SOVEREIGN-28 EXECUTIVE GOVERNANCE NARRATIVE

Independent Telemetry Observation & Control Posture Evaluation

0.1 DATA CUSTODY & BUSINESS CONTEXT
• **METHODOLOGY:** Observational Metadata Handshake. Zero write-access.
• **INDUSTRY BENCHMARK:** Aligned with Foundational Technical Review (FTR) & SOC2.
• **SCOPE:** (EC2, EBS, RDS, ECR, ECS, KMS, SecretMgr, Lambda, WAF, Config, Trail, SG)

2.0 EXECUTIVE FORENSIC INTERPRETATION:
This artifact represents a deterministic validation of the target AWS Organization's compliance with FTR and SOC2 standards. The multi-regional sweep identified material 'Fiscal Drift' where abandoned digital assets consume capital with zero organizational utility. Critically, the absence of active CloudTrail anchors and Configuration Recorders creates a 'Forensic Blindspot'. Remediating these vectors immediately optimizes cloud cost efficiency and establishes a cryptographically verifiable security posture.

CONTROL EVALUATION POSTURE (TAXONOMY BREAKDOWN):
• **Total Telemetry Observations:** 79 records evaluated across 17 commercial regions.
• **Class A (Directly Verified Configurations):** 0 confirmed resource variances.
• **Class B (Control & Coverage Review):** 79 contextual perimeter observations.
• **Class C (Evidence Unverified / Bounded):** 0 restricted scope indicators.
• **Annualized Cloud Cost Recovery Potential:** $3,043.20 annualized projected savings.

ANNUALIZED CLOUD COST RECOVERY POTENTIAL

$3,043.20 **USD / Annualized Basis**

SOVEREIGN-28 APEX OMNI ARTIFACT CUSTODY

Cryptographic Evidence Envelope & Forensic Control Coverage

ARTIFACT CLASSIFICATION	CONFIDENTIAL - Institutional Governance Audit Record
ARTIFACT ID	SO28-20260808-140037-3C2A8926
SCAN EXECUTION ID	SCAN-20260808-135950-914
AWS ACCOUNT ID	563336977148
ASSUMED ROLE ARN	arn:aws:sts::563336977148:assumed-role/Sovereign-28-Audit-Role/Sovereign28Audit-1786197590
IDENTITY STATUS	VERIFIED — AWS STS GetCallerIdentity
DISCOVERY METHOD	AWS STS GetCallerIdentity
RECORD A: EVIDENCE ENVELOPE SHA-384	3C2A8926F9ED6760CF10D1D4C33F71D03CF2F8D7E6AC2692 D36066F34DB97267F59BB84DA55DC2A50E58B78157FE79A4
RECORD B: ARTIFACT MANIFEST SHA-384	A297BE0FC49CDE838E01DDD4C2EA395F69C6E4550313F3BA E80FFAAAD7A5A1E958EF7E374FD009556C43FBFD68D2F7E0
EVIDENCE CAPTURED	2026-08-08T14:00:29.369934+00:00
ARTIFACT RENDERED	2026-08-08T14:00:37.136318+00:00 | DUAL SEALED

Field Institutional Forensic Audit Definition & Business Logic Coverage:

- **F1-F4 COMPUTE CORE:** EC2 Zombie drift, Lambda hygiene, and ECS Cluster maturity.
- **F5-F8 STORAGE VAULT:** EBS unattached leakage and ECR image storage tax.
- **F9-F12 DATABASE LAYER:** RDS Stopped instances and S3 Exposure risk.
- **F13-F16 VAULT & SECRET:** KMS Key Rotation and SecretMgr Credential Tax.
- **F17-F20 NETWORK PATH:** Idle EIP namespace waste and Transit Gateway drift.
- **F21-F24 IDENTITY & EDGE:** IAM MFA identity drift and WAF-less ALB exposure.
- **F25-F28 AUDIT & CERT:** Config Recorder, CloudTrail Anchor, and SHA-384 Seal.

3.0 VERIFIED GOVERNANCE SIGNALS & REMEDIATION PLAN

EXECUTIVE AUDIT RESUME & ITEMIZED CLOUD COST RECOVERY BREAKDOWN:
• **Total Quantified Annualized Recovery:** **$3,043.20 USD / yr**
• **Total Verified Control Observations:** 79 vectors isolated across 17 regions.

Service-Level Cost Leakage & Provenance:
• **EBS Service:** **$3,043.20 USD/yr** across 14 finding(s). *Calculation Provenance: Orphaned block storage volumes incurring continuous monthly charges without compute attachment.*
• **KMS Service:** 4 security/compliance control variance(s) isolated (0 direct financial waste).
• **WAF Service:** 17 security/compliance control variance(s) isolated (0 direct financial waste).
• **CONFIG Service:** 17 security/compliance control variance(s) isolated (0 direct financial waste).
• **CLOUDTRAIL Service:** 17 security/compliance control variance(s) isolated (0 direct financial waste).
• **SECURITYGROUPS Service:** 4 security/compliance control variance(s) isolated (0 direct financial waste).
• **RDS Service:** 6 security/compliance control variance(s) isolated (0 direct financial waste).

• **Remediation Priority:** Execute recommended CLI mitigations immediately to eliminate idle asset bleeding and satisfy SOC2 / FTR baselines.

VECTOR #1 | F5 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	EBS
RESOURCE ID	vol-02d1539fb8f380bfe
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-02d1539fb8f380bfe (500 GB gp2) isolated in ap-northeast-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region ap-northeast-1`

VECTOR #2 | F5 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	EBS
RESOURCE ID	vol-0800852926424f11d
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-0800852926424f11d (5 GB gp2) isolated in ap-northeast-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region ap-northeast-1`

VECTOR #3 | F5 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	EBS
RESOURCE ID	vol-07a67a5e2a7d53940
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-07a67a5e2a7d53940 (200 GB io1) isolated in ap-northeast-1.

BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region ap-northeast-1`

VECTOR #4 | F13 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	KMS
RESOURCE ID	fd79404c-074c-4045-93b6-6d182fb4d905
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	KMS Customer Managed Key fd79404c-074c-4045-93b6-6d182fb4d905 has automatic rotation disabled.
EVIDENCE	KMS Customer Managed Key fd79404c-074c-4045-93b6-6d182fb4d905 has automatic rotation disabled.
BUSINESS / SECURITY IMPACT	Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.
ACTIONABLE REMEDIATION	`aws kms enable-key-rotation --key-id fd79404c-074c-4045-93b6-6d182fb4d905 --region ap-northeast-1`

VECTOR #5 | F22 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-northeast-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-northeast-1.
EVIDENCE	No WAF Web ACLs configured in region ap-northeast-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-1`

VECTOR #6 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-northeast-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-northeast-1.
EVIDENCE	AWS Config recorder is not enabled in region ap-northeast-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-northeast-1`

VECTOR #7 | F26 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ap-northeast-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-northeast-1.
EVIDENCE	No CloudTrail trail configured in region ap-northeast-1.

BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-northeast-1`

VECTOR #8 | F21 — Governance Control Observation	
REGION	ap-northeast-1
SERVICE	SecurityGroups
RESOURCE ID	sg-0efb8fb625eb7dd0d
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	Security Group Sovereign-Test-Insecure-SG (sg-0efb8fb625eb7dd0d) exposes sensitive port 22 to 0.0.0.0/0.
EVIDENCE	Security Group Sovereign-Test-Insecure-SG (sg-0efb8fb625eb7dd0d) exposes sensitive port 22 to 0.0.0.0/0.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws ec2 revoke-security-group-ingress --group-id sg-0efb8fb625eb7dd0d --protocol tcp --port 22 --cidr 0.0.0.0/0 --region ap-northeast-1`

VECTOR #9 | F22 — Governance Control Observation	
REGION	ap-northeast-2
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-northeast-2
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-northeast-2.
EVIDENCE	No WAF Web ACLs configured in region ap-northeast-2.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-2`

VECTOR #10 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-northeast-2
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-northeast-2
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-northeast-2.
EVIDENCE	AWS Config recorder is not enabled in region ap-northeast-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-northeast-2`

VECTOR #11 | F26 — Governance Control Observation	
REGION	ap-northeast-2
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ap-northeast-2
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-northeast-2.

EVIDENCE	No CloudTrail trail configured in region ap-northeast-2.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-northeast-2`

VECTOR #12 | F22 — Governance Control Observation	
REGION	ap-northeast-3
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-northeast-3
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-northeast-3.
EVIDENCE	No WAF Web ACLs configured in region ap-northeast-3.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-3`

VECTOR #13 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-northeast-3
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-northeast-3
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-northeast-3.
EVIDENCE	AWS Config recorder is not enabled in region ap-northeast-3.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-northeast-3`

VECTOR #14 | F26 — Governance Control Observation	
REGION	ap-northeast-3
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ap-northeast-3
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-northeast-3.
EVIDENCE	No CloudTrail trail configured in region ap-northeast-3.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-3 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-northeast-3`

VECTOR #15 | F22 — Governance Control Observation	
REGION	ap-south-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-south-1
SEVERITY / TAXONOMY	LOW (Class B)

ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-south-1.
EVIDENCE	No WAF Web ACLs configured in region ap-south-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-south-1`

VECTOR #16 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-south-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-south-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-south-1.
EVIDENCE	AWS Config recorder is not enabled in region ap-south-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-south-1`

VECTOR #17 | F26 — Governance Control Observation	
REGION	ap-south-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ap-south-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-south-1.
EVIDENCE	No CloudTrail trail configured in region ap-south-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-south-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-south-1`

VECTOR #18 | F22 — Governance Control Observation	
REGION	ap-southeast-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-southeast-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-southeast-1.
EVIDENCE	No WAF Web ACLs configured in region ap-southeast-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-southeast-1`

VECTOR #19 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-southeast-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-southeast-1

SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-southeast-1.
EVIDENCE	AWS Config recorder is not enabled in region ap-southeast-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-southeast-1`

VECTOR #20 | F26 — Governance Control Observation	
REGION	ap-southeast-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ap-southeast-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-southeast-1.
EVIDENCE	No CloudTrail trail configured in region ap-southeast-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-southeast-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-southeast-1`

VECTOR #21 | F22 — Governance Control Observation	
REGION	ap-southeast-2
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ap-southeast-2
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ap-southeast-2.
EVIDENCE	No WAF Web ACLs configured in region ap-southeast-2.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-southeast-2`

VECTOR #22 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ap-southeast-2
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ap-southeast-2
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ap-southeast-2.
EVIDENCE	AWS Config recorder is not enabled in region ap-southeast-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ap-southeast-2`

VECTOR #23 | F26 — Governance Control Observation	
REGION	ap-southeast-2
SERVICE	CloudTrail

RESOURCE ID	CLOUDTRAIL-ap-southeast-2
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ap-southeast-2.
EVIDENCE	No CloudTrail trail configured in region ap-southeast-2.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ap-southeast-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ap-southeast-2`

VECTOR #24 | F22 — Governance Control Observation	
REGION	ca-central-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-ca-central-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region ca-central-1.
EVIDENCE	No WAF Web ACLs configured in region ca-central-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ca-central-1`

VECTOR #25 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	ca-central-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-ca-central-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region ca-central-1.
EVIDENCE	AWS Config recorder is not enabled in region ca-central-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region ca-central-1`

VECTOR #26 | F26 — Governance Control Observation	
REGION	ca-central-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-ca-central-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region ca-central-1.
EVIDENCE	No CloudTrail trail configured in region ca-central-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-ca-central-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region ca-central-1`

VECTOR #27 | F22 — Governance Control Observation	
REGION	eu-north-1

SERVICE	WAF
RESOURCE ID	WAF-SCOPE-eu-north-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region eu-north-1.
EVIDENCE	No WAF Web ACLs configured in region eu-north-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-north-1`

VECTOR #28 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	eu-north-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-eu-north-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region eu-north-1.
EVIDENCE	AWS Config recorder is not enabled in region eu-north-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region eu-north-1`

VECTOR #29 | F26 — Governance Control Observation	
REGION	eu-north-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-eu-north-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region eu-north-1.
EVIDENCE	No CloudTrail trail configured in region eu-north-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-eu-north-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region eu-north-1`

VECTOR #30 | F5 — Governance Control Observation	
REGION	eu-central-1
SERVICE	EBS
RESOURCE ID	vol-008f494ecb303be26
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-008f494ecb303be26 (200 GB io1) isolated in eu-central-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region eu-central-1`

VECTOR #31 | F5 — Governance Control Observation

REGION	eu-central-1
SERVICE	EBS
RESOURCE ID	vol-05f3fe4fd163a680e
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-05f3fe4fd163a680e (5 GB gp2) isolated in eu-central-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region eu-central-1`

VECTOR #32 | F5 — Governance Control Observation	
REGION	eu-central-1
SERVICE	EBS
RESOURCE ID	vol-008f45774f74d98a8
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-008f45774f74d98a8 (500 GB gp2) isolated in eu-central-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region eu-central-1`

VECTOR #33 | F13 — Governance Control Observation	
REGION	eu-central-1
SERVICE	KMS
RESOURCE ID	2a09b7a2-74da-49f1-885d-68d4768d04ed
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	KMS Customer Managed Key 2a09b7a2-74da-49f1-885d-68d4768d04ed has automatic rotation disabled.
EVIDENCE	KMS Customer Managed Key 2a09b7a2-74da-49f1-885d-68d4768d04ed has automatic rotation disabled.
BUSINESS / SECURITY IMPACT	Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.
ACTIONABLE REMEDIATION	`aws kms enable-key-rotation --key-id 2a09b7a2-74da-49f1-885d-68d4768d04ed --region eu-central-1`

VECTOR #34 | F22 — Governance Control Observation	
REGION	eu-central-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-eu-central-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region eu-central-1.
EVIDENCE	No WAF Web ACLs configured in region eu-central-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-central-1`

VECTOR #35 | SO28-CONFIG-RECORDER — Governance Control Observation

REGION	eu-central-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-eu-central-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region eu-central-1.
EVIDENCE	AWS Config recorder is not enabled in region eu-central-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region eu-central-1`

VECTOR #36 | F26 — Governance Control Observation	
REGION	eu-central-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-eu-central-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region eu-central-1.
EVIDENCE	No CloudTrail trail configured in region eu-central-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-eu-central-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region eu-central-1`

VECTOR #37 | F21 — Governance Control Observation	
REGION	eu-central-1
SERVICE	SecurityGroups
RESOURCE ID	sg-00edc9b574e7dca72
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	Security Group Sovereign-Test-Insecure-SG (sg-00edc9b574e7dca72) exposes sensitive port 22 to 0.0.0.0/0.
EVIDENCE	Security Group Sovereign-Test-Insecure-SG (sg-00edc9b574e7dca72) exposes sensitive port 22 to 0.0.0.0/0.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws ec2 revoke-security-group-ingress --group-id sg-00edc9b574e7dca72 --protocol tcp --port 22 --cidr 0.0.0.0/0 --region eu-central-1`

VECTOR #38 | F22 — Governance Control Observation	
REGION	eu-west-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-eu-west-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region eu-west-1.
EVIDENCE	No WAF Web ACLs configured in region eu-west-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-1`

VECTOR #39 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	eu-west-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-eu-west-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region eu-west-1.
EVIDENCE	AWS Config recorder is not enabled in region eu-west-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region eu-west-1`

VECTOR #40 | F26 — Governance Control Observation	
REGION	eu-west-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-eu-west-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region eu-west-1.
EVIDENCE	No CloudTrail trail configured in region eu-west-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region eu-west-1`

VECTOR #41 | F22 — Governance Control Observation	
REGION	eu-west-2
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-eu-west-2
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region eu-west-2.
EVIDENCE	No WAF Web ACLs configured in region eu-west-2.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-2`

VECTOR #42 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	eu-west-2
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-eu-west-2
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region eu-west-2.
EVIDENCE	AWS Config recorder is not enabled in region eu-west-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region eu-west-2`

VECTOR #43 | F26 — Governance Control Observation	
REGION	eu-west-2
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-eu-west-2
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region eu-west-2.
EVIDENCE	No CloudTrail trail configured in region eu-west-2.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region eu-west-2`

VECTOR #44 | F22 — Governance Control Observation	
REGION	eu-west-3
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-eu-west-3
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region eu-west-3.
EVIDENCE	No WAF Web ACLs configured in region eu-west-3.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-3`

VECTOR #45 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	eu-west-3
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-eu-west-3
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region eu-west-3.
EVIDENCE	AWS Config recorder is not enabled in region eu-west-3.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region eu-west-3`

VECTOR #46 | F26 — Governance Control Observation	
REGION	eu-west-3
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-eu-west-3
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region eu-west-3.
EVIDENCE	No CloudTrail trail configured in region eu-west-3.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.

ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-3 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region eu-west-3`

VECTOR #47 | F5 — Governance Control Observation	
REGION	us-east-1
SERVICE	EBS
RESOURCE ID	vol-027b8c8f2d5d48dc8
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-027b8c8f2d5d48dc8 (5 GB gp2) isolated in us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-east-1`

VECTOR #48 | F5 — Governance Control Observation	
REGION	us-east-1
SERVICE	EBS
RESOURCE ID	vol-0aba25df62e81d60a
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-0aba25df62e81d60a (250 GB gp2) isolated in us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-east-1`

VECTOR #49 | F5 — Governance Control Observation	
REGION	us-east-1
SERVICE	EBS
RESOURCE ID	vol-09d3824b5d92e6697
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-09d3824b5d92e6697 (200 GB io1) isolated in us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-east-1`

VECTOR #50 | F5 — Governance Control Observation	
REGION	us-east-1
SERVICE	EBS
RESOURCE ID	vol-08b55af761ddb56e3
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-08b55af761ddb56e3 (500 GB gp2) isolated in us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.

ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-east-1`

VECTOR #51 | F5 — Governance Control Observation	
REGION	us-east-1
SERVICE	EBS
RESOURCE ID	vol-089ff05621c6217da
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-089ff05621c6217da (100 GB io1) isolated in us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-east-1`

VECTOR #52 | F10 — Governance Control Observation	
REGION	us-east-1
SERVICE	RDS
RESOURCE ID	sovereign-highrisk-db
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-highrisk-db is publicly accessible.
EVIDENCE	RDS Database instance sovereign-highrisk-db is publicly accessible.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws rds modify-db-instance --db-instance-identifier sovereign-highrisk-db --no-publicly-accessible --apply-immediately --region us-east-1`

VECTOR #53 | F11 — Governance Control Observation	
REGION	us-east-1
SERVICE	RDS
RESOURCE ID	sovereign-highrisk-db
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-highrisk-db storage is unencrypted.
EVIDENCE	RDS Database instance sovereign-highrisk-db storage is unencrypted.
BUSINESS / SECURITY IMPACT	Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection.
ACTIONABLE REMEDIATION	`Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.`

VECTOR #54 | F10 — Governance Control Observation	
REGION	us-east-1
SERVICE	RDS
RESOURCE ID	sovereign-risk-01
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-risk-01 is publicly accessible.
EVIDENCE	RDS Database instance sovereign-risk-01 is publicly accessible.

BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws rds modify-db-instance --db-instance-identifier sovereign-risk-01 --no-publicly-accessible --apply-immediately --region us-east-1`

VECTOR #55 | F11 — Governance Control Observation	
REGION	us-east-1
SERVICE	RDS
RESOURCE ID	sovereign-risk-01
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-risk-01 storage is unencrypted.
EVIDENCE	RDS Database instance sovereign-risk-01 storage is unencrypted.
BUSINESS / SECURITY IMPACT	Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection.
ACTIONABLE REMEDIATION	`Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.`

VECTOR #56 | F13 — Governance Control Observation	
REGION	us-east-1
SERVICE	KMS
RESOURCE ID	e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	KMS Customer Managed Key e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 has automatic rotation disabled.
EVIDENCE	KMS Customer Managed Key e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 has automatic rotation disabled.
BUSINESS / SECURITY IMPACT	Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.
ACTIONABLE REMEDIATION	`aws kms enable-key-rotation --key-id e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 --region us-east-1`

VECTOR #57 | F22 — Governance Control Observation	
REGION	us-east-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-us-east-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region us-east-1.
EVIDENCE	No WAF Web ACLs configured in region us-east-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-east-1`

VECTOR #58 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	us-east-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-us-east-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region us-east-1.

EVIDENCE	AWS Config recorder is not enabled in region us-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region us-east-1`

VECTOR #59 | F26 — Governance Control Observation	
REGION	us-east-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-us-east-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region us-east-1.
EVIDENCE	No CloudTrail trail configured in region us-east-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-us-east-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region us-east-1`

VECTOR #60 | F21 — Governance Control Observation	
REGION	us-east-1
SERVICE	SecurityGroups
RESOURCE ID	sg-0795b7bf80d854916
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	Security Group Sovereign-Test-Insecure-SG (sg-0795b7bf80d854916) exposes sensitive port 22 to 0.0.0.0/0.
EVIDENCE	Security Group Sovereign-Test-Insecure-SG (sg-0795b7bf80d854916) exposes sensitive port 22 to 0.0.0.0/0.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws ec2 revoke-security-group-ingress --group-id sg-0795b7bf80d854916 --protocol tcp --port 22 --cidr 0.0.0.0/0 --region us-east-1`

VECTOR #61 | F22 — Governance Control Observation	
REGION	us-east-2
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-us-east-2
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region us-east-2.
EVIDENCE	No WAF Web ACLs configured in region us-east-2.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-east-2`

VECTOR #62 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	us-east-2
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-us-east-2
SEVERITY / TAXONOMY	MEDIUM (Class B)

ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region us-east-2.
EVIDENCE	AWS Config recorder is not enabled in region us-east-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region us-east-2`

VECTOR #63 | F26 — Governance Control Observation	
REGION	us-east-2
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-us-east-2
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region us-east-2.
EVIDENCE	No CloudTrail trail configured in region us-east-2.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-us-east-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region us-east-2`

VECTOR #64 | F22 — Governance Control Observation	
REGION	sa-east-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-sa-east-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region sa-east-1.
EVIDENCE	No WAF Web ACLs configured in region sa-east-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region sa-east-1`

VECTOR #65 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	sa-east-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-sa-east-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region sa-east-1.
EVIDENCE	AWS Config recorder is not enabled in region sa-east-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region sa-east-1`

VECTOR #66 | F26 — Governance Control Observation	
REGION	sa-east-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-sa-east-1

SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region sa-east-1.
EVIDENCE	No CloudTrail trail configured in region sa-east-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-sa-east-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region sa-east-1`

VECTOR #67 | F22 — Governance Control Observation	
REGION	us-west-1
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-us-west-1
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region us-west-1.
EVIDENCE	No WAF Web ACLs configured in region us-west-1.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-west-1`

VECTOR #68 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	us-west-1
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-us-west-1
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region us-west-1.
EVIDENCE	AWS Config recorder is not enabled in region us-west-1.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region us-west-1`

VECTOR #69 | F26 — Governance Control Observation	
REGION	us-west-1
SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-us-west-1
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region us-west-1.
EVIDENCE	No CloudTrail trail configured in region us-west-1.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-us-west-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region us-west-1`

VECTOR #70 | F5 — Governance Control Observation	
REGION	us-west-2
SERVICE	EBS

RESOURCE ID	vol-041e43e1f1bb04282
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-041e43e1f1bb04282 (500 GB gp2) isolated in us-west-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-west-2`

VECTOR #71 | F5 — Governance Control Observation	
REGION	us-west-2
SERVICE	EBS
RESOURCE ID	vol-0d17277f27f9c8943
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-0d17277f27f9c8943 (5 GB gp2) isolated in us-west-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-west-2`

VECTOR #72 | F5 — Governance Control Observation	
REGION	us-west-2
SERVICE	EBS
RESOURCE ID	vol-03ee6c78d0efdbf4e
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	F5
EVIDENCE	Unattached EBS Volume vol-03ee6c78d0efdbf4e (200 GB io1) isolated in us-west-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws ebs describe-resources --region us-west-2`

VECTOR #73 | F10 — Governance Control Observation	
REGION	us-west-2
SERVICE	RDS
RESOURCE ID	sovereign-truth-test
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-truth-test is publicly accessible.
EVIDENCE	RDS Database instance sovereign-truth-test is publicly accessible.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws rds modify-db-instance --db-instance-identifier sovereign-truth-test --no-publicly-accessible --apply-immediately --region us-west-2`

VECTOR #74 | F11 — Governance Control Observation	
REGION	us-west-2
SERVICE	RDS

RESOURCE ID	sovereign-truth-test
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	RDS Database instance sovereign-truth-test storage is unencrypted.
EVIDENCE	RDS Database instance sovereign-truth-test storage is unencrypted.
BUSINESS / SECURITY IMPACT	Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection.
ACTIONABLE REMEDIATION	`Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.`

VECTOR #75 | F13 — Governance Control Observation	
REGION	us-west-2
SERVICE	KMS
RESOURCE ID	b5c09cee-da3b-4647-aae4-76d08be83f94
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	KMS Customer Managed Key b5c09cee-da3b-4647-aae4-76d08be83f94 has automatic rotation disabled.
EVIDENCE	KMS Customer Managed Key b5c09cee-da3b-4647-aae4-76d08be83f94 has automatic rotation disabled.
BUSINESS / SECURITY IMPACT	Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.
ACTIONABLE REMEDIATION	`aws kms enable-key-rotation --key-id b5c09cee-da3b-4647-aae4-76d08be83f94 --region us-west-2`

VECTOR #76 | F22 — Governance Control Observation	
REGION	us-west-2
SERVICE	WAF
RESOURCE ID	WAF-SCOPE-us-west-2
SEVERITY / TAXONOMY	LOW (Class B)
ISSUE & DESCRIPTION	No WAF Web ACLs configured in region us-west-2.
EVIDENCE	No WAF Web ACLs configured in region us-west-2.
BUSINESS / SECURITY IMPACT	Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.
ACTIONABLE REMEDIATION	`aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-west-2`

VECTOR #77 | SO28-CONFIG-RECORDER — Governance Control Observation	
REGION	us-west-2
SERVICE	Config
RESOURCE ID	CONFIG-RECORDER-us-west-2
SEVERITY / TAXONOMY	MEDIUM (Class B)
ISSUE & DESCRIPTION	AWS Config recorder is not enabled in region us-west-2.
EVIDENCE	AWS Config recorder is not enabled in region us-west-2.
BUSINESS / SECURITY IMPACT	Deviation from Well-Architected operational baseline parameters.
ACTIONABLE REMEDIATION	`aws config describe-resources --region us-west-2`

VECTOR #78 | F26 — Governance Control Observation	
REGION	us-west-2

SERVICE	CloudTrail
RESOURCE ID	CLOUDTRAIL-us-west-2
SEVERITY / TAXONOMY	HIGH (Class B)
ISSUE & DESCRIPTION	No CloudTrail trail configured in region us-west-2.
EVIDENCE	No CloudTrail trail configured in region us-west-2.
BUSINESS / SECURITY IMPACT	Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.
ACTIONABLE REMEDIATION	`aws cloudtrail create-trail --name enterprise-audit-trail-us-west-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region us-west-2`

VECTOR #79 | F21 — Governance Control Observation	
REGION	us-west-2
SERVICE	SecurityGroups
RESOURCE ID	sg-0dc1703cfbcdea03e
SEVERITY / TAXONOMY	CRITICAL (Class B)
ISSUE & DESCRIPTION	Security Group Sovereign-Test-Insecure-SG (sg-0dc1703cfbcdea03e) exposes sensitive port 22 to 0.0.0.0/0.
EVIDENCE	Security Group Sovereign-Test-Insecure-SG (sg-0dc1703cfbcdea03e) exposes sensitive port 22 to 0.0.0.0/0.
BUSINESS / SECURITY IMPACT	Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.
ACTIONABLE REMEDIATION	`aws ec2 revoke-security-group-ingress --group-id sg-0dc1703cfbcdea03e --protocol tcp --port 22 --cidr 0.0.0.0/0 --region us-west-2`

APPENDIX A: MACHINE-READABLE GRC MANIFEST

Canonical JSON evidence envelope for ServiceNow, Splunk, and enterprise GRC pipeline ingestion.


```
{
  "artifact_id": "SO28-20260808-140037-3C2A8926",
  "scan_execution_id": "SCAN-20260808-135950-914",
  "schema_version": "S28-ENTERPRISE-A2",
  "hash_algorithm": "SHA-384",
  "evidence_envelope_sha384": "3C2A8926F9ED6760CF10D1D4C33F71D03CF2F8D7E6AC2692D36066F34DB97267F59BB84DA55DC2A50E58B78157FE79A4",
  "artifact_manifest_sha384": "A297BE0FC49CDE838E01DDD4C2EA395F69C6E4550313F3BAE80FFAAAD7A5A1E958EF7E374FD009556C43FBFD68D2F7E0",
  "principal_account": "563336977148",
  "assumed_role": "arn:aws:sts::563336977148:assumed-role/Sovereign-28-Audit-Role/Sovereign28Audit-1786197590",
  "engine_version": "Sovereign-28 v236.40-production-ready",
  "evidence_captured_at": "2026-08-08T14:00:29.369934+00:00",
  "finding_class_distribution": {
    "A": 0,
    "B": 79,
    "C": 0
  },
  "projected_annual_recovery_usd": 3043.2,
  "regions_evaluated": [
    "ap-northeast-1",
    "ap-northeast-2",
    "ap-northeast-3",
    "ap-south-1",
    "ap-southeast-1",
    "ap-southeast-2",
    "ca-central-1",
    "eu-central-1",
    "eu-north-1",
    "eu-west-1",
    "eu-west-2",
    "eu-west-3",
    "sa-east-1",
    "us-east-1",
    "us-east-2",
    "us-west-1",
    "us-west-2"
  ],
  "findings": [
    {
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "evidence": "Unattached EBS Volume vol-02d1539fb8f380bfe (500 GB gp2) isolated in ap-northeast-1.",
      "resource_id": "vol-02d1539fb8f380bfe",
      "field_id": "F5",
      "remediation": "aws ebs describe-resources --region ap-northeast-1",
      "field_name": "Governance Control Observation",
      "service": "EBS",
      "id": "F5",
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "region": "ap-northeast-1",
      "severity": "MEDIUM",
      "annual_recovery": 480,
      "monthly_exposure": 40,
      "title": "F5"
    },
    {
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "evidence": "Unattached EBS Volume vol-0800852926424f11d (5 GB gp2) isolated in ap-northeast-1.",
      "annual_recovery": 4.800000000000001,
      "severity": "MEDIUM",
      "region": "ap-northeast-1",
      "id": "F5",
      "remediation": "aws ebs describe-resources --region ap-northeast-1",
      "field_id": "F5",
      "field_name": "Governance Control Observation",
      "service": "EBS",
      "title": "F5",
      "monthly_exposure": 0.4,
      "resource_id": "vol-0800852926424f11d"
    },
    {
      "annual_recovery": 192,
      "id": "F5",
      "monthly_exposure": 16,
      "remediation": "aws ebs describe-resources --region ap-northeast-1",
      "evidence": "Unattached EBS Volume vol-07a67a5e2a7d53940 (200 GB io1) isolated in ap-northeast-1.",
      "resource_id": "vol-07a67a5e2a7d53940",
      "field_name": "Governance Control Observation",
      "field_id": "F5",
      "region": "ap-northeast-1",
      "service": "EBS",
      "title": "F5",
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "severity": "MEDIUM",
      "impact": "Deviation from Well-Architected operational baseline parameters."
    },
    {
      "remediation": "aws kms enable-key-rotation --key-id fd79404c-074c-4045-93b6-6d182fb4d905 --region ap-northeast-1",
      "field_name": "Governance Control Observation",
```

```
      "resource_id": "fd79404c-074c-4045-93b6-6d182fb4d905",
      "severity": "MEDIUM",
      "domain": "KMS",
      "impact": "Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.",
      "id": "SO28-KMS-ROTATION",
      "region": "ap-northeast-1",
      "annual_recovery": 0,
      "title": "KMS Customer Managed Key fd79404c-074c-4045-93b6-6d182fb4d905 has automatic rotation disabled.",
      "metadata": {
        "key_arn": "arn:aws:kms:ap-northeast-1:563336977148:key/fd79404c-074c-4045-93b6-6d182fb4d905"
      },
      "evidence": "KMS Customer Managed Key fd79404c-074c-4045-93b6-6d182fb4d905 has automatic rotation disabled.",
      "field_id": "F13"
    },
    {
      "resource_id": "WAF-SCOPE-ap-northeast-1",
      "region": "ap-northeast-1",
      "annual_recovery": 0,
      "title": "No WAF Web ACLs configured in region ap-northeast-1.",
      "field_id": "F22",
      "severity": "LOW",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "domain": "WAF",
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_name": "Governance Control Observation",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-1",
      "id": "SO28-WAF-MISSING",
      "evidence": "No WAF Web ACLs configured in region ap-northeast-1."
    },
    {
      "field_id": "SO28-CONFIG-RECORDER",
      "evidence": "AWS Config recorder is not enabled in region ap-northeast-1.",
      "remediation": "aws config describe-resources --region ap-northeast-1",
      "domain": "Config",
      "severity": "MEDIUM",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "region": "ap-northeast-1",
      "resource_id": "CONFIG-RECORDER-ap-northeast-1",
      "field_name": "Governance Control Observation",
      "annual_recovery": 0,
      "title": "AWS Config recorder is not enabled in region ap-northeast-1.",
      "id": "SO28-CONFIG-RECORDER",
      "metadata": {
        "region": "ap-northeast-1"
      }
    },
    {
      "id": "SO28-TRAIL-MISSING",
      "field_id": "F26",
      "annual_recovery": 0,
      "domain": "CloudTrail",
      "evidence": "No CloudTrail trail configured in region ap-northeast-1.",
      "resource_id": "CLOUDTRAIL-ap-northeast-1",
      "region": "ap-northeast-1",
      "field_name": "Governance Control Observation",
      "title": "No CloudTrail trail configured in region ap-northeast-1.",
      "severity": "HIGH",
      "metadata": {
        "region": "ap-northeast-1"
      },
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --reg
ion ap-northeast-1"
    },
    {
      "severity": "CRITICAL",
      "metadata": {
        "group_name": "Sovereign-Test-Insecure-SG",
        "port": 22
      },
      "annual_recovery": 0,
      "field_name": "Governance Control Observation",
      "region": "ap-northeast-1",
      "id": "SO28-SG-UNRESTRICTED",
      "resource_id": "sg-0efb8fb625eb7dd0d",
      "field_id": "F21",
      "evidence": "Security Group Sovereign-Test-Insecure-SG (sg-0efb8fb625eb7dd0d) exposes sensitive port 22 to 0.0.0.0/0.",
      "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
      "domain": "SecurityGroups",
      "remediation": "aws ec2 revoke-security-group-ingress --group-id sg-0efb8fb625eb7dd0d --protocol tcp --port 22 --cidr 0.0.0.0/0 --region ap-northeast-1",
      "title": "Security Group Sovereign-Test-Insecure-SG (sg-0efb8fb625eb7dd0d) exposes sensitive port 22 to 0.0.0.0/0."
    },
    {
      "title": "No WAF Web ACLs configured in region ap-northeast-2.",
      "resource_id": "WAF-SCOPE-ap-northeast-2",
      "evidence": "No WAF Web ACLs configured in region ap-northeast-2.",
      "domain": "WAF",
      "annual_recovery": 0,
      "id": "SO28-WAF-MISSING",
      "region": "ap-northeast-2",
      "severity": "LOW",
      "metadata": {
        "scope": "REGIONAL"
```

```
      },
      "field_id": "F22",
      "field_name": "Governance Control Observation",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-2"
    },
    {
      "evidence": "AWS Config recorder is not enabled in region ap-northeast-2.",
      "field_name": "Governance Control Observation",
      "remediation": "aws config describe-resources --region ap-northeast-2",
      "severity": "MEDIUM",
      "annual_recovery": 0,
      "resource_id": "CONFIG-RECORDER-ap-northeast-2",
      "domain": "Config",
      "id": "SO28-CONFIG-RECORDER",
      "title": "AWS Config recorder is not enabled in region ap-northeast-2.",
      "metadata": {
        "region": "ap-northeast-2"
      },
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "region": "ap-northeast-2",
      "field_id": "SO28-CONFIG-RECORDER"
    },
    {
      "id": "SO28-TRAIL-MISSING",
      "resource_id": "CLOUDTRAIL-ap-northeast-2",
      "field_name": "Governance Control Observation",
      "title": "No CloudTrail trail configured in region ap-northeast-2.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --reg
ion ap-northeast-2",
      "evidence": "No CloudTrail trail configured in region ap-northeast-2.",
      "domain": "CloudTrail",
      "region": "ap-northeast-2",
      "metadata": {
        "region": "ap-northeast-2"
      },
      "field_id": "F26",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "annual_recovery": 0,
      "severity": "HIGH"
    },
    {
      "field_id": "F22",
      "annual_recovery": 0,
      "severity": "LOW",
      "region": "ap-northeast-3",
      "resource_id": "WAF-SCOPE-ap-northeast-3",
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_name": "Governance Control Observation",
      "title": "No WAF Web ACLs configured in region ap-northeast-3.",
      "evidence": "No WAF Web ACLs configured in region ap-northeast-3.",
      "domain": "WAF",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-northeast-3",
      "id": "SO28-WAF-MISSING"
    },
    {
      "region": "ap-northeast-3",
      "severity": "MEDIUM",
      "resource_id": "CONFIG-RECORDER-ap-northeast-3",
      "evidence": "AWS Config recorder is not enabled in region ap-northeast-3.",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "remediation": "aws config describe-resources --region ap-northeast-3",
      "id": "SO28-CONFIG-RECORDER",
      "field_id": "SO28-CONFIG-RECORDER",
      "domain": "Config",
      "title": "AWS Config recorder is not enabled in region ap-northeast-3.",
      "field_name": "Governance Control Observation",
      "annual_recovery": 0,
      "metadata": {
        "region": "ap-northeast-3"
      }
    },
    {
      "domain": "CloudTrail",
      "annual_recovery": 0,
      "metadata": {
        "region": "ap-northeast-3"
      },
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-northeast-3 --s3-bucket-name your-audit-bucket --is-multi-region-trail --reg
ion ap-northeast-3",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "field_name": "Governance Control Observation",
      "id": "SO28-TRAIL-MISSING",
      "region": "ap-northeast-3",
      "evidence": "No CloudTrail trail configured in region ap-northeast-3.",
      "field_id": "F26",
      "title": "No CloudTrail trail configured in region ap-northeast-3.",
      "severity": "HIGH",
      "resource_id": "CLOUDTRAIL-ap-northeast-3"
    },
    {
      "title": "No WAF Web ACLs configured in region ap-south-1.",
```

```
      "region": "ap-south-1",
      "metadata": {
        "scope": "REGIONAL"
      },
      "id": "SO28-WAF-MISSING",
      "annual_recovery": 0,
      "domain": "WAF",
      "evidence": "No WAF Web ACLs configured in region ap-south-1.",
      "field_id": "F22",
      "resource_id": "WAF-SCOPE-ap-south-1",
      "field_name": "Governance Control Observation",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "severity": "LOW",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-south-1"
    },
    {
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "id": "SO28-CONFIG-RECORDER",
      "evidence": "AWS Config recorder is not enabled in region ap-south-1.",
      "remediation": "aws config describe-resources --region ap-south-1",
      "annual_recovery": 0,
      "domain": "Config",
      "title": "AWS Config recorder is not enabled in region ap-south-1.",
      "metadata": {
        "region": "ap-south-1"
      },
      "severity": "MEDIUM",
      "region": "ap-south-1",
      "field_id": "SO28-CONFIG-RECORDER",
      "resource_id": "CONFIG-RECORDER-ap-south-1",
      "field_name": "Governance Control Observation"
    },
    {
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-south-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region
ap-south-1",
      "severity": "HIGH",
      "annual_recovery": 0,
      "resource_id": "CLOUDTRAIL-ap-south-1",
      "field_id": "F26",
      "metadata": {
        "region": "ap-south-1"
      },
      "evidence": "No CloudTrail trail configured in region ap-south-1.",
      "field_name": "Governance Control Observation",
      "region": "ap-south-1",
      "title": "No CloudTrail trail configured in region ap-south-1.",
      "domain": "CloudTrail",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "id": "SO28-TRAIL-MISSING"
    },
    {
      "title": "No WAF Web ACLs configured in region ap-southeast-1.",
      "evidence": "No WAF Web ACLs configured in region ap-southeast-1.",
      "id": "SO28-WAF-MISSING",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-southeast-1",
      "annual_recovery": 0,
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "region": "ap-southeast-1",
      "domain": "WAF",
      "metadata": {
        "scope": "REGIONAL"
      },
      "severity": "LOW",
      "field_id": "F22",
      "field_name": "Governance Control Observation",
      "resource_id": "WAF-SCOPE-ap-southeast-1"
    },
    {
      "evidence": "AWS Config recorder is not enabled in region ap-southeast-1.",
      "id": "SO28-CONFIG-RECORDER",
      "title": "AWS Config recorder is not enabled in region ap-southeast-1.",
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "resource_id": "CONFIG-RECORDER-ap-southeast-1",
      "annual_recovery": 0,
      "region": "ap-southeast-1",
      "domain": "Config",
      "severity": "MEDIUM",
      "metadata": {
        "region": "ap-southeast-1"
      },
      "remediation": "aws config describe-resources --region ap-southeast-1",
      "field_id": "SO28-CONFIG-RECORDER"
    },
    {
      "title": "No CloudTrail trail configured in region ap-southeast-1.",
      "resource_id": "CLOUDTRAIL-ap-southeast-1",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "domain": "CloudTrail",
      "annual_recovery": 0,
      "severity": "HIGH",
      "region": "ap-southeast-1",
      "field_id": "F26",
      "id": "SO28-TRAIL-MISSING",
      "field_name": "Governance Control Observation",
```

```
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-southeast-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --reg
ion ap-southeast-1",
      "metadata": {
        "region": "ap-southeast-1"
      },
      "evidence": "No CloudTrail trail configured in region ap-southeast-1."
    },
    {
      "id": "SO28-WAF-MISSING",
      "domain": "WAF",
      "region": "ap-southeast-2",
      "metadata": {
        "scope": "REGIONAL"
      },
      "title": "No WAF Web ACLs configured in region ap-southeast-2.",
      "field_id": "F22",
      "evidence": "No WAF Web ACLs configured in region ap-southeast-2.",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "annual_recovery": 0,
      "severity": "LOW",
      "resource_id": "WAF-SCOPE-ap-southeast-2",
      "field_name": "Governance Control Observation",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ap-southeast-2"
    },
    {
      "field_id": "SO28-CONFIG-RECORDER",
      "annual_recovery": 0,
      "field_name": "Governance Control Observation",
      "evidence": "AWS Config recorder is not enabled in region ap-southeast-2.",
      "remediation": "aws config describe-resources --region ap-southeast-2",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "id": "SO28-CONFIG-RECORDER",
      "title": "AWS Config recorder is not enabled in region ap-southeast-2.",
      "severity": "MEDIUM",
      "resource_id": "CONFIG-RECORDER-ap-southeast-2",
      "region": "ap-southeast-2",
      "metadata": {
        "region": "ap-southeast-2"
      },
      "domain": "Config"
    },
    {
      "domain": "CloudTrail",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ap-southeast-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --reg
ion ap-southeast-2",
      "region": "ap-southeast-2",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "field_id": "F26",
      "metadata": {
        "region": "ap-southeast-2"
      },
      "title": "No CloudTrail trail configured in region ap-southeast-2.",
      "id": "SO28-TRAIL-MISSING",
      "resource_id": "CLOUDTRAIL-ap-southeast-2",
      "severity": "HIGH",
      "annual_recovery": 0,
      "field_name": "Governance Control Observation",
      "evidence": "No CloudTrail trail configured in region ap-southeast-2."
    },
    {
      "resource_id": "WAF-SCOPE-ca-central-1",
      "severity": "LOW",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "domain": "WAF",
      "title": "No WAF Web ACLs configured in region ca-central-1.",
      "evidence": "No WAF Web ACLs configured in region ca-central-1.",
      "id": "SO28-WAF-MISSING",
      "field_name": "Governance Control Observation",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region ca-central-1",
      "annual_recovery": 0,
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_id": "F22",
      "region": "ca-central-1"
    },
    {
      "resource_id": "CONFIG-RECORDER-ca-central-1",
      "metadata": {
        "region": "ca-central-1"
      },
      "title": "AWS Config recorder is not enabled in region ca-central-1.",
      "severity": "MEDIUM",
      "field_id": "SO28-CONFIG-RECORDER",
      "field_name": "Governance Control Observation",
      "evidence": "AWS Config recorder is not enabled in region ca-central-1.",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "id": "SO28-CONFIG-RECORDER",
      "remediation": "aws config describe-resources --region ca-central-1",
      "region": "ca-central-1",
      "annual_recovery": 0,
      "domain": "Config"
    },
    {
      "region": "ca-central-1",
```

```
      "field_id": "F26",
      "evidence": "No CloudTrail trail configured in region ca-central-1.",
      "id": "SO28-TRAIL-MISSING",
      "metadata": {
        "region": "ca-central-1"
      },
      "resource_id": "CLOUDTRAIL-ca-central-1",
      "domain": "CloudTrail",
      "field_name": "Governance Control Observation",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-ca-central-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --regio
n ca-central-1",
      "title": "No CloudTrail trail configured in region ca-central-1.",
      "severity": "HIGH",
      "annual_recovery": 0
    },
    {
      "field_id": "F22",
      "metadata": {
        "scope": "REGIONAL"
      },
      "id": "SO28-WAF-MISSING",
      "title": "No WAF Web ACLs configured in region eu-north-1.",
      "severity": "LOW",
      "annual_recovery": 0,
      "resource_id": "WAF-SCOPE-eu-north-1",
      "field_name": "Governance Control Observation",
      "evidence": "No WAF Web ACLs configured in region eu-north-1.",
      "domain": "WAF",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "region": "eu-north-1",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-north-1"
    },
    {
      "field_id": "SO28-CONFIG-RECORDER",
      "title": "AWS Config recorder is not enabled in region eu-north-1.",
      "field_name": "Governance Control Observation",
      "resource_id": "CONFIG-RECORDER-eu-north-1",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "remediation": "aws config describe-resources --region eu-north-1",
      "metadata": {
        "region": "eu-north-1"
      },
      "evidence": "AWS Config recorder is not enabled in region eu-north-1.",
      "id": "SO28-CONFIG-RECORDER",
      "domain": "Config",
      "severity": "MEDIUM",
      "region": "eu-north-1",
      "annual_recovery": 0
    },
    {
      "annual_recovery": 0,
      "resource_id": "CLOUDTRAIL-eu-north-1",
      "severity": "HIGH",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "domain": "CloudTrail",
      "title": "No CloudTrail trail configured in region eu-north-1.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-eu-north-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region
eu-north-1",
      "id": "SO28-TRAIL-MISSING",
      "region": "eu-north-1",
      "field_id": "F26",
      "field_name": "Governance Control Observation",
      "metadata": {
        "region": "eu-north-1"
      },
      "evidence": "No CloudTrail trail configured in region eu-north-1."
    },
    {
      "field_id": "F5",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "evidence": "Unattached EBS Volume vol-008f494ecb303be26 (200 GB io1) isolated in eu-central-1.",
      "annual_recovery": 192,
      "id": "F5",
      "resource_id": "vol-008f494ecb303be26",
      "region": "eu-central-1",
      "severity": "MEDIUM",
      "service": "EBS",
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "remediation": "aws ebs describe-resources --region eu-central-1",
      "title": "F5",
      "field_name": "Governance Control Observation",
      "monthly_exposure": 16
    },
    {
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "severity": "MEDIUM",
      "monthly_exposure": 0.4,
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "id": "F5",
      "evidence": "Unattached EBS Volume vol-05f3fe4fd163a680e (5 GB gp2) isolated in eu-central-1.",
      "region": "eu-central-1",
      "remediation": "aws ebs describe-resources --region eu-central-1",
      "field_name": "Governance Control Observation",
      "title": "F5",
```

```
      "service": "EBS",
      "field_id": "F5",
      "resource_id": "vol-05f3fe4fd163a680e",
      "annual_recovery": 4.800000000000001
    },
    {
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "id": "F5",
      "region": "eu-central-1",
      "remediation": "aws ebs describe-resources --region eu-central-1",
      "service": "EBS",
      "resource_id": "vol-008f45774f74d98a8",
      "monthly_exposure": 40,
      "evidence": "Unattached EBS Volume vol-008f45774f74d98a8 (500 GB gp2) isolated in eu-central-1.",
      "field_name": "Governance Control Observation",
      "annual_recovery": 480,
      "title": "F5",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "field_id": "F5",
      "severity": "MEDIUM"
    },
    {
      "region": "eu-central-1",
      "field_id": "F13",
      "impact": "Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.",
      "remediation": "aws kms enable-key-rotation --key-id 2a09b7a2-74da-49f1-885d-68d4768d04ed --region eu-central-1",
      "severity": "MEDIUM",
      "annual_recovery": 0,
      "domain": "KMS",
      "resource_id": "2a09b7a2-74da-49f1-885d-68d4768d04ed",
      "evidence": "KMS Customer Managed Key 2a09b7a2-74da-49f1-885d-68d4768d04ed has automatic rotation disabled.",
      "id": "SO28-KMS-ROTATION",
      "metadata": {
        "key_arn": "arn:aws:kms:eu-central-1:563336977148:key/2a09b7a2-74da-49f1-885d-68d4768d04ed"
      },
      "title": "KMS Customer Managed Key 2a09b7a2-74da-49f1-885d-68d4768d04ed has automatic rotation disabled.",
      "field_name": "Governance Control Observation"
    },
    {
      "resource_id": "WAF-SCOPE-eu-central-1",
      "annual_recovery": 0,
      "id": "SO28-WAF-MISSING",
      "domain": "WAF",
      "region": "eu-central-1",
      "evidence": "No WAF Web ACLs configured in region eu-central-1.",
      "title": "No WAF Web ACLs configured in region eu-central-1.",
      "severity": "LOW",
      "field_id": "F22",
      "field_name": "Governance Control Observation",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "metadata": {
        "scope": "REGIONAL"
      },
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-central-1"
    },
    {
      "evidence": "AWS Config recorder is not enabled in region eu-central-1.",
      "annual_recovery": 0,
      "severity": "MEDIUM",
      "domain": "Config",
      "region": "eu-central-1",
      "resource_id": "CONFIG-RECORDER-eu-central-1",
      "field_id": "SO28-CONFIG-RECORDER",
      "remediation": "aws config describe-resources --region eu-central-1",
      "id": "SO28-CONFIG-RECORDER",
      "metadata": {
        "region": "eu-central-1"
      },
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "title": "AWS Config recorder is not enabled in region eu-central-1."
    },
    {
      "annual_recovery": 0,
      "severity": "HIGH",
      "resource_id": "CLOUDTRAIL-eu-central-1",
      "title": "No CloudTrail trail configured in region eu-central-1.",
      "field_name": "Governance Control Observation",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-eu-central-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --regio
n eu-central-1",
      "field_id": "F26",
      "evidence": "No CloudTrail trail configured in region eu-central-1.",
      "domain": "CloudTrail",
      "id": "SO28-TRAIL-MISSING",
      "metadata": {
        "region": "eu-central-1"
      },
      "region": "eu-central-1"
    },
    {
      "region": "eu-central-1",
      "field_id": "F21",
      "evidence": "Security Group Sovereign-Test-Insecure-SG (sg-00edc9b574e7dca72) exposes sensitive port 22 to 0.0.0.0/0.",
      "annual_recovery": 0,
```

```
      "metadata": {
        "group_name": "Sovereign-Test-Insecure-SG",
        "port": 22
      },
      "field_name": "Governance Control Observation",
      "id": "SO28-SG-UNRESTRICTED",
      "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
      "remediation": "aws ec2 revoke-security-group-ingress --group-id sg-00edc9b574e7dca72 --protocol tcp --port 22 --cidr 0.0.0.0/0 --region eu-central-1",
      "domain": "SecurityGroups",
      "title": "Security Group Sovereign-Test-Insecure-SG (sg-00edc9b574e7dca72) exposes sensitive port 22 to 0.0.0.0/0.",
      "severity": "CRITICAL",
      "resource_id": "sg-00edc9b574e7dca72"
    },
    {
      "resource_id": "WAF-SCOPE-eu-west-1",
      "annual_recovery": 0,
      "region": "eu-west-1",
      "evidence": "No WAF Web ACLs configured in region eu-west-1.",
      "domain": "WAF",
      "id": "SO28-WAF-MISSING",
      "title": "No WAF Web ACLs configured in region eu-west-1.",
      "severity": "LOW",
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_id": "F22",
      "field_name": "Governance Control Observation",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-1",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks."
    },
    {
      "field_id": "SO28-CONFIG-RECORDER",
      "metadata": {
        "region": "eu-west-1"
      },
      "annual_recovery": 0,
      "severity": "MEDIUM",
      "resource_id": "CONFIG-RECORDER-eu-west-1",
      "field_name": "Governance Control Observation",
      "evidence": "AWS Config recorder is not enabled in region eu-west-1.",
      "id": "SO28-CONFIG-RECORDER",
      "region": "eu-west-1",
      "domain": "Config",
      "title": "AWS Config recorder is not enabled in region eu-west-1.",
      "remediation": "aws config describe-resources --region eu-west-1",
      "impact": "Deviation from Well-Architected operational baseline parameters."
    },
    {
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region e
u-west-1",
      "evidence": "No CloudTrail trail configured in region eu-west-1.",
      "annual_recovery": 0,
      "resource_id": "CLOUDTRAIL-eu-west-1",
      "title": "No CloudTrail trail configured in region eu-west-1.",
      "id": "SO28-TRAIL-MISSING",
      "domain": "CloudTrail",
      "region": "eu-west-1",
      "severity": "HIGH",
      "metadata": {
        "region": "eu-west-1"
      },
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "field_id": "F26",
      "field_name": "Governance Control Observation"
    },
    {
      "annual_recovery": 0,
      "resource_id": "WAF-SCOPE-eu-west-2",
      "severity": "LOW",
      "id": "SO28-WAF-MISSING",
      "metadata": {
        "scope": "REGIONAL"
      },
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "field_name": "Governance Control Observation",
      "evidence": "No WAF Web ACLs configured in region eu-west-2.",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-2",
      "domain": "WAF",
      "region": "eu-west-2",
      "title": "No WAF Web ACLs configured in region eu-west-2.",
      "field_id": "F22"
    },
    {
      "annual_recovery": 0,
      "field_id": "SO28-CONFIG-RECORDER",
      "remediation": "aws config describe-resources --region eu-west-2",
      "resource_id": "CONFIG-RECORDER-eu-west-2",
      "region": "eu-west-2",
      "severity": "MEDIUM",
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "domain": "Config",
      "id": "SO28-CONFIG-RECORDER",
      "evidence": "AWS Config recorder is not enabled in region eu-west-2.",
      "title": "AWS Config recorder is not enabled in region eu-west-2.",
```

```
      "metadata": {
        "region": "eu-west-2"
      }
    },
    {
      "annual_recovery": 0,
      "field_name": "Governance Control Observation",
      "resource_id": "CLOUDTRAIL-eu-west-2",
      "region": "eu-west-2",
      "metadata": {
        "region": "eu-west-2"
      },
      "evidence": "No CloudTrail trail configured in region eu-west-2.",
      "id": "SO28-TRAIL-MISSING",
      "title": "No CloudTrail trail configured in region eu-west-2.",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "field_id": "F26",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region e
u-west-2",
      "severity": "HIGH",
      "domain": "CloudTrail"
    },
    {
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "annual_recovery": 0,
      "field_id": "F22",
      "region": "eu-west-3",
      "field_name": "Governance Control Observation",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region eu-west-3",
      "id": "SO28-WAF-MISSING",
      "resource_id": "WAF-SCOPE-eu-west-3",
      "title": "No WAF Web ACLs configured in region eu-west-3.",
      "severity": "LOW",
      "metadata": {
        "scope": "REGIONAL"
      },
      "domain": "WAF",
      "evidence": "No WAF Web ACLs configured in region eu-west-3."
    },
    {
      "resource_id": "CONFIG-RECORDER-eu-west-3",
      "remediation": "aws config describe-resources --region eu-west-3",
      "severity": "MEDIUM",
      "id": "SO28-CONFIG-RECORDER",
      "field_id": "SO28-CONFIG-RECORDER",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "evidence": "AWS Config recorder is not enabled in region eu-west-3.",
      "domain": "Config",
      "annual_recovery": 0,
      "title": "AWS Config recorder is not enabled in region eu-west-3.",
      "field_name": "Governance Control Observation",
      "region": "eu-west-3",
      "metadata": {
        "region": "eu-west-3"
      }
    },
    {
      "id": "SO28-TRAIL-MISSING",
      "metadata": {
        "region": "eu-west-3"
      },
      "evidence": "No CloudTrail trail configured in region eu-west-3.",
      "annual_recovery": 0,
      "resource_id": "CLOUDTRAIL-eu-west-3",
      "severity": "HIGH",
      "region": "eu-west-3",
      "field_id": "F26",
      "field_name": "Governance Control Observation",
      "title": "No CloudTrail trail configured in region eu-west-3.",
      "domain": "CloudTrail",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-eu-west-3 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region e
u-west-3"
    },
    {
      "region": "us-east-1",
      "resource_id": "vol-027b8c8f2d5d48dc8",
      "field_name": "Governance Control Observation",
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "id": "F5",
      "annual_recovery": 4.800000000000001,
      "severity": "MEDIUM",
      "service": "EBS",
      "monthly_exposure": 0.4,
      "evidence": "Unattached EBS Volume vol-027b8c8f2d5d48dc8 (5 GB gp2) isolated in us-east-1.",
      "field_id": "F5",
      "title": "F5",
      "remediation": "aws ebs describe-resources --region us-east-1",
      "impact": "Deviation from Well-Architected operational baseline parameters."
    },
    {
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "finding_type": "UNATTACHED_EBS_VOLUME",
      "service": "EBS",
```

```
    "monthly_exposure": 20,
    "region": "us-east-1",
    "id": "F5",
    "evidence": "Unattached EBS Volume vol-0aba25df62e81d60a (250 GB gp2) isolated in us-east-1.",
    "resource_id": "vol-0aba25df62e81d60a",
    "severity": "MEDIUM",
    "annual_recovery": 240,
    "remediation": "aws ebs describe-resources --region us-east-1",
    "field_id": "F5",
    "title": "F5"
  },
  {
    "id": "F5",
    "resource_id": "vol-09d3824b5d92e6697",
    "annual_recovery": 192,
    "monthly_exposure": 16,
    "evidence": "Unattached EBS Volume vol-09d3824b5d92e6697 (200 GB io1) isolated in us-east-1.",
    "severity": "MEDIUM",
    "field_id": "F5",
    "remediation": "aws ebs describe-resources --region us-east-1",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "title": "F5",
    "region": "us-east-1",
    "impact": "Deviation from Well-Architected operational baseline parameters.",
    "field_name": "Governance Control Observation",
    "service": "EBS"
  },
  {
    "remediation": "aws ebs describe-resources --region us-east-1",
    "field_id": "F5",
    "annual_recovery": 480,
    "severity": "MEDIUM",
    "resource_id": "vol-08b55af761ddb56e3",
    "id": "F5",
    "service": "EBS",
    "monthly_exposure": 40,
    "evidence": "Unattached EBS Volume vol-08b55af761ddb56e3 (500 GB gp2) isolated in us-east-1.",
    "region": "us-east-1",
    "field_name": "Governance Control Observation",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "title": "F5",
    "impact": "Deviation from Well-Architected operational baseline parameters."
  },
  {
    "severity": "MEDIUM",
    "service": "EBS",
    "monthly_exposure": 8,
    "id": "F5",
    "evidence": "Unattached EBS Volume vol-089ff05621c6217da (100 GB io1) isolated in us-east-1.",
    "field_name": "Governance Control Observation",
    "resource_id": "vol-089ff05621c6217da",
    "title": "F5",
    "impact": "Deviation from Well-Architected operational baseline parameters.",
    "annual_recovery": 96,
    "field_id": "F5",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "remediation": "aws ebs describe-resources --region us-east-1",
    "region": "us-east-1"
  },
  {
    "resource_id": "sovereign-highrisk-db",
    "severity": "CRITICAL",
    "title": "RDS Database instance sovereign-highrisk-db is publicly accessible.",
    "domain": "RDS",
    "annual_recovery": 0,
    "id": "SO28-RDS-PUBLIC",
    "region": "us-east-1",
    "metadata": {
      "publicly_accessible": true,
      "engine": "postgres"
    },
    "field_id": "F10",
    "field_name": "Governance Control Observation",
    "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
    "evidence": "RDS Database instance sovereign-highrisk-db is publicly accessible.",
    "remediation": "aws rds modify-db-instance --db-instance-identifier sovereign-highrisk-db --no-publicly-accessible --apply-immediately --region us-east-1"
  },
  {
    "annual_recovery": 0,
    "region": "us-east-1",
    "id": "SO28-RDS-UNENCRYPTED",
    "remediation": "Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.",
    "resource_id": "sovereign-highrisk-db",
    "field_id": "F11",
    "field_name": "Governance Control Observation",
    "severity": "HIGH",
    "metadata": {
      "engine": "postgres",
      "encrypted": false
    },
    "domain": "RDS",
    "title": "RDS Database instance sovereign-highrisk-db storage is unencrypted.",
    "evidence": "RDS Database instance sovereign-highrisk-db storage is unencrypted.",
    "impact": "Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection."
  },
```

```
    {
      "field_name": "Governance Control Observation",
      "annual_recovery": 0,
      "id": "SO28-RDS-PUBLIC",
      "title": "RDS Database instance sovereign-risk-01 is publicly accessible.",
      "region": "us-east-1",
      "resource_id": "sovereign-risk-01",
      "domain": "RDS",
      "severity": "CRITICAL",
      "evidence": "RDS Database instance sovereign-risk-01 is publicly accessible.",
      "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
      "remediation": "aws rds modify-db-instance --db-instance-identifier sovereign-risk-01 --no-publicly-accessible --apply-immediately --region us-east-1",
      "metadata": {
        "publicly_accessible": true,
        "engine": "mysql"
      },
      "field_id": "F10"
    },
    {
      "field_name": "Governance Control Observation",
      "severity": "HIGH",
      "evidence": "RDS Database instance sovereign-risk-01 storage is unencrypted.",
      "remediation": "Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.",
      "id": "SO28-RDS-UNENCRYPTED",
      "title": "RDS Database instance sovereign-risk-01 storage is unencrypted.",
      "domain": "RDS",
      "resource_id": "sovereign-risk-01",
      "region": "us-east-1",
      "annual_recovery": 0,
      "field_id": "F11",
      "impact": "Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection.",
      "metadata": {
        "engine": "mysql",
        "encrypted": false
      }
    },
    {
      "severity": "MEDIUM",
      "evidence": "KMS Customer Managed Key e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 has automatic rotation disabled.",
      "impact": "Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.",
      "resource_id": "e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53",
      "title": "KMS Customer Managed Key e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 has automatic rotation disabled.",
      "field_id": "F13",
      "field_name": "Governance Control Observation",
      "remediation": "aws kms enable-key-rotation --key-id e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53 --region us-east-1",
      "id": "SO28-KMS-ROTATION",
      "domain": "KMS",
      "annual_recovery": 0,
      "region": "us-east-1",
      "metadata": {
        "key_arn": "arn:aws:kms:us-east-1:563336977148:key/e3eaf7f3-6c8f-4bf9-be5d-394a39b93c53"
      }
    },
    {
      "id": "SO28-WAF-MISSING",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-east-1",
      "annual_recovery": 0,
      "evidence": "No WAF Web ACLs configured in region us-east-1.",
      "region": "us-east-1",
      "title": "No WAF Web ACLs configured in region us-east-1.",
      "domain": "WAF",
      "severity": "LOW",
      "resource_id": "WAF-SCOPE-us-east-1",
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_id": "F22",
      "field_name": "Governance Control Observation",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks."
    },
    {
      "id": "SO28-CONFIG-RECORDER",
      "resource_id": "CONFIG-RECORDER-us-east-1",
      "evidence": "AWS Config recorder is not enabled in region us-east-1.",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "title": "AWS Config recorder is not enabled in region us-east-1.",
      "metadata": {
        "region": "us-east-1"
      },
      "field_id": "SO28-CONFIG-RECORDER",
      "severity": "MEDIUM",
      "field_name": "Governance Control Observation",
      "remediation": "aws config describe-resources --region us-east-1",
      "annual_recovery": 0,
      "domain": "Config",
      "region": "us-east-1"
    },
    {
      "evidence": "No CloudTrail trail configured in region us-east-1.",
      "annual_recovery": 0,
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-us-east-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region u
s-east-1",
      "field_id": "F26",
      "metadata": {
        "region": "us-east-1"
```

```
      },
      "field_name": "Governance Control Observation",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "region": "us-east-1",
      "resource_id": "CLOUDTRAIL-us-east-1",
      "id": "SO28-TRAIL-MISSING",
      "domain": "CloudTrail",
      "title": "No CloudTrail trail configured in region us-east-1.",
      "severity": "HIGH"
    },
    {
      "title": "Security Group Sovereign-Test-Insecure-SG (sg-0795b7bf80d854916) exposes sensitive port 22 to 0.0.0.0/0.",
      "field_name": "Governance Control Observation",
      "remediation": "aws ec2 revoke-security-group-ingress --group-id sg-0795b7bf80d854916 --protocol tcp --port 22 --cidr 0.0.0.0/0 --region us-east-1",
      "metadata": {
        "group_name": "Sovereign-Test-Insecure-SG",
        "port": 22
      },
      "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
      "annual_recovery": 0,
      "field_id": "F21",
      "id": "SO28-SG-UNRESTRICTED",
      "evidence": "Security Group Sovereign-Test-Insecure-SG (sg-0795b7bf80d854916) exposes sensitive port 22 to 0.0.0.0/0.",
      "severity": "CRITICAL",
      "resource_id": "sg-0795b7bf80d854916",
      "domain": "SecurityGroups",
      "region": "us-east-1"
    },
    {
      "annual_recovery": 0,
      "domain": "WAF",
      "metadata": {
        "scope": "REGIONAL"
      },
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-east-2",
      "field_name": "Governance Control Observation",
      "resource_id": "WAF-SCOPE-us-east-2",
      "title": "No WAF Web ACLs configured in region us-east-2.",
      "region": "us-east-2",
      "severity": "LOW",
      "field_id": "F22",
      "evidence": "No WAF Web ACLs configured in region us-east-2.",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "id": "SO28-WAF-MISSING"
    },
    {
      "annual_recovery": 0,
      "remediation": "aws config describe-resources --region us-east-2",
      "metadata": {
        "region": "us-east-2"
      },
      "id": "SO28-CONFIG-RECORDER",
      "severity": "MEDIUM",
      "title": "AWS Config recorder is not enabled in region us-east-2.",
      "region": "us-east-2",
      "field_name": "Governance Control Observation",
      "domain": "Config",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "resource_id": "CONFIG-RECORDER-us-east-2",
      "field_id": "SO28-CONFIG-RECORDER",
      "evidence": "AWS Config recorder is not enabled in region us-east-2."
    },
    {
      "domain": "CloudTrail",
      "evidence": "No CloudTrail trail configured in region us-east-2.",
      "title": "No CloudTrail trail configured in region us-east-2.",
      "field_id": "F26",
      "id": "SO28-TRAIL-MISSING",
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "resource_id": "CLOUDTRAIL-us-east-2",
      "region": "us-east-2",
      "annual_recovery": 0,
      "severity": "HIGH",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-us-east-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region u
s-east-2",
      "field_name": "Governance Control Observation",
      "metadata": {
        "region": "us-east-2"
      }
    },
    {
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region sa-east-1",
      "id": "SO28-WAF-MISSING",
      "resource_id": "WAF-SCOPE-sa-east-1",
      "title": "No WAF Web ACLs configured in region sa-east-1.",
      "region": "sa-east-1",
      "domain": "WAF",
      "severity": "LOW",
      "annual_recovery": 0,
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_id": "F22",
      "field_name": "Governance Control Observation",
```

```
      "evidence": "No WAF Web ACLs configured in region sa-east-1."
    },
    {
      "severity": "MEDIUM",
      "title": "AWS Config recorder is not enabled in region sa-east-1.",
      "field_name": "Governance Control Observation",
      "resource_id": "CONFIG-RECORDER-sa-east-1",
      "evidence": "AWS Config recorder is not enabled in region sa-east-1.",
      "metadata": {
        "region": "sa-east-1"
      },
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "remediation": "aws config describe-resources --region sa-east-1",
      "field_id": "SO28-CONFIG-RECORDER",
      "domain": "Config",
      "annual_recovery": 0,
      "id": "SO28-CONFIG-RECORDER",
      "region": "sa-east-1"
    },
    {
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-sa-east-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region s
a-east-1",
      "metadata": {
        "region": "sa-east-1"
      },
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "field_name": "Governance Control Observation",
      "evidence": "No CloudTrail trail configured in region sa-east-1.",
      "id": "SO28-TRAIL-MISSING",
      "severity": "HIGH",
      "resource_id": "CLOUDTRAIL-sa-east-1",
      "annual_recovery": 0,
      "domain": "CloudTrail",
      "region": "sa-east-1",
      "title": "No CloudTrail trail configured in region sa-east-1.",
      "field_id": "F26"
    },
    {
      "domain": "WAF",
      "severity": "LOW",
      "evidence": "No WAF Web ACLs configured in region us-west-1.",
      "annual_recovery": 0,
      "metadata": {
        "scope": "REGIONAL"
      },
      "id": "SO28-WAF-MISSING",
      "region": "us-west-1",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "resource_id": "WAF-SCOPE-us-west-1",
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-west-1",
      "field_id": "F22",
      "title": "No WAF Web ACLs configured in region us-west-1.",
      "field_name": "Governance Control Observation"
    },
    {
      "remediation": "aws config describe-resources --region us-west-1",
      "resource_id": "CONFIG-RECORDER-us-west-1",
      "id": "SO28-CONFIG-RECORDER",
      "metadata": {
        "region": "us-west-1"
      },
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "field_id": "SO28-CONFIG-RECORDER",
      "domain": "Config",
      "region": "us-west-1",
      "annual_recovery": 0,
      "severity": "MEDIUM",
      "evidence": "AWS Config recorder is not enabled in region us-west-1.",
      "title": "AWS Config recorder is not enabled in region us-west-1."
    },
    {
      "resource_id": "CLOUDTRAIL-us-west-1",
      "id": "SO28-TRAIL-MISSING",
      "severity": "HIGH",
      "field_id": "F26",
      "metadata": {
        "region": "us-west-1"
      },
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "region": "us-west-1",
      "title": "No CloudTrail trail configured in region us-west-1.",
      "field_name": "Governance Control Observation",
      "evidence": "No CloudTrail trail configured in region us-west-1.",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-us-west-1 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region u
s-west-1",
      "domain": "CloudTrail",
      "annual_recovery": 0
    },
    {
      "region": "us-west-2",
      "field_id": "F5",
      "remediation": "aws ebs describe-resources --region us-west-2",
      "annual_recovery": 480,
      "id": "F5",
```

```
    "severity": "MEDIUM",
    "resource_id": "vol-041e43e1f1bb04282",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "impact": "Deviation from Well-Architected operational baseline parameters.",
    "service": "EBS",
    "title": "F5",
    "monthly_exposure": 40,
    "field_name": "Governance Control Observation",
    "evidence": "Unattached EBS Volume vol-041e43e1f1bb04282 (500 GB gp2) isolated in us-west-2."
  },
  {
    "title": "F5",
    "impact": "Deviation from Well-Architected operational baseline parameters.",
    "service": "EBS",
    "annual_recovery": 4.800000000000001,
    "remediation": "aws ebs describe-resources --region us-west-2",
    "id": "F5",
    "evidence": "Unattached EBS Volume vol-0d17277f27f9c8943 (5 GB gp2) isolated in us-west-2.",
    "monthly_exposure": 0.4,
    "severity": "MEDIUM",
    "field_id": "F5",
    "field_name": "Governance Control Observation",
    "resource_id": "vol-0d17277f27f9c8943",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "region": "us-west-2"
  },
  {
    "severity": "MEDIUM",
    "region": "us-west-2",
    "remediation": "aws ebs describe-resources --region us-west-2",
    "title": "F5",
    "field_id": "F5",
    "finding_type": "UNATTACHED_EBS_VOLUME",
    "service": "EBS",
    "monthly_exposure": 16,
    "annual_recovery": 192,
    "evidence": "Unattached EBS Volume vol-03ee6c78d0efdbf4e (200 GB io1) isolated in us-west-2.",
    "field_name": "Governance Control Observation",
    "impact": "Deviation from Well-Architected operational baseline parameters.",
    "resource_id": "vol-03ee6c78d0efdbf4e",
    "id": "F5"
  },
  {
    "metadata": {
      "engine": "mysql",
      "publicly_accessible": true
    },
    "field_id": "F10",
    "evidence": "RDS Database instance sovereign-truth-test is publicly accessible.",
    "region": "us-west-2",
    "annual_recovery": 0,
    "id": "SO28-RDS-PUBLIC",
    "field_name": "Governance Control Observation",
    "domain": "RDS",
    "title": "RDS Database instance sovereign-truth-test is publicly accessible.",
    "severity": "CRITICAL",
    "resource_id": "sovereign-truth-test",
    "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
    "remediation": "aws rds modify-db-instance --db-instance-identifier sovereign-truth-test --no-publicly-accessible --apply-immediately --region us-west-2"
  },
  {
    "remediation": "Create an encrypted snapshot of the DB instance, restore from snapshot with encryption enabled, and promote the new instance.",
    "field_id": "F11",
    "domain": "RDS",
    "severity": "HIGH",
    "resource_id": "sovereign-truth-test",
    "metadata": {
      "engine": "mysql",
      "encrypted": false
    },
    "field_name": "Governance Control Observation",
    "title": "RDS Database instance sovereign-truth-test storage is unencrypted.",
    "id": "SO28-RDS-UNENCRYPTED",
    "evidence": "RDS Database instance sovereign-truth-test storage is unencrypted.",
    "annual_recovery": 0,
    "impact": "Fails standard compliance mandates (PCI-DSS, HIPAA, SOC2) regarding data-at-rest protection.",
    "region": "us-west-2"
  },
  {
    "region": "us-west-2",
    "remediation": "aws kms enable-key-rotation --key-id b5c09cee-da3b-4647-aae4-76d08be83f94 --region us-west-2",
    "resource_id": "b5c09cee-da3b-4647-aae4-76d08be83f94",
    "title": "KMS Customer Managed Key b5c09cee-da3b-4647-aae4-76d08be83f94 has automatic rotation disabled.",
    "field_id": "F13",
    "annual_recovery": 0,
    "evidence": "KMS Customer Managed Key b5c09cee-da3b-4647-aae4-76d08be83f94 has automatic rotation disabled.",
    "impact": "Stale cryptographic keys increase blast radius exposure if compromise occurs over extended operational cycles.",
    "domain": "KMS",
    "id": "SO28-KMS-ROTATION",
    "severity": "MEDIUM",
    "metadata": {
      "key_arn": "arn:aws:kms:us-west-2:563336977148:key/b5c09cee-da3b-4647-aae4-76d08be83f94"
    },
    "field_name": "Governance Control Observation"
  },
```

```
    {
      "remediation": "aws wafv2 associate-web-acl --web-acl-arn <WEB_ACL_ARN> --resource-arn <RESOURCE_ARN> --region us-west-2",
      "region": "us-west-2",
      "evidence": "No WAF Web ACLs configured in region us-west-2.",
      "severity": "LOW",
      "field_id": "F22",
      "id": "SO28-WAF-MISSING",
      "domain": "WAF",
      "annual_recovery": 0,
      "title": "No WAF Web ACLs configured in region us-west-2.",
      "metadata": {
        "scope": "REGIONAL"
      },
      "field_name": "Governance Control Observation",
      "impact": "Exposes regional endpoints to common web exploits, SQL injection, cross-site scripting, and Layer 7 volumetric attacks.",
      "resource_id": "WAF-SCOPE-us-west-2"
    },
    {
      "resource_id": "CONFIG-RECORDER-us-west-2",
      "field_name": "Governance Control Observation",
      "impact": "Deviation from Well-Architected operational baseline parameters.",
      "region": "us-west-2",
      "remediation": "aws config describe-resources --region us-west-2",
      "title": "AWS Config recorder is not enabled in region us-west-2.",
      "id": "SO28-CONFIG-RECORDER",
      "metadata": {
        "region": "us-west-2"
      },
      "field_id": "SO28-CONFIG-RECORDER",
      "evidence": "AWS Config recorder is not enabled in region us-west-2.",
      "severity": "MEDIUM",
      "annual_recovery": 0,
      "domain": "Config"
    },
    {
      "impact": "Governance blind spots; unmonitored API actions can obscure forensic reconstruction during security incidents.",
      "metadata": {
        "region": "us-west-2"
      },
      "title": "No CloudTrail trail configured in region us-west-2.",
      "id": "SO28-TRAIL-MISSING",
      "domain": "CloudTrail",
      "resource_id": "CLOUDTRAIL-us-west-2",
      "field_id": "F26",
      "evidence": "No CloudTrail trail configured in region us-west-2.",
      "severity": "HIGH",
      "annual_recovery": 0,
      "region": "us-west-2",
      "field_name": "Governance Control Observation",
      "remediation": "aws cloudtrail create-trail --name enterprise-audit-trail-us-west-2 --s3-bucket-name your-audit-bucket --is-multi-region-trail --region u
s-west-2"
    },
    {
      "severity": "CRITICAL",
      "domain": "SecurityGroups",
      "resource_id": "sg-0dc1703cfbcdea03e",
      "field_id": "F21",
      "evidence": "Security Group Sovereign-Test-Insecure-SG (sg-0dc1703cfbcdea03e) exposes sensitive port 22 to 0.0.0.0/0.",
      "metadata": {
        "group_name": "Sovereign-Test-Insecure-SG",
        "port": 22
      },
      "remediation": "aws ec2 revoke-security-group-ingress --group-id sg-0dc1703cfbcdea03e --protocol tcp --port 22 --cidr 0.0.0.0/0 --region us-west-2",
      "field_name": "Governance Control Observation",
      "id": "SO28-SG-UNRESTRICTED",
      "region": "us-west-2",
      "impact": "Direct exposure of database or management ports to the public internet, dramatically increasing attack surfaces.",
      "title": "Security Group Sovereign-Test-Insecure-SG (sg-0dc1703cfbcdea03e) exposes sensitive port 22 to 0.0.0.0/0.",
      "annual_recovery": 0
    }
  ]
}
```