening: The staging copy of the database re-created from an encrypted snapshot copy
- Planned February 10, Hardening: The last unencrypted volumes replaced as node groups and instances rotated

H-2: IMDSv1 on every instance

High. 52 EC2 instances and their launch templates. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 22.

What was read

- ec2 describe-instances (HttpTokens optional on 52 of 52), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: EC2. 8 (EC2 instances should use IMDSv2) failed on 52 resources.

Plan

- Planned January 22, Hardening: HttpTokens required on every instance and launch template; a declarative policy in the Foundation's policy set keeps it that way

H-3: No MFA on any of the 16 IAM users with a console password

High. 16 IAM users. **Owner:** Sasha Ilyin. **Status on January 15:** Closed January 13.

What was read

- The credential report (mfa_active false for all 16), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: IAM. 5 (MFA should be enabled for all IAM users that have a console password) failed on 16 resources.

Plan

- Done January 13, Hardening: A policy condition requiring MFA applied to every console user; the remaining users' IAM identities were replaced by Identity Center sign-in on January 28, when the permission sets reached tp-prod

H-4: SSH open to the internet on 18 instances

High. 6 security groups covering 18 instances. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 14.

What was read

- ec2 describe-security-groups (port 22 from 0.0.0.0/0 in 6 groups), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: EC2. 13 (Security groups should not allow ingress from 0.0.0.0/0 to port 22) failed on 6 resources.

Plan

- Done January 14, Hardening: Port 22 rules removed from all six groups; shell access through SSM Session Manager

H-5: Account-level S3 Block Public Access off

High. S3 account settings in tp-prod. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 6.

What was read

- s3control get-public-access-block (no configuration), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: S3. 1 (S3 general purpose buckets should have account-level block public access settings enabled) failed on 1 resource.

Plan

- Done January 6, Tidepost on notice: Account-level Block Public Access turned on in the same sitting as C-2; app versions older than 4.2, which read the originals bucket on its S3 address, were sent to the update prompt that afternoon (C-2)

H-6: GuardDuty, Inspector, and Security Hub off in both Regions

High. Detection services in tp-prod. **Owner:** Sasha Ilyin. **SOC 2:** CC6.8, CC7.2. **Status on January 15:** Planned January 29.

What was read

- guardduty list-detectors, inspector2 batch-get-account-status, and securityhub describe-hub (all empty), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: GuardDuty.1 (GuardDuty should be enabled) failed on 2 resources; SecurityHub.1 (Security Hub CSPM should be enabled) failed on 2 resources; Inspector.1 (Amazon Inspector EC2 scanning should be enabled) failed on 2 resources.

Plan

- Planned January 29, Hardening: GuardDuty (with runtime monitoring on EKS), Inspector, and Security Hub enabled, delegated to tp-audit

H-7: Redis without AUTH, TLS, or automatic backups

High. ElastiCache Redis OSS 7.1 replication group. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.6. **Status on January 15:** Planned January 27.

What was read

- elasticache describe-replication-groups (TransitEncryptionEnabled false, AuthTokenEnabled false, SnapshotRetentionLimit 0), read-only through the SecurityAudit and ViewOnlyAccess managed policies
- AUTH is a manual check, because the scan's AUTH control covers only Redis versions before 6.0

What the checks showed: ElastiCache.1 (ElastiCache (Redis OSS) clusters should have automatic backups enabled) failed on 1 resource; ElastiCache.5 (ElastiCache replication groups should be encrypted in transit) failed on 1 resource.

Plan

- Planned January 27, Hardening: Replication group rebuilt with in-transit encryption, an AUTH token read from Secrets Manager, and a daily automatic backup

H-8: SageMaker notebooks with direct internet access and root access

High. 6 SageMaker notebook instances. **Owner:** Yuki Sorensen. **Status on January 15:** Planned February 4.

What was read

- sagemaker describe-notebook-instance (DirectInternetAccess Enabled, RootAccess Enabled on all six), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: SageMaker . 1 (SageMaker notebook instances should not have direct internet access) failed on 6 resources.

Plan

- Planned February 4, Hardening: Notebooks moved to VPC-only access with root disabled by a lifecycle configuration

H-9: EKS endpoint public, with every developer mapped to cluster administrator

High. 3 EKS clusters (production, staging, development). **Owner:** Kofi Brandvold. **SOC 2:** CC6.3. **Status on January 15:** Planned January 30.

What was read

- eks describe-cluster (endpointPublicAccess true, 0.0.0.0/0) and the aws-auth ConfigMap read through the audit role (all 15 engineers in system:masters)

What the checks showed: EKS . 1 (EKS cluster endpoints should not be publicly accessible) failed on 3 resources.

Plan

- Planned January 30, Hardening: Endpoints made private on all three clusters; developers moved to EKS access entries with namespace-scoped roles

H-10: No web application firewall on the two public load balancers

High. 2 Application Load Balancers. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.6. **Status on January 15:** Planned February 4.

What was read

- elbv2 describe-load-balancers and wafv2 list-web-acls (no association), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: ELB. 16 (Application Load Balancers should be associated with an AWS WAF web ACL) failed on 2 resources.

Plan

- Planned February 4, Hardening: AWS WAF web ACL with the managed rule groups and a rate limit associated with both

H-11: Two customer-managed KMS keys whose policies allow any identity in the account

High. 2 KMS keys. **Owner:** Sasha Ilyin. **Status on January 15:** Planned January 23.

What was read

- kms get-key-policy (kms:* to the account root principal, so IAM policy alone grants access), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 23, Hardening: Both key policies rewritten with named key administrators and per-service grants

H-12: No deletion pipeline for removed posts' media

High. Originals, renditions, and backups of removed posts. **Owner:** Marcus Oyelaran. **SOC 2:** C1.2. **Status on January 15:** Deferral proposed, to May 20.

What was read

- A sample of 40 posts removed in the last 60 days: all 40 still had objects in the originals bucket and the renditions bucket
- the delete-post path in the API code has no media step
- read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Proposed dated deferral, to be signed by Sasha Ilyin: the app team cannot ship the deletion pipeline before the retention schedule exists, and the schedule waits on counsel. The risk that remains until then: a removed post's renditions still load through the distribution for anyone who kept their address, and its original for anyone holding a signed URL issued before the removal, until that URL expires.

H-13: Moderation Lambda functions share one execution role with s3:* and sagemaker:*

High. 11 Lambda functions, one execution role. **Owner:** Amara Delacroix. **SOC 2:** CC6.3. **Status on January 15:** Planned February 9.

What was read

- lambda list-functions grouped by Role, and iam get-role-policy, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 9, Hardening: One role per function, each limited to its own buckets and endpoints

H-14: CI on 400-day-old access keys instead of OIDC federation

High. The CI IAM user and its 2 access keys. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 20.

What was read

- The credential report (the CI user's 2 keys, 391 and 412 days old) and the repository's workflow files, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: IAM.3 (IAM users' access keys should be rotated every 90 days or less) failed on 16 resources.

Plan

- Planned January 20, Hardening: GitHub Actions moved to OIDC federation with a deploy role per repository; the CI user and both its keys deleted

Medium findings

15 Medium findings.

M-1: No VPC flow logs

Medium. The production VPC. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 15.

What was read

- ec2 describe-flow-logs (none), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: EC2 . 6 (VPC flow logging should be enabled in all VPCs) failed on 1 resource.

Plan

- Done January 15, Hardening: Flow logs turned on for the VPC and kept 90 days

M-2: The default security group allows all traffic between members, and 9 instances use it

Medium. The VPC's default security group. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 22.

What was read

- ec2 describe-security-groups and describe-instances, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: EC2 . 2 (VPC default security groups should not allow inbound or outbound traffic) failed on 1 resource.

Plan

- Planned January 22, Hardening: The nine instances moved to purpose-built groups and the default group emptied

M-3: Secrets in the environment variables of 9 Lambda functions

Medium. 9 Lambda functions. **Owner:** Marcus Oyelaran. **Status on January 15:** Planned February 2.

What was read

- lambda get-function-configuration (names matching key, secret, token, or password values not printed), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 2, Hardening: Values moved to Secrets Manager and read at start-up

M-4: AWS Config not recording in either Region

Medium. AWS Config in tp-prod. **Owner:** Sasha Ilyin. **SOC 2:** CC7.1. **Status on January 15:** Planned January 29.

What was read

- configservice describe-configuration-records (none), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: Config. 1 (AWS Config should be enabled and use the service-linked role for resource recording) failed on 2 resources.

Plan

- Planned January 29, Hardening: Config recording turned on in tp-prod with the aggregator delegated to tp-audit

M-5: 11 buckets accept requests over plain HTTP

Medium. 11 S3 buckets. **Owner:** Kofi Brandvold. **SOC 2:** CC6.7. **Status on January 15:** Planned January 30.

What was read

- s3 get-bucket-policy (no aws:SecureTransport condition), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: S3.5 (S3 buckets should require requests to use TLS) failed on 11 resources.

Plan

- Planned January 30, Hardening: A TLS-only deny statement added to all 11 buckets

M-6: 14 buckets use SSE-S3 where the data class needs customer-managed keys

Medium. 14 S3 buckets. **Owner:** Lior Haddad. **Status on January 15:** Planned February 9.

What was read

- s3 get-bucket-encryption (AES256 on 14 buckets holding user data), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 9, Hardening: Default encryption moved to SSE-KMS with a bucket key on all 14

M-7: Server access logging off on 7 buckets

Medium. 7 S3 buckets. **Owner:** Kofi Brandvold. **Status on January 15:** Acceptance proposed, to June 30.

What was read

- s3 get-bucket-logging (empty on 7 of 23 buckets), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: S3.9 (S3 buckets should have server access logging enabled) failed on 7 resources.

Proposed written acceptance, to be signed by Sasha Ilyin: object-level CloudTrail data events cover the two buckets that hold user data, and the other five hold public news media; access logs on the media buckets would be among the largest log volumes in the account.

M-8: 11 access keys unused for more than 90 days

Medium. 11 IAM access keys. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 13.

What was read

- The credential report (access_key_last_used_date), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: IAM.8 (Unused IAM user credentials should be removed) failed on 11 resources.

Plan

- Done January 13, Hardening: All 11 keys deactivated, then deleted after one week of no complaints

M-9: No IAM Access Analyzer

Medium. Access Analyzer in tp-prod. **Owner:** Sasha Ilyin. **Status on January 15:** Planned January 29.

What was read

- accessanalyzer list-analyzers (none), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: IAM. 28 (IAM Access Analyzer external access analyzer should be enabled) failed on 2 resources.

Plan

- Planned January 29, Hardening: External-access analyzers enabled in both Regions, delegated to tp-audit

M-10: SageMaker endpoints and training jobs without customer-managed volume keys

Medium. 5 endpoints and the training job template. **Owner:** Yuki Sorensen. **Status on January 15:** Planned February 6.

What was read

- sagemaker describe-endpoint-config (KmsKeyId absent), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 6, Hardening: Volume keys set on the endpoint configurations and the training template

M-11: No alarms on root sign-in, unauthorized API calls, or IAM changes, and PostgreSQL logs not exported

Medium. CloudWatch and RDS in tp-prod. **Owner:** Kofi Brandvold. **SOC 2:** CC7.2. **Status on January 15:** Planned January 20.

What was read

- cloudwatch describe-alarms and rds describe-db-instances (EnabledCloudwatchLogsExports empty), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: RDS. 9 (RDS DB instances should publish logs to CloudWatch Logs) failed on 2 resources.

Plan

- Planned January 20, Hardening: Metric filters and alarms on the trail's log group, and PostgreSQL logs exported

M-12: Public IPv4 addresses on 14 private-tier instances

Medium. 14 EC2 instances. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 28.

What was read

- ec2 describe-instances (PublicIpAddress set on 14 instances with no public listener), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 28, Hardening: Public addresses released; traffic through the NAT gateway

M-13: CloudFront accepts TLS 1.0 from viewers

Medium. 3 CloudFront distributions. **Owner:** Bea Okafor. **Status on January 15:** Planned January 27.

What was read

- cloudfront get-distribution-config (MinimumProtocolVersion TLSv1), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 27, Hardening: Minimum protocol TLSv1.2_2021 after the release train showed no app version older than TLS 1.2

M-14: Four vendor cross-account roles without an external ID

Medium. 4 IAM roles. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 22.

What was read

- iam get-role (trust policies with no sts:ExternalId condition), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 22, Hardening: External IDs added with each vendor

M-15: Session Manager sessions not logged

Medium. SSM preferences in tp-prod. **Owner:** Kofi Brandvold. **SOC 2:** CC6.6. **Status on January 15:** Planned January 20.

What was read

- ssm get-document SSM-SessionManagerRunShell (no logging destination), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 20, Hardening: Session logs written to CloudWatch Logs and a locked bucket

Low findings

8 Low findings.

L-1: 41 unused security groups, 18 with blank descriptions

Low. 41 security groups. **Owner:** Kofi Brandvold. **Status on January 15:** Planned February 4.

What was read

- ec2 describe-security-groups with describe-network-interfaces, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 4, Hardening: Unused groups deleted; descriptions written on the rest

L-2: Three DNS records point at released Elastic IP addresses

Low. 3 Route 53 records. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 15.

What was read

- route53 list-resource-record-sets compared with ec2 describe-addresses, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Done January 15, Hardening: The three records deleted

L-3: Billing and operations alternate contacts are the founders' personal addresses

Low. Account alternate contacts. **Owner:** Gwen Tallis. **Status on January 15:** Closed January 9.

What was read

- account get-alternate-contact, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Done January 9, Tidepost on notice: Contacts changed to role mailboxes

L-4: Bucket names disclose internal project names

Low. 3 S3 buckets. **Owner:** Kofi Brandvold. **Status on January 15:** Acceptance proposed, to June 30.

What was read

- s3 list-buckets (three names reveal a vendor and a project), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Proposed written acceptance, to be signed by Sasha Ilyin: S3 bucket names cannot be changed in place, and the names disclose nothing that is not already in public contracts.

L-5: Two public ECR repositories

Low. 2 ECR repositories. **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 8.

What was read

- ecr-public describe-repositories, read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Done January 8, Tidepost on notice: Both repositories made private and their images checked for secrets

L-6: Two unused IAM roles trust an account no one at Tidepost can identify

Low. 2 IAM roles. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 20.

What was read

- iam get-role and get-role-last-used (never used)
- trusted account 7XXX not in the vendor list), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 20, Hardening: Both roles deleted

L-7: No DMARC policy on the company domain

Low. Route 53 hosted zone for tidepost.example. **Owner:** Sasha Ilyin. **Status on January 15:** Planned January 22.

What was read

- route53 list-resource-record-sets (no _dmarc TXT record), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned January 22, Hardening: A DMARC record in monitoring mode published, with a later move to enforcement planned by Tidepost

L-8: Deletion protection off on 6 DynamoDB tables

Low. 6 DynamoDB tables. **Owner:** Lior Haddad. **Status on January 15:** Planned February 6.

What was read

- dynamodb describe-table (DeletionProtectionEnabled false), read-only through the SecurityAudit and ViewOnlyAccess managed policies

What the checks showed: nothing; no control in the 50 covers it.

Plan

- Planned February 6, Hardening: Deletion protection turned on for all six

© 2026 Vantalect, LLC. Sample deliverable; Tidepost, Inc. is fictional.

AWS, Amazon Web Services, AWS Graviton, AWS Inferentia, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Kubernetes is a registered trademark of The Linux Foundation. Redis is a registered trademark of Redis Ltd. Valkey is a trademark of the Linux Foundation. OpenSearch is a registered trademark of Amazon.com, Inc. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. CIS Benchmarks is a trademark of the Center for Internet Security, Inc. GitHub is a trademark of GitHub, Inc. Jupyter is a trademark of LF Charities. Vantalect is not affiliated with or endorsed by any of them. Tidepost, Inc. is fictional.