# AWS Security Baseline Report

## ARX-Internal — ARX-2026-VALIDATION2

**Prepared by:** ARX Cloud Security **Account:** `[ACCOUNT-ID]` **Primary Region:** `eu-west-2` **Baseline Captured:** — **Report Generated:** 2026-07-02T22:15:59+00:00 **Tool Version:** arx-baseline 0.1.0

---

## Scope of Engagement

**Account assessed:** `[ACCOUNT-ID]` **Regions covered:** eu-west-2

**Covered by this assessment:** - CIS AWS Foundations Benchmark v4.0 automated checks (Prowler, dual-scan) - 90-day cost baseline (AWS Cost Explorer) - Resource inventory (EC2, RDS, Lambda, S3, Load Balancers, NAT Gateways, ECS) - Orphan resource detection (unattached EBS, unassociated Elastic IPs, stopped EC2, CloudWatch log groups without retention, idle load balancers) - IAM & identity posture (13 checks: root/user MFA, access key age, wildcard policies, cross-account trust, exposed snapshots, identity federation)

**Explicitly out of scope:** - Architecture review or design recommendations - Compliance framework mapping (SOC 2, ISO 27001, PCI DSS, HIPAA, GDPR) - Manual validation of automated findings - Risk scoring by business context - Remediation guidance beyond high-level finding descriptions - Multi-account or AWS Organizations-level assessment - Attack path analysis or penetration testing

*Point-in-time only. This assessment reflects the state of the environment at 2026-06-30T19:08:05+00:00.*

---

## 1. Executive Summary

This report documents the security and cost posture of the ARX-Internal AWS environment at the point of ARX Cloud Security engagement, captured on 2026-06-30T19:08:05+00:00.

**Findings captured using a dual-scan methodology:** Prowler was run twice against the same account with 22 minutes between scans. Only findings confirmed in both scans are included below. This eliminates API eventual-consistency noise and Prowler non-determinism.

| Metric | Value |
|---|---|
| Confirmed security findings (Critical + High) | **39** |
| Total confirmed findings (all severities) | 104 |
| Drift findings (single-scan only, excluded) | 0 |
| Drift rate | 0.0% |
| Monthly orphan cost estimate | £0.00 |
| 90-day spend (at engagement) | £24.80 |

---

# 2. Cost State at Engagement

*This section establishes the pre-engagement cost baseline. It is the liability reference point — ARX Cloud Security is not responsible for costs incurred before this date.*

**90-Day Spend Summary (by service)**

| Service | 90-Day Cost (£) |
|---|---|
| AWS CloudTrail | 13.33 |
| Tax | 4.13 |
| AWS Key Management Service | 2.97 |
| AWS Security Hub | 2.17 |
| AWS Secrets Manager | 1.19 |
| Amazon Macie | 0.45 |
| Amazon Simple Storage Service | 0.35 |
| Amazon GuardDuty | 0.13 |
| AWS Cost Explorer | 0.05 |
| AWS Config | 0.04 |

**Spend by Region**

| Region | 90-Day Cost (£) |
|---|---|
| eu-west-2 | 19.29 |
| NoRegion | 4.13 |
| us-east-1 | 1.37 |

| Region | 90-Day Cost (£) |
|---|---|
| us-west-2 | 0.01 |
| ap-northeast-1 | 0.00 |
| ap-northeast-2 | 0.00 |
| ap-northeast-3 | 0.00 |
| ap-south-1 | 0.00 |
| ap-southeast-1 | 0.00 |
| ap-southeast-2 | 0.00 |
| ca-central-1 | 0.00 |
| eu-central-1 | 0.00 |
| eu-north-1 | 0.00 |
| eu-west-1 | 0.00 |
| eu-west-3 | 0.00 |
| sa-east-1 | 0.00 |
| us-east-2 | 0.00 |
| us-west-1 | 0.00 |

**Billing Alarms:** None configured. Unexpected spend spikes will not trigger alerts.

---

# 3. Resource Inventory

*What existed in the account at the point of engagement.*

---

# 4. Cost-Relevant Orphan Resources

*Resources identified as billing but serving no active purpose. These are not security findings — they are waste. Prowler does not detect these.*

No orphan resources detected.

---

# 6. Confirmed Security Findings (Critical and High)

*Only findings confirmed in both Prowler scans are listed here. Medium and Low findings are captured in the evidence vault but excluded from this deliverable.*

## [CRITICAL] Attached AWS-managed IAM policy does not allow ‘:’ administrative privileges

| Field | Value |
|---|---|
| Check ID | `iam_aws_attached_policy_no_administrative_privileges` |
| Resource | `arn:aws:iam::aws:policy/AdministratorAccess` |
| Region | `eu-west-2` |
| Service | iam |

**Detail:** AWS policy AdministratorAccess is attached and allows ‘:’ administrative privileges.

**Risk: IAM AWS-managed policies** attached to identities are inspected for statements that allow `Action:'*'` on `Resource:'*'`-i.e., full administrative `*:*` permissions

**Recommendation:** Apply **least privilege**: avoid attaching AWS-managed policies that grant `*:*`. - Use **customer-managed, scoped policies** per role - Enforce **separation of duties** and **permissions boundaries** - Prefer **temporary, time-bound elevation** for emergencies with MFA - Regularly review access and use conditions to constrain context

| ### [CRITICAL] Root account has a hardware MFA device enabled |
|---|
| ### [HIGH] Region has at least one CloudTrail trail logging<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `cloudtrail_multi_region_enabled` \| \| Resource \| `arn:aws:cloudtrail:ap-northeast-1:[ACCOUNT-ID]:trail` \| \| Region \| `ap-northeast-1` \| \| Service \| cloudtrail \|<br>**Detail:** No CloudTrail trails enabled with logging were found.<br>**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.<br>**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in |

| ### [CRITICAL] Root account has a hardware MFA device enabled |
| --- |
| every region, including unused ones.<br>Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps. |

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
| --- | --- |
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:ap-northeast-2:[ACCOUNT-ID]:trail` |
| Region | `ap-northeast-2` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

| ### [HIGH] Region has at least one CloudTrail trail logging |
| --- |
| ### [HIGH] Region has at least one CloudTrail trail logging<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `cloudtrail_multi_region_enabled` \| \| Resource \| `arn:aws:cloudtrail:ap-south-1:[ACCOUNT-ID]:trail` \| \| Region \| `ap-south-1` \| \| Service \| cloudtrail \| |

| ### [HIGH] Region has at least one CloudTrail trail logging |
| --- |
| **Detail:** No CloudTrail trails enabled with logging were found. |
| **Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region. |
| **Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones. |
| Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps. |

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
| --- | --- |
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:ap-southeast-1:[ACCOUNT-ID]:trail` |
| Region | `ap-southeast-1` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

| ### [HIGH] Region has at least one CloudTrail trail logging |
| --- |
| ### [HIGH] Region has at least one CloudTrail trail logging<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `cloudtrail_multi_region_enabled` \| \| Resource \| `arn:aws:cloudtrail:ca-central-1:[ACCOUNT-ID]:trail` \| \| Region \| `ca-central-1` \| \| Service \| cloudtrail \|<br>**Detail:** No CloudTrail trails enabled with logging were found.<br>**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.<br>**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.<br>Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps. |

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
| --- | --- |
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:eu-central-1:[ACCOUNT-ID]:trail` |
| Region | `eu-central-1` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

| ### [HIGH] Region has at least one CloudTrail trail logging |
|---|
| ### [HIGH] Region has at least one CloudTrail trail logging<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `cloudtrail_multi_region_enabled` \| \| Resource \| `arn:aws:cloudtrail:eu-west-1:[ACCOUNT-ID]:trail` \| \| Region \| `eu-west-1` \| \| Service \| cloudtrail \|<br>**Detail:** No CloudTrail trails enabled with logging were found.<br>**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.<br>**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.<br>Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps. |

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
|---|---|
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:eu-west-2:[ACCOUNT-ID]:trail` |
| Region | `eu-west-2` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

---

**### [HIGH] Region has at least one CloudTrail trail logging**

---

### [HIGH] Region has at least one CloudTrail trail logging

| Field | Value | |—|—| | Check ID | `cloudtrail_multi_region_enabled` | | Resource | `arn:aws:cloudtrail:sa-east-1:[ACCOUNT-ID]:trail` | | Region | `sa-east-1` | | Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

---

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
|---|---|
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:us-east-1:[ACCOUNT-ID]:trail` |
| Region | `us-east-1` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

| **### [HIGH] Region has at least one CloudTrail trail logging** |
|---|
| ### [HIGH] Region has at least one CloudTrail trail logging<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `cloudtrail_multi_region_enabled` \| \| Resource \| `arn:aws:cloudtrail:us-west-1:[ACCOUNT-ID]:trail` \| \| Region \| `us-west-1` \| \| Service \| cloudtrail \|<br>**Detail:** No CloudTrail trails enabled with logging were found.<br>**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.<br>**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones. |

| ### [HIGH] Region has at least one CloudTrail trail logging |
| --- |
| Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps. |

## [HIGH] Region has at least one CloudTrail trail logging

| Field | Value |
| --- | --- |
| Check ID | `cloudtrail_multi_region_enabled` |
| Resource | `arn:aws:cloudtrail:us-west-2:[ACCOUNT-ID]:trail` |
| Region | `us-west-2` |
| Service | cloudtrail |

**Detail:** No CloudTrail trails enabled with logging were found.

**Risk: AWS CloudTrail** has at least one trail with `logging` enabled in every region. A **multi-region trail** or a regional trail counts for coverage in that region.

**Recommendation:** Use a **multi-region CloudTrail trail** or per-region trails so `logging` is active in every region, including unused ones.

Centralize logs, enforce **least privilege** to log stores, and add **defense-in-depth** with encryption, integrity validation, and retention. Continuously monitor trail health to catch gaps.

| ### [HIGH] Network ACL does not allow ingress from 0.0.0.0/0 to any port |
| --- |
| ### [HIGH] IAM user has MFA enabled for console access or no console password is set<br>\| Field \| Value \| \|—\|—\| \| Check ID \| `iam_user_mfa_enabled_console_access` \| \| Resource \| `arn:aws:iam::[ACCOUNT-ID]:user/primeone_intern` \| \| Region \| `eu-west-2` \| \| Service \| iam \| |

| ### [HIGH] Network ACL does not allow ingress from 0.0.0.0/0 to any port |
| --- |
| **Detail:** User primeone_intern has Console Password enabled but MFA disabled.<br><br>**Risk: IAM users** that have a console password are expected to have **multi-factor authentication** enabled. The evaluation identifies users who can sign in to the AWS Management Console but do not have an active MFA device associated.<br><br>**Recommendation:** Enforce **MFA** for all console-capable IAM users; prefer **phishing-resistant** authenticators (FIDO2/security keys) and register backups. Remove console passwords for users that don't need them and favor **federation/SSO**. Apply least privilege and require MFA for sensitive actions to prevent unauthorized changes. |

## [HIGH] KMS customer-managed symmetric CMK has automatic rotation enabled

| Field | Value |
| --- | --- |
| Check ID | `kms_cmk_rotation_enabled` |
| Resource | `arn:aws:kms:eu-west-2:[ACCOUNT-ID]:key/mrk-fc248a638fc64decb43c71f4e82cb37f` |
| Region | `eu-west-2` |
| Service | kms |

**Detail:** KMS CMK mrk-fc248a638fc64decb43c71f4e82cb37f has automatic rotation disabled.

**Risk: Customer-managed KMS symmetric keys** in the `Enabled` state are evaluated to confirm `automatic rotation` of key material is configured

**Recommendation:** Enable **automatic rotation** on customer-managed symmetric KMS keys and choose a rotation period that meets policy. Enforce **least privilege** and **separation of duties** for key administration versus usage. Monitor key lifecycle events and use on-demand rotation when compromise is suspected.

---

**### [HIGH] Security Hub is enabled with standards or integrations configured**

---

### [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value | |—|—| | Check ID | `securityhub_enabled` | | Resource | `arn:aws:securityhub:ap-northeast-2:[ACCOUNT-ID]:hub/unknown` | | Region | `ap-northeast-2` | | Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

---

## [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value |
|---|---|
| Check ID | `securityhub_enabled` |
| Resource | `arn:aws:securityhub:ap-northeast-3:[ACCOUNT-ID]:hub/unknown` |
| Region | `ap-northeast-3` |
| Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

| **### [HIGH] Security Hub is enabled with standards or integrations configured** |
|---|
| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| \| Field \| Value \| \|—\|—\| \| Check ID \| `securityhub_enabled` \| \| Resource \| `arn:aws:securityhub:ap-southeast-1:[ACCOUNT-ID]:hub/unknown` \| \| Region \| `ap-southeast-1` \| \| Service \| securityhub \| |
| **Detail:** Security Hub is not enabled. |
| **Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security** |

| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| --- |
| **standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.<br>**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth** |

## [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value |
| --- | --- |
| Check ID | `securityhub_enabled` |
| Resource | `arn:aws:securityhub:ap-southeast-2:[ACCOUNT-ID]:hub/unknown` |
| Region | `ap-southeast-2` |
| Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

| ### **[HIGH] Security Hub is enabled with standards or integrations configured** |
| --- |
| ### [HIGH] Security Hub is enabled with standards or integrations configured<br>| Field | Value | |—|—| |<br>Check ID | `securityhub_enabled` | |<br>Resource | `arn:aws:securityhub:eu-central-1:[ACCOUNT-ID]:hub/unknown` | |<br>Region | `eu-central-1` | |<br>Service | securityhub |<br>**Detail:** Security Hub is not enabled.<br>**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.<br>**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth** |

## [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value |
|---|---|
| Check ID | `securityhub_enabled` |
| Resource | `arn:aws:securityhub:eu-north-1:[ACCOUNT-ID]:hub/unknown` |
| Region | `eu-north-1` |
| Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

| ### **[HIGH] Security Hub is enabled with standards or integrations configured** |
|---|
| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| \| Field \| Value \| \|—\|—\| \| Check ID \| `securityhub_enabled` \| \| Resource \| `arn:aws:securityhub:eu-west-2:[ACCOUNT-ID]:hub/unknown` \| \| Region \| `eu-west-2` \| \| Service \| securityhub \| |
| **Detail:** Security Hub is not enabled. |
| **Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it |

| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| --- |
| is either not enabled or enabled without standards/integrations.<br>**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth** |

## [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value |
| --- | --- |
| Check ID | `securityhub_enabled` |
| Resource | `arn:aws:securityhub:eu-west-3:[ACCOUNT-ID]:hub/unknown` |
| Region | `eu-west-3` |
| Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

### **[HIGH] Security Hub is enabled with standards or integrations configured**

### [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value | |—|—| | Check ID | `securityhub_enabled` | | Resource | `arn:aws:securityhub:us-east-1:[ACCOUNT-ID]:hub/unknown` | | Region | `us-east-1` | | Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

## [HIGH] Security Hub is enabled with standards or integrations configured

| Field | Value |
|---|---|
| Check ID | `securityhub_enabled` |
| Resource | `arn:aws:securityhub:us-east-2:[ACCOUNT-ID]:hub/unknown` |
| Region | `us-east-2` |
| Service | securityhub |

**Detail:** Security Hub is not enabled.

**Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it is either not enabled or enabled without standards/integrations.

**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth**

| ### **[HIGH] Security Hub is enabled with standards or integrations configured** |
|---|
| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| \| Field \| Value \| \|—\|—\| \| Check ID \| `securityhub_enabled` \| \| Resource \| `arn:aws:securityhub:us-west-2:[ACCOUNT-ID]:hub/unknown` \| \| Region \| `us-west-2` \| \| Service \| securityhub \| |
| **Detail:** Security Hub is not enabled. |
| **Risk: AWS Security Hub** is `ACTIVE` in the Region and has at least one enabled **security standard** or connected **integration**. Otherwise, it |

| ### [HIGH] Security Hub is enabled with standards or integrations configured |
| --- |
| is either not enabled or enabled without standards/integrations.<br>**Recommendation:** - Enable in all required accounts/Regions - Turn on relevant **standards** (`AWS FSBP`, `CIS`) - Connect AWS and third-party **integrations** - Use **central configuration** and **least privilege** - Automate triage and monitor continuously for **defense in depth** |

---

# 7. Dual-Scan Methodology

This engagement uses a dual-scan approach to eliminate false positives from Prowler output:

1. **Scan 1** is run at engagement start
2. **Scan 2** is run 22 minutes later against the same account
3. Findings are matched on `(check_id, resource_arn, region)`
4. Only findings present in **both** scans as `FAIL` are confirmed

This eliminates: - AWS API eventual-consistency (a resource may appear misconfigured in one API call but correctly configured in the next) - Prowler non-determinism from parallel check execution - Boundary-condition timing artifacts (e.g. a key that is exactly 90 days old) - Rate-limiting artifacts where throttled API calls produce `ERROR` instead of a real finding

**Scan files used:** - Scan 1: `arx_output/ARX-2026-VALIDATION2/prowler/prowler-output-[ACCOUNT-ID]-20260630202639.ocsf.json` - Scan 2: `arx_output/ARX-2026-VALIDATION2/prowler_scan2/prowler-output-[ACCOUNT-ID]-20260630204842.ocsf.json` - Intersection timestamp: `2026-06-30T20:20:15+00:00`

---

# 8. Evidence Vault

All output files are stored in the engagement evidence directory with SHA-256 hashes recorded in `manifest.json`. This manifest serves as a tamper-evident record of the pre-engagement state.

| File | Purpose |
|---|---|
| `metadata.json` | Engagement identity, account, caller ARN |
| `cost_snapshot.json` | Raw Cost Explorer data (90 days) |
| `resource_inventory.json` | Full resource inventory across all regions |
| `orphan_findings.json` | Orphan detection with cost estimates |
| `iam_findings.json` | IAM & identity posture check results |
| `org_context.json` | AWS Organization membership and engagement coverage |
| `prowler_intersected.json` | Dual-scan intersection result (all severities) |
| `manifest.json` | SHA-256 hash of every file in this directory |

---

# 9. Limitations

This is a point-in-time, automated diagnosis-only assessment using Prowler (CIS 4.0) and custom baseline tooling as of 2026-06-30T19:08:05+00:00. It does not constitute a full security audit, penetration test, or compliance certification. Findings are based on confirmed automated checks only. Absence of findings is not proof of absence of risk. AWS environments change rapidly; re-testing is recommended.

The scope of automated checking is constrained by the permissions granted to ARX Cloud Security for this engagement. Resources or configurations not accessible with the provided credentials will not appear in this report.

---

# 10. Evidence Statement

This report is generated from captured evidence files stored in the engagement evidence directory. File integrity is protected by SHA-256 hashes recorded in `manifest.json`, verified immediately after capture.

| Evidence parameter | Value |
|---|---|
| Prowler version | `5.31.1` |
| Scan mode | CIS AWS Foundations Benchmark v4.0 (dual-run, confirmed findings only) |
| Prowler command | `prowler aws --profile iamadmin --compliance cis_4.0_aws --output-formats json-ocsf` |
| Scan 1 file | `arx_output/ARX-2026-VALIDATION2/prowler/prowler-output-[ACCOUNT-ID]-20260630202639.ocsf.json` |
| Scan 2 file | `arx_output/ARX-2026-VALIDATION2/prowler_scan2/prowler-output-[ACCOUNT-ID]-20260630204842.ocsf.json` |
| Intersection computed | 2026-06-30T20:20:15+00:00 |

Only findings confirmed in both independent Prowler scans are used in this report. Client-provided AWS credentials and assume-role permissions determined what could be observed.

---