



AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Detection and Response from the Audit Account

Week 5 of 6: Detection and response · prepared for Tidepost,
Inc.

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

February 6, 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

Summary	2
Coverage, before and after	3
By account	4
Delegated administrators	6
Turning each service on	6
AWS Config	6
Amazon GuardDuty	6
AWS Security Hub CSPM	7
Amazon Inspector	7
IAM Access Analyzer	7
Routing findings to people	8
The routes, tested	10
What fails by decision	11
First response, by finding type	12
The organization trail and the log archive	14
What the detection stack costs	14
What is not finished	16

Summary

As of February 6, 2026, detection runs from one account, tp-audit, and covers 8 of the 9 accounts in the organization in both governed Regions (us-east-1 and us-west-2). The ninth, tp-backup, is created on February 10 and is enrolled the day it joins, because auto-enable is on. Five services are running: AWS Config, Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, and IAM Access Analyzer. On January 29, the day after the join on January 28, the Foundation designated tp-audit as their delegated administrator, and the Hardening configured them. On the first day all of them were off in both Regions, so a finding could not have been raised.

Findings now reach people. A rule for each source sends what matters to an SNS topic in tp-audit, which posts to the security channel and the security mailbox and, for the top severity, to the phones of two named people: Sasha Ilyin first, Kofi Brandvold second. Each of the 5 routes was

proved by raising a real or sample finding and timing the arrival ([The routes, tested](#)). The first-response runbooks for the five kinds of finding most likely to page someone are written, and their full text is in security-8-runbooks-handover.

The detection services and the logging around them cost **\$2,584 a month** at list price, priced from the AWS Price List on the usage the accounts produce once all 9 are enrolled. That is 1.6% of the January bill of \$157,565 a month, the bill this engagement started from, and it is the figure the cost engagement takes as its security services line ([What the detection stack costs](#)).

Detection and response in numbers on February 6, 2026.

Week 5 at a glance	Result
Detection services running	5
Accounts covered on February 6	8 of 9
Governed Regions	2
Delegated administrator	tp-audit
Alert routes proved by a test	5
Routes that page a person	2
First-response runbooks	5
Controls that fail by written decision	5
Cost of the security services, a month	\$2,584

Decision for the sponsor

Dev Raman: confirm that Sasha Ilyin and Kofi Brandvold are the two people whose phones receive a page, until the Well-Architected Review sets an on-call rotation. Pages are rare by design, but when one arrives, the person who answers owns the first fifteen minutes, so they should both agree to it. Tell Kofi Brandvold before the handover on February 12 if you want a different pair; nothing in the route changes except the subscription list.

Coverage, before and after

On January 5, 2026 none of the detection services was on, in either Region. The scan's checks for them each failed on two resources, the two Regions:

The detection checks on the first day. Each failing resource is one Region of the one account.

Check	What it tests	Failing on the first day
GuardDuty.1	GuardDuty should be enabled	2
SecurityHub.1	Security Hub should be enabled	2
Inspector.1	Amazon Inspector EC2 scanning should be enabled	2
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	2
IAM.28	IAM Access Analyzer external access analyzer should be enabled	2

By account

Every account is covered from the day it joined or the day the delegated administrator turned the services on, whichever is later. An account that exists before January 29 was activated by the administrator in each Region; one created after is enrolled by auto-enable the day it joins.

Coverage by account in us-east-1 and us-west-2. All five services, in every account, are covered together or not at all.

Account	OU	Created	Covered from	How	On February 6
tp-management	Root	Jan 12	Jan 29	Activated by the delegated administrator	Covered
tp-log-archive	Security	Jan 21	Jan 29	Activated by the delegated administrator	Covered
tp-audit	Security	Jan 21	Jan 29	Activated by the delegated administrator	Covered
tp-backup	Infrastructure	Feb 10	Feb 10	Enrolls by auto-enable the day it joins	Not yet created
tp-prod	Workloads/Prod	Jan 28	Jan 29	Activated by the delegated administrator	Covered
tp-staging	Workloads/NonProd	Jan 29	Jan 29	Activated by the delegated administrator	Covered
tp-dev	Workloads/NonProd	Feb 3	Feb 3	Enrolled by auto-enable the day it joined	Covered
tp-sandbox-ml	Sandbox	Feb 5	Feb 5	Enrolled by auto-enable the day it joined	Covered
tp-policy-test	Policy Staging	Jan 29	Jan 29	Activated by the delegated administrator	Covered

Delegated administrators

Each service is administered from tp-audit, so a compromised workload account cannot turn off what watches it, and a new account is covered the day it joins. The Foundation designated the administrator (its check MAF-04); the Hardening turned on and configured what runs there. Designation is per service and, for GuardDuty, Security Hub, and Inspector, per Region.

The delegated administrator of each detection service. Before the join there was no organization to delegate from.

Service principal	Before	After	From
config.amazonaws.com	None	tp-audit	Jan 29
guardduty.amazonaws.com	None	tp-audit	Jan 29
securityhub.amazonaws.com	None	tp-audit	Jan 29
inspector2.amazonaws.com	None	tp-audit	Jan 29
access-analyzer.amazonaws.com	None	tp-audit	Jan 29

Turning each service on

The order was Config first, because Security Hub reads it, then GuardDuty, Security Hub, Inspector, and Access Analyzer. Each service's section says what is on, what is deliberately off and why, and what it costs.

AWS Config

On since January 29, administered from tp-audit (finding M-4).

What is on. Continuous recording of every supported resource type in every governed account and Region, with one aggregator in tp-audit that every account and Region reports to.

What is off, and why. Conformance packs: Security Hub already evaluates the two standards from the same recordings.

Cost. \$360 a month: 120,000 configuration items.

Amazon GuardDuty

On since January 29, administered from tp-audit (finding H-6).

What is on. The foundational sources (management events from the trail, VPC flow logs, DNS logs), EKS audit log monitoring, and EKS runtime monitoring with the GuardDuty-managed agent. Auto-enable is ALL, so every account that joins is covered the day it enrolls.

What is off, and why. S3 Protection, Malware Protection for EC2, RDS login monitoring, and Lambda network monitoring. Each is a toggle in the delegated administrator, priced by usage, and not in the cost below; they wait for the first monthly review (the two buckets that matter carry Block Public Access and object-level trail events).

Cost. \$1,330 a month: 60 million management events, 1 TB of flow and DNS logs, 25 million audit events, 192 vCPUs.

AWS Security Hub CSPM

On since January 29, administered from tp-audit (finding H-6).

What is on. AWS Foundational Security Best Practices v1.0.0 and the CIS AWS Foundations Benchmark v5.0.0 in every governed account, set from one central configuration policy, with findings from both Regions aggregated into us-east-1.

What is off, and why. The newer Security Hub exposure-correlation service: one queue to learn before a second.

Cost. \$90 a month: 90,000 checks.

Amazon Inspector

On since January 29, administered from tp-audit (finding H-6).

What is on. EC2 instances (through Systems Manager) and container images in ECR, with enhanced scanning on continuous mode so a new CVE in an image pushed last month is found without a re-push.

What is off, and why. Lambda standard and code scanning: the bill line prices EC2 and ECR.

Cost. \$292 a month: 45 instances, 1,500 new images, 10,000 rescans.

IAM Access Analyzer

On since January 29, administered from tp-audit (finding M-9).

What is on. One organization-wide external-access analyzer per governed Region, administered from tp-audit. It finds what an outside party can reach: a public bucket, a shared snapshot, a role anyone can assume. There is no charge for external-access findings.

What is off, and why. Unused-access analysis, which is billed by role and user analyzed; with 14 people on permission sets and one IAM user, there is little to find.

Cost. External-access findings are free.

Two products with nearly the same name

AWS Security Hub CSPM is the service that owns the controls (IAM.4, EC2.8), the two standards, and the findings, and it is the one turned on here. AWS Security Hub, a newer service that correlates findings from GuardDuty, Inspector, and Security Hub CSPM into prioritized exposures, is not turned on: a small team should learn one queue before it adds a second. The decision to revisit it is on the agenda of the first monthly review in [security-8-runbooks-handover](#).

The 50 checks of the Audit's own scan use the same control IDs as the two Security Hub CSPM standards, so a Security Hub finding and a scan check name the same thing: the same ID, the same resource, the same fix.

Routing findings to people

A finding nobody reads is a log line. Every route ends at one of two SNS topics in `tp-audit`. `tp-security-alerts` posts to a channel in the company chat (through Amazon Q Developer in chat applications, the service formerly called AWS Chatbot) and to the security mailbox. `tp-security-page` sends an SMS to Sasha Ilyin and Kofi Brandvold. A rule for a page targets both topics, and every other rule targets only the first, so the two phones ring only for what is urgent. GuardDuty and Inspector in the second Region forward to the same topic through the first Region's default event bus.

The 6 routes. "Page" means the SMS subscription is used; every other route goes to the channel and a ticket.

Source	What fires it	Where it goes	Urgency	First response
GuardDuty	Severity 7.0 and above (High and Critical)	The security channel and mailbox, and an SMS to both responders	Page	SR-1, SR-2, or SR-3 by finding type
GuardDuty	Severity 4.0 to 6.9 (Medium)	A ticket in the security queue, read every business day	Business day	The finding's first-response row
Security Hub CSPM	New failed CRITICAL and HIGH findings that Security Hub itself generated (GuardDuty and Inspector findings it imports are routed by their own rules, so nothing pages twice)	The security channel and a ticket	Business day	SR-2 for a public data store
Amazon Inspector	New CRITICAL package vulnerabilities	A ticket for the platform team: patching work, not an incident	Business day	None: patching
IAM Access Analyzer	New active external-access findings	The security channel and a ticket	Business day; page if the resource holds user data	SR-2
CloudTrail through EventBridge	Root sign-in, sts:AssumeRoot, a break-glass sign-in, StopLogging, DeleteTrail, or an attempt to disable a detection service	The security channel and mailbox, and an SMS to both responders	Page	SR-4 or SR-5

The GuardDuty rule, and the rule for changes to the detection services themselves:

JSON

```
{
  "source": ["aws.guardduty"],
  "detail-type": ["GuardDuty Finding"],
  "detail": {"severity": [{"numeric": [">=", 7]}]}
}
```

JSON

```
{
  "source": ["aws.cloudtrail"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["cloudtrail.amazonaws.com", "guardduty.amazonaws.com",
"securityhub.amazonaws.com", "config.amazonaws.com"],
    "eventName": ["StopLogging", "DeleteTrail", "UpdateTrail", "DeleteDetector",
"DisableSecurityHub", "StopConfigurationRecorder"]
  }
}
```

BASH

```
aws sns create-topic --name tp-security-alerts --region us-east-1 # the channel and the
mailbox subscribe
aws sns create-topic --name tp-security-page --region us-east-1 # the SMS subscriptions,
one per responder
aws sns subscribe --topic-arn <tp-security-page-topic-arn> --protocol sms --notification-
endpoint <responder-phone> --region us-east-1
# each topic's access policy lets events.amazonaws.com publish to it
aws events put-rule --name tp-guardduty-high --event-pattern file://guardduty-high.json --
region us-east-1
aws events put-targets --rule tp-guardduty-high --region us-east-1 \
  --targets Id=alerts,Arn=<tp-security-alerts-topic-arn> Id=page,Arn=<tp-security-page-topic-
arn>
# us-west-2: the same rule, with the us-east-1 default event bus as its target and a role that
lets EventBridge put events there
```

Responders: Sasha Ilyin, Head of Security and Compliance, first; Kofi Brandvold, Head of Platform, second. This is a pair of named people, not an on-call rotation. The rotation, the severity levels, and the incident process around them are the Well-Architected Review's, exercised in a tabletop on March 26; until then, a page goes to these two.

The routes, tested

A route is not a route until a finding has traveled it. Each source was driven with a harmless real or sample finding and the time to the first message was written down.

The route tests. Repeat them every quarter and log the times; a route that takes longer than it did is a route that is breaking.

Source	How it was driven	Day	Time to the channel
GuardDuty	aws guardduty create-sample-findings with a High-severity command-and-control finding type	Feb 4	74 seconds
Security Hub CSPM	A scratch security group open on port 22 in tp-dev, which failed EC2.13 on the next change-triggered Config evaluation	Feb 4	7 minutes
Inspector	A known-vulnerable test image pushed to a scratch ECR repository in tp-dev	Feb 5	3 minutes
Access Analyzer	A scratch bucket policy granting read to an outside account	Feb 5	11 minutes
CloudTrail through EventBridge	StopLogging on a scratch trail in tp-dev	Feb 5	3 minutes

What fails by decision

Security Hub will report a failure on 5 controls that Tidepost has decided to leave failing, each with a name, a date, and a reason. They are written into the Security Hub configuration as automation rules that mark the finding suppressed, with the finding number and the review date in the rule's description, so the next person reading the queue sees why instead of re-opening it.

Controls that fail by written decision. A decision that reaches its date comes back to this table and is renewed or closed.

Control	Why it fails	Resources itDecision covers	Decided
RDS.2	The production database is publicly accessible until the cutover	1C-4, by Dev Raman	Jan 16
RDS.3	The same instance is unencrypted until the cutover	1H-1, by Dev Raman	Jan 16
S3.9	Server access logging is off by written acceptance	7M-7, by Sasha Ilyin	Jan 21
EC2.172	VPC Block Public Access would block the public load balancers	18D-3, by Kofi Brandvold	Feb 5
Macie.1	Macie is not enabled, by decision	18D-1, by Sasha Ilyin	Jan 16

First response, by finding type

Each of these is a real GuardDuty finding type. The first action is the one thing to do in the first five minutes; the runbook has the rest.

Six finding types and where each one starts.

Finding	What it means here	First action	Runbook
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.0outsideAWS	An instance role's temporary credentials are being used from outside AWS. The path C-6 closed; if it fires now, something else is leaking them.	Revoke older sessions on the role, then find the instance	SR-1
Policy:S3/BucketAnonymousAccessGranted	A bucket policy or ACL now allows anonymous access. Account-level Block Public Access (G-I) should make this impossible, so the question is who turned it off.	Block Public Access on the bucket, then look at the trail	SR-2
CryptoCurrency:EC2/BitcoinTool.B!DNS	An instance is querying a cryptocurrency domain. The pattern the forgotten GPU instance (C-10) fit.	Quarantine the instance and snapshot its volumes	SR-3
Execution:Runtime/NewBinaryExecuted	A container ran a binary that was not in its image. EKS runtime monitoring raises it.	Cordon the node and isolate the pod's namespace	SR-3
Policy:IAMUser/RootCredentialUsage	The root user did something. Nothing should: root credentials leave tp-prod on January 29.	Match it to a root task ticket; if none, treat as a stolen credential	SR-4
Stealth:IAMUser/CloudTrailLoggingDisabled	Someone stopped or changed a trail. The organization policy set will deny it from February 5.	Start logging again, then find the caller	SR-5

The five runbooks, who owns each, and whom each pages:

The first-response runbooks. Their full text, with commands, is in `security-8-runbooks-handover`.

Runbook	Title	Owner	Second	Pages
SR-1	A credential is leaked or misused	Sasha Ilyin	Kofi Brandvold	Page
SR-2	A bucket, snapshot, or database is public	Kofi Brandvold	Sasha Ilyin	Page for user data; business day otherwise
SR-3	An instance or a container is compromised	Kofi Brandvold	Sasha Ilyin	Page
SR-4	A root sign-in, a break-glass sign-in, or an IAM change nobody planned	Sasha Ilyin	Kofi Brandvold	Page
SR-5	A detection service stops, or an account drops out of it	Sasha Ilyin	Kofi Brandvold	Page

The organization trail and the log archive

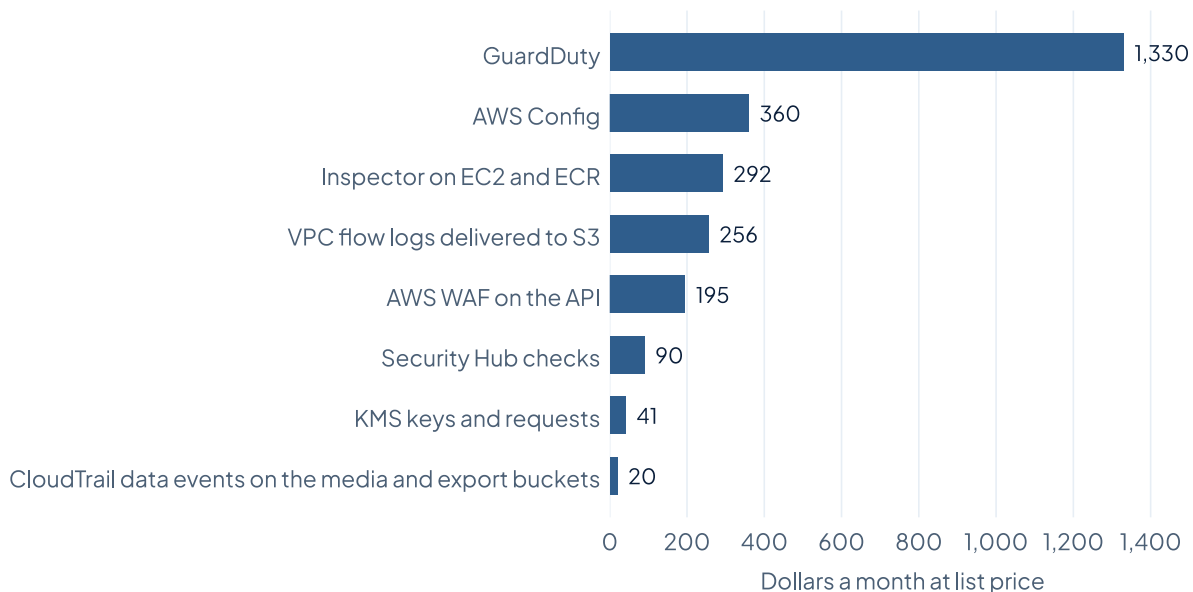
Detection is only as good as the record it reads. The organization trail has logged into `tp-log-archive` since January 21, and receives `tp-prod`'s events from the join on January 28, which closed C-9. Audit logs are kept 400 days there, so an investigation in the autumn can still read January. Security Hub, GuardDuty, and the Config aggregator read from the same sources, so a gap in one is visible in the others, and runbook SR-5 treats a stopped service as an incident in its own right.

What the detection stack costs

Each line is a quantity times a price from the AWS Price List, priced at list. The quantities are what the accounts are expected to produce once all 9 are enrolled, and the lines add to the figure the cost engagement carries as security services.

The security services line. Each row is rounded to the dollar and the rounded rows add to the total.

Line	Account	Quantity	Price	A month
GuardDuty: management events, flow and DNS logs, EKS audit logs, and runtime monitoring on 192 vCPUs	tp-audit	60 million management events, 1 TB of flow and DNS logs, 25 million audit events, 192 vCPUs	the published tiers	\$1,330
AWS Config, continuous recording	tp-audit	120,000 configuration items	\$0.003 an item	\$360
Security Hub checks	tp-audit	90,000 checks	the published tiers	\$90
Inspector on EC2 and ECR	tp-audit	45 instances, 1,500 new images, 10,000 rescans	per instance-hour and image	\$292
KMS keys and requests, Secrets Manager	tp-prod	20 keys, 3 million requests, 30 secrets	monthly and per request	\$41
AWS WAF on the API	tp-prod	1 web ACL, 10 rules, 300 million requests	monthly and per million	\$195
CloudTrail data events on the media and export buckets	tp-log-archive	20 million events	\$0.10 per 100,000	\$20
VPC flow logs delivered to S3	tp-log-archive	1 TB	the published tiers	\$256
Detection services (GuardDuty, Config, Security Hub, Inspector)				\$2,072
Protection and logging (KMS and secrets, WAF, trail data events, flow logs)				\$512
Security services				\$2,584



Monthly cost by service line.

Over a year the total is \$31,010. It buys the thing the first day lacked: a record of who did what, and a reader for it. GuardDuty is the largest line because it reads management events, flow and DNS logs, EKS audit logs, and runtime activity on the cluster nodes. The services that are off (S3 Protection, malware scanning, RDS and Lambda monitoring, Lambda scanning) are not in the figure and each would add to it; they are on the first monthly review's agenda, with the cost estimate.

What is not finished

- **tp-backup joins on February 10.** Auto-enable covers it that day; the Foundation's re-scan checks it.
- **Runbooks tested on a live sample.** The five runbooks are rehearsed on February 12, the handover day, and again in the tabletop on March 26.
- **The services that are off** are decided at the first monthly review, and each decision is written down with its cost.

© 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.