



AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Week-One Scan, Including the Foundation Checks

Week 1 of 6: Scan · prepared for Tidepost, Inc.

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

January 9, 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

- Executive summary** 2
- What we scanned**..... 4
- Access** 5
 - What the role can and cannot do 5
 - What we checked from outside the role 5
 - How the role is deployed 6
- Method** 7
- The score** 8
 - By severity 8
- Failed checks** 10
 - The Critical checks 10
 - The High checks 11
- The Foundation’s checks, run beside the scan** 11
- The inventory** 13
 - The account as found 13
 - Engine versions and their support dates 14
- What Tidepost closed after our call** 15
- What week 2 does** 17
 - What we need from you this week 17
- Appendix: the checks in the score** 18

Executive summary

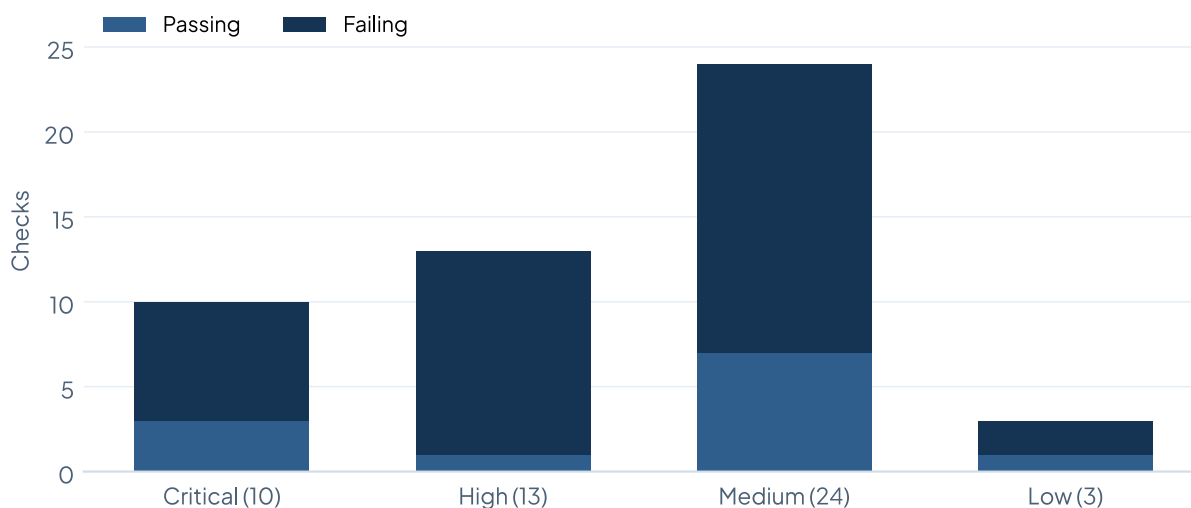
Tidepost’s AWS account passes 12 of the 50 checks in the scan (24.0%), and the other 38 fail on 207 resources. We ran it read-only on January 5, 2026, the first day of the Audit, against the one account Tidepost has, in 2 Regions. We ran the Foundation’s 13 checks (MAF-01 to MAF-13) beside it, and the inventory in this report is the one the Foundation add-on would otherwise have issued on its own.

Four things to take from it:

- 1. 7 of the 10 Critical checks fail.** They are IAM.4, IAM.6, IAM.9, S3.2, RDS.2, Opensearch.2, EC2.19: a root user with access keys and no MFA, public reads on S3, a public database, a public search domain, and administrative ports open to the internet. Tidepost's engineers did not wait for the register. We gave notice on January 6, 2026, and by January 9, 2026 they had closed 4 of the 10 critical findings outright and started 5 more (see [What Tidepost closed after our call](#)).
- 2. The High checks pass 1 of 13.** 52 instances still allow the older instance metadata service, 6 security groups admit the internet on administrative ports, and 3 EKS cluster endpoints are public.
- 3. Nothing is watching.** CloudTrail, AWS Config, GuardDuty, Security Hub CSPM, and Amazon Inspector all fail their first check (CloudTrail.1, Config.1, GuardDuty.1, SecurityHub.1, Inspector.1). A compromise through any other result would leave only the 90 days of management events that AWS keeps without a trail.
- 4. These are raw scan results, not findings.** The register of verified findings is delivered on January 15, 2026, and the readout is January 16, 2026. Do not act on a number here as if it were a verified finding; the exceptions are the 10 critical results we phoned in, which we had already verified by hand.

The Foundation's checks start nearly all red, as they should: with no organization there is nothing to pass. Of the 12 in-scope checks, 1 passes (MAF-13), and only because the operator role it checks for does not exist yet.

Checks by severity, week one



The 50 checks at week one, passing and failing, by severity.

What we scanned

The scan covers **one account and 2 Regions: us-east-1 and us-west-2**. Everything Tidepost runs is in us-east-1; we scanned us-west-2 as well because an unused Region is a place an attacker can start resources that no one is watching.

The scope of the week-one scan.

Item	In scope
Account	The founders' account, opened by the founders in March 2024, its own payer, with no AWS organization. The register calls it tp-prod, its name once it joins the organization
Regions	us-east-1, us-west-2
Standards	CIS AWS Foundations Benchmark v5.0.0 and AWS Foundational Security Best Practices v1.0.0, as implemented by AWS Security Hub CSPM
Checks	50 distinct controls: 27 from CIS and 50 from AWS Foundational Security Best Practices, of which 27 are in both. The full list is in Appendix: the checks in the score
Foundation checks	13, MAF-01 to MAF-13, run beside the scan; 12 are in scope (The Foundation's checks, run beside the scan)
Out of scope	MAF-11 (shared networking: one VPC and no Transit Gateway). What the application stores, and how its code behaves, beyond the one request each C-finding needed to prove itself
Date	January 5, 2026, run from the audit role described below

How the scan runs when Security Hub CSPM is off

AWS Security Hub CSPM is not enabled in this account, so there are no Security Hub results to read. The collector evaluates each control's documented pass or fail condition against the configuration it reads through the audit role, and counts a resource as failed when the condition is not met. The same collector runs again in week six, and nothing is turned on to run it.

Access

We read the account with one role: `vantalect-audit-readonly`. It carries the AWS managed policies **SecurityAudit** and **ViewOnlyAccess** and nothing else. Kofi Brandvold deployed it from a CloudFormation stack on January 5, 2026, and it is the only access Vantalect has.

What the role can and cannot do

The role reads how resources are configured. It cannot create, change, or delete anything, and it cannot read what the systems store.

What the audit role can and cannot do.

The role can	The role cannot
List and describe resources in every service the scan covers: instances, security groups, buckets and their policies, databases, clusters, keys (not their material), roles, and policies	Change any resource, policy, or setting
Read the IAM credential report and account summary: which users have passwords, keys, and MFA, and when each was last used	Read the contents of S3 objects, database rows, or log events
Read key and bucket policies, trust policies, and CloudTrail's configuration and recent event history	Read secret values (Secrets Manager or SecureString parameters), or use a KMS key to decrypt or sign
Read each Lambda function's configuration	Assume any other role, or reach the VPC or the instances

Two of the reads need a deliberate choice on our side. A Lambda function's configuration includes its environment variable values, which can hold secrets, so the collector keeps variable names only and discards the values when it receives them. And the credential report lists people by user name, which we keep in the engagement workspace and delete with the rest of the scan data after the engagement.

What we checked from outside the role

The role cannot read objects, so the 5 critical results that depend on an exposure being real were proved from outside the account, the way an attacker would, with one request each and nothing kept beyond what the table says.

The 5 outside probes. None used the audit role, and none changed anything.

Finding	What we did	What we kept
C-2	A HEAD request on 20 sampled keys, and the EXIF GPS tags read from 1,000 sampled image objects	A count: 610 of 1,000 carried coordinates. No image was copied out of the bucket
C-3	An unauthenticated list of the bucket, and a streamed read to count the export's rows	A count: 104,318 data rows. No record was kept or printed
C-4	A TCP handshake from outside the account to the database listener	Nothing. No login was attempted
C-5	One unauthenticated GET of the search endpoint's root page	The cluster banner. No index was read
C-10	A status-code request to the Jupyter server's API	The status code, 200. No notebook was opened and no code was run

Checked by hand: AUTH on the Redis OSS 7.1 replication group. ElastiCache's describe-replication-groups returned AuthTokenEnabled false, read through the audit role. It is recorded under H-7 because the scan's AUTH control, ElastiCache.6, applies only to Redis versions before 6.0, so no automated check in the 50 tests this group.

How the role is deployed

The role trusts one Vantalect principal, and only when the caller presents an external ID unique to Tidepost, so no one else who learns the role's name can use it.

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Vantalect read-only audit role (SecurityAudit and ViewOnlyAccess). It cannot change anything.
Parameters:
  VantalectAuditPrincipal:
    Type: String
    Description: ARN of the Vantalect audit role that is allowed to assume this role
  ExternalId:
    Type: String
    NoEcho: true
    MinLength: 16
    Description: External ID agreed for this engagement
Resources:
  AuditRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: vantalect-audit-readonly
      MaxSessionDuration: 3600
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
```

```
Statement:
  - Effect: Allow
    Principal:
      AWS: !Ref VantalectAuditPrincipal
    Action: sts:AssumeRole
    Condition:
      StringEquals:
        sts:ExternalId: !Ref ExternalId
ManagedPolicyArns:
  - arn:aws:iam::aws:policy/SecurityAudit
  - arn:aws:iam::aws:policy/job-function/ViewOnlyAccess
```

Tidepost removes the stack when the Audit ends. If anything in this report depends on a permission the role does not have, we say so rather than guess.

Method

A **check** is one control from one of the two standards. A check **fails** when at least one resource it applies to fails its condition, and a **failed resource** is each resource that does. A control on a Regional service setting, such as GuardDuty, Inspector, Config, or EBS default encryption, counts the account once in each Region, which is why such a setting that is off shows as 2 failed resources. A control on a setting that is not Regional counts the account once: S3.1 (the account's Block Public Access) and CloudTrail.1 (one multi-Region trail is enough) each show 1 failed resource. IAM.4 counts each root access key, so the two keys show as 2. Severity is the standard's own rating of the control.

Four things the scan does not do:

- **It does not verify.** A failing check is a reason to look, and a few fail for reasons that are not a risk. The Audit's week two reads every Critical and High result by hand before it becomes a finding.
- **It does not rate exploitability.** Every failure of one severity counts the same here. The register rates how reachable each finding is, and the readout orders them that way.
- **It does not see application behavior.** The link-preview service's request handling (C-6) is a code review, not a check; no control in the 50 covers it.
- **It does not see inside the data.** It cannot tell a public bucket that holds public news from one that holds private records. The outside probes above did that for the buckets that mattered.

The score

The week-one score by standard. A check in both standards is counted once in the last row.

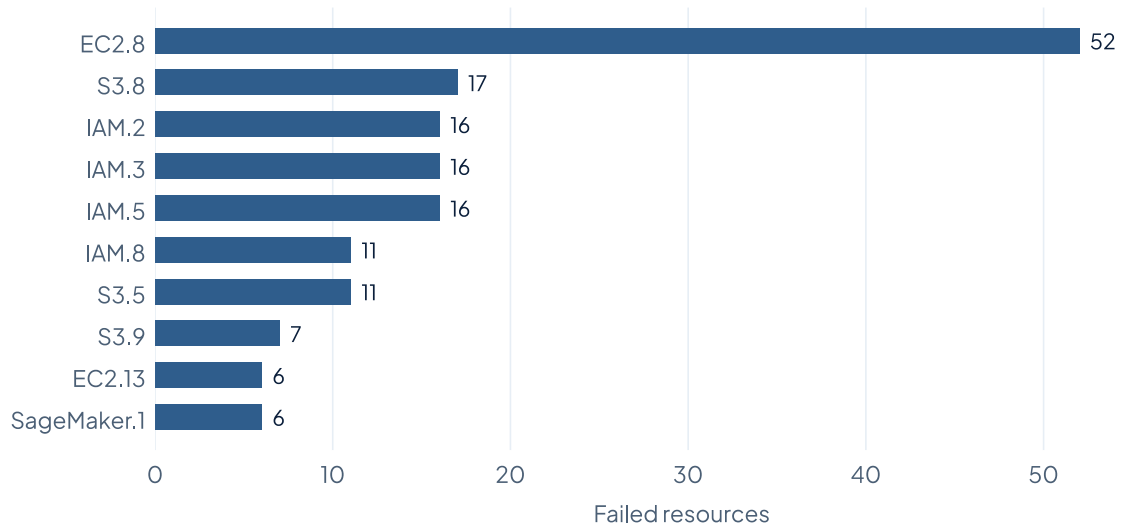
	Checks	Passing	Failing	Pass rate
CIS AWS Foundations Benchmark v5.0.0	27	4	23	14.8%
AWS Foundational Security Best Practices v1.0.0	50	12	38	24.0%
All 50 checks (each counted once)	50	12	38	24.0%

By severity

Checks and failed resources by severity.

Severity	Checks	Passing	Failing	Failed resources
Critical	10	3	7	12
High	13	1	12	97
Medium	24	7	17	81
Low	3	1	2	17
Total	50	12	38	207

Failed resources by check, week one (top 10)



The ten checks with the most failed resources. A count of resources is not a ranking of risk.

Failed checks

The Critical checks

All 10 Critical checks. The register column names the verified finding behind each failure.

Control	Check	Week one	FailedRegister resources
IAM.4	IAM root user access key should not exist	Fail	2C-1
IAM.6	Hardware MFA should be enabled for the root user	Fail	1C-1
IAM.9	MFA should be enabled for the root user	Fail	1C-1
S3.2	S3 buckets should prohibit public read access	Fail	2C-2, C-3
S3.3	S3 buckets should prohibit public write access	Pass	0None
RDS.1	RDS snapshots should prohibit public access	Pass	0None
RDS.2	RDS DB instances should prohibit public access	Fail	2C-4
Opensearch.2	OpenSearch domains should not be publicly accessible	Fail	1C-5
EC2.1	EBS snapshots should not be publicly restorable	Pass	0None
EC2.19	Security groups should not allow unrestricted access to high-risk ports	Fail	3C-10

3 Critical checks pass: public write on S3, public RDS snapshots, and public EBS snapshots. That is not luck. It is the absence of one particular mistake, and the public reads and the public database show the same account made the nearby ones.

The High checks

All 13 High checks.

Control	Check	Week one	Failed resources
IAM.1	IAM policies should not allow full '*' administrative privileges	Fail	4
IAM.28	IAM Access Analyzer external access analyzer should be enabled	Fail	2
CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail	Fail	1
GuardDuty.1	GuardDuty should be enabled	Fail	2
Inspector.1	Amazon Inspector EC2 scanning should be enabled	Fail	2
S3.8	S3 buckets should have block public access settings enabled	Fail	17
RDS.13	RDS automatic minor version upgrades should be enabled	Pass	0
ElastiCache.1	ElastiCache (Redis OSS) clusters should have automatic backups enabled	Fail	1
EC2.2	VPC default security groups should not allow inbound or outbound traffic	Fail	1
EC2.8	EC2 instances should use IMDSv2	Fail	52
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 to port 22	Fail	6
EKS.1	EKS cluster endpoints should not be publicly accessible	Fail	3
SageMaker.1	SageMaker notebook instances should not have direct internet access	Fail	6

The Foundation's checks, run beside the scan

The Multi-Account Foundation add-on has its own scan, MAF-01 to MAF-13, scored on its own gate and not among the 50 above. We ran it on the same day with the same collector, so the Audit and the add-on start from one set of facts. 12 are in scope; MAF-11 is out because there is one VPC and no Transit Gateway.

The Foundation's checks at week one. The add-on re-runs them at its end.

Check	Passes when	Week one	What we found
MAF-01 Landing zone	The landing zone is enrolled, active, and not drifted; all features are on in the organization	Fail	No organization and no landing zone
MAF-02 Accounts placed	Every in-scope account is in its target OU and enrolled	Fail	One standalone account; no organization to place it in
MAF-03 Organization trail	A multi-Region organization trail, logging, with log file validation, delivers to a bucket in the Log Archive account	Fail	No trail of any kind (C-9)
MAF-04 Security delegated	GuardDuty, Security Hub, IAM Access Analyzer, and the Config aggregator (and Inspector) are administered from the Audit account, with new accounts enrolled automatically	Fail	No security service enabled
MAF-05 Identity	IAM Identity Center is the organization's instance and is connected to the identity provider; no workload account has an IAM user with a console password or an active access key, except in the Exceptions OU with a written exception	Fail	No Identity Center; 18 IAM users, seven of them administrators with long-lived keys
MAF-06 Root	The management account's root user has MFA; centralized root access is on; member accounts hold no root password or access keys	Fail	Two active root access keys and no root MFA (C-1)
MAF-07 Guardrails	The agreed SCPs, RCPs, and declarative policies are attached at the agreed OUs, inherited by every in-scope account, and match the repository	Fail	No organization, so no SCP, RCP, or declarative policy
MAF-08 Controls	The agreed Control Tower controls are enabled on every target OU	Fail	No Control Tower
MAF-09 Vending	New accounts are vended through Account Factory, and one account vended in week five passes MAF-02 through MAF-08 untouched by hand	Fail	No Account Factory
MAF-10 Backup	A backup policy is attached to the agreed OUs, AWS Backup is administered from a delegated account, and copies land in a central vault in a separate account	Fail	No central backup; a snapshot cron job in the one account
MAF-11 Network	Shared networking is owned by a Network account and shared through AWS RAM	Out of scope	One VPC and no Transit Gateway

Check	Passes when	Week one	What we found
MAF-12 Tagging	The agreed tag policy is attached and effective, with its compliance report readable from the management account	Fail	No tags on 94% of resources and no tag policy
MAF-13 No lingering access	Vantalect's operator role and any temporary assignment are gone from the management account	Pass	No role yet

11 of the 12 in-scope checks fail and 1 passes, which is the whole story: nothing exists that could pass them. The add-on's gate is that every in-scope check passes at its end, with a check waived in writing counting as passed; the Audit's re-scan counts the 3 critical findings that only an organization can finish (C-1, C-7, C-9).

The inventory

This chapter is the Foundation's inventory. The add-on does not issue a separate one, because a single account with no organization has little to list beyond what the scan already shows, and a second report that repeated it would only invite two versions of the same count. Every figure below is the scan's or the register's.

The account as found

The account as found. Every count is the scan's, except where a row names the register.

Area	As found on January 5, 2026	Where it shows
Accounts and organization	1 account, its own payer, no AWS organization, no organizational units, and no policies of any kind above it	MAF-01, MAF-02, MAF-07
Regions	Everything runs in us-east-1; us-west-2 is enabled and empty	Scope
People and keys	18 IAM users: 16 with console passwords (7 of them administrators, 2 of those people who have left), the CI user, and one for a video analytics vendor. No IAM Identity Center	IAM.2, IAM.3, IAM.5; C-7, H-3, H-14
Root user	Two active access keys and no MFA	IAM.4, IAM.6, IAM.9; C-1
Logging and detection	No trail, AWS Config off, no GuardDuty, no Security Hub CSPM, no Inspector, no IAM Access Analyzer, no VPC flow logs	CloudTrail.1, Config.1, GuardDuty.1, EC2.6; C-9, H-6

Area	As found on January 5, 2026	Where it shows
Compute	52 EC2 instances, all with the older metadata service on, 18 reachable on SSH from anywhere	EC2.8, EC2.13; H-2, H-4
Block storage	61 EBS volumes, 58 unencrypted, and default encryption off	EC2.7; H-1
Object storage	23 buckets: 17 without Block Public Access settings, 11 accepting plain HTTP, 7 without access logging, and 2 public to the internet	S3.2, S3.5, S3.8, S3.9; C-2, C-3
Databases and search	2 RDS instances reachable from the internet and 2 unencrypted, one Redis group with no AUTH, in-transit encryption, or automatic backups (AUTH checked by hand), and one OpenSearch domain with a public endpoint	RDS.2, RDS.3, ElastiCache.1, ElastiCache.5, Opensearch.2; C-4, C-5, H-7
Clusters and notebooks	3 EKS clusters with public endpoints and 6 SageMaker notebook instances with direct internet access	EKS.1, SageMaker.1; H-8, H-9
Edge	2 public Application Load Balancers with no web application firewall	ELB.16; H-10
Commitments and credits	No Savings Plan and no Reserved Instance; the AWS Activate credits ran out in June 2025	The Foundation's risk register, FR-2
Support	Business Support+, set on this account	The Foundation's risk register, FR-4
Tags	No cost allocation tags and no tag policy	MAF-12
Infrastructure as code	About half of production in the CDK; the rest built in the console	The Well-Architected Review

Engine versions and their support dates

Support dates decide what a version costs and when it must change, so the Audit records them now and the Well-Architected Review and the cost engagement act on them.

Engine versions and support dates in the account.

Service	Version	Support
RDS for PostgreSQL 13 (production and staging)	PostgreSQL 13	Standard support ended February 28, 2026; RDS Extended Support bills from March 1, 2026
Amazon EKS, production and staging	Kubernetes 1.30	Standard support ended July 23, 2025; extended support until July 23, 2026
Amazon EKS, development	Kubernetes 1.33	Standard support to July 29, 2026
Amazon ElastiCache	Redis OSS 7.1	Supported
Amazon OpenSearch Service	OpenSearch 2.13	Supported

What Tidepost closed after our call

We told Tidepost about the critical results on January 6, 2026, the day after the scan, and did not wait for the register. Kofi Brandvold’s team and the owners acted the same day. The register assigns the IDs below. Each row is what was done by January 9, 2026; the scan numbers above are as found on January 5, 2026 and are not re-run until week six.

What changed in the account between the scan and this report.

ID	Severity	Finding	Done by January 9	Complete
C-1	Critical	Root user with two active access keys and no MFA	January 6, Tidepost on notice: Both root access keys deleted after the pipeline and the script moved to roles; two FIDO2 keys registered	No, more to do
C-2	Critical	tp-media-originals public-read, and location metadata on 61% of images	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	No, more to do
C-3	Critical	tp-exports public with listing on: 104,318 user records	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)	Yes
C-4	Critical	RDS PostgreSQL publicly accessible from 0.0.0.0/0	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	No, more to do
C-6	Critical	Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	January 8, Hardening: Allowlisted egress proxy and URL validation added; IMDSv2 required on the tier; the role cut to 14 actions	Yes
C-7	Critical	Seven IAM users with administrator access and long-lived keys, two of them departed	January 6, Tidepost on notice: The two departed users' passwords and keys deleted, and the users with them	No, more to do
C-8	Critical	Database password and a third-party API key in the repository and in launch template user data	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	Yes
C-9	Critical	No CloudTrail trail	January 6, Hardening: An account trail created, multi-Region, writing to a locked bucket	No, more to do

ID	Severity	Finding	Done by January 9	Complete
C-10	Critical	A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	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	Yes
H-5	High	Account-level S3 Block Public Access off	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)	Yes
L-3	Low	Billing and operations alternate contacts are the founders' personal addresses	January 9, Tidepost on notice: Contacts changed to role mailboxes	Yes
L-5	Low	Two public ECR repositories	January 8, Tidepost on notice: Both repositories made private and their images checked for secrets	Yes

7 of the 12 findings above are complete, and 5 have a first step done with more to come. A step labeled "Tidepost on notice" was made by Tidepost's engineers within about a day of our call; a step labeled "Hardening" was specified, reviewed, and verified by Vantalect and made by Tidepost's engineers.

What week 2 does

Week 2 reads every Critical and High result by hand, rates each finding by who can reach it and what it reaches, and reviews how the account is governed. It delivers the findings register, the governance review, the target organization, and the first SOC 2 technical map on January 15, 2026, and we present them with the Foundation plan at the readout on January 16, 2026.

What we need from you this week

- **Dev Raman:** hold January 16, 2026 for the readout, and decide there whether the Foundation follows a greenfield path (a new management account) or a retrofit.

- **Kofi Brandvold:** create the new management account by January 12, 2026 with its root email on a company group alias and two hardware keys on its root user, held by Noor Castellanos and Sasha Ilyin in separate places.
- **Sasha Ilyin:** name who receives security notices, and confirm that counsel has what it needs on the two exposure findings (C-3 and C-10). Whether to notify anyone is Tidepost's decision; these reports record only that counsel was told.
- **The owners of C-4 and C-8:** Kofi Brandvold confirms the BI vendor's four published address ranges, and Marcus Oyelaran confirms the secrets that were rotated.

Appendix: the checks in the score

All 50 checks at week one.

Control	Check	Severity	Standards	Week one	Failed resources
IAM.1	IAM policies should not allow full '*' administrative privileges	High	CIS and FSBP	Fail	4
IAM.2	IAM users should not have IAM policies attached	Low	CIS and FSBP	Fail	16
IAM.3	IAM users' access keys should be rotated every 90 days or less	Medium	CIS and FSBP	Fail	16
IAM.4	IAM root user access key should not exist	Critical	CIS and FSBP	Fail	2
IAM.5	MFA should be enabled for all IAM users that have a console password	Medium	CIS and FSBP	Fail	16
IAM.6	Hardware MFA should be enabled for the root user	Critical	CIS and FSBP	Fail	1
IAM.8	Unused IAM user credentials should be removed	Medium	CIS and FSBP	Fail	11
IAM.9	MFA should be enabled for the root user	Critical	CIS and FSBP	Fail	1
IAM.15	IAM password policies should have strong configurations	Medium	CIS and FSBP	Pass	0
IAM.28	IAM Access Analyzer external access analyzer should be enabled	High	FSBP	Fail	2

Control	Check	Severity	Standards	Week one	Failed resources
CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail	High	CIS and FSBP	Fail	1
CloudTrail.2	CloudTrail should have encryption at rest enabled	Medium	CIS and FSBP	Fail	1
CloudTrail.4	CloudTrail log file validation should be enabled	Low	CIS and FSBP	Fail	1
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	Medium	CIS and FSBP	Fail	2
EC2.6	VPC flow logging should be enabled in all VPCs	Medium	CIS and FSBP	Fail	1
GuardDuty.1	GuardDuty should be enabled	High	FSBP	Fail	2
SecurityHub.1	Security Hub CSPM should be enabled	Medium	FSBP	Fail	2
Inspector.1	Amazon Inspector EC2 scanning should be enabled	High	FSBP	Fail	2
S3.1	S3 general purpose buckets should have account-level block public access settings enabled	Medium	CIS and FSBP	Fail	1
S3.2	S3 buckets should prohibit public read access	Critical	CIS and FSBP	Fail	2
S3.3	S3 buckets should prohibit public write access	Critical	CIS and FSBP	Pass	0
S3.5	S3 buckets should require requests to use TLS	Medium	CIS and FSBP	Fail	11
S3.8	S3 buckets should have block public access settings enabled	High	CIS and FSBP	Fail	17
S3.9	S3 buckets should have server access logging enabled	Medium	CIS and FSBP	Fail	7
RDS.1	RDS snapshots should prohibit public access	Critical	CIS and FSBP	Pass	0
RDS.2	RDS DB instances should prohibit public access	Critical	CIS and FSBP	Fail	2

Control	Check	Severity	Standards	Week one	Failed resources
RDS.3	RDS DB instances should have encryption at rest enabled	Medium	CIS and FSBP	Fail	2
RDS.8	RDS DB instances should have deletion protection enabled	Low	FSBP	Pass	0
RDS.9	RDS DB instances should publish logs to CloudWatch Logs	Medium	FSBP	Fail	2
RDS.13	RDS automatic minor version upgrades should be enabled	High	FSBP	Pass	0
ElastiCache.1	ElastiCache (Redis OSS) clusters should have automatic backups enabled	High	FSBP	Fail	1
ElastiCache.5	ElastiCache replication groups should be encrypted in transit	Medium	FSBP	Fail	1
Opensearch.1	OpenSearch domains should have encryption at rest enabled	Medium	FSBP	Pass	0
Opensearch.2	OpenSearch domains should not be publicly accessible	Critical	FSBP	Fail	1
EC2.1	EBS snapshots should not be publicly restorable	Critical	FSBP	Pass	0
EC2.2	VPC default security groups should not allow inbound or outbound traffic	High	CIS and FSBP	Fail	1
EC2.7	EBS default encryption should be enabled	Medium	CIS and FSBP	Fail	2
EC2.8	EC2 instances should use IMDSv2	High	FSBP	Fail	52
EC2.13	Security groups should not allow ingress from 0.0.0.0/0 to port 22	High	CIS and FSBP	Fail	6
EC2.19	Security groups should not allow unrestricted access to high-risk ports	Critical	FSBP	Fail	3
EC2.172	EC2 VPC Block Public Access settings should block internet gateway traffic	Medium	FSBP	Fail	2
ELB.16	Application Load Balancers should be associated with an AWS WAF web ACL	Medium	FSBP	Fail	2

Control	Check	Severity	Standards	Week one	Failed resources
EKS.1	EKS cluster endpoints should not be publicly accessible	High	FSBP	Fail	3
SageMaker.1	SageMaker notebook instances should not have direct internet access	High	FSBP	Fail	6
SecretsManager.4	Secrets Manager secrets should be rotated within a specified number of days	Medium	FSBP	Pass	0
KMS.4	AWS KMS key rotation should be enabled	Medium	CIS and FSBP	Pass	0
Kinesis.1	Kinesis streams should be encrypted at rest	Medium	FSBP	Pass	0
Macie.1	Amazon Macie should be enabled	Medium	FSBP	Fail	2
Lambda.2	Lambda functions should use supported runtimes	Medium	FSBP	Pass	0
DynamoDB.2	DynamoDB tables should have point-in-time recovery enabled	Medium	FSBP	Pass	0

© 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.