



Sample deliverable

Sample: AWS Security Posture Assessment

Sample document. All findings, scores, account identifiers, and company details are fictional demonstration data created to show report format and depth. This is not a real client engagement.

CLIENT	ACCOUNTS	ASSESSED	FINDINGS
Harborline Logistics (sample)	4 accounts, 2 Regions	14 Mar 2026	11

Executive summary



Posture grade

Harborline's AWS environment shows solid foundational controls: CloudTrail is enabled organization-wide, S3 public access is blocked at the account level, and KMS encryption is applied consistently to production data stores. Risk concentrates in two areas: identity hygiene in the legacy production account, and detection coverage gaps in the two Regions added during last year's expansion.

Three findings are rated High and should be closed within 30 days. None indicate active compromise.

Control coverage

Identity and access management 7 of 13 checks passing

Logging and monitoring 12 of 17 checks passing

Configuration and compliance 9 of 14 checks passing

Data protection 15 of 17 checks passing

Multi-account guardrails 5 of 11 checks passing

Findings summary

#	SEVERITY	FINDING	AWS SERVICE	WELL-ARCHITECTED
1	High	Root account has an active access key in the legacy production account	AWS IAM	SEC01-BP02
2	High	GuardDuty not enabled in two of four active Regions	Amazon GuardDuty	SEC04-BP01
3	High	Nine IAM users hold console access without MFA enforced	AWS IAM	SEC02-BP01
4	Medium	Service control policies absent for three member accounts	AWS Organizations	SEC01-BP01
5	Medium	AWS Config recorder disabled in us-west-2	AWS Config	SEC04-BP02
6	Medium	CloudTrail log file validation not enabled on the organization trail	AWS CloudTrail	SEC04-BP01
7	Medium	Access keys older than 365 days on four programmatic identities	AWS IAM	SEC02-BP02
8	Medium	Security Hub enabled but AWS Foundational Security Best Practices standard not turned on	AWS Security Hub	SEC04-BP02
9	Low	KMS key rotation not enabled on two customer managed	AWS KMS	SEC08-BP01

keys

10	Low	Macie not configured; sensitive data discovery relies on manual tagging	Amazon Macie	SEC07-BP01
11	Info	No break-glass procedure documented for emergency root access	AWS IAM	SEC03-BP02

Detailed findings

Finding 1 — Root account access key in legacy production account

Severity: High · Account: 4418-sample-prod · Service: AWS IAM · Well-Architected: SEC01-BP02

Observation. The root user in the legacy production account has an access key created in 2021 and last used 94 days ago. Root credentials bypass every permission boundary and IAM policy in the account.

Risk. A leaked root key grants unrestricted control of the account, including the ability to delete CloudTrail trails and disable detective controls. The 94-day last-used timestamp indicates it is embedded in an automated process, so rotation alone will not remove the exposure.

Recommendation. Identify the consuming process through CloudTrail, migrate it to an IAM role with scoped permissions, then delete the root access key and confirm MFA is enforced on the root user. Add an AWS Config rule or Security Hub control to alert on any future root key creation.

Finding 2 — GuardDuty not enabled in two active Regions

Severity: High · Regions: us-west-2, eu-west-1 · Service: Amazon GuardDuty · Well-Architected: SEC04-BP01

Observation. GuardDuty is enabled in us-east-1 and ca-central-1 only. Both unmonitored Regions carry production workloads added during the 2025 expansion, including EC2 instances with public ingress.

Risk. Credential compromise, cryptomining, and command-and-control traffic in those Regions would go undetected. Regional gaps are a common blind spot because detection is typically enabled once, at first deployment, and not revisited as the footprint grows.

Recommendation. Enable GuardDuty organization-wide with auto-enable for new accounts and Regions, route findings to Security Hub, and define triage ownership with a response SLA.

Finding 3 — Console users without enforced MFA

Severity: High · Accounts: 3 of 4 · Service: AWS IAM · Well-Architected: SEC02-BP01

Observation. Nine IAM users have console passwords without an MFA device registered. Six belong to contractors onboarded for the warehouse management migration.

Risk. Password-only console access is the most frequently exploited initial access path into cloud environments, and contractor accounts commonly outlive the engagement that created them.

Recommendation. Enforce MFA through an IAM policy condition, migrate human access to IAM Identity Center with your existing identity provider, and set a quarterly access review covering contractor accounts.

Remediation roadmap

WINDOW	ACTIONS	OWNER	EFFORT
Immediate (0-30 days)	Remove root access key and enforce root MFA; enable GuardDuty in all Regions; enforce MFA for console users	Cloud Ops	3-5 days
30-60 days	Enable AWS Config in us-west-2; turn on Foundational Security Best Practices in Security Hub; enable CloudTrail log file validation; rotate aged access keys	Cloud Ops	4-6 days
60-90 days	Apply service control policies to member accounts; migrate human access to IAM Identity Center; enable KMS key rotation	Cloud Ops + IT	6-8 days
Beyond 90 days	Deploy Macie for sensitive data discovery; document break-glass procedure; establish quarterly access review	Security	Ongoing

What this assessment does not cover. No penetration testing, exploitation, or application code review was performed. Findings reflect configuration observed during the assessment window through read-only access. This document is not a certification or an audit opinion.