Infrastructure Security Posture Audit Report

Confidential

Scan window	2026-10-08 11:04 to 11:16 UTC
Scope	1 AWS account, 1 region
Account	)
Region	
Report reviewer	Ekalavya Babu ekalavya@stavir.com

Findings

12 Critical	12 High	38 Medium	18 Low	222 Passed

Critical findings (12)

Critical findings require immediate attention due to their severity.

Result	Account	Region	Resource	Observed evidence	Check
Fail				Potential secrets found in Lambda function code -> .env: AWS Secret Access Key on line 1, Generic API Key on line 2, Base64-PEM-Encoded Private Key on line 6, Contains Private Key on line 6, PEM-Encoded Private Key on line 6; package-lock.json: ZeroTier API Token on line 859; node_modules\.package-lock.json: ZeroTier API Token on line 828; node_modules\@aws-sdk\protocol-http\dist-cjs\httpRequest.js: Generic Username and Password on line 19; node_modules\@aws-sdk\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\protocol-http\dist-cjs\index.js: Generic Username and Password on line 177; node_modules\@smithy\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\@types\node\url.d.ts: URI with Username and Secret on line 353; node_modules\axios\dist\node\axios.cjs: Generic Username and Password on line 2651; node_modules\axios\dist\node\axios.cjs.map: Generic Username and Password on line 1; node_modules\axios\lib\adapters\http.js: Generic Username and Password on line 100; node_modules\axios-proxy-builder\dist\proxy-builder.js: Generic Username and Password on line 13; node_modules\chalk\readme.md: hCaptcha Site Verify Secret Key on line 24; node_modules\chai-http\README.md: Generic Password on line 112, Generic Username and Password on line 150, Generic Username and Password on line 200; node_modules\chai-http\dist\chai-http.js: Generic Username and Password on line 3565; node_modules\follow-redirects\README.md: Generic Username and Password on line 81; node_modules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\events\.travis.yml: Travis CI Encrypted	awslambda_function_no_secrets_in_code prowler Critical

Result	Account	Region	Resource	Observed evidence	Check
				Variable on line 17; node_modules\jszip\.travis.yml: Travis CI Encrypted Variable on line 15; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username and Password on line 475; node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\serverless\node_modules\.bin\serverless-windows-amd64-0.0.2: Generic Username and Password on line 5514, Generic Secret on line 6266, Generic Username and Password on line 6302; node_modules\superagent\.travis.yml: Generic API Key on line 11, Sauce Labs Access Key on line 11; node_modules\superagent\superagent.js: Generic Username and Password on line 1844; node_modules\superagent\docs\index.md: Generic Username and Password on line 477; node_modules\superagent\docs\test.html: URI with Username and Secret on line 461; node_modules\superagent\lib\client.js: Generic Username and Password on line 732; node_modules\superagent\lib\node\index.js: Generic Username and Password on line 656; node_modules\superagent\node_modules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\supertest\node_modules\superagent\dist\superagent.js: Generic Username and Password on line 2668; node_modules\supertest\node_modules\superagent\lib\client.js: Generic Username and Password on line 744, Generic Username and Password on line 944, Generic Password on line 944, Generic Username and Password on line 944; node_modules\supertest\node_modules\superagent\lib\request-base.js: Generic Username and Password on line 720, Generic Username and Password on line 720, Generic Password on line 720; node_modules\supertest\node_modules\superagent\lib\node\index.js: Generic Username and Password on line 775, Generic Username and Password on line 778, Generic Username and Password on line 1307, Generic Username and Password on line 1307, Generic Username and Password on line 1307; node_modules\swagger-jsdoc\docusaurus\yarn.lock:	

Result	Account	Region	Resource	Observed evidence	Check
				Algolia Admin API Key on line 14, Algolia Admin API Key on line 1524, Algolia Admin API Key on line 2415; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js: Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1, Generic Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\typedarray-to-buffer\.travis.yml: Travis CI Encrypted Variable on line 10; node_modules\ws\lib\websocket.js: Generic Username and Password on line 790; node_modules\z-schema\node_modules\commander\Readme.md: Generic Username and Password on line 568.	

Result	Account	Region	Resource	Observed evidence	Check
Fail				Potential secrets found in Lambda function code -> node_modules\@aws-sdk\nested-clients\dist-types\submodules\sso-oidc\commands\CreateTokenCommand.d.ts: Generic Secret on line 124, Generic Secret on line 145;	awslambda_function_no_secrets_in_code prowler Critical

Result	Account	Region	Resource	Observed evidence	Check
				node_modules\@smithy\core\dist-cjs\submodules\transport\index.js: Generic Username and Password on line 33; node_modules\@smithy\core\dist-es\submodules\transport\httpRequest.js: Generic Username and Password on line 27; node_modules\@supabase\auth-js\dist\main\GoTrueAdminApi.js: Generic Username and Password on line 1096; node_modules\@supabase\auth-js\dist\main\GoTrueClient.d.ts: Generic Password on line 274, Generic Password on line 371, Generic Password on line 385, Generic Password on line 397, Generic Password on line 416, Generic Password on line 442, Generic Password on line 549, Generic Username and Password on line 1011, Generic Username and Password on line 2030, Generic Password on line 2066; node_modules\@supabase\auth-js\dist\main\GoTrueClient.js: Generic Password on line 516, Generic Password on line 613, Generic Password on line 627, Generic Password on line 639, Generic Password on line 658, Generic Password on line 747, Generic Password on line 854, Generic Username and Password on line 1699, Generic Username and Password on line 3351, Generic Username and Password on line 3467, Generic Username and Password on line 3552, Generic Password on line 3588; node_modules\@supabase\auth-js\dist\main\lib\error-codes.d.ts: Generic Password on line 6, Generic Password on line 6; node_modules\@supabase\auth-js\dist\module\GoTrueAdminApi.js: Generic Username and Password on line 1094; node_modules\@supabase\auth-js\dist\module\GoTrueClient.d.ts: Generic Password on line 274, Generic Password on line 371, Generic Password on line 385, Generic Password on line 397, Generic Password on line 416, Generic Password on line 442, Generic Password on line 549, Generic Username and Password on line 1011, Generic Username and Password on line 2030, Generic Password on line 2066; node_modules\@supabase\auth-js\dist\module\GoTrueClient.js: Generic Password on line 513, Generic Password on line 610, Generic Password on line 624, Generic Password on line 636, Generic Password on line 655, Generic Password on line 744, Generic Password on line 851, Generic Username and Password on line 1696, Generic Username and Password on line 3348, Generic Username and Password on line 3464, Generic Username and Password on line 3549,	

Result	Account	Region	Resource	Observed evidence	Check
				Generic Password on line 3585; node_modules\@supabase\auth-js\dist\module\lib\error-codes.d.ts: Generic Password on line 6, Generic Password on line 6; node_modules\@supabase\auth-js\src\GoTrueAdminApi.ts: Generic Username and Password on line 1256; node_modules\@supabase\auth-js\src\GoTrueClient.ts: Generic Password on line 793, Generic Password on line 890, Generic Password on line 904, Generic Password on line 916, Generic Password on line 935, Generic Password on line 1031, Generic Password on line 1138, Generic Username and Password on line 2099, Generic Username and Password on line 4011, Generic Username and Password on line 4127, Generic Username and Password on line 4222, Generic Password on line 4258; node_modules\@supabase\auth-js\src\lib\error-codes.ts: Generic Password on line 66, Generic Password on line 71; node_modules\@supabase\supabase-js\dist\umd\supabase.js: Generic Username and Password on line 21; node_modules\nodemailer\lib\smtp-connection\index.js: Generic Username and Password on line 535; src\main\services\otpAuthService.js: Generic Username and Password on line 87.	

Result	Account	Region	Resource	Observed evidence	Check
Fail				Potential secrets found in Lambda function code -> .env: AWS Secret Access Key on line 1, Generic API Key on line 2, Base64-PEM-Encoded Private Key on line 6, Contains Private Key on line 6, PEM-Encoded Private Key on line 6; postman-collection.json: Generic Password on line 92, Weak Password Pattern on line 92, Generic Password on line 128, Weak Password Pattern on line 128, Generic Password on line 506, Weak Password Pattern on line 506, Generic Password on line 1195, Weak Password Pattern on line 1195, Generic Password on line 1222, Weak Password Pattern on line 1222; .git\config: HTTP Basic Authentication on line 12, GitHub App Server-to-Server Token (stateless JWT format) on line 12, JSON Web Token (base64url-encoded) on line 12; node_modules\.bin\esbuild: Generic Secret on line 11733; node_modules\@aws-sdk\nested-clients\dist-types\sub	awslambda_function_no_secrets_in_code prowler Critical

Result	Account	Region	Resource	Observed evidence	Check
				modules\sso-oidc\commands\CreateTokenCommand.d.ts: Generic Secret on line 119, Generic Secret on line 140; node_modules\@esbuild\linux-x64\bin\esbuild: Generic Secret on line 11733; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\core\dist-cjs\submodules\transport\index.js: Generic Username and Password on line 31; node_modules\@smithy\core\dist-es\submodules\transport\httpRequest.js: Generic Username and Password on line 27; node_modules\chalk\readme.md: hCaptcha Site Verify Secret Key on line 24; node_modules\esbuild\bin\esbuild: Generic Secret on line 11733; node_modules\fast-uri\test\parse.test.js: Generic Username and Password on line 162; node_modules\fast-uri\test\security.test.js: Generic Username and Password on line 70, Generic Username and Password on line 70, Generic Username and Password on line 70, Generic Username and Password on line 88, Generic Username and Password on line 88, Generic Username and Password on line 88; node_modules\fast-uri\test\fixtures\uri-js-parse.json: Generic Username and Password on line 91, Generic Username and Password on line 104; node_modules\jszip\.travis.yml: Travis CI Encrypted Variable on line 15; node_modules\jszip\node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username and Password on line 475; node_modules\nodemailer\lib\shared\url.js: Generic Username and Password on line 105, Generic Username and Password on line 105; node_modules\nodemailer\lib\smtp-connection\index.js: Generic Username and Password on line 560; node_modules\serverless\node_modules\.bin\serverless-linux-amd64-0.0.2: Generic Username and Password on line 5934, Generic Secret on line 6485, Generic Username and Password on line 6532, Generic Username and Password on line 6542; node_modules\swagger-ui-dist\swagger-ui	

Result	Account	Region	Resource	Observed evidence	Check
				-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js: Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1, Generic Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\typedarray-to-buffer\.travis.yml: Travis CI Encrypted Variable on line 10; node_modules\undici\docs\docs\api\ProxyAgent.md: Generic Username and Password on line 95; node_modules\undici\docs\docs\best-practices\proxy.md: Generic Username and Password on line 82, Generic Username and Password on line 97; node_modules\undici\lib\web\fetch\index.js: Generic Username and Password on line 1260; node_modules\swagger-jsdoc\docusaurus\yarn.lock: Algolia Admin API Key on line 14, Algolia Admin API Key on line 1564, Algolia Admin API Key on line 2455; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\ws\lib\websocket.js: Generic Username and Password on line 807; privatetutor.sql\privatetutorapp_teacher.sql: Weak Password Pattern on line 56; src\main\db\mappers\studentMapper.js: Generic	

Result	Account	Region	Resource	Observed evidence	Check
				Username and Password on line 11; src\main\db\mappers\teacherMapper.js: Generic Username and Password on line 11; src\main\routes\login.js: Generic Username and Password on line 34, Generic Username and Password on line 34, Generic Username and Password on line 39, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 61; src\main\routes\student.js: Generic Username and Password on line 103, Weak Password Pattern on line 105; src\main\services\loginService.js: Generic Username and Password on line 15, Generic Username and Password on line 16, Generic Username and Password on line 16; src\test\db\mappers\teacherMapper.test.js: Weak Password Pattern on line 14, Weak Password Pattern on line 52; src\test\services\loginService.test.js: Generic Password on line 41, Generic Username and Password on line 42, Generic Password on line 58, Generic Password on line 74, Generic Password on line 100, Generic Username and Password on line 101, Generic Password on line 117, Generic Password on line 133.	

Result	Account	Region	Resource	Observed evidence	Check
Fail				Potential secrets found in Lambda function code -> postman-collection.json: Generic Password on line 57, Weak Password Pattern on line 57, Generic Password on line 88, Weak Password Pattern on line 88, Generic Password on line 889, Weak Password Pattern on line 889, Generic Password on line 916, Weak Password Pattern on line 916; .git\config: HTTP Basic Authentication on line 12, GitHub App Server-to-Server Token on line 12; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\CreateTokenCommand.d.ts: Generic Secret on line 120, Generic Secret on line 142; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\CreateTokenWithIAMCommand.d.ts: JSON Web Token (base64url-encoded) on line 146, JSON Web Token (base64url-encoded) on line 191, JSON Web Token (base64url-encoded) on line 201, JSON Web Token (base64url-encoded) on line 231; node_modules\	awslambda_function_no_secrets_in_code prowler Critical

Result	Account	Region	Resource	Observed evidence	Check
				@aws-sdk\client-sso-oidc\dist-types\commands\RegisterClientCommand.d.ts: Generic Secret on line 123; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\StartDeviceAuthorizationCommand.d.ts: Generic Secret on line 92; node_modules\@aws-sdk\client-sts\dist-types\commands\AssumeRoleWithSAMLCommand.d.ts: Generic API Key on line 268; node_modules\@aws-sdk\client-sts\dist-types\commands\AssumeRootCommand.d.ts: Generic API Key on line 107, Generic Secret on line 107; node_modules\@aws-sdk\client-sts\dist-types\models\models_0.d.ts: Generic Username and Password on line 921; node_modules\@aws-sdk\lib-storage\node_modules\events\.travis.yml: Travis CI Encrypted Variable on line 17; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\protocol-http\dist-cjs\index.js: Generic Username and Password on line 172; node_modules\@smithy\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\aws-sdk\apis\ds-2015-04-16.min.json: Generic Password on line 357; node_modules\aws-sdk\apis\cloudhsmv2-2017-04-28.min.json: Generic Password on line 465; node_modules\aws-sdk\apis\elasticmapreduce-2009-03-31.min.json: Generic Password on line 2541; node_modules\aws-sdk\apis\iam-2010-05-08.examples.json: Generic Password on line 110, Generic Password on line 1155, Generic Password on line 1163, Generic Password on line 1472, Weak Password Pattern on line 1472; node_modules\aws-sdk\apis\iam-2010-05-08.min.json: Generic Password on line 3918; node_modules\aws-sdk\apis\kms-2014-11-01.examples.json: Generic API Key on line 93, Generic Secret on line 93, Generic API Key on line 127, Generic Secret on line 127, Generic Secret on line 646, Generic Password on line 2303, Generic API Key on line 2343, Generic Secret on line 2343; node_modules\aws-sdk\apis\cognito-idp-2016-04-18.examples.json: Generic Secret on line 608; node_modules\aws-sdk\apis\redshift-2012-12-01.min.json: Generic Password on line 605; node_modules\aws-sdk\apis\rekognition-2016-06-27.examples.json: AWS Secret Access Key on line 108; node_modules\aws-sdk\apis\secretsmanager-2017-10-17.examples.json: Generic Password on line 22, Generic	

Result	Account	Region	Resource	Observed evidence	Check
				Password on line 32, Generic Password on line 42, Generic Username and Password on line 87, Generic Password on line 87, Generic Username and Password on line 87, Generic Password on line 206, Generic Password on line 249, Generic Username and Password on line 374, Generic Password on line 374, Generic Username and Password on line 374; node_modules\aws-sdk\apis\sso-oidc-2019-06-10.examples.json: Generic Secret on line 8, Generic Secret on line 31, JSON Web Token (base64url-encoded) on line 71, JSON Web Token (base64url-encoded) on line 121, JSON Web Token (base64url-encoded) on line 128, JSON Web Token (base64url-encoded) on line 159, Generic Secret on line 201, Generic Secret on line 219; node_modules\aws-sdk\apis\storagegateway-2013-06-30.examples.json: Generic Password on line 1177; node_modules\aws-sdk\apis\storagegateway-2013-06-30.min.json: Generic Username and Password on line 162; node_modules\aws-sdk\apis\sts-2011-06-15.examples.json: Generic API Key on line 71; node_modules\aws-sdk\apis\timestream-influxdb-2023-01-27.min.json: Generic Password on line 24; node_modules\aws-sdk\clients\appstream.d.ts: Generic Password on line 679, Generic Password on line 2518; node_modules\aws-sdk\clients\bedrock.d.ts: Generic Password on line 1845; node_modules\aws-sdk\clients\cognitoidentityserviceprovider.d.ts: Generic Username and Password on line 159, Generic Username and Password on line 163, Generic Password on line 1321, Generic Username and Password on line 1391, Generic Password on line 1599, Generic Username and Password on line 1599, Generic Username and Password on line 1599, Generic Password on line 1634, Generic Password on line 1634, Generic Password on line 2533, Generic Username and Password on line 2535, Generic Password on line 2535, Generic Username and Password on line 2535, Generic Password on line 2535, Generic Password on line 3501, Generic Password on line 4698; node_modules\aws-sdk\clients\deadline.d.ts: Generic Username and Password on line 6477; node_modules\aws-sdk\clients\dms.d.ts: Generic Username and Password on line 3918; node_modules\aws-sdk\clients\ec2.d.ts: Generic Password on line 33513;	

Result	Account	Region	Resource	Observed evidence	Check
				node_modules\aws-sdk\clients\elasticache.d.ts: Generic Username and Password on line 1797, Generic Password on line 2776; node_modules\aws-sdk\clients\emr.d.ts: Generic Username and Password on line 1149; node_modules\aws-sdk\clients\finspacedata.d.ts: Generic Username and Password on line 299; node_modules\aws-sdk\clients\glue.d.ts: Generic Password on line 3788, Generic Username and Password on line 3788, Generic Password on line 3788, Generic Password on line 3788, Generic Password on line 3788, Generic Password on line 3788, Generic Password on line 3788; node_modules\aws-sdk\clients\iam.d.ts: Generic Username and Password on line 3833; node_modules\aws-sdk\clients\kendra.d.ts: Generic Username and Password on line 785; node_modules\aws-sdk\clients\kms.d.ts: Generic Username and Password on line 399, Generic Username and Password on line 403; node_modules\aws-sdk\clients\lightsail.d.ts: Generic Username and Password on line 5075; node_modules\aws-sdk\clients\accessanalyzer.d.ts: Generic Username and Password on line 1169, Generic Password on line 1169, Generic Username and Password on line 1169, Generic Username and Password on line 1405; node_modules\aws-sdk\clients\amplify.d.ts: Generic Username and Password on line 378, Generic Username and Password on line 456, Generic Username and Password on line 594, Generic Username and Password on line 720, Generic Username and Password on line 817, Generic Username and Password on line 1772, Generic Username and Password on line 1856; node_modules\aws-sdk\clients\amplifybackend.d.ts: Generic Username and Password on line 505, Generic Username and Password on line 1620; node_modules\aws-sdk\clients\machinelearning.d.ts: Generic Username and Password on line 1475, Generic Username and Password on line 1563; node_modules\aws-sdk\clients\rds.d.ts: Generic Password on line 1703, Generic Username and Password on line 2238, Generic Username and Password on line 2529, Generic Username and Password on line 7539, Generic Username and Password on line 7543, Generic Username and Password on line 7827, Generic Username	

Result	Account	Region	Resource	Observed evidence	Check
				and Password on line 7831, Generic Username and Password on line 9412, Generic Username and Password on line 10028; node_modules\aws-sdk\clients\redshift.d.ts: Generic Username and Password on line 1999, Generic Username and Password on line 2115, Generic Username and Password on line 2117, Generic Username and Password on line 4484, Generic Username and Password on line 4560, Generic Username and Password on line 4562; node_modules\aws-sdk\clients\redshiftserverless.d.ts: Generic Username and Password on line 579, Generic Username and Password on line 607, Generic Username and Password on line 609, Generic Username and Password on line 2141, Generic Username and Password on line 2147, Generic Username and Password on line 2165, Generic Username and Password on line 2167; node_modules\aws-sdk\clients\securityhub.d.ts: Generic Username and Password on line 8480, Generic Username and Password on line 9136, Generic Username and Password on line 9855; node_modules\aws-sdk\clients\timestreaminfluxdb.d.ts: Generic Username and Password on line 238, Generic Username and Password on line 421, Generic Username and Password on line 498, Generic Username and Password on line 758; node_modules\aws-sdk\clients\transfer.d.ts: Generic Username and Password on line 552, Generic Password on line 2579, Generic Password on line 2579; node_modules\aws-sdk\clients\wafv2.d.ts: Generic Username and Password on line 2274, Generic Password on line 2447, Weak Password Pattern on line 2447, Weak Password Pattern on line 2447, Generic Password on line 2769, Weak Password Pattern on line 2769, Weak Password Pattern on line 2769, Generic Password on line 2783, Weak Password Pattern on line 2783, Weak Password Pattern on line 2783; node_modules\aws-sdk\clients\workdocs.d.ts: Generic Username and Password on line 681; node_modules\aws-sdk\clients\workspaces.d.ts: Generic Password on line 4011; node_modules\aws-sdk\dist\aws-sdk-react-native.js: Generic Password on line 37366, Generic Password on line 39223, Generic Username and Password on line	

Result	Account	Region	Resource	Observed evidence	Check
				39617, Generic Password on line 39617, Generic Password on line 40393, Generic Username and Password on line 40393, Generic Password on line 40393, Generic Password on line 41060, Generic Username and Password on line 41060, Generic Username and Password on line 41060, Generic Password on line 41060, Generic Password on line 41072, Generic Username and Password on line 41072, Generic Username and Password on line 41072, Generic Password on line 41072, Generic Password on line 41084, Generic Username and Password on line 41084, Generic Username and Password on line 41084, Generic Password on line 41084, Generic Password on line 41102, Generic Username and Password on line 41102, Generic Password on line 41102, Generic Username and Password on line 41102, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 55527, Generic Username and Password on line 55937, Generic Password on line 55937, Generic Password on line 55937, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 57214, Generic Username and Password on line 57214, Generic Password on line 57650, Generic Password on line 57920, Generic Username and Password on line 57920, Generic Username and Password on line 57920, Generic	

Result	Account	Region	Resource	Observed evidence	Check
				Password on line 57920, Generic Password on line 59190, Generic Password on line 63053, Generic Password on line 63053, Generic Password on line 65698, Generic Password on line 65892; node_modules\aws-sdk\dist\aws-sdk.js: Generic Password on line 41730, Generic Password on line 145123, Generic Password on line 163365, Generic Password on line 227171, Generic Username and Password on line 263475; node_modules\aws-sdk\dist\aws-sdk.min.js: Generic Username and Password on line 22, Generic Username and Password on line 23, Generic Username and Password on line 23, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 59, Generic Username and Password on line 60, Generic Password on line 60, Generic Username and Password on line 60, Generic Password on line 83, Generic Username and Password on line 83, Generic Username and Password on line 83; node_modules\aws-sdk\clients\opsworks.d.ts: Generic Username and Password on line 2410, Generic Password on line 2410, Generic Password on line 2410; node_modules\axios\dist\node\axios.cjs: Generic Username and Password on line 2645; node_modules\axios\dist\node\axios.cjs.map: Generic Username and Password on line 1; node_modules\axios\lib\adapters\http.js: Generic Username and Password on line 100; node_modules\axios-proxy-builder\dist\proxy-builder.js: Generic Username and Password on line 13; node_modules\buffer\.travis.yml: Travis CI Encrypted Variable on line 7; node_modules\buffer\bin\download-node-tests.js: Generic Username and Password on line 23; node_modules\events\.travis.yml: Travis CI Encrypted Variable on line 7; node_modules\follow-redirects\README.md: Generic Username and Password on line 81; node_modules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\jszip\.travis.yml: Travis CI Encrypted	

Result	Account	Region	Resource	Observed evidence	Check
				Variable on line 15; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username and Password on line 475; node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\serverless\node_modules\.bin\serverless-linux-amd64-0.0.2: Generic Username and Password on line 5782, Generic Username and Password on line 6254, Generic Username and Password on line 6260; node_modules\swagger-jsdoc\docusaurus\yarn.lock: Algolia Admin API Key on line 14, Algolia Admin API Key on line 1524, Algolia Admin API Key on line 2415; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js: Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\url\.travis.yml: Travis CI Encrypted Variable on line 6; node_modules\url\README.md: Generic Username and	

Result	Account	Region	Resource	Observed evidence	Check
				Password on line 17, Generic Username and Password on line 21; node_modules\url\test.js: Generic Username and Password on line 227, Generic Username and Password on line 307, Generic Username and Password on line 308, Generic Username and Password on line 322, Generic Username and Password on line 323, URI with Username and Secret on line 381, URI with Username and Secret on line 382, Generic Username and Password on line 590, Generic Username and Password on line 687, Generic Username and Password on line 693, Generic Username and Password on line 698, Generic Username and Password on line 705, Generic Username and Password on line 720, Generic Username and Password on line 726, Generic Username and Password on line 742, Generic Username and Password on line 749, URI with Username and Secret on line 933, URI with Username and Secret on line 934, URI with Username and Secret on line 941; node_modules\ws\lib\websocket.js: Generic Username and Password on line 790; node_modules\z-schema\node_modules\commander\Readme.md: Generic Username and Password on line 568; routes\teacher.js: Weak Password Pattern on line 29.	
Fail				AWS policy AdministratorAccess is attached and allows '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical

Result	Account	Region	Resource	Observed evidence	Check
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail				S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical

High findings (12)

High findings represent significant security risks and should be prioritized.

Result	Account	Region	Resource	Observed evidence	Check
Fail				GuardDuty is not enabled.	guardduty_is_enabled prowler High
Fail				User has Console Password enabled but MFA disabled.	iam_user_mfa_enabled_console_access prowler High
Fail				Block Public Access is not configured for the account .	s3_account_level_public_access_blocks prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High

Result	Account	Region	Resource	Observed evidence	Check
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail				Security Hub is not enabled.	securityhub_enabled prowler High

Medium findings (38)

Medium findings identify weaknesses that should be addressed in planned remediation.

Result	Account	Region	Resource	Observed evidence	Check
Fail		global	-	No completed AWS Backup restore job in the last 90 days and the evidence register is unavailable (not configured).	backup_restore_validated custom Medium
Fail				Log Group has less than 365 days retention period (30 days).	cloudwatch_log_group_retention_policy_specific_days_enabled prowler Medium
Fail				AWS Config recorder is disabled.	config_recorder_all_regions_enabled prowler Medium
Fail				IAM password policy does not require minimum length of 14 characters.	iam_password_policy_minimum_length_14 prowler Medium
Fail				IAM password policy does not require at least one number.	iam_password_policy_number prowler Medium
Fail				IAM password policy reuse prevention is less than 24 or not set.	iam_password_policy_reuse_24 prowler Medium
Fail				IAM password policy does not require at least one symbol.	iam_password_policy_symbol prowler Medium
Fail				IAM password policy does not require at least one uppercase letter.	iam_password_policy_uppercase prowler Medium
Fail				User has not rotated access key 1 in over 90 days (195 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 1 in over 90 days (643 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 1 in over 90 days (119 days).	iam_rotate_access_key_90_days prowler Medium

Result	Account	Region	Resource	Observed evidence	Check
Fail				User has not rotated access key 1 in over 90 days (434 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 2 in over 90 days (584 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 1 in over 90 days (962 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 1 in over 90 days (549 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 1 in over 90 days (642 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not rotated access key 2 in over 90 days (313 days).	iam_rotate_access_key_90_days prowler Medium
Fail				User has not used access key 1 in the last 90 days (189 days).	iam_user_accesskey_unused prowler Medium
Fail				User has not used access key 1 in the last 90 days (643 days).	iam_user_accesskey_unused prowler Medium
Fail				User has not used access key 1 in the last 90 days (844 days).	iam_user_accesskey_unused prowler Medium
Fail				User has not used access key 1 in the last 90 days (530 days).	iam_user_accesskey_unused prowler Medium
Fail				User has not used access key 1 in the last 90 days (314 days).	iam_user_accesskey_unused prowler Medium
Fail				User has 2 active access keys.	iam_user_two_active_access_key prowler Medium
Fail				User has 2 active access keys.	iam_user_two_active_access_key prowler Medium

Result	Account	Region	Resource	Observed evidence	Check
Fail				Inspector2 is not enabled in this account.	inspector2_is_enabled prowler Medium
Fail				S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium

Result	Account	Region	Resource	Observed evidence	Check
Fail				S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium

Low findings (18)

Low findings identify lower severity weaknesses and opportunities for hardening.

Result	Account	Region	Resource	Observed evidence	Check
Fail				IAM Access Analyzer in account is not enabled.	accessanalyzer_enabled prowler Low
Fail				IAM password policy does not require at least one lowercase letter.	iam_password_policy_lowercase prowler Low
Fail				User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonAPIGatewayAdministrator attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonAPIGatewayInvokeFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low

Result	Account	Region	Resource	Observed evidence	Check
Fail				User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the inline policy CloudfrotInvalidate attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonAPIGatewayAdministrator attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonAPIGatewayInvokeFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail				User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low

Passed findings (222)

These observations verified the required condition for the assessed resource or record.

Result	Account	Region	Resource	Observed evidence	Check
Pass				No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass				No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass				No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass				No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass				No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass				Multiregion trail new has encryption enabled.	cloudtrail_kms_encryption_enabled prowler
Pass				Multiregion trail new has log file validation enabled.	cloudtrail_log_file_validation_enabled prowler
Pass				Trail new is multiregion and it is logging.	cloudtrail_multi_region_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass				EBS Snapshot is not Public.	ec2_ebs_public_snapshot prowler
Pass				EBS Snapshot is encrypted.	ec2_ebs_snapshots_encrypted prowler
Pass				Root user in the account wasn't accessed in the last 1 days.	iam_avoid_root_usage prowler
Pass				AWS policy AWSBillingReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSCertificateManagerReadOnly is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSIAMIdentityCenterAllowListForIdentityContext is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSLambdaExecute is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSLambda_FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				AWS policy AWSSSODirectoryAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSSSOMasterAccountAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonAPIGatewayAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonAPIGatewayInvokeFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonCognitoDeveloperAuthenticatedIdentities is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonCognitoPowerUser is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonCognitoUnAuthedIdentitiesSessionPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonCognitoUnauthenticatedIdentities is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonDynamoDBFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonEC2FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				AWS policy AmazonEC2ReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonESCognitoAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonEventBridgeFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonOpenSearchServiceCognitoAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRDSFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRDSReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRoute53FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonS3FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonS3ReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy CloudFrontReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				AWS policy CloudWatchFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy ElasticLoadBalancingReadOnly is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy IAMFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy SecurityAudit is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy APIGatewayServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSBackupServiceLinkedRolePolicyForBackup is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSCloudFrontLogger is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSElasticLoadBalancingServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSGlobalAcceleratorSLRPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSOrganizationsServiceTrustPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				AWS policy AWSResourceExplorerServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSSSOServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSSupportServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSTrustedAdvisorServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSUserNotificationsServiceLinkedRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRDSServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AutoScalingServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy ElastiCacheServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy DatabaseAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AWSLambdaBasicExecutionRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				AWS policy AWSLambdaDynamoDBExecutionRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonAPIGatewayPushToCloudWatchLogs is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRDSDirectoryServiceAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonRDSEnhancedMonitoringRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy AmazonSNSRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				AWS policy ROSAKMSProviderPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass				Inline policy backup-s3 attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy RDSExportToS3Role attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy StavirOpenWikiBedrockAccess attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy AwsSSOInlinePolicy attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Inline policy ec2-instance attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy putitem attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy stavir-s3-cloudfront-deployPolicy attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy CloudfrotInvalidate attached to user does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass				Inline policy backup-s3 attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy RDSExportToS3Role attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy StavirOpenWikiBedrockAccess attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy AwsSSOInlinePolicy attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy ec2-instance attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Inline policy putitem attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy stavir-s3-cloudfront-deployPolicy attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Inline policy CloudfrotInvalidate attached to user does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass				Root account does not have access keys.	iam_no_root_access_key prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass				User has no inline or attached policies.	iam_policy_attached_only_to_group_or_roles prowler
Pass		global	iam-policies	31 of 65 policies examined have no unconditioned wildcard grants (full-administrator grants are evaluated by Prowler).	iam_policy_broad_wildcards custom
Pass				MFA is enabled for root account.	iam_root_mfa_enabled prowler
Pass				User <root_account> does not have access keys.	iam_rotate_access_key_90_days prowler
Pass				User <root_account> does not have access keys.	iam_user_accesskey_unused prowler
Pass				User does not have unused access keys for 90 days.	iam_user_accesskey_unused prowler
Pass				User does not have unused access keys for 90 days.	iam_user_accesskey_unused prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass				User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass		global		Active: last activity 2026-10-06 (2 days ago; threshold 90).	iam_user_inactive custom
Pass		global		Active: last activity 2026-07-31 (68 days ago; threshold 90).	iam_user_inactive custom
Pass		global		Active: last activity 2026-09-09 (29 days ago; threshold 90).	iam_user_inactive custom
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass				User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				User <root_account> does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass				Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass				Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass				Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass				Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass				Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 public access blocked at bucket level for .	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler

Result	Account	Region	Resource	Observed evidence	Check
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler
Pass				S3 Bucket is not public.	s3_bucket_public_access prowler

Prioritize Critical findings and known exploited vulnerabilities, regardless of their assigned severity. Known exploited vulnerabilities retain their original severity and evidence in the tables.

Regions were set on the command line for this run (--regions), replacing the regions in config.yaml.

Findings by account

80 failed result(s) across all checklist requirements, by severity. Each failed resource or record counts once. Severity is the rating of the check that produced it.

Account	Critical	High	Medium	Low	Total
	12	12	38	18	80
Organization-wide	0	0	0	0	0
Total	**12**	**12**	**38**	**18**	**80**

Results by category

Pass and Fail results for each checklist category, all accounts combined. 'Not verified' is Unable to verify plus Manual review required.

Category	Pass	Fail	Not verified	Not applicable
IAM-01 IAM users review	137	22	41	1
IAM-02 Authentication controls	16	18	0	0
S3-01 S3 storage	37	29	0	0
EC2-01 Compute	2	0	0	4
NET-01 Network	0	0	1	7
DB-01 Databases	0	0	0	10
LOG-01 Logging and monitoring	16	1	1	0
DET-01 Threat detection and findings	0	5	2	1
KMS-01 Key management	0	0	0	2
SNS-01 Notifications	0	0	1	1
SEC-01 Secrets management	14	4	1	3
BKP-01 Backup and recovery	0	1	0	2
CHG-01 Change management	0	0	1	0
Total	**222**	**80**	**48**	**31**

Checklist summary

Each cell shows the requirement outcome for that account, the mix of underlying results, and whether coverage is complete. A requirement fails if any underlying result fails.

Requirement		Organization-wide
IAM-01 IAM users review		
IAM-01a Unused IAM users are removed when no longer required	Manual review required 4 manual, 3 pass	not in scope
IAM-01b Unused access keys are deactivated or removed	Fail 5 fail, 3 pass	not in scope
IAM-01c Unused console passwords are disabled	Pass 7 pass	not in scope
IAM-01d Temporary users are deleted after their approved period	Unable to verify 1 unable coverage incomplete	not in scope
IAM-01e Former employees' access has been removed	Unable to verify 1 unable coverage incomplete	Unable to verify 1 unable coverage incomplete
IAM-01f Users and roles do not have excessive permissions	Fail 17 fail, 34 manual, 124 pass, 1 n/a	not in scope
IAM-02 Authentication controls		
IAM-02a Console users have MFA enabled	Fail 1 fail, 6 pass	not in scope
IAM-02b Root account is protected and not used	Pass 3 pass	not in scope
IAM-02c Password policy meets the standard	Fail 6 fail	not in scope

Requirement		Organization-wide
IAM-02d Access keys are rotated and limited to one active key per user	Fail 11 fail, 7 pass	not in scope
S3-01 S3 storage		
S3-01a S3 buckets are not publicly accessible	Fail 16 fail, 24 pass	not in scope
S3-01b S3 buckets are encrypted and require TLS	Fail 13 fail, 13 pass	not in scope
EC2-01 Compute		
EC2-01a EC2 instances require IMDSv2	Not applicable 1 n/a	not in scope
EC2-01b EBS volumes and snapshots are encrypted and snapshots are not public	Pass 2 pass, 2 n/a	not in scope
EC2-01c No secrets in EC2 user data	Not applicable 1 n/a	not in scope
NET-01 Network		
NET-01a Security groups do not allow unrestricted inbound access to administrative or database ports	Not applicable 6 n/a	not in scope
NET-01b Workloads run only in approved VPCs	Unable to verify 1 unable coverage incomplete	not in scope
NET-01c VPC flow logs are enabled	Not applicable 1 n/a	not in scope
DB-01 Databases		
DB-01a RDS storage and snapshots are encrypted	Not applicable 3 n/a	not in scope

Requirement		Organization-wide
DB-01b RDS instances and snapshots are not public	Not applicable 2 n/a	not in scope
DB-01c RDS enforces encrypted connections	Not applicable 1 n/a	not in scope
DB-01d RDS does not rely on default parameter groups	Not applicable 1 n/a	not in scope
DB-01e Automated backups and deletion protection are enabled	Not applicable 3 n/a	not in scope
LOG-01 Logging and monitoring		
LOG-01a CloudTrail is enabled in all regions with validated, encrypted, private logs	Manual review required 1 manual, 3 pass	not in scope
LOG-01b CloudWatch log groups have a retention period	Fail 1 fail, 13 pass	not in scope
DET-01 Threat detection and findings		
DET-01a GuardDuty, Security Hub, AWS Config, Inspector and Access Analyzer are enabled	Fail 5 fail	not in scope
DET-01b No unresolved high-severity threat or known-exploited vulnerability findings	Unable to verify 1 unable, 1 n/a coverage incomplete	not in scope
DET-01c Security findings are reviewed monthly	Unable to verify 1 unable coverage incomplete	not in scope
KMS-01 Key management		
KMS-01a Customer-managed keys rotate and are not public	Not applicable 2 n/a	not in scope

Requirement		Organization-wide
SNS-01 Notifications		
SNS-01a SNS topics are not public and subscribers are known	Unable to verify 1 unable, 1 n/a coverage incomplete	not in scope
SEC-01 Secrets management		
SEC-01a No secrets in AWS configuration (Lambda, ECS, CloudFormation, SSM)	Fail 4 fail, 14 pass, 3 n/a	not in scope
SEC-01b No secrets committed to source repositories	not in scope	Unable to verify 1 unable coverage incomplete
BKP-01 Backup and recovery		
BKP-01a Backup plans exist and vaults are encrypted	Not applicable 2 n/a	not in scope
BKP-01b Restores are tested periodically	Fail 1 fail	not in scope
CHG-01 Change management		
CHG-01a Security changes with application impact are approved before implementation	not in scope	Unable to verify 1 unable coverage incomplete

Requirement details

IAM-01a Unused IAM users are removed when no longer required Manual review required

No IAM user is inactive beyond policy.inactive_user_days unless the identity register records an approved retention reason.
Custom: iam_user_inactive

: Manual review required (4 manual, 3 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Manual review required	global		Inactive 189 days (last activity 2026-04-01; threshold 90); no retention decision recorded for ' ' in the identity register.	iam_user_inactive custom
Manual review required	global		Inactive 643 days (last activity 2025-01-03; threshold 90); no retention decision recorded for ' ' in the identity register.	iam_user_inactive custom
Manual review required	global		Inactive 844 days (last activity 2024-06-15; threshold 90); no retention decision recorded for ' ' in the identity register.	iam_user_inactive custom
Manual review required	global		Inactive 530 days (last activity 2025-04-26; threshold 90); no retention decision recorded for ' ' in the identity register.	iam_user_inactive custom
Pass	global		Active: last activity 2026-10-06 (2 days ago; threshold 90).	iam_user_inactive custom
Pass	global		Active: last activity 2026-07-31 (68 days ago; threshold 90).	iam_user_inactive custom
Pass	global		Active: last activity 2026-09-09 (29 days ago; threshold 90).	iam_user_inactive custom

IAM-01b Unused access keys are deactivated or removed Fail

No active access key unused beyond prowler.config_overrides.max_unused_access_keys_days.
Prowler: iam_user_accesskey_unused

: Fail (5 fail, 3 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			User has not used access key 1 in the last 90 days (189 days).	iam_user_accesskey_unused prowler Medium
Fail			User has not used access key 1 in the last 90 days (643 days).	iam_user_accesskey_unused prowler Medium
Fail			User has not used access key 1 in the last 90 days (844 days).	iam_user_accesskey_unused prowler Medium
Fail			User has not used access key 1 in the last 90 days (530 days).	iam_user_accesskey_unused prowler Medium
Fail			User has not used access key 1 in the last 90 days (314 days).	iam_user_accesskey_unused prowler Medium
Pass			User <root_account> does not have access keys.	iam_user_accesskey_unused prowler
Pass			User does not have unused access keys for 90 days.	iam_user_accesskey_unused prowler
Pass			User does not have unused access keys for 90 days.	iam_user_accesskey_unused prowler

IAM-01c Unused console passwords are disabled Pass

No console password unused beyond prowler.config_overrides.max_console_access_days.
Prowler: iam_user_console_access_unused

: Pass (7 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler
Pass			User does not have console access enabled or is unused.	iam_user_console_access_unused prowler

IAM-01d Temporary users are deleted after their approved period Unable to verify

No temporary IAM user exists past its expiry date (identity register or expiry tag).
Custom: iam_temporary_user_expired

: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	-	No temporary users identified by tag 'spr:temporary', and the register cannot confirm none exist: Identity register unavailable (not configured).	iam_temporary_user_expired custom

IAM-01e Former employees' access has been removed Unable to verify

No IAM user or IAM Identity Center user exists for an identity marked as a leaver; every identity is registered.
Custom: iam_former_employee_access, identity_center_former_employee_access

: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	-	Identity register unavailable (not configured). Employment status cannot be derived from AWS data; inactivity is not proof of leaving.	iam_former_employee_access custom

Organization-wide: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	identity-center	identity_center is not configured in config.yaml; federated users were not assessed.	identity_center_former_employee_acces s custom

IAM-01f Users and roles do not have excessive permissions Fail

No administrator or privilege-escalation grants (Prowler); unconditioned wildcard grants are reviewed (custom, manual review).
Prowler: iam_user_administrator_access_policy, iam_group_administrator_access_policy, iam_aws_attached_policy_no_administrative_privileges, iam_customer_attached_policy_no_administrative_privileges, iam_inline_policy_no_administrative_privileges, iam_policy_allows_privilege_escalation, iam_inline_policy_allows_privilege_escalation, iam_policy_attached_only_to_group_or_roles
Custom: iam_policy_broad_wildcards

: Fail (17 fail, 34 manual, 124 pass, 1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			AWS policy AdministratorAccess is attached and allows '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler Critical
Fail			User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonAPIGatewayAdministrator attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonAPIGatewayInvokeFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low

Result	Region	Resource	Observed evidence	Check
Fail			User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the inline policy CloudfrotInvalidate attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonAPIGatewayAdministrator attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonAPIGatewayInvokeFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonDynamoDBFullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AmazonS3FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Fail			User has the policy AWSLambda_FullAccess attached.	iam_policy_attached_only_to_group_or_roles prowler Low
Manual review required	global		Customer-managed policy needs least-privilege review - wildcard action on all resources: cognito-idp:*	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom

Result	Region	Resource	Observed evidence	Check
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonRDSFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonRDSFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed IAMFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: IAMFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed IAMFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: IAMFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AWSLambda_FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AWSLambda_FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonEC2FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonEC2FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonEventBridgeFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonEventBridgeFullAccess	iam_policy_broad_wildcards custom

Result	Region	Resource	Observed evidence	Check
Manual review required	global		AWS-managed AmazonRoute53FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonRoute53FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed CloudWatchFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: CloudWatchFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed IAMFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: IAMFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed CloudWatchFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: CloudWatchFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonEventBridgeFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonEventBridgeFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom

Result	Region	Resource	Observed evidence	Check
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to role needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AWSLambda_FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AWSLambda_FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonAPIGatewayInvokeFullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonAPIGatewayInvokeFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AWSLambda_FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AWSLambda_FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom

Result	Region	Resource	Observed evidence	Check
Manual review required	global		AWS-managed AmazonS3FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AWSLambda_FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AWSLambda_FullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonAPIGatewayInvokeFullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonAPIGatewayInvokeFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonDynamoDBFullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonDynamoDBFullAccess	iam_policy_broad_wildcards custom
Manual review required	global		AWS-managed AmazonS3FullAccess attached to user needs least-privilege review - AWS-managed *FullAccess policy: AmazonS3FullAccess	iam_policy_broad_wildcards custom
Pass			AWS policy AWSBillingReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSCertificateManagerReadOnly is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSIAMIdentityCenterAllowListForIdentityContext is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSLambdaExecute is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSLambda_FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			AWS policy AWSSSODirectoryAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSSSOMasterAccountAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonAPIGatewayAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonAPIGatewayInvokeFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonCognitoDeveloperAuthenticatedIdentities is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonCognitoPowerUser is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonCognitoUnAuthedIdentitiesSessionPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonCognitoUnauthenticatedIdentities is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonDynamoDBFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonEC2FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			AWS policy AmazonEC2ReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonESCognitoAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonEventBridgeFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonOpenSearchServiceCognitoAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRDSFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRDSReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRoute53FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonS3FullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonS3ReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy CloudFrontReadOnlyAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			AWS policy CloudWatchFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy ElasticLoadBalancingReadOnly is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy IAMFullAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy SecurityAudit is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy APIGatewayServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSBackupServiceLinkedRolePolicyForBackup is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSCloudFrontLogger is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSElasticLoadBalancingServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSGlobalAcceleratorSLRPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSOrganizationsServiceTrustPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			AWS policy AWSResourceExplorerServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSSSOServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSSupportServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSTrustedAdvisorServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSUserNotificationsServiceLinkedRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRDSServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AutoScalingServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy ElastiCacheServiceRolePolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy DatabaseAdministrator is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AWSLambdaBasicExecutionRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			AWS policy AWSLambdaDynamoDBExecutionRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonAPIGatewayPushToCloudWatchLogs is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRDSDirectoryServiceAccess is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonRDSEnhancedMonitoringRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy AmazonSNSRole is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			AWS policy ROSAKMSProviderPolicy is attached but does not allow '*:*' administrative privileges.	iam_aws_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Custom policy is attached but does not allow '*:*' administrative privileges.	iam_customer_attached_policy_no_administrative_privileges prowler
Pass			Inline policy backup-s3 attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy RDSExportToS3Role attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy StavirOpenWikiBedrockAccess attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy AwsSSOInlinePolicy attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler

Result	Region	Resource	Observed evidence	Check
Pass			Inline policy ec2-instance attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy putitem attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy stavir-s3-cloudfront-deployPolicy attached to role does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy CloudfrotInvalidate attached to user does not allow privilege escalation.	iam_inline_policy_allows_privilege_escalation prowler
Pass			Inline policy backup-s3 attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy RDSExportToS3Role attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy StavirOpenWikiBedrockAccess attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy AwsSSOInlinePolicy attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy ec2-instance attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy putitem attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler

Result	Region	Resource	Observed evidence	Check
Pass			Inline policy stavir-s3-cloudfront-deployPolicy attached to role does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Inline policy CloudfrotInvalidate attached to user does not allow '*:*' administrative privileges.	iam_inline_policy_no_administrative_privileges prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Region	Resource	Observed evidence	Check
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Region	Resource	Observed evidence	Check
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler
Pass			Custom Policy does not allow privilege escalation.	iam_policy_allows_privilege_escalation prowler

Result	Region	Resource	Observed evidence	Check
Pass			User has no inline or attached policies.	iam_policy_attached_only_to_group_or_roles prowler
Pass	global	iam-policies	31 of 65 policies examined have no unconditioned wildcard grants (full-administrator grants are evaluated by Prowler).	iam_policy_broad_wildcards custom
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Pass			IAM User does not have AdministratorAccess policy.	iam_user_administrator_access_policy prowler
Not applicable	global	-	No in-scope resources: iam:list_groups -> global=0. Prowler returned no result and logged no errors.	iam_group_administrator_access_policy orchestrator

IAM-02a Console users have MFA enabled Fail

Prowler: iam_user_mfa_enabled_console_access

: Fail (1 fail, 6 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			User has Console Password enabled but MFA disabled.	iam_user_mfa_enabled_console_access prowler High
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler
Pass			User does not have Console Password enabled.	iam_user_mfa_enabled_console_access prowler

IAM-02b Root account is protected and not used Pass

Prowler: iam_root_mfa_enabled, iam_no_root_access_key, iam_avoid_root_usage

: Pass (3 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Pass			Root user in the account wasn't accessed in the last 1 days.	iam_avoid_root_usage prowler
Pass			Root account does not have access keys.	iam_no_root_access_key prowler
Pass			MFA is enabled for root account.	iam_root_mfa_enabled prowler

IAM-02c Password policy meets the standard Fail

Prowler: iam_password_policy_minimum_length_14, iam_password_policy_reuse_24, iam_password_policy_uppercase, iam_password_policy_lowercase, iam_password_policy_number, iam_password_policy_symbol

: Fail (6 fail; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			IAM password policy does not require at least one lowercase letter.	iam_password_policy_lowercase prowler Low
Fail			IAM password policy does not require minimum length of 14 characters.	iam_password_policy_minimum_length_14 prowler Medium
Fail			IAM password policy does not require at least one number.	iam_password_policy_number prowler Medium
Fail			IAM password policy reuse prevention is less than 24 or not set.	iam_password_policy_reuse_24 prowler Medium
Fail			IAM password policy does not require at least one symbol.	iam_password_policy_symbol prowler Medium
Fail			IAM password policy does not require at least one uppercase letter.	iam_password_policy_uppercase prowler Medium

IAM-02d Access keys are rotated and limited to one active key per user Fail

Prowler: iam_rotate_access_key_90_days, iam_user_two_active_access_key

: Fail (11 fail, 7 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			User has not rotated access key 1 in over 90 days (195 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (643 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (119 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (434 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 2 in over 90 days (584 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (962 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (549 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 1 in over 90 days (642 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has not rotated access key 2 in over 90 days (313 days).	iam_rotate_access_key_90_days prowler Medium
Fail			User has 2 active access keys.	iam_user_two_active_access_key prowler Medium
Fail			User has 2 active access keys.	iam_user_two_active_access_key prowler Medium
Pass			User <root_account> does not have access keys.	iam_rotate_access_key_90_days prowler

Result	Region	Resource	Observed evidence	Check
Pass			User <root_account> does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass			User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass			User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass			User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass			User does not have 2 active access keys.	iam_user_two_active_access_key prowler
Pass			User does not have 2 active access keys.	iam_user_two_active_access_key prowler

S3-01a S3 buckets are not publicly accessible Fail

Prowler: s3_account_level_public_access_blocks, s3_bucket_level_public_access_block, s3_bucket_public_access, s3_bucket_policy_public_write_access

: Fail (16 fail, 24 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			Block Public Access is not configured for the account .	s3_account_level_public_access_blocks prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			Block Public Access is not configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler High
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical

Result	Region	Resource	Observed evidence	Check
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Fail			S3 Bucket has public access due to bucket policy.	s3_bucket_public_access prowler Critical
Pass			Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass			Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass			Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass			Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass			Block Public Access is configured for the S3 Bucket .	s3_bucket_level_public_access_block prowler
Pass			S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 public access blocked at bucket level for .	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler

Result	Region	Resource	Observed evidence	Check
Pass			S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not have a bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket does not allow public write access in the bucket policy.	s3_bucket_policy_public_write_access prowler
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler

Result	Region	Resource	Observed evidence	Check
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler
Pass			S3 Bucket is not public.	s3_bucket_public_access prowler

S3-01b S3 buckets are encrypted and require TLS Fail

Prowler: s3_bucket_default_encryption, s3_bucket_secure_transport_policy

: Fail (13 fail, 13 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket does not have a bucket policy, thus it allows HTTP requests.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium

Result	Region	Resource	Observed evidence	Check
Fail			S3 Bucket allows requests over insecure transport in the bucket policy.	s3_bucket_secure_transport_policy prowler Medium
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler

Result	Region	Resource	Observed evidence	Check
Pass			S3 Bucket has Server Side Encryption with AES256.	s3_bucket_default_encryption prowler

EC2-01a EC2 instances require IMDSv2 Not applicable

Prowler: ec2_instance_imdsv2_enabled

: Not applicable (1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: ec2:describe_instances -> =0. Prowler returned no result and logged no errors.	ec2_instance_imdsv2_enabled orchestrator

EC2-01b EBS volumes and snapshots are encrypted and snapshots are not public Pass

Prowler: ec2_ebs_default_encryption, ec2_ebs_volume_encryption, ec2_ebs_snapshots_encrypted, ec2_ebs_public_snapshot

: Pass (2 pass, 2 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Pass			EBS Snapshot is not Public.	ec2_ebs_public_snapshot prowler
Pass			EBS Snapshot is encrypted.	ec2_ebs_snapshots_encrypted prowler
Not applicable	global	-	No in-scope resources: ec2:describe_volumes -> =0. Prowler returned no result and logged no errors.	ec2_ebs_default_encryption orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_volumes -> =0. Prowler returned no result and logged no errors.	ec2_ebs_volume_encryption orchestrator

EC2-01c No secrets in EC2 user data Not applicable

Prowler: ec2_instance_secrets_user_data

: Not applicable (1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: ec2:describe_instances -> =0. Prowler returned no result and logged no errors.	ec2_instance_secrets_user_data orchestrator

NET-01a Security groups do not allow unrestricted inbound access to administrative or database ports Not applicable

Prowler: ec2_securitygroup_allow_ingress_from_internet_to_all_ports, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_22, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_3389, ec2_securitygroup_allow_ingress_from_internet_to_high_risk_tcp_ports, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_mysql_3306, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_postgres_5432

: Not applicable (6 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_all_ports orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_high_risk_tcp_ports orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_22 orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_3389 orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_mysql_3306 orchestrator
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_postgres_5432 orchestrator

NET-01b Workloads run only in approved VPCs Unable to verify

Custom: vpc_resources_in_approved_vpcs

: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	-	approved_vpc_ids is not configured for account ''.	vpc_resources_in_approved_vpcs custom

NET-01c VPC flow logs are enabled Not applicable

Prowler: vpc_flow_logs_enabled

: Not applicable (1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: ec2:describe_network_interfaces -> =0. Prowler returned no result and logged no errors.	vpc_flow_logs_enabled orchestrator

DB-01a RDS storage and snapshots are encrypted Not applicable

Prowler: rds_instance_storage_encrypted, rds_cluster_storage_encrypted, rds_snapshots_encrypted

: Not applicable (3 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: rds:describe_db_clusters -> =0. Prowler returned no result and logged no errors.	rds_cluster_storage_encrypted orchestrator
Not applicable	global	-	No in-scope resources: rds:describe_db_instances -> =0. Prowler returned no result and logged no errors.	rds_instance_storage_encrypted orchestrator
Not applicable	global	-	No in-scope resources: rds:describe_db_snapshots -> =0. Prowler returned no result and logged no errors.	rds_snapshots_encrypted orchestrator

DB-01b RDS instances and snapshots are not public Not applicable

Prowler: rds_instance_no_public_access, rds_snapshots_public_access

: Not applicable (2 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: rds:describe_db_instances -> =0. Prowler returned no result and logged no errors.	rds_instance_no_public_access orchestrator
Not applicable	global	-	No in-scope resources: rds:describe_db_snapshots -> =0. Prowler returned no result and logged no errors.	rds_snapshots_public_access orchestrator

DB-01c RDS enforces encrypted connections Not applicable

Prowler: rds_instance_transport_encrypted

: Not applicable (1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: rds:describe_db_instances -> =0. Prowler returned no result and logged no errors.	rds_instance_transport_encrypted orchestrator

DB-01d RDS does not rely on default parameter groups Not applicable

Result for default groups is set by policy.rds_default_parameter_group (manual_review by default).
Custom: rds_default_parameter_group

: Not applicable (1 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable		-	No RDS instances or clusters in this region.	rds_default_parameter_group custom

DB-01e Automated backups and deletion protection are enabled Not applicable

Prowler: rds_instance_backup_enabled, rds_instance_deletion_protection, rds_cluster_deletion_protection

: Not applicable (3 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: rds:describe_db_clusters -> =0. Prowler returned no result and logged no errors.	rds_cluster_deletion_protection orchestrator
Not applicable	global	-	No in-scope resources: rds:describe_db_instances -> =0. Prowler returned no result and logged no errors.	rds_instance_backup_enabled orchestrator
Not applicable	global	-	No in-scope resources: rds:describe_db_instances -> =0. Prowler returned no result and logged no errors.	rds_instance_deletion_protection orchestrator

LOG-01a CloudTrail is enabled in all regions with validated, encrypted, private logs Manual review required

Prowler: cloudtrail_multi_region_enabled, cloudtrail_log_file_validation_enabled, cloudtrail_kms_encryption_enabled, cloudtrail_logs_s3_bucket_is_not_publicly_accessible

: Manual review required (1 manual, 3 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Manual review required			Trail new bucket (logsexportbucketdemo) is a cross-account bucket or out of Prowler's audit scope, please check it manually.	cloudtrail_logs_s3_bucket_is_not_publicly_accessible prowler
Pass			Multiregion trail new has encryption enabled.	cloudtrail_kms_encryption_enabled prowler
Pass			Multiregion trail new has log file validation enabled.	cloudtrail_log_file_validation_enabled prowler
Pass			Trail new is multiregion and it is logging.	cloudtrail_multi_region_enabled prowler

LOG-01b CloudWatch log groups have a retention period Fail

Retention at least prowler.config_overrides.log_group_retention_days.
Prowler: cloudwatch_log_group_retention_policy_specific_days_enabled

: Fail (1 fail, 13 pass; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			Log Group has less than 365 days retention period (30 days).	cloudwatch_log_group_retention_policy_specific_days_enabled prowler Medium
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler

Result	Region	Resource	Observed evidence	Check
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler
Pass			Log Group comply with 365 days retention period since it never expires.	cloudwatch_log_group_retention_policy_specific_days_enabled prowler

DET-01a GuardDuty, Security Hub, AWS Config, Inspector and Access Analyzer are enabled Fail

Prowler: guardduty_is_enabled, securityhub_enabled, config_recorder_all_regions_enabled, inspector2_is_enabled, accessanalyzer_enabled

: Fail (5 fail; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			IAM Access Analyzer in account is not enabled.	accessanalyzer_enabled prowler Low
Fail			AWS Config recorder is disabled.	config_recorder_all_regions_enabled prowler Medium
Fail			GuardDuty is not enabled.	guardduty_is_enabled prowler High
Fail			Inspector2 is not enabled in this account.	inspector2_is_enabled prowler Medium
Fail			Security Hub is not enabled.	securityhub_enabled prowler High

DET-01b No unresolved high-severity threat or known-exploited vulnerability findings Unable to verify

Prowler: guardduty_no_high_severity_findings, inspector2_active_findings_no_known_exploited_vulnerabilities

: Unable to verify (1 unable, 1 n/a; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	-	Prowler returned no result and absence of resources could not be confirmed (no discovery probe is defined for this check).	inspector2_active_findings_no_known_exploited_vulnerabilities orchestrator
Not applicable	global	-	No in-scope resources: guardduty:list_detectors -> =0. Prowler returned no result and logged no errors.	guardduty_no_high_severity_findings orchestrator

DET-01c Security findings are reviewed monthly Unable to verify

Evidence register: monthly_findings_review within 35 days

: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	evidence:monthly_findings_review	Cannot verify: the evidence register is unavailable (not configured).	evidence:monthly_findings_review evidence

KMS-01a Customer-managed keys rotate and are not public Not applicable

Prowler: kms_cmk_rotation_enabled, kms_key_not_publicly_accessible

: Not applicable (2 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: enabled customer-managed KMS keys: =0. Prowler returned no result and logged no errors.	kms_cmk_rotation_enabled orchestrator
Not applicable	global	-	No in-scope resources: enabled customer-managed KMS keys: =0. Prowler returned no result and logged no errors.	kms_key_not_publicly_accessible orchestrator

SNS-01a SNS topics are not public and subscribers are known Unable to verify

Prowler: sns_topics_not_publicly_accessible
Custom: sns_subscriptions_known_endpoints

: Unable to verify (1 unable, 1 n/a; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	-	known_sns_endpoints is not configured for account ''.	sns_subscriptions_known_endpoints custom
Not applicable	global	-	No in-scope resources: sns:list_topics -> =0. Prowler returned no result and logged no errors.	sns_topics_not_publicly_accessible orchestrator

SEC-01a No secrets in AWS configuration (Lambda, ECS, CloudFormation, SSM) Fail

Prowler: awslambda_function_no_secrets_in_variables, awslambda_function_no_secrets_in_code, ecs_task_definitions_no_environment_secrets, cloudformation_stack_outputs_find_secrets, ssm_document_secrets

: Fail (4 fail, 14 pass, 3 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail			Potential secrets found in Lambda function code -> .env: AWS Secret Access Key on line 1, Generic API Key on line 2, Base64-PEM-Encoded Private Key on line 6, Contains Private Key on line 6, PEM-Encoded Private Key on line 6; package-lock.json: ZeroTier API Token on line 859; node_modules\.package-lock.json: ZeroTier API Token on line 828; node_modules\@aws-sdk\protocol-http\dist-cjs\httpRequest.js: Generic Username and Password on line 19; node_modules\@aws-sdk\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\protocol-http\dist-cjs\index.js: Generic Username and Password on line 177; node_modules\@smithy\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\@types\node\url.d.ts: URI with Username and Secret on line 353; node_modules\axios\dist\node\axios.cjs: Generic Username and Password on line 2651; node_modules\axios\dist\node\axios.cjs.map: Generic Username and Password on line 1; node_modules\axios\lib\adapters\http.js: Generic Username and Password on line 100; node_modules\axios-proxy-builder\dist\proxy-builder.js: Generic Username and Password on line 13; node_modules\chalk\readme.md: hCaptcha Site Verify Secret Key on line 24; node_modules\chai-http\README.md: Generic Password on line 112, Generic Username and Password on line 150, Generic Username and Password on line 200; node_modules\chai-http\dist\chai-http.js: Generic Username and Password on line 3565; node_modules\follow-redirects\README.md: Generic Username and Password on line 81; node_modules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\events\.travis.yml: Travis CI Encrypted Variable on line 17; node_modules\jszip\.travis.yml: Travis CI Encrypted Variable on line 15; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username	awslambda_function_no_secrets_in_code prowler Critical

Result	Region	Resource	Observed evidence	Check
			and Password on line 475; node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\serverless\node_modules\.bin \serverless-windows-amd64-0.0.2: Generic Username and Password on line 5514, Generic Secret on line 6266, Generic Username and Password on line 6302; node_modules\superagent\.travis.yml: Generic API Key on line 11, Sauce Labs Access Key on line 11; node_modules\superagent\superagent.js: Generic Username and Password on line 1844; node_modules\superagent\docs\index.md: Generic Username and Password on line 477; node_modules\superagent\docs\test.html: URI with Username and Secret on line 461; node_modules\superagent\lib\client.js: Generic Username and Password on line 732; node_modules\superagent\lib\node\index.js: Generic Username and Password on line 656; node_modules\superagent\node_mod ules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\supertest\node_modules\superagent\dist \superagent.js: Generic Username and Password on line 2668; node_modules\supertest\node_modules\superagent\lib\client.js: Generic Username and Password on line 744, Generic Username and Password on line 944, Generic Password on line 944, Generic Username and Password on line 944; node_modules\su pertest\node_modules\superagent\lib\request-base.js: Generic Username and Password on line 720, Generic Username and Password on line 720, Generic Password on line 720; node_mod ules\supertest\node_modules\superagent\lib\node\index.js: Generic Username and Password on line 775, Generic Username and Password on line 778, Generic Username and Password on line 1307, Generic Username and Password on line 1307, Generic Username and Password on line 1307; node_modules\swagger-jsdoc\docusaurus\yarn.lock: Algolia Admin API Key on line 14, Algolia Admin API Key on line 1524, Algolia Admin API Key on line 2415; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js:	

Result	Region	Resource	Observed evidence	Check
			Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1, Generic Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\typedarray-to-buffer\.travis.yml: Travis CI Encrypted Variable on line 10; node_modules\ws\lib\websocket.js: Generic Username and Password on line 790; node_modules\z-schema\node_modules\commander\Readme.md: Generic Username and Password on line 568.	

Result	Region	Resource	Observed evidence	Check
Fail			Potential secrets found in Lambda function code -> node_modules\@aws-sdk\nested-clients\dist-types\submodules\sso-oidc\commands\CreateTokenCommand.d.ts: Generic Secret on line 124, Generic Secret on line 145; node_modules\@smithy\core\dist-cjs\submodules\transport\index.js: Generic Username and Password on line 33; node_modules\@smithy\core\dist-es\submodules\transport\httpRequest.js: Generic Username and Password on line 27; node_modules\@supabase\auth-js\dist\main\GoTrueAdminApi.js: Generic Username and Password on line 1096; node_modules\@supabase\auth-js\dist\main\GoTrueClient.d.ts: Generic Password on line 274, Generic Password on line 371, Generic Password on line 385, Generic Password on line 397, Generic Password on line 416, Generic Password on line 442, Generic Password on line 549, Generic Username and Password	awslambda_function_no_secrets_in_code prowler Critical

Result	Region	Resource	Observed evidence	Check
			on line 1011, Generic Username and Password on line 2030, Generic Password on line 2066; node_modules\@supabase\auth-js\dist\main\GoTrueClient.js: Generic Password on line 516, Generic Password on line 613, Generic Password on line 627, Generic Password on line 639, Generic Password on line 658, Generic Password on line 747, Generic Password on line 854, Generic Username and Password on line 1699, Generic Username and Password on line 3351, Generic Username and Password on line 3467, Generic Username and Password on line 3552, Generic Password on line 3588; node_modules\@supabase\auth-js\dist\main\lib\error-codes.d.ts: Generic Password on line 6, Generic Password on line 6; node_modules\@supabase\auth-js\dist\module\GoTrueAdminApi.js: Generic Username and Password on line 1094; node_modules\@supabase\auth-js\dist\module\GoTrueClient.d.ts: Generic Password on line 274, Generic Password on line 371, Generic Password on line 385, Generic Password on line 397, Generic Password on line 416, Generic Password on line 442, Generic Password on line 549, Generic Username and Password on line 1011, Generic Username and Password on line 2030, Generic Password on line 2066; node_modules\@supabase\auth-js\dist\module\GoTrueClient.js: Generic Password on line 513, Generic Password on line 610, Generic Password on line 624, Generic Password on line 636, Generic Password on line 655, Generic Password on line 744, Generic Password on line 851, Generic Username and Password on line 1696, Generic Username and Password on line 3348, Generic Username and Password on line 3464, Generic Username and Password on line 3549, Generic Password on line 3585; node_modules\@supabase\auth-js\dist\module\lib\error-codes.d.ts: Generic Password on line 6, Generic Password on line 6; node_modules\@supabase\auth-js\src\GoTrueAdminApi.ts: Generic Username and Password on line 1256; node_modules\@supabase\auth-js\src\GoTrueClient.ts: Generic Password on line 793, Generic Password on line 890, Generic Password on line 904, Generic Password on line 916, Generic Password on line 935, Generic Password on line 1031, Generic Password on line 1138, Generic Username and Password on line 2099, Generic Username and Password on line 4011, Generic Username and Password on line 4127, Generic Username and Password on line 4222, Generic Password on line 4258; node_modules\@supabase\auth-js\src\lib\error-codes.ts: Generic Password on line 66, Generic Password on line 71;	

Result	Region	Resource	Observed evidence	Check
			node_modules\@supabase\supabase-js\dist\umd\supabase.js: Generic Username and Password on line 21; node_modules\nodemailer\lib\smtp-connection\index.js: Generic Username and Password on line 535; src\main\services\otpAuthService.js: Generic Username and Password on line 87.	

Result	Region	Resource	Observed evidence	Check
Fail			Potential secrets found in Lambda function code -> .env: AWS Secret Access Key on line 1, Generic API Key on line 2, Base64-PEM-Encoded Private Key on line 6, Contains Private Key on line 6, PEM-Encoded Private Key on line 6; postman-collection.json: Generic Password on line 92, Weak Password Pattern on line 92, Generic Password on line 128, Weak Password Pattern on line 128, Generic Password on line 506, Weak Password Pattern on line 506, Generic Password on line 1195, Weak Password Pattern on line 1195, Generic Password on line 1222, Weak Password Pattern on line 1222; .git\config: HTTP Basic Authentication on line 12, GitHub App Server-to-Server Token (stateless JWT format) on line 12, JSON Web Token (base64url-encoded) on line 12; node_modules\.bin\esbuild: Generic Secret on line 11733; node_modules\@aws-sdk\nested-clients\dist-types\submodules\sso-oidc\commands\CreateTokenCommand.d.ts: Generic Secret on line 119, Generic Secret on line 140; node_modules\@esbuild\linux-x64\bin\esbuild: Generic Secret on line 11733; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\core\dist-cjs\submodules\transport\index.js: Generic Username and Password on line 31; node_modules\@smithy\core\dist-es\submodules\transport\httpRequest.js: Generic Username and Password on line 27; node_modules\chalk\readme.md: hCaptcha Site Verify Secret Key on line 24; node_modules\esbuild\bin\esbuild: Generic Secret on line 11733; node_modules\fast-uri\test\parse.test.js: Generic Username and Password on line 162; node_modules\fast-uri\test\security.test.js: Generic Username and Password on line 70, Generic Username and Password on line 70, Generic Username and Password on line 70, Generic Username and Password on line 88, Generic Username and Password on line 88, Generic Username and Password on line	awslambda_function_no_secrets_in_code prowler Critical

Result	Region	Resource	Observed evidence	Check
			88; node_modules\fast-uri\test\fixtures\uri-js-parse.json: Generic Username and Password on line 91, Generic Username and Password on line 104; node_modules\jszip\.travis.yml: Travis CI Encrypted Variable on line 15; node_modules\jszip\node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username and Password on line 475; node_modules\nodemailer\lib\shared\url.js: Generic Username and Password on line 105, Generic Username and Password on line 105; node_modules\nodemailer\lib\smtp-connection\index.js: Generic Username and Password on line 560; node_modules\serverless\node_modules\.bin\serverless-linux-amd64-0.0.2: Generic Username and Password on line 5934, Generic Secret on line 6485, Generic Username and Password on line 6532, Generic Username and Password on line 6542; node_modules\swagger-ui-dist\swagger-ui-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js: Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1, Generic Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\typedarray-to-buffer\.travis.yml: Travis CI Encrypted Variable on line 10; node_modules\undici\docs\docs\api\ProxyAgent.md: Generic	

Result	Region	Resource	Observed evidence	Check
			Username and Password on line 95; node_modules\undici\docs\docs\best-practices\proxy.md: Generic Username and Password on line 82, Generic Username and Password on line 97; node_modules\undici\lib\web\fetch\index.js: Generic Username and Password on line 1260; node_modules\swagger-jsdoc\docusaurus\yarn.lock: Algolia Admin API Key on line 14, Algolia Admin API Key on line 1564, Algolia Admin API Key on line 2455; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\ws\lib\websocket.js: Generic Username and Password on line 807; privatetutor.sql\privatetutorapp_teacher.sql: Weak Password Pattern on line 56; src\main\db\mappers\studentMapper.js: Generic Username and Password on line 11; src\main\db\mappers\teacherMapper.js: Generic Username and Password on line 11; src\main\routes\login.js: Generic Username and Password on line 34, Generic Username and Password on line 34, Generic Username and Password on line 39, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 61; src\main\routes\student.js: Generic Username and Password on line 103, Weak Password Pattern on line 105; src\main\services\loginService.js: Generic Username and Password on line 15, Generic Username and Password on line 16, Generic Username and Password on line 16; src\test\db\mappers\teacherMapper.test.js: Weak Password Pattern on line 14, Weak Password Pattern on line 52; src\test\services\loginService.test.js: Generic Password on line 41, Generic Username and Password on line 42, Generic Password on line 58, Generic Password on line 74, Generic Password on line 100, Generic Username and Password on line 101, Generic Password on line 117, Generic Password on line 133.	

Result	Region	Resource	Observed evidence	Check
Fail			Potential secrets found in Lambda function code -> postman-collection.json: Generic Password on line 57, Weak Password Pattern on line 57, Generic Password on line 88,	awslambda_function_no_secrets_in_code prowler Critical

Result	Region	Resource	Observed evidence	Check
			Weak Password Pattern on line 88, Generic Password on line 889, Weak Password Pattern on line 889, Generic Password on line 916, Weak Password Pattern on line 916; .git\config: HTTP Basic Authentication on line 12, GitHub App Server-to-Server Token on line 12; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\CreateTokenCommand.d.ts: Generic Secret on line 120, Generic Secret on line 142; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\CreateTokenWithIAMCommand.d.ts: JSON Web Token (base64url-encoded) on line 146, JSON Web Token (base64url-encoded) on line 191, JSON Web Token (base64url-encoded) on line 201, JSON Web Token (base64url-encoded) on line 231; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\RegisterClientCommand.d.ts: Generic Secret on line 123; node_modules\@aws-sdk\client-sso-oidc\dist-types\commands\StartDeviceAuthorizationCommand.d.ts: Generic Secret on line 92; node_modules\@aws-sdk\client-sts\dist-types\commands\AssumeRoleWithSAMLCommand.d.ts: Generic API Key on line 268; node_modules\@aws-sdk\client-sts\dist-types\commands\AssumeRootCommand.d.ts: Generic API Key on line 107, Generic Secret on line 107; node_modules\@aws-sdk\client-sts\dist-types\models\models_0.d.ts: Generic Username and Password on line 921; node_modules\@aws-sdk\lib-storage\node_modules\events\.travis.yml: Travis CI Encrypted Variable on line 17; node_modules\@hapi\wreck\lib\index.js: Generic Username and Password on line 679; node_modules\@smithy\protocol-http\dist-cjs\index.js: Generic Username and Password on line 172; node_modules\@smithy\protocol-http\dist-es\httpRequest.js: Generic Username and Password on line 16; node_modules\aws-sdk\apis\ds-2015-04-16.min.json: Generic Password on line 357; node_modules\aws-sdk\apis\cloudhsmv2-2017-04-28.min.json: Generic Password on line 465; node_modules\aws-sdk\apis\elasticmapreduce-2009-03-31.min.json: Generic Password on line 2541; node_modules\aws-sdk\apis\iam-2010-05-08.examples.json: Generic Password on line 110, Generic Password on line 1155, Generic Password on line 1163, Generic Password on line 1472, Weak Password Pattern on line 1472; node_modules\aws-sdk\apis\iam-2010-05-08.min.json: Generic Password on line 3918; node_modules\aws-sdk\apis\kms-2014-11-01.examples.json: Generic API Key on line 93, Generic Secret on line 93, Generic	

Result	Region	Resource	Observed evidence	Check
			API Key on line 127, Generic Secret on line 127, Generic Secret on line 646, Generic Password on line 2303, Generic API Key on line 2343, Generic Secret on line 2343; node_modules\aws-sdk\apis\cognito-idp-2016-04-18.examples.json: Generic Secret on line 608; node_modules\aws-sdk\apis\redshift-2012-12-01.min.json: Generic Password on line 605; node_modules\aws-sdk\apis\rekognition-2016-06-27.examples.json: AWS Secret Access Key on line 108; node_modules\aws-sdk\apis\secretsmanager-2017-10-17.examples.json: Generic Password on line 22, Generic Password on line 32, Generic Password on line 42, Generic Username and Password on line 87, Generic Password on line 87, Generic Username and Password on line 87, Generic Password on line 206, Generic Password on line 249, Generic Username and Password on line 374, Generic Password on line 374, Generic Username and Password on line 374; node_modules\aws-sdk\apis\sso-oidc-2019-06-10.examples.json: Generic Secret on line 8, Generic Secret on line 31, JSON Web Token (base64url-encoded) on line 71, JSON Web Token (base64url-encoded) on line 121, JSON Web Token (base64url-encoded) on line 128, JSON Web Token (base64url-encoded) on line 159, Generic Secret on line 201, Generic Secret on line 219; node_modules\aws-sdk\apis\storagegateway-2013-06-30.examples.json: Generic Password on line 1177; node_modules\aws-sdk\apis\storagegateway-2013-06-30.min.json: Generic Username and Password on line 162; node_modules\aws-sdk\apis\sts-2011-06-15.examples.json: Generic API Key on line 71; node_modules\aws-sdk\apis\timestream-influxdb-2023-01-27.min.json: Generic Password on line 24; node_modules\aws-sdk\clients\appstream.d.ts: Generic Password on line 679, Generic Password on line 2518; node_modules\aws-sdk\clients\bedrock.d.ts: Generic Password on line 1845; node_modules\aws-sdk\clients\cognitoidentityserviceprovider.d.ts: Generic Username and Password on line 159, Generic Username and Password on line 163, Generic Password on line 1321, Generic Username and Password on line 1391, Generic Password on line 1599, Generic Username and Password on line 1599, Generic Username and Password on line 1599, Generic Password on line 1634, Generic Password on line 1634, Generic Password on line 2533, Generic Username and Password on line 2535, Generic Password on line 2535, Generic Username and Password on line 2535, Generic Password on line 2535, Generic Password on line 3501, Generic Password on line 4698; node_modules\aws-sdk\clients\deadline.d.ts: Generic	

Result	Region	Resource	Observed evidence	Check
			Username and Password on line 6477; node_modules\aws-sdk\clients\dms.d.ts: Generic Username and Password on line 3918; node_modules\aws-sdk\clients\ec2.d.ts: Generic Password on line 33513; node_modules\aws-sdk\clients\elasticache.d.ts: Generic Username and Password on line 1797, Generic Password on line 2776; node_modules\aws-sdk\clients\emr.d.ts: Generic Username and Password on line 1149; node_modules\aws-sdk\clients\finspacedata.d.ts: Generic Username and Password on line 299; node_modules\aws-sdk\clients\glue.d.ts: Generic Password on line 3788, Generic Username and Password on line 3788, Generic Password on line 3788, Generic Password on line 3788, Generic Password on line 3788, Generic Password on line 3788; node_modules\aws-sdk\clients\iam.d.ts: Generic Username and Password on line 3833; node_modules\aws-sdk\clients\kendra.d.ts: Generic Username and Password on line 785; node_modules\aws-sdk\clients\kms.d.ts: Generic Username and Password on line 399, Generic Username and Password on line 403; node_modules\aws-sdk\clients\lightsail.d.ts: Generic Username and Password on line 5075; node_modules\aws-sdk\clients\accessanalyzer.d.ts: Generic Username and Password on line 1169, Generic Password on line 1169, Generic Username and Password on line 1169, Generic Username and Password on line 1405; node_modules\aws-sdk\clients\amplify.d.ts: Generic Username and Password on line 378, Generic Username and Password on line 456, Generic Username and Password on line 594, Generic Username and Password on line 720, Generic Username and Password on line 817, Generic Username and Password on line 1772, Generic Username and Password on line 1856; node_modules\aws-sdk\clients\amplifybackend.d.ts: Generic Username and Password on line 505, Generic Username and Password on line 1620; node_modules\aws-sdk\clients\machinelearning.d.ts: Generic Username and Password on line 1475, Generic Username and Password on line 1563; node_modules\aws-sdk\clients\rds.d.ts: Generic Password on line 1703, Generic Username and Password on line 2238, Generic Username and Password on line 2529, Generic Username and Password on line 7539, Generic Username and Password on line 7543, Generic Username and	

Result	Region	Resource	Observed evidence	Check
			Password on line 7827, Generic Username and Password on line 7831, Generic Username and Password on line 9412, Generic Username and Password on line 10028; node_modules\aws-sdk\clients\redshift.d.ts: Generic Username and Password on line 1999, Generic Username and Password on line 2115, Generic Username and Password on line 2117, Generic Username and Password on line 4484, Generic Username and Password on line 4560, Generic Username and Password on line 4562; node_modules\aws-sdk\clients\redshiftserverless.d.ts: Generic Username and Password on line 579, Generic Username and Password on line 607, Generic Username and Password on line 609, Generic Username and Password on line 2141, Generic Username and Password on line 2147, Generic Username and Password on line 2165, Generic Username and Password on line 2167; node_modules\aws-sdk\clients\securityhub.d.ts: Generic Username and Password on line 8480, Generic Username and Password on line 9136, Generic Username and Password on line 9855; node_modules\aws-sdk\clients\timestreaminfluxdb.d.ts: Generic Username and Password on line 238, Generic Username and Password on line 421, Generic Username and Password on line 498, Generic Username and Password on line 758; node_modules\aws-sdk\clients\transfer.d.ts: Generic Username and Password on line 552, Generic Password on line 2579, Generic Password on line 2579; node_modules\aws-sdk\clients\wafv2.d.ts: Generic Username and Password on line 2274, Generic Password on line 2447, Weak Password Pattern on line 2447, Weak Password Pattern on line 2447, Generic Password on line 2769, Weak Password Pattern on line 2769, Weak Password Pattern on line 2769, Generic Password on line 2783, Weak Password Pattern on line 2783, Weak Password Pattern on line 2783; node_modules\aws-sdk\clients\workdocs.d.ts: Generic Username and Password on line 681; node_modules\aws-sdk\clients\workspaces.d.ts: Generic Password on line 4011; node_modules\aws-sdk\dist\aws-sdk-react-native.js: Generic Password on line 37366, Generic Password on line 39223, Generic Username and Password on line 39617, Generic Password on line 39617, Generic Password on line 40393, Generic Username and Password on line 40393, Generic Password on line 40393, Generic Password on line 41060, Generic Username and Password on line 41060, Generic Username and Password on line 41060, Generic Password on	

Result	Region	Resource	Observed evidence	Check
			line 41060, Generic Password on line 41072, Generic Username and Password on line 41072, Generic Username and Password on line 41072, Generic Password on line 41072, Generic Password on line 41084, Generic Username and Password on line 41084, Generic Username and Password on line 41084, Generic Password on line 41084, Generic Password on line 41102, Generic Username and Password on line 41102, Generic Password on line 41102, Generic Username and Password on line 41102, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Username and Password on line 41114, Generic Password on line 41114, Generic Password on line 41114, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 41157, Generic Password on line 55527, Generic Username and Password on line 55937, Generic Password on line 55937, Generic Password on line 55937, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 56841, Generic Username and Password on line 56841, Generic Password on line 57214, Generic Username and Password on line 57214, Generic Password on line 57650, Generic Password on line 57920, Generic Username and Password on line 57920, Generic Username and Password on line 57920, Generic Password on line 57920, Generic Password on line 59190, Generic Password on line 63053, Generic Password on line 63053, Generic Password on line 65698, Generic Password on line 65892; node_modules\aws-sdk\dist\aws-sdk.js: Generic Password on line 41730, Generic Password on line 145123, Generic Password on line 163365, Generic Password on line 227171, Generic Username and Password on line 263475; node_modules\aws-sdk\dist\aws-sdk.min.js: Generic Username and Password on line 22, Generic Username and Password on line 23, Generic Username and Password on line 23, Generic Username and Password on line 56, Generic Username and	

Result	Region	Resource	Observed evidence	Check
			Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 56, Generic Username and Password on line 59, Generic Username and Password on line 60, Generic Password on line 60, Generic Username and Password on line 60, Generic Password on line 83, Generic Username and Password on line 83, Generic Username and Password on line 83; node_modules\aws-sdk\clients\opsworks.d.ts: Generic Username and Password on line 2410, Generic Password on line 2410, Generic Password on line 2410; node_modules\axios\dist\node\axios.cjs: Generic Username and Password on line 2645; node_modules\axios\dist\node\axios.cjs.map: Generic Username and Password on line 1; node_modules\axios\lib\adapters\http.js: Generic Username and Password on line 100; node_modules\axios-proxy-builder\dist\proxy-builder.js: Generic Username and Password on line 13; node_modules\buffer\.travis.yml: Travis CI Encrypted Variable on line 7; node_modules\buffer\bin\download-node-tests.js: Generic Username and Password on line 23; node_modules\events\.travis.yml: Travis CI Encrypted Variable on line 7; node_modules\follow-redirects\README.md: Generic Username and Password on line 81; node_modules\form-data\Readme.md: Generic Username and Password on line 170; node_modules\jszip\.travis.yml: Travis CI Encrypted Variable on line 15; node_modules\nock\README.md: Generic Username and Password on line 231, Generic Username and Password on line 813, Generic Username and Password on line 839; node_modules\nock\lib\interceptor.js: Generic Username and Password on line 475; node_modules\readable-stream\.travis.yml: Travis CI Encrypted Variable on line 33; node_modules\serverless\node_modules\.bin\serverless-linux-amd64-0.0.2: Generic Username and Password on line 5782, Generic Username and Password on line 6254, Generic Username and Password on line 6260; node_modules\swagger-jsdoc\docusaurus\yarn.lock: Algolia Admin API Key on line 14, Algolia Admin API Key on line 1524, Algolia Admin API Key on line 2415; node_modules\swagger-ui-dist\swagger-ui-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2;	

Result	Region	Resource	Observed evidence	Check
			node_modules\swagger-ui-dist\swagger-ui-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js: Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle-core.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js: Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2, Generic Username and Password on line 2, Generic Password on line 2; node_modules\swagger-ui-dist\swagger-ui-es-bundle.js.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.css.map: Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js: Generic Username and Password on line 1, Generic Password on line 1; node_modules\swagger-ui-dist\swagger-ui.js.map: Generic Username and Password on line 1, Generic Password on line 1; node_modules\url\.travis.yml: Travis CI Encrypted Variable on line 6; node_modules\url\README.md: Generic Username and Password on line 17, Generic Username and Password on line 21; node_modules\url\test.js: Generic Username and Password on line 227, Generic Username and Password on line 307, Generic Username and Password on line 308, Generic Username and Password on line 322, Generic Username and Password on line 323, URI with Username and Secret on line 381, URI with Username and Secret on line 382, Generic Username and Password on line 590, Generic Username and Password on line 687, Generic Username and Password on line 693, Generic Username and Password on line 698, Generic Username and Password on line 705, Generic Username and Password on line 720, Generic Username and Password on line 726, Generic Username and Password on line 742, Generic Username and Password on line 749, URI with Username and Secret on line 933, URI with Username and Secret on line 934, URI with Username and Secret on line 941; node_modules\ws\lib\websocket.js: Generic Username and Password on line 790; node_modules\z-schema\node_modules\commander\Readme.md: Generic Username and Password on line 568; routes\teacher.js: Weak Password Pattern on line 29.	

Result	Region	Resource	Observed evidence	Check
Pass			No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass			No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass			No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass			No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass			No secrets found in Lambda function code.	awslambda_function_no_secrets_in_code prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler

Result	Region	Resource	Observed evidence	Check
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Pass			No secrets found in Lambda function variables.	awslambda_function_no_secrets_in_variables prowler
Not applicable	global	-	No in-scope resources: cloudformation:describe_stacks -> =0. Prowler returned no result and logged no errors.	cloudformation_stack_outputs_find_secrets orchestrator
Not applicable	global	-	No in-scope resources: ecs:list_task_definitions -> =0. Prowler returned no result and logged no errors.	ecs_task_definitions_no_environment_secrets orchestrator
Not applicable	global	-	No in-scope resources: ssm:list_documents -> =0. Prowler returned no result and logged no errors.	ssm_document_secrets orchestrator

SEC-01b No secrets committed to source repositories Unable to verify

Custom: repo_secret_scan

Organization-wide: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	repositories	repo_secret_scan has no repositories or imported_reports configured.	repo_secret_scan custom

BKP-01a Backup plans exist and vaults are encrypted Not applicable

Prowler: backup_plans_exist, backup_vaults_encrypted

: Not applicable (2 n/a; coverage complete)

Result	Region	Resource	Observed evidence	Check
Not applicable	global	-	No in-scope resources: backup:list_backup_plans -> =0. Prowler returned no result and logged no errors.	backup_plans_exist orchestrator
Not applicable	global	-	No in-scope resources: backup:list_backup_vaults -> =0. Prowler returned no result and logged no errors.	backup_vaults_encrypted orchestrator

BKP-01b Restores are tested periodically Fail

Completed AWS Backup restore job, or a 'restore_validation' evidence entry, within policy.restore_validation_max_age_days.
Custom: backup_restore_validated

: Fail (1 fail; coverage complete)

Result	Region	Resource	Observed evidence	Check
Fail	global	-	No completed AWS Backup restore job in the last 90 days and the evidence register is unavailable (not configured).	backup_restore_validated custom Medium

CHG-01a Security changes with application impact are approved before implementation Unable to verify

Evidence register: change_impact_approval within 35 days

Organization-wide: Unable to verify (1 unable; coverage incomplete)

Result	Region	Resource	Observed evidence	Check
Unable to verify	global	evidence:change_impact_approval	Cannot verify: the evidence register is unavailable (not configured).	evidence:change_impact_approval evidence

Execution issues

Stage	Account	Affects	Message
input	ALL		Input 'identity_register' is not configured; dependent checks will report 'Unable to verify'.
input	ALL		Input 'evidence_register' is not configured; dependent checks will report 'Unable to verify'.
input	ALL		Input 'accepted_risks' is not configured; dependent checks will report 'Unable to verify'.

Inputs and identities

Input	File	Rows	As of	Problems
identity_register	not configured	0		
evidence_register	not configured	0		
accepted_risks	not configured	0		

Account	Assessed as	Prowler
)		exit 0, 675.1s

Definitions

Pass

The required condition was verified from collected data for that resource or record.

Fail

Collected evidence shows the requirement is not met. Accepted risks stay Fail and are annotated.

Not applicable

Successful discovery found no in-scope resources, or an explicit rule excludes the item.

Unable to verify

Permissions, errors, missing or stale inputs, or incomplete data prevent a conclusion. Never treated as Pass.

Manual review required

Data was collected but the conclusion needs human judgement.

Coverage incomplete

At least one underlying result for that requirement and account is Unable to verify.

Attested evidence

An evidence-register entry (date, person, link). The tool checks the date, not the linked content.

Confidential. Generated 2026-10-08.