SECURITY AUDIT REPORT

Example Organisation

Scan date	25 September 2026
Scope	Synthetic organization (4 fabricated account(s), synthetic:12:4x17x1) — demonstration data, not a real AWS environment
Coverage	4/4 accounts · 4,984 resources audited

Moderate risk exposure

Overall security posture score, 0–100 (see Appendix B for how it is calculated)

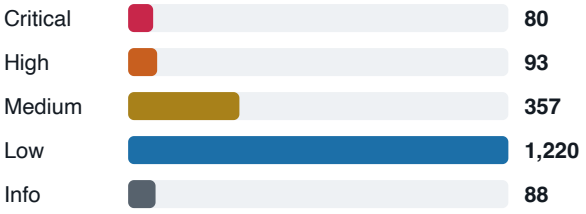
1,838	80	93	8/60
FINDINGS	CRITICAL	HIGH	CIS CONTROLS PASSING

SECTION 1

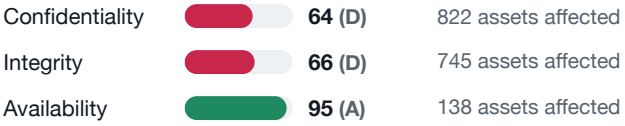
Executive summary

The AWS estate of Example Organisation scores **71/100 (C-)**, which we describe as **moderate risk exposure**. The scan audited **4,984** resources across 4 of 4 accounts and raised **1,838** findings: 80 critical, 93 high, 357 medium and 1220 low. The score has **declined by 1 point** since the previous scan (72/100). Since 25 September 2026, **217** findings are new and **131** were resolved; 1621 remain open. Against the CIS AWS Foundations Benchmark, **8 of 60** evaluable recommendations pass and **52** fail.

FINDINGS BY SEVERITY



POSTURE BY SECURITY PROPERTY

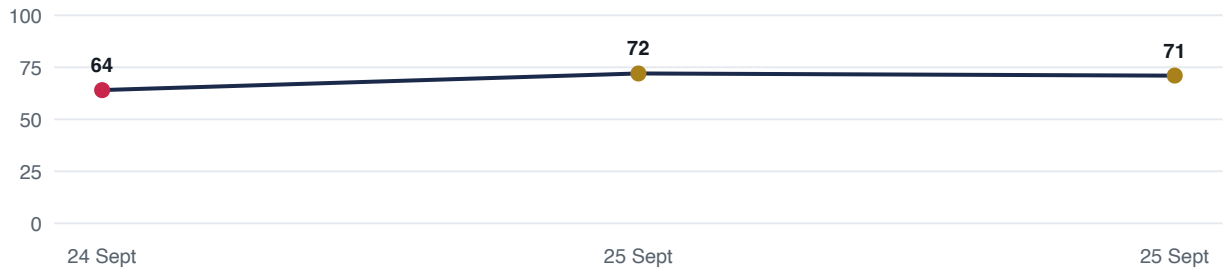


Where to focus first

The checks producing the most serious findings. Each points to its entry in the Remediation Plan (section 4).

SEVERITY	ISSUE	AFFECTED	PLAN
Critical	**High-risk port open to the internet (database, mail, admin or development ports)** Replace wide or public rules with rules for the specific ports the workload serves, restricted to the addresses that need them; databases and caches should never be reachable from 0.0.0.0/0.	27 assets	#1
Critical	**SSH or RDP open to the whole IPv4 internet** Restrict ports 22 and 3389 to a bastion host, VPN or office address range, or remove the rule; use Systems Manager Session Manager instead of open SSH where possible.	20 assets	#2
Critical	**Lambda function invokable by anyone** Remove unconditional Principal "*" statements from the function policy and set function URLs to AWS_IAM authentication.	11 assets	#3
Critical	**S3 bucket publicly accessible** Remove public ACL grants and Principal "*" policy statements, then enable Block Public Access on the bucket.	8 assets	#4
Critical	**SSH or RDP open to the whole IPv6 internet** Restrict ports 22 and 3389 to trusted IPv6 ranges or remove the ::/0 rule.	7 assets	#5

Score over time



Score of the last 3 completed scans of this type, oldest first. Resource counts change as coverage grows or infrastructure changes, so compare the grade and the critical/high counts rather than raw totals.

SECTION 2

What changed since the previous scan

Compared with the scan of **25 September 2026** of the same scope. Findings are matched by check and resource: a finding whose severity changed counts as still open, and a resolved finding means the issue was fixed or the resource removed.

217	131	1621	New by severity
NEW	RESOLVED	STILL OPEN	9 critical · 16 high · 42 medium · 131 low · 19 info

New findings

SEVERITY	FINDING	RESOURCE
Critical	S3 bucket "platform-api-dev-data-4243-0" is publicly accessible	`platform-api-dev-data-4243-0` staging
Critical	SSH (port 22) open to the internet	`sg-51cae9ed` dev-sandbox
Critical	RDP (port 3389) open to the internet	`sg-456027f2` prod-us
Critical	SMB/CIFS (port 445) open to the internet	`sg-456027f2` prod-us
Critical	23 high-risk ports open to the internet (all ports)	`sg-456027f2` prod-us
Critical	Redis (port 6379) open to the internet	`sg-171f8ded` staging
Critical	Lambda function "platform-notify-dev-fn-2" can be invoked by anyone	`arn:aws:lambda:us-west-2:101261694243:function:platform-notify-dev-fn-2` staging
Critical	Lambda function "ml-worker-prod-fn-4" can be invoked by anyone	`arn:aws:lambda:us-east-1:101244916624:function:ml-worker-prod-fn-4` dev-sandbox
Critical	Lambda function "web-api-stg-fn-18" can be invoked by anyone	`arn:aws:lambda:us-east-2:101244916624:function:web-api-stg-fn-18` dev-sandbox
High	IAM user "gudrun.svc-5" has console access without MFA	`arn:aws:iam::101278471862:user/gudrun.svc-5` prod-us
High	IAM user "finn.qa-27" has console access without MFA	`arn:aws:iam::101244916624:user/finn.qa-27` dev-sandbox
High	EC2 instance "web-web-prod-2 (i-f635ef7e0c87169fb)" allows IMDSv1	`i-f635ef7e0c87169fb` dev-sandbox
High	EC2 instance "growth-ingest-prod-7 (i-3aaa9da7c64000bd6)" allows IMDSv1	`i-3aaa9da7c64000bd6` prod-eu
High	EC2 instance "core-ingest-stg-7 (i-78734f8721e5601a0)" allows IMDSv1	`i-78734f8721e5601a0` dev-sandbox
High	EC2 instance "platform-notify-prod-13 (i-9589096f64f7c598d)" allows IMDSv1	`i-9589096f64f7c598d` staging

SEVERITY	FINDING	RESOURCE
High	EC2 instance "ml-cache-prod-15 (i-93890649e38c03395)" allows IMDSv1	i-93890649e38c03395 staging
High	EC2 instance "platform-auth-stg-30 (i-0a83b17009f650ee6)" allows IMDSv1	i-0a83b17009f650ee6 staging
High	EC2 instance "infra-auth-prod-33 (i-b5091863a2e23455b)" allows IMDSv1	i-b5091863a2e23455b prod-eu
High	EC2 instance "platform-search-prod-34 (i-1d1e6138742456c9a)" allows IMDSv1	i-1d1e6138742456c9a dev-sandbox
High	EC2 instance "core-cache-dev-35 (i-f169574570cfcc4c7)" allows IMDSv1	i-f169574570cfcc4c7 staging
High	EC2 instance "ops-gateway-dev-38 (i-1283be08143459cc2)" allows IMDSv1	i-1283be08143459cc2 staging
High	SNS topic "platform-cache-stg-events-5" is open to anyone	arn:aws:sns:us-west-2:101261694243:platform-cache-stg-events-5 staging
High	SQS queue "mobile-api-stg-queue-3" is open to anyone	arn:aws:sqs:us-west-2:101261694243:mobile-api-stg-queue-3 staging
High	SQS queue "ml-report-dev-queue-4" is open to anyone	arn:aws:sqs:us-east-2:101278471862:ml-report-dev-queue-4 prod-us
High	SQS queue "core-cache-dev-queue-5" is open to anyone	arn:aws:sqs:us-west-2:101261694243:core-cache-dev-queue-5 staging

+192 more, listed in the CSV export.

Resolved findings

SEVERITY	FINDING	RESOURCE
Critical	IAM role "data-worker-prod-role-71" can be assumed by any AWS account	arn:aws:iam::101261694243:role/data-worker-prod-role-71 staging
Critical	SSH (port 22) open to the internet	sg-dfc2b520 prod-eu
Critical	SMB/CIFS (port 445) open to the internet	sg-dea5cfd2 dev-sandbox
High	EC2 instance "web-notify-stg-3 (i-36aa975bae015eca3)" allows IMDSv1	i-36aa975bae015eca3 prod-eu
High	EC2 instance "data-web-prod-6 (i-fa35f5cafba93c9ed)" allows IMDSv1	i-fa35f5cafba93c9ed dev-sandbox
High	EC2 instance "data-web-dev-8 (i-49bb2dcd6a4221a90)" allows IMDSv1	i-49bb2dcd6a4221a90 prod-eu
High	EC2 instance "platform-search-stg-10 (i-8d238eb69bd553271)" allows IMDSv1	i-8d238eb69bd553271 dev-sandbox

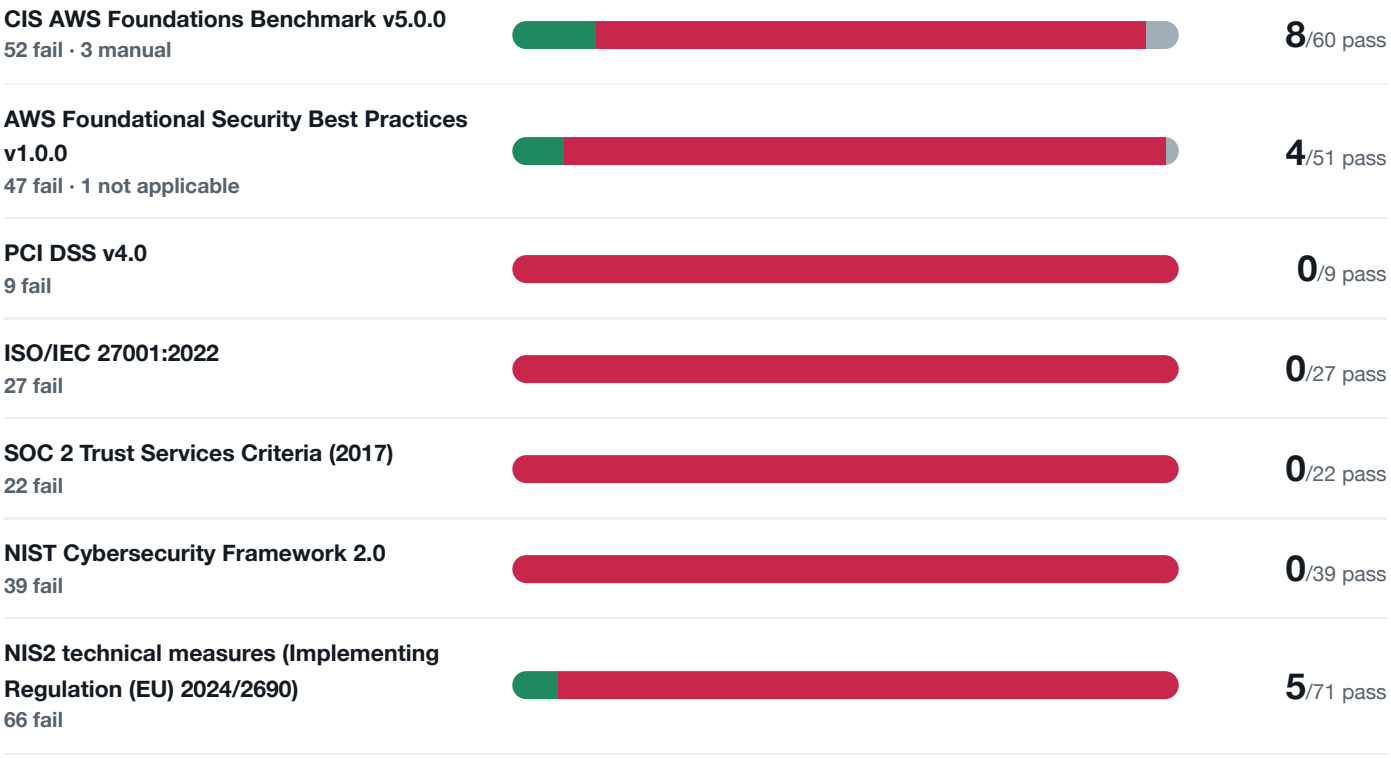
SEVERITY	FINDING	RESOURCE
High	EC2 instance "data-api-prod-26 (i-706c5dc9dd7fa4a16)" allows IMDSv1	`i-706c5dc9dd7fa4a16` staging
High	EC2 instance "platform-cache-dev-29 (i-80926ba9db78fc35e)" allows IMDSv1	`i-80926ba9db78fc35e` prod-us
High	EC2 instance "mobile-web-dev-35 (i-7c8c622aa4bfe2a5e)" allows IMDSv1	`i-7c8c622aa4bfe2a5e` prod-eu
Info	EC2 instance "infra-search-stg-2 (i-f635ef7ebfd8f9ccd)" has a public IP address	`i-f635ef7ebfd8f9ccd` dev-sandbox
Info	EC2 instance "core-ingest-stg-3 (i-62500fc2cd0b0fd70)" has a public IP address	`i-62500fc2cd0b0fd70` prod-eu
Info	EC2 instance "growth-cache-prod-3 (i-2c9a1a31161d04f19)" has a public IP address	`i-2c9a1a31161d04f19` prod-eu
Info	EC2 instance "data-web-dev-8 (i-49bb2dcd6a4221a90)" has a public IP address	`i-49bb2dcd6a4221a90` prod-eu
Info	EC2 instance "platform-search-stg-10 (i-8d238eb69bd553271)" has a public IP address	`i-8d238eb69bd553271` dev-sandbox
Info	EC2 instance "infra-billing-stg-22 (i-758a188e37a02e430)" has a public IP address	`i-758a188e37a02e430` prod-eu
Info	EC2 instance "core-billing-stg-29 (i-83ceb19318234a269)" has a public IP address	`i-83ceb19318234a269` staging
Info	EC2 instance "payments-api-stg-36 (i-12d1d147d5a2a6fbf)" has a public IP address	`i-12d1d147d5a2a6fbf` staging
Low	IAM user "ines.svc-2" has policies attached directly	`arn:aws:iam::101261694243:user/ines.svc-2` staging
Low	IAM user "eva.qa-10" has policies attached directly	`arn:aws:iam::101295249481:user/eva.qa-10` prod-eu
Low	IAM user "jonas.data-15" has policies attached directly	`arn:aws:iam::101278471862:user/jonas.data-15` prod-us
Low	IAM user "alice.data-52" has policies attached directly	`arn:aws:iam::101295249481:user/alice.data-52` prod-eu
Low	IAM user "ines.svc-53" has 2 active access keys	`arn:aws:iam::101261694243:user/ines.svc-53` staging
Low	IAM user "hakon.svc-56" has policies attached directly	`arn:aws:iam::101295249481:user/hakon.svc-56` prod-eu
Low	S3 bucket "ops-cache-dev-backups-9481-0" has no server access logging	`ops-cache-dev-backups-9481-0` prod-eu

+106 more, listed in the CSV export.

SECTION 3

Compliance verdicts

Every control the checks map to receives one of six verdicts. A control **passes** only when every check behind it ran over at least one resource and raised nothing. **Not applicable** means the checks ran and found no resource of that type; **not evaluated** means a check could not run, and the entry says which permission was missing; **manual** marks recommendations that need human judgement and are never automated.



These verdicts come from automated configuration checks against published control text. This report is not a PCI DSS Report on Compliance, a QSA assessment, a CIS-certified audit, or an ISO 27001 / SOC 2 attestation; it is evidence for the technical controls those frameworks map onto AWS configuration. For ISO 27001, SOC 2, NIST CSF and NIS2 a pass means the mapped technical checks raised nothing; each of those controls also covers people and process requirements no scanner can assess. CIS numbering follows v5.0.0; where v3.0.0 numbered a control differently, both numbers are shown.

SECTION 3.1 CIS AWS Foundations Benchmark v5.0.0

All 63 recommendations. Level 1 is the baseline every account should meet; Level 2 is defence in depth.

CONTROL	LEVEL	CONTROL TEXT	VERDICT	EVIDENCE
1.1	L1	Maintain current contact details Whether the account contact details are current and reach more than one person cannot be verified through an API.	Manual	—
1.2	L1	Ensure security contact information is registered	Fail 1/4 accounts failing	1 finding on 1 asset
1.3 v3.0.0: 1.4	L1	Ensure no 'root' user account access key exists	Pass 0/4 accounts failing	4 accounts
1.4 v3.0.0: 1.5	L1	Ensure MFA is enabled for the 'root' user account	Pass 0/4 accounts failing	4 accounts
1.5 v3.0.0: 1.6	L2	Ensure hardware MFA is enabled for the 'root' user account	Fail 3/4 accounts failing	3 findings on 3 assets
1.6 v3.0.0: 1.7	L1	Eliminate use of the 'root' user for administrative and daily tasks	Pass 0/4 accounts failing	4 accounts
1.7 v3.0.0: 1.8	L1	Ensure IAM password policy requires minimum length of 14 or greater	Pass 0/4 accounts failing	4 accounts
1.8 v3.0.0: 1.9	L1	Ensure IAM password policy prevents password reuse	Fail 3/4 accounts failing	3 findings on 3 assets
1.9 v3.0.0: 1.10	L1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Fail 4/4 accounts failing	21 findings on 21 assets
1.10 v3.0.0: 1.11	L1	Do not create access keys during initial setup for IAM users with a console password	Pass 0/4 accounts failing	240 IAM users
1.11 v3.0.0: 1.12	L1	Ensure credentials unused for 45 days or more are disabled	Fail 4/4 accounts failing	27 findings on 27 assets
1.12 v3.0.0: 1.13	L1	Ensure there is only one active access key for any single IAM user	Fail 4/4 accounts failing	10 findings on 10 assets
1.13 v3.0.0: 1.14	L1	Ensure access keys are rotated every 90 days or less	Fail 4/4 accounts failing	58 findings on 56 assets
1.14 v3.0.0: 1.15	L1	Ensure IAM users receive permissions only through groups	Fail 4/4 accounts failing	71 findings on 71 assets
1.15 v3.0.0: 1.16	L1	Ensure IAM policies that allow full "*:*" administrative privileges are not attached	Fail 3/4 accounts failing	4 findings on 4 assets
1.16 v3.0.0: 1.17	L1	Ensure a support role has been created to manage incidents with AWS Support	Fail 1/4 accounts failing	1 finding on 1 asset

CONTROL	LEVEL	CONTROL TEXT	VERDICT	EVIDENCE
1.17 v3.0.0: 1.18	L2	Ensure IAM instance roles are used for AWS resource access from instances	Fail 4/4 accounts failing	111 findings on 111 assets
1.18 v3.0.0: 1.19	L1	Ensure that all expired SSL/TLS certificates stored in AWS IAM are removed	Pass 0/4 accounts failing	4 accounts
1.19 v3.0.0: 1.20	L1	Ensure that IAM External Access Analyzer is enabled for all regions	Fail 4/4 accounts failing	4 findings on 4 assets
1.20 v3.0.0: 1.21	L2	Ensure IAM users are managed centrally via identity federation or AWS Organizations for multi-account environments Identity federation is an organisational design choice; the presence of a SAML provider does not prove users are managed centrally.	Manual	—
1.21 v3.0.0: 1.22	L1	Ensure access to AWSCloudShellFullAccess is restricted	Pass 0/4 accounts failing	4 accounts
2.1.1	L2	Ensure S3 Bucket Policy is set to deny HTTP requests	Fail 4/4 accounts failing	162 findings on 162 assets
2.1.2	L2	Ensure MFA Delete is enabled on S3 buckets	Fail 4/4 accounts failing	121 findings on 121 assets
2.1.3	L2	Ensure all data in Amazon S3 has been discovered, classified, and secured when necessary	Pass 0/4 accounts failing	4 accounts
2.1.4	L1	Ensure that S3 is configured with 'Block Public Access' enabled	Fail 4/4 accounts failing	37 findings on 37 assets
2.2.1 v3.0.0: 2.3.1	L1	Ensure that encryption-at-rest is enabled for RDS Instances	Fail 3/4 accounts failing	7 findings on 7 assets
2.2.2 v3.0.0: 2.3.2	L1	Ensure the Auto Minor Version Upgrade feature is enabled for RDS instances	Fail 4/4 accounts failing	33 findings on 33 assets
2.2.3 v3.0.0: 2.3.3	L1	Ensure that RDS instances are not publicly accessible	Fail 2/4 accounts failing	4 findings on 4 assets
2.2.4	L1	Ensure Multi-AZ deployments are used for enhanced availability in Amazon RDS	Fail 4/4 accounts failing	36 findings on 36 assets
2.3.1 v3.0.0: 2.4.1	L1	Ensure that encryption is enabled for EFS file systems	Fail 3/4 accounts failing	6 findings on 6 assets
3.1	L1	Ensure CloudTrail is enabled in all regions	Fail 2/4 accounts failing	2 findings on 2 assets
3.2	L2	Ensure CloudTrail log file validation is enabled	Fail 1/4 accounts failing	1 finding on 1 asset
3.3	L2	Ensure AWS Config is enabled in all regions	Fail 4/4 accounts failing	5 findings on 4 assets
3.4	L1	Ensure that server access logging is enabled on the CloudTrail S3 bucket	Fail 2/4 accounts failing	2 findings on 2 assets

CONTROL	LEVEL	CONTROL TEXT	VERDICT	EVIDENCE
3.5	L2	Ensure CloudTrail logs are encrypted at rest using KMS CMKs	Fail 4/4 accounts failing	4 findings on 4 assets
3.6	L2	Ensure rotation for customer-created symmetric CMKs is enabled	Fail 4/4 accounts failing	33 findings on 33 assets
3.7	L2	Ensure VPC flow logging is enabled in all VPCs	Fail 4/4 accounts failing	16 findings on 16 assets
3.8	L2	Ensure that object-level logging for write events is enabled for S3 buckets	Fail 4/4 accounts failing	4 findings on 4 assets
3.9	L2	Ensure that object-level logging for read events is enabled for S3 buckets	Fail 2/4 accounts failing	2 findings on 2 assets
4.1	L2	Ensure unauthorized API calls are monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.2	L1	Ensure management console sign-in without MFA is monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.3	L1	Ensure usage of the 'root' account is monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.4	L1	Ensure IAM policy changes are monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.5	L1	Ensure CloudTrail configuration changes are monitored	Fail 4/4 accounts failing	4 findings on 4 assets
4.6	L2	Ensure AWS Management Console authentication failures are monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.7	L2	Ensure disabling or scheduled deletion of customer created CMKs is monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.8	L1	Ensure S3 bucket policy changes are monitored	Fail 2/4 accounts failing	2 findings on 2 assets
4.9	L2	Ensure AWS Config configuration changes are monitored	Fail 4/4 accounts failing	4 findings on 4 assets
4.10	L2	Ensure security group changes are monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.11	L2	Ensure Network Access Control List (NACL) changes are monitored	Fail 3/4 accounts failing	3 findings on 3 assets
4.12	L1	Ensure changes to network gateways are monitored	Fail 2/4 accounts failing	2 findings on 2 assets
4.13	L1	Ensure route table changes are monitored	Fail 2/4 accounts failing	2 findings on 2 assets
4.14	L1	Ensure VPC changes are monitored	Fail 2/4 accounts failing	2 findings on 2 assets
4.15	L1	Ensure AWS Organizations changes are monitored	Fail 1/4 accounts failing	1 finding on 1 asset
4.16	L2	Ensure AWS Security Hub is enabled	Fail 4/4 accounts failing	4 findings on 4 assets

CONTROL	LEVEL	CONTROL TEXT	VERDICT	EVIDENCE
5.1.1 v3.0.0: 2.2.1	L1	Ensure EBS Volume Encryption is Enabled in all Regions	Fail 4/4 accounts failing	54 findings on 54 assets
5.1.2	L1	Ensure CIFS access is restricted to trusted networks to prevent unauthorized access	Fail 2/4 accounts failing	2 findings on 2 assets
5.2 v3.0.0: 5.1	L1	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports	Fail 4/4 accounts failing	49 findings on 49 assets
5.3 v3.0.0: 5.2	L1	Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports	Fail 4/4 accounts failing	24 findings on 20 assets
5.4 v3.0.0: 5.3	L1	Ensure no security groups allow ingress from ::/0 to remote server administration ports	Fail 2/4 accounts failing	7 findings on 7 assets
5.5 v3.0.0: 5.4	L2	Ensure the default security group of every VPC restricts all traffic	Fail 4/4 accounts failing	14 findings on 14 assets
5.6 v3.0.0: 5.5	L2	Ensure routing tables for VPC peering are least access Whether a peering route is "least access" depends on what the peered networks are for — a judgement, not a configuration value.	Manual	—
5.7 v3.0.0: 5.6	L1	Ensure that the EC2 Metadata Service only allows IMDSv2	Fail 4/4 accounts failing	45 findings on 45 assets

SECTION 3.2

Other frameworks

The same checks viewed through the other frameworks they map onto. Only controls that are not a clean pass are listed; the complete table for every framework is in the controls CSV export.

AWS Foundational Security Best Practices v1.0.0 47 fail · 1 not applicable

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
Account.1	Security contact information should be provided for an AWS account	Fail 1/4 accounts failing	1 finding on 1 asset
CloudFront.3	CloudFront distributions should require encryption in transit	Fail 4/4 accounts failing	10 findings on 10 assets
CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events	Fail 2/4 accounts failing	2 findings on 2 assets
CloudTrail.2	CloudTrail should have encryption at-rest enabled	Fail 4/4 accounts failing	4 findings on 4 assets
CloudTrail.4	CloudTrail log file validation should be enabled	Fail 1/4 accounts failing	1 finding on 1 asset
Config.1	AWS Config should be enabled and use the service-linked role for resource recording	Fail 4/4 accounts failing	5 findings on 4 assets
DynamoDB.2	DynamoDB tables should have point-in-time recovery enabled	Fail 4/4 accounts failing	87 findings on 87 assets
EC2.1	Amazon EBS snapshots should not be configured to be publicly restorable	Fail 4/4 accounts failing	5 findings on 5 assets
EC2.2	VPC default security groups should not allow inbound or outbound traffic	Fail 4/4 accounts failing	14 findings on 14 assets
EC2.3	Attached Amazon EBS volumes should be encrypted at-rest	Fail 4/4 accounts failing	50 findings on 50 assets
EC2.6	VPC flow logging should be enabled in all VPCs	Fail 4/4 accounts failing	16 findings on 16 assets
EC2.7	EBS default encryption should be enabled	Fail 4/4 accounts failing	4 findings on 4 assets
EC2.8	EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	Fail 4/4 accounts failing	45 findings on 45 assets
EC2.9	Amazon EC2 instances should not have a public IPv4 address	Fail 4/4 accounts failing	88 findings on 88 assets
EC2.19	Security groups should not allow unrestricted access to ports with high risk	Fail 4/4 accounts failing	60 findings on 50 assets
EC2.21	Network ACLs should not allow ingress from 0.0.0.0/0 to port 22 or port 3389	Fail 4/4 accounts failing	49 findings on 49 assets
EC2.182	Block public access settings should be enabled for Amazon EBS snapshots	Fail 4/4 accounts failing	4 findings on 4 assets
ECR.1	ECR private repositories should have image scanning configured	Fail 4/4 accounts failing	39 findings on 39 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
EFS.1	Elastic File System should be configured to encrypt file data at-rest using AWS KMS	Fail 3/4 accounts failing	6 findings on 6 assets
EKS.1	EKS cluster endpoints should not be publicly accessible	Fail 3/4 accounts failing	6 findings on 6 assets
EKS.8	EKS clusters should have audit logging enabled	Fail 4/4 accounts failing	9 findings on 9 assets
ELB.1	Application Load Balancer should be configured to redirect all HTTP requests to HTTPS	Fail 4/4 accounts failing	17 findings on 17 assets
ELB.4	Application Load Balancer should be configured to drop invalid http headers	Fail 4/4 accounts failing	43 findings on 43 assets
ELB.5	Application and Classic Load Balancers logging should be enabled	Fail 4/4 accounts failing	37 findings on 37 assets
GuardDuty.1	GuardDuty should be enabled	Fail 4/4 accounts failing	4 findings on 4 assets
IAM.1	IAM policies should not allow full "*" administrative privileges	Fail 3/4 accounts failing	4 findings on 4 assets
IAM.2	IAM users should not have IAM policies attached	Fail 4/4 accounts failing	71 findings on 71 assets
IAM.3	IAM users' access keys should be rotated every 90 days or less	Fail 4/4 accounts failing	58 findings on 56 assets
IAM.5	MFA should be enabled for all IAM users that have a console password	Fail 4/4 accounts failing	21 findings on 21 assets
IAM.6	Hardware MFA should be enabled for the root user	Fail 3/4 accounts failing	3 findings on 3 assets
IAM.7	Password policies for IAM users should have strong configurations	Fail 3/4 accounts failing	3 findings on 3 assets
IAM.8	Unused IAM user credentials should be removed	Fail 4/4 accounts failing	27 findings on 27 assets
Lambda.1	Lambda function policies should prohibit public access	Fail 4/4 accounts failing	11 findings on 11 assets
RDS.2	RDS DB Instances should prohibit public access, as determined by the PubliclyAccessible configuration	Fail 2/4 accounts failing	4 findings on 4 assets
RDS.3	RDS DB instances should have encryption at-rest enabled	Fail 3/4 accounts failing	7 findings on 7 assets
RDS.5	RDS DB instances should be configured with multiple Availability Zones	Fail 4/4 accounts failing	27 findings on 27 assets
RDS.11	RDS instances should have automatic backups enabled	Fail 4/4 accounts failing	10 findings on 10 assets
RDS.13	RDS automatic minor version upgrades should be enabled	Fail 4/4 accounts failing	33 findings on 33 assets
RDS.15	RDS DB clusters should be configured for multiple Availability Zones	Fail 4/4 accounts failing	9 findings on 9 assets
S3.1	S3 general purpose buckets should have block public access settings enabled	Fail 3/4 accounts failing	3 findings on 3 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
S3.2	S3 general purpose buckets should block public read access	Fail 4/4 accounts failing	8 findings on 8 assets
S3.5	S3 general purpose buckets should require requests to use TLS	Fail 4/4 accounts failing	162 findings on 162 assets
S3.8	S3 general purpose buckets should block public access	Fail 4/4 accounts failing	26 findings on 26 assets
S3.9	S3 general purpose buckets should have server access logging enabled	Fail 4/4 accounts failing	189 findings on 189 assets
SecretsManager.1	Secrets Manager secrets should have automatic rotation enabled	Fail 4/4 accounts failing	104 findings on 104 assets
SNS.4	SNS topic access policies should not allow public access	Fail 2/4 accounts failing	3 findings on 3 assets
SQS.3	SQS queue access policies should not allow public access	Fail 3/4 accounts failing	7 findings on 7 assets

PCI DSS v4.0 9 fail

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
1.3.1	Inbound traffic to the cardholder data environment is restricted	Fail 4/4 accounts failing	196 findings on 186 assets
3.5.1	PAN is rendered unreadable anywhere it is stored	Fail 4/4 accounts failing	57 findings on 57 assets
3.7.4	Cryptographic keys are changed at the end of their cryptoperiod	Fail 4/4 accounts failing	33 findings on 33 assets
7.2.1	Access control model is based on least privilege	Fail 4/4 accounts failing	10 findings on 10 assets
8.3.9	Passwords/passphrases are changed at least once every 90 days	Fail 4/4 accounts failing	58 findings on 56 assets
8.4.2	MFA is implemented for all access into the cardholder data environment	Fail 4/4 accounts failing	21 findings on 21 assets
10.2.1	Audit logs are enabled and active for all system components	Fail 2/4 accounts failing	2 findings on 2 assets
10.3.2	Audit log files are protected from modification	Fail 1/4 accounts failing	1 finding on 1 asset
11.5.1	Intrusion-detection and/or intrusion-prevention techniques are in use	Fail 4/4 accounts failing	4 findings on 4 assets

ISO/IEC 27001:2022 27 fail

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
A.5.1	Policies for information security	Fail 4/4 accounts failing	4 findings on 4 assets
A.5.5	Contact With Authorities	Fail 1/4 accounts failing	1 finding on 1 asset

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
A.5.15	Access Control	Fail 4/4 accounts failing	180 findings on 125 assets
A.5.16	Identity Management	Fail 4/4 accounts failing	5 findings on 4 assets
A.5.17	Authentication Information	Fail 4/4 accounts failing	21 findings on 21 assets
A.5.18	Access Rights	Fail 3/4 accounts failing	4 findings on 4 assets
A.5.19	Information Security In Supplier Relationships	Fail 4/4 accounts failing	4 findings on 4 assets
A.5.21	Managing Information Security In The ICT Supply Chain	Fail 4/4 accounts failing	4 findings on 4 assets
A.5.22	Monitor, Review And Change Management Of Supplier Services	Fail 4/4 accounts failing	5 findings on 4 assets
A.5.25	Assessment And Decision On Information Security Events	Fail 4/4 accounts failing	4 findings on 4 assets
A.5.28	Collection Of Evidence	Fail 4/4 accounts failing	4 findings on 4 assets
A.5.29	Information Security During Disruption	Fail 4/4 accounts failing	4 findings on 4 assets
A.8.1	User Endpoint Devices	Fail 4/4 accounts failing	135 findings on 135 assets
A.8.2	Privileged Access Rights	Fail 4/4 accounts failing	115 findings on 115 assets
A.8.3	Information Access Restriction	Fail 4/4 accounts failing	4 findings on 4 assets
A.8.5	Secure Authentication	Fail 4/4 accounts failing	54 findings on 54 assets
A.8.7	Protection Against Malware	Fail 4/4 accounts failing	4 findings on 4 assets
A.8.9	Configuration Management	Fail 4/4 accounts failing	4 findings on 4 assets
A.8.11	Data Masking	Fail 4/4 accounts failing	123 findings on 123 assets
A.8.14	Redundancy of information processing facilities	Fail 4/4 accounts failing	36 findings on 36 assets
A.8.15	Logging	Fail 4/4 accounts failing	303 findings on 263 assets
A.8.16	Monitoring Activities	Fail 4/4 accounts failing	68 findings on 28 assets
A.8.20	Network Security	Fail 4/4 accounts failing	399 findings on 352 assets
A.8.21	Security of Network Services	Fail 4/4 accounts failing	399 findings on 352 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
A.8.22	Segregation of Networks	Fail 4/4 accounts failing	399 findings on 352 assets
A.8.23	Web Filtering	Fail 4/4 accounts failing	34 findings on 34 assets
A.8.24	Use of Cryptography	Fail 4/4 accounts failing	123 findings on 123 assets

SOC 2 Trust Services Criteria (2017) 22 fail

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
A1.1	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up…	Fail 4/4 accounts failing	327 findings on 327 assets
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of…	Fail 4/4 accounts failing	102 findings on 91 assets
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control	Fail 4/4 accounts failing	13 findings on 8 assets
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	Fail 4/4 accounts failing	13 findings on 12 assets
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risk…	Fail 4/4 accounts failing	4 findings on 4 assets
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control	Fail 4/4 accounts failing	5 findings on 4 assets
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective ac…	Fail 4/4 accounts failing	4 findings on 4 assets
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives	Fail 4/4 accounts failing	26 findings on 4 assets
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security event…	Fail 4/4 accounts failing	8 findings on 8 assets
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administere…	Fail 2/4 accounts failing	4 findings on 4 assets
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or th…	Fail 3/4 accounts failing	4 findings on 4 assets
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries	Fail 4/4 accounts failing	206 findings on 196 assets
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives	Fail 4/4 accounts failing	8 findings on 8 assets
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vu…	Fail 4/4 accounts failing	8 findings on 8 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors…	Fail 4/4 accounts failing	343 findings on 330 assets
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) an…	Fail 4/4 accounts failing	260 findings on 255 assets
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate securi…	Fail 4/4 accounts failing	114 findings on 109 assets
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and pro…	Fail 4/4 accounts failing	5 findings on 4 assets
pi_1_2	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements	Fail 4/4 accounts failing	41 findings on 41 assets
pi_1_3	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements	Fail 4/4 accounts failing	20 findings on 11 assets
pi_1_4	System outputs are complete, accurate, distributed only to intended parties, and retained to meet the entity's processing integrity commitments and system requ…	Fail 4/4 accounts failing	19 findings on 19 assets
pi_1_5	Stored data is maintained complete, accurate, and protected from unauthorized modification to meet the entity's processing integrity commitments and system req…	Fail 4/4 accounts failing	90 findings on 90 assets

NIST Cybersecurity Framework 2.0 39 fail

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.	Fail 4/4 accounts failing	32 findings on 20 assets
DE.AE-2	Detected events are analyzed to understand attack targets and methods.	Fail 4/4 accounts failing	34 findings on 4 assets
DE.AE-3	Event data are collected and correlated from multiple sources and sensors.	Fail 4/4 accounts failing	13 findings on 4 assets
DE.CM-1	The network is monitored to detect potential cybersecurity events.	Fail 4/4 accounts failing	43 findings on 24 assets
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.	Fail 4/4 accounts failing	10 findings on 4 assets
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.	Fail 4/4 accounts failing	33 findings on 8 assets
DE.DP-4	Event detection information is communicated.	Fail 4/4 accounts failing	27 findings on 4 assets
GV.OV-2	Cybersecurity risk management performance is measured and reported.	Fail 4/4 accounts failing	8 findings on 8 assets
GV.OV-3	Cybersecurity risk management strategy and practices are reviewed and adjusted to adapt to changes in the threat landscape, technologies, or mission, business,…	Fail 4/4 accounts failing	30 findings on 16 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
GV.PO-1	Cybersecurity policy is established, communicated, and enforced.	Fail 4/4 accounts failing	75 findings on 75 assets
GV.PO-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Fail 4/4 accounts failing	13 findings on 12 assets
GV.PO-4	Governance and risk management processes address cybersecurity risks.	Fail 4/4 accounts failing	29 findings on 28 assets
GV.RM-1	Organizational cybersecurity risk management strategy is established, communicated, and maintained.	Fail 4/4 accounts failing	9 findings on 8 assets
GV.RR-1	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	Fail 4/4 accounts failing	75 findings on 75 assets
GV.RR-2	Cybersecurity responsibilities are established and communicated.	Fail 4/4 accounts failing	75 findings on 75 assets
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Fail 4/4 accounts failing	71 findings on 71 assets
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal op…	Fail 3/4 accounts failing	6 findings on 6 assets
ID.RA-1	Asset vulnerabilities are identified and documented.	Fail 4/4 accounts failing	8 findings on 8 assets
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Fail 4/4 accounts failing	21 findings on 4 assets
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	Fail 4/4 accounts failing	116 findings on 100 assets
PR.AC-3	Remote access is managed.	Fail 4/4 accounts failing	121 findings on 117 assets
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Fail 4/4 accounts failing	75 findings on 75 assets
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).	Fail 4/4 accounts failing	72 findings on 64 assets
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.	Fail 4/4 accounts failing	147 findings on 113 assets
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' securi…	Fail 4/4 accounts failing	103 findings on 99 assets
PR.DS-1	Data-at-rest is protected.	Fail 4/4 accounts failing	36 findings on 36 assets
PR.DS-2	Data-in-transit is protected.	Fail 4/4 accounts failing	172 findings on 172 assets
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.	Fail 4/4 accounts failing	29 findings on 29 assets
PR.DS-4	Adequate capacity to ensure availability is maintained.	Fail 4/4 accounts failing	37 findings on 32 assets
PR.DS-5	Protections against data leaks are implemented.	Fail 4/4 accounts failing	21 findings on 21 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Fail 1/4 accounts failing	1 finding on 1 asset
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of leas…	Fail 4/4 accounts failing	181 findings on 181 assets
PR.IP-4	Backups of information are conducted, maintained, and tested periodically.	Fail 4/4 accounts failing	10 findings on 10 assets
PR.IP-7	Protection processes are improved.	Fail 4/4 accounts failing	114 findings on 111 assets
PR.IP-8	Effectiveness of protection technologies is shared.	Fail 4/4 accounts failing	20 findings on 4 assets
PR.IP-12	A vulnerability management plan is developed and implemented.	Fail 4/4 accounts failing	4 findings on 4 assets
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Fail 4/4 accounts failing	44 findings on 28 assets
PR.PT-4	Communications and control networks are protected.	Fail 4/4 accounts failing	192 findings on 192 assets
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident.	Fail 4/4 accounts failing	10 findings on 10 assets

NIS2 technical measures (Implementing Regulation (EU) 2024/2690) 66 fail

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
1.1.1.a	1.1 Policy on the security of network and information systems: set out the relevant entities approach to managing the security of their network and information…	Fail 1/4 accounts failing	1 finding on 1 asset
1.1.1.d	1.1 Policy on the security of network and information systems: include a commitment to continual improvement of the security of network and information systems;	Fail 4/4 accounts failing	58 findings on 56 assets
1.1.1.h	1.1 Policy on the security of network and information systems: list the documentation to be kept and the duration of retention of the documentation;	Fail 4/4 accounts failing	189 findings on 189 assets
1.1.2	1.1 Policy on the security of network and information systems: The network and information system security policy shall be reviewed and, where appropriate, upd…	Fail 4/4 accounts failing	58 findings on 56 assets
1.2.1	1.2 Roles, responsibilities and authorities: As part of their policy on the security of network and information systems referred to in point 1.1., the relevant…	Fail 4/4 accounts failing	71 findings on 71 assets
1.2.3	1.2 Roles, responsibilities and authorities: At least one person shall report directly to the management bodies on matters of network and information system se…	Fail 1/4 accounts failing	1 finding on 1 asset
2.1.1	1.2 Roles, responsibilities and authorities: For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and…	Fail 1/4 accounts failing	1 finding on 1 asset
2.1.2.a	2.1 Risk management framework: follow a risk management methodology;	Fail 1/4 accounts failing	1 finding on 1 asset
2.1.2.f	2.1 Risk management framework: evaluate the identified risks based on the risk criteria;	Fail 4/4 accounts failing	71 findings on 71 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
2.1.4	2.1 Risk management framework: The relevant entities shall review and, where appropriate, update the risk assessment results and the risk treatment plan at pla…	Fail 4/4 accounts failing	58 findings on 56 assets
2.2.1	2.2 Compliance monitoring: The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-sp…	Fail 2/4 accounts failing	2 findings on 2 assets
2.2.3	2.2 Compliance monitoring: The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant cha…	Fail 4/4 accounts failing	26 findings on 4 assets
2.3.1	2.3 Independent review of information and network security: The relevant entities shall review independently their approach to managing network and information…	Fail 4/4 accounts failing	61 findings on 59 assets
3.1.2.d	3.1 Incident handling policy: documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, conta…	Fail 2/4 accounts failing	2 findings on 2 assets
3.1.3	3.1 Incident handling policy: The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated a…	Fail 4/4 accounts failing	58 findings on 56 assets
3.2.1	3.2 Monitoring and logging: The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information system…	Fail 3/4 accounts failing	3 findings on 3 assets
3.2.2	3.2 Monitoring and logging: To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to busi…	Fail 4/4 accounts failing	10 findings on 4 assets
3.2.3.a	3.2 Monitoring and logging: relevant outbound and inbound network traffic;	Fail 3/4 accounts failing	7 findings on 3 assets
3.2.3.b	3.2 Monitoring and logging: creation, modification or deletion of users of the relevant entities network and information systems and extension of the permissio…	Fail 4/4 accounts failing	9 findings on 4 assets
3.2.3.c	3.2 Monitoring and logging: access to systems and applications;	Fail 4/4 accounts failing	298 findings on 261 assets
3.2.3.d	3.2 Monitoring and logging: authentication-related events;	Fail 4/4 accounts failing	6 findings on 4 assets
3.2.3.e	3.2 Monitoring and logging: all privileged access to systems and applications, and activities performed by administrative accounts;	Fail 4/4 accounts failing	7 findings on 7 assets
3.2.3.f	3.2 Monitoring and logging: access or changes to critical configuration and backup files;	Fail 4/4 accounts failing	26 findings on 4 assets
3.2.3.g	3.2 Monitoring and logging: event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;	Fail 4/4 accounts failing	38 findings on 8 assets
3.2.4	3.2 Monitoring and logging: The logs shall be regularly reviewed for any unusual or unwanted trends. Where appropriate, the relevant entities shall lay down ap…	Fail 4/4 accounts failing	13 findings on 4 assets
3.4.2.c	3.4 Event assessment and classification: review the appropriate logs for the purposes of event assessment and classification;	Fail 3/4 accounts failing	5 findings on 5 assets
3.4.2.d	3.4 Event assessment and classification: put in place a process for log correlation and analysis, and reassess and reclassify events in case of new information…	Fail 1/4 accounts failing	1 finding on 1 asset

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
3.5.3.a	3.5 Incident response: with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notific…	Fail 1/4 accounts failing	1 finding on 1 asset
3.5.4	3.5 Incident response: The relevant entities shall log incident response activities in accordance with the procedures referred to in point 3.2.1., and record e…	Fail 4/4 accounts failing	32 findings on 4 assets
3.6.2	3.6 Post-incident reviews: The relevant entities shall ensure that post-incident reviews contribute to improving their approach to network and information secu…	Fail 4/4 accounts failing	10 findings on 10 assets
4.1.1	4.1 Business continuity and disaster recovery plan: For the purpose of Article 21(2), point (c) of Directive (EU) 2022/2555, the relevant entities shall lay do…	Fail 4/4 accounts failing	10 findings on 10 assets
4.1.2.g	4.1 Business continuity and disaster recovery plan: required resources, including backups and redundancies;	Fail 4/4 accounts failing	10 findings on 10 assets
4.2.2.e	4.2 Backup and redundancy management: restoring data from backup copies;	Fail 4/4 accounts failing	10 findings on 10 assets
4.3.2.a	4.3 Crisis management: roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in…	Fail 1/4 accounts failing	1 finding on 1 asset
5.1.7.b	5.1 Supply chain security policy: review incidents related to ICT products and ICT services from suppliers and service providers;	Fail 2/4 accounts failing	2 findings on 2 assets
6.2.4	6.2 Secure development life cycle: The relevant entities shall review and, where necessary, update their secure development rules at planned intervals.	Fail 4/4 accounts failing	58 findings on 56 assets
6.4.1	6.4 Change management, repairs and maintenance: The relevant entities shall apply change management procedures to control changes of network and information sy…	Fail 4/4 accounts failing	9 findings on 4 assets
6.7.2.e	6.7 Network security: not use systems used for administration of the security policy implementation for other purposes;	Fail 3/4 accounts failing	4 findings on 4 assets
6.7.2.g	6.7 Network security: where appropriate, exclusively allow access to the relevant entities network and information systems by devices authorised by those entit…	Fail 4/4 accounts failing	51 findings on 51 assets
6.7.2.i	6.7 Network security: establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic or physical…	Fail 4/4 accounts failing	45 findings on 45 assets
7.2.b	7.2 The policy and procedures referred to in point 7.1. shall take into account results of the risk assessment pursuant to point 2.1. and past significant inci…	Fail 4/4 accounts failing	23 findings on 4 assets
9.2.a	9.2 Cryptography: in accordance with the relevant entities classification of assets, the type, strength and quality of the cryptographic measures required to p…	Fail 4/4 accounts failing	4 findings on 4 assets
9.2.c	9.2 Cryptography: the relevant entities approach to key management, including, where appropriate, methods for the following:	Fail 4/4 accounts failing	68 findings on 57 assets
9.2.c.iv	9.2 Cryptography: storing keys, including how authorised users obtain access to keys;	Fail 4/4 accounts failing	104 findings on 104 assets
9.2.c.v	9.2 Cryptography: changing or updating keys, including rules on when and how to change keys;	Fail 3/4 accounts failing	3 findings on 3 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
9.2.c.vii	9.2 Cryptography: logging and auditing of key management-related activities;	Fail 4/4 accounts failing	6 findings on 4 assets
9.2.c.xii	9.2 Cryptography: setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the…	Fail 4/4 accounts failing	58 findings on 56 assets
11.1.1	11.1 Access control policy: For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implem…	Fail 4/4 accounts failing	121 findings on 121 assets
11.1.2.c	11.1 Access control policy: ensure that access is only granted to users that have been adequately authenticated.	Fail 4/4 accounts failing	21 findings on 21 assets
11.2.1	11.2 Management of access rights: The relevant entities shall provide, modify, remove and document access rights to network and information systems in accordan…	Fail 4/4 accounts failing	4 findings on 4 assets
11.2.2.a	11.2 Management of access rights: assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	Fail 4/4 accounts failing	71 findings on 71 assets
11.2.2.d	11.2 Management of access rights: ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in par…	Fail 4/4 accounts failing	115 findings on 115 assets
11.2.2.e	11.2 Management of access rights: maintain a register of access rights granted;	Fail 4/4 accounts failing	4 findings on 4 assets
11.2.2.f	11.2 Management of access rights: apply logging to the management of access rights.	Fail 4/4 accounts failing	191 findings on 191 assets
11.3.2.a	11.3 Privileged accounts and system administration accounts: establish strong identification, authentication such as multi-factor authentication, and authorisa…	Fail 4/4 accounts failing	21 findings on 21 assets
11.3.2.c	11.3 Privileged accounts and system administration accounts: individualise and restrict system administration privileges to the highest extent possible,	Fail 3/4 accounts failing	4 findings on 4 assets
11.3.2.d	11.3 Privileged accounts and system administration accounts: provide that system administration accounts are only used to connect to system administration syst…	Fail 4/4 accounts failing	27 findings on 27 assets
11.4.2.b	11.4 Administration systems: separate logically such systems from application software not used for system administrative purposes,	Fail 3/4 accounts failing	4 findings on 4 assets
11.4.2.c	11.4 Administration systems: protect access to system administration systems through authentication and encryption.	Fail 4/4 accounts failing	21 findings on 21 assets
11.5.2.d	11.5 Identification: apply logging to the management of identities.	Fail 4/4 accounts failing	7 findings on 4 assets
11.5.4	11.5 Identification: The relevant entities shall regularly review the identities for network and information systems and their users and, if no longer needed,…	Fail 4/4 accounts failing	27 findings on 27 assets
11.6.1	11.6 Authentication: The relevant entities shall implement secure authentication procedures and technologies based on access restrictions and the policy on acc…	Fail 4/4 accounts failing	24 findings on 24 assets
11.6.2.c	11.6 Authentication: require the change of authentication credentials initially, at predefined intervals and upon suspicion that the credentials were compromis…	Fail 4/4 accounts failing	195 findings on 193 assets

CONTROL	CONTROL TEXT	VERDICT	EVIDENCE
11.7.2	11.7 Multi-factor authentication: The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to…	Fail 4/4 accounts failing	148 findings on 148 assets
12.1.2.c	12.1 Asset classification: align the availability requirements of the assets with the delivery and recovery objectives set out in their business continuity and…	Fail 4/4 accounts failing	9 findings on 9 assets
12.2.2.b	12.2 Handling of assets: provide rules on the safe use, safe storage, safe transport, and the irretrievable deletion and destruction of the assets;	Fail 4/4 accounts failing	9 findings on 9 assets

SECTION 4 Remediation plan

Every check that produced findings, most severe and most widespread first, with what to do about it and every affected resource. Each entry fixes one class of problem across the estate; the findings in Appendix A refer to these entries by number.

#1 Critical High-risk port open to the internet (database, mail, admin or development ports)

27 findings · 27 assets

AWS FSBP EC2.19 · PCI DSS 1.3.1

What to do. Replace wide or public rules with rules for the specific ports the workload serves, restricted to the addresses that need them; databases and caches should never be reachable from 0.0.0.0/0.

EXAMPLE COMMANDS

```
aws ec2 revoke-security-group-ingress --group-id sg-e1c2b846 --protocol tcp --port 3306 --cidr 0.0.0.0/0, then re-add the rule restricted to the addresses that need it.
```

```
Replace the wide rule on sg-55c8ec43 with rules for the specific ports the workload serves, restricted to the addresses that need them: aws ec2 revoke-security-group-ingress --group-id sg-55c8ec43 --ip-permissions '[{"IpProtocol":"-1","IpRanges":[{"CidrIp":"0.0.0.0/0"}]}]'
```

```
aws ec2 revoke-security-group-ingress --group-id sg-e4c2bcff --protocol tcp --port 6379 --cidr 0.0.0.0/0, then re-add the rule restricted to the addresses that need it.
```

AFFECTED RESOURCES

sg-e1c2b846 prod-eu
sg-55c8ec43 staging
sg-e4c2bcff prod-eu
sg-8a3d26e3 dev-sandbox
sg-456027f2 prod-us
sg-42cad250 dev-sandbox
sg-171f8ded staging
sg-7b4c3450 staging
sg-0f34a019 prod-us
sg-ef39e24d staging
sg-40f7802e prod-eu
sg-54c8eab0 staging
sg-59ac70f4 prod-us
sg-e939d8db staging
sg-fe4c7944 prod-us
sg-e8a21e8c staging
sg-1c36f327 prod-us
sg-1936ee6e prod-us
sg-9e2e298d prod-eu
sg-0a718a1c staging
sg-1536e822 prod-us
sg-d158b591 prod-us
sg-588554f2 prod-eu
sg-814c3dc2 staging
sg-0d1f7e2f staging
sg-3bd6285b dev-sandbox
sg-0c1f7c9c staging

#2 Critical SSH or RDP open to the whole IPv4 internet

24 findings · 20 assets

CIS 5.3 · AWS FSBP EC2.19 · PCI DSS 1.3.1

What to do. Restrict ports 22 and 3389 to a bastion host, VPN or office address range, or remove the rule; use Systems Manager Session Manager instead of open SSH where possible.

EXAMPLE COMMANDS

```
Restrict the ingress rule for port 22 on sg-88d69668 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-88d69668 --protocol tcp --port 22 --cidr 0.0.0.0/0
```

```
Restrict the ingress rule for port 22 on sg-55c8ec43 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-55c8ec43 --protocol tcp --port 22 --cidr 0.0.0.0/0
```

```
Restrict the ingress rule for port 3389 on sg-55c8ec43 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-55c8ec43 --protocol tcp --port 3389 --cidr 0.0.0.0/0
```

AFFECTED RESOURCES

sg-88d69668 dev-sandbox
sg-55c8ec43 staging
sg-40f7802e prod-eu
sg-9eaed0fb dev-sandbox
sg-9faed28e dev-sandbox
sg-787e1b5b staging
sg-1936ee6e prod-us
sg-51cae9ed dev-sandbox
sg-456027f2 prod-us
sg-c8ceb78d dev-sandbox
sg-e4886fed prod-eu
sg-1071938e staging
sg-5c2c79e3 staging
sg-d058b3fe prod-us
sg-943f7538 dev-sandbox
sg-59855685 prod-eu
sg-5f2c7e9c staging
sg-9b3f803d dev-sandbox
sg-0973c720 staging
sg-cea19642 prod-eu

#3 Critical Lambda function invokable by anyone

11 findings · 11 assets

AWS FSBP Lambda.1 · PCI DSS 1.3.1

What to do. Remove unconditional Principal "*" statements from the function policy and set function URLs to AWS_IAM authentication.

EXAMPLE COMMANDS

```
aws lambda update-function-url-config --function-name data-auth-prod-fn-2 --auth-type AWS_IAM --region us-west-1
```

```
aws lambda update-function-url-config --function-name platform-notify-dev-fn-2 --auth-type AWS_IAM --region us-west-2
```

```
aws lambda remove-permission --function-name ml-worker-prod-fn-4 --statement-id AllowEveryone --region us-east-1
```

AFFECTED RESOURCES

arn:aws:lambda:us-west-1:101278471862:function:data-auth-prod-fn-2 prod-us
arn:aws:lambda:us-west-2:101261694243:function:platform-notify-dev-fn-2 staging
arn:aws:lambda:us-east-1:101244916624:function:ml-worker-prod-fn-4 dev-sandbox
arn:aws:lambda:us-east-1:101261694243:function:infra-billing-prod-fn-12 staging
arn:aws:lambda:us-west-2:101295249481:function:data-auth-stg-fn-14 prod-eu
arn:aws:lambda:us-west-2:101244916624:function:web-cache-prod-fn-17 dev-sandbox
arn:aws:lambda:us-east-2:101244916624:function:web-api-stg-fn-18 dev-sandbox
arn:aws:lambda:us-east-1:101278471862:function:ops-search-stg-fn-22 prod-us
arn:aws:lambda:us-west-1:101261694243:function:mobile-cache-stg-fn-22 staging
arn:aws:lambda:us-east-1:101244916624:function:platform-ingest-prod-fn-22 dev-sandbox
arn:aws:lambda:us-west-1:101244916624:function:ops-search-stg-fn-22 dev-sandbox

#4 Critical S3 bucket publicly accessible

8 findings · 8 assets

CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1

What to do. Remove public ACL grants and Principal "*" policy statements, then enable Block Public Access on the bucket.

EXAMPLE COMMANDS

```
Remove public grants: aws s3api put-bucket-acl --bucket platform-api-dev-data-4243-0 --acl private, and review/remove any policy statement with Principal "*". Then enable Block Public Access.
```

```
Remove public grants: aws s3api put-bucket-acl --bucket mobile-billing-prod-data-9481-1 --acl private, and review/remove any policy statement with Principal "*". Then enable Block Public Access.
```

```
Remove public grants: aws s3api put-bucket-acl --bucket mobile-auth-stg-backups-4243-2 --acl private, and review/remove any policy statement with Principal "*". Then enable Block Public Access.
```

AFFECTED RESOURCES

`platform-api-dev-data-4243-0` staging
`mobile-billing-prod-data-9481-1` prod-eu
`mobile-auth-stg-backups-4243-2` staging
`infra-web-stg-data-1862-8` prod-us
`ops-notify-stg-assets-9481-60` prod-eu
`web-billing-prod-uploads-6624-60` dev-sandbox
`mobile-notify-stg-logs-4243-72` staging
`core-ingest-dev-data-9481-76` prod-eu

#5 Critical SSH or RDP open to the whole IPv6 internet

7 findings · 7 assets

CIS 5.4 · AWS FSBP EC2.19 · PCI DSS 1.3.1

What to do. Restrict ports 22 and 3389 to trusted IPv6 ranges or remove the ::/0 rule.

EXAMPLE COMMANDS

```
Restrict the ingress rule for port 22 on sg-777e19c8 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-777e19c8 --protocol tcp --port 22 --cidr ::/0
```

```
Restrict the ingress rule for port 22 on sg-f54c6b19 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-f54c6b19 --protocol tcp --port 22 --cidr ::/0
```

```
Restrict the ingress rule for port 22 on sg-3f601e80 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-3f601e80 --protocol tcp --port 22 --cidr ::/0
```

AFFECTED RESOURCES

`sg-777e19c8` staging
`sg-f54c6b19` prod-us
`sg-3f601e80` prod-us
`sg-1e36f64d` prod-us
`sg-1b36f194` prod-us
`sg-7d6e16e4` prod-us
`sg-0d73cd6c` staging

#6 Critical IAM role assumable by any AWS account

6 findings · 6 assets

PCI DSS 7.2.1

What to do. Replace Principal "*" in the trust policy with the specific accounts or roles that need it, or add a Condition (sts:ExternalId, aws:PrincipalOrgID).

EXAMPLE COMMANDS

```
Replace Principal "*" with the specific account or role ARNs that need access, or at minimum add a Condition (sts:ExternalId for third parties, aws:PrincipalOrgID for your own organization): aws iam update-assume-role-policy --role-name ops-billing-dev-role-17 --policy-document file://trust.json
```

```
Replace Principal "*" with the specific account or role ARNs that need access, or at minimum add a Condition (sts:ExternalId for third parties, aws:PrincipalOrgID for your own organization): aws iam update-assume-role-policy --role-name infra-api-prod-role-31 --policy-document file://trust.json
```

```
Replace Principal "*" with the specific account or role ARNs that need access, or at minimum add a Condition (sts:ExternalId for third parties, aws:PrincipalOrgID for your own organization): aws iam update-assume-role-policy --role-name payments-cache-prod-role-40 --policy-document file://trust.json
```

AFFECTED RESOURCES

arn:aws:iam::101278471862:role/ops-billing-dev-role-17 prod-us
arn:aws:iam::101295249481:role/infra-api-prod-role-31 prod-eu
arn:aws:iam::101295249481:role/payments-cache-prod-role-40 prod-eu
arn:aws:iam::101244916624:role/ops-auth-dev-role-73 dev-sandbox
arn:aws:iam::101244916624:role/ops-notify-stg-role-94 dev-sandbox
arn:aws:iam::101295249481:role/core-api-dev-role-101 prod-eu

#7 Critical EBS snapshot publicly restorable

5 findings · 5 assets

AWS FSBP EC2.1 · PCI DSS 1.3.1

What to do. Remove the "all" create-volume permission from the snapshot, then treat its contents as exposed and rotate any secrets on the image.

EXAMPLE COMMANDS

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-e6164dce4a55fad4d --attribute createVolumePermission --operation-type remove --group-names all --region us-west-2, then assume the contents are exposed and rotate any secrets on the image.
```

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-d7fb1f9000ed4c39a --attribute createVolumePermission --operation-type remove --group-names all --region us-east-1, then assume the contents are exposed and rotate any secrets on the image.
```

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-6e12469a340d3f14e --attribute createVolumePermission --operation-type remove --group-names all --region us-west-1, then assume the contents are exposed and rotate any secrets on the image.
```

AFFECTED RESOURCES

snap-e6164dce4a55fad4d prod-eu
snap-d7fb1f9000ed4c39a prod-us
snap-6e12469a340d3f14e staging
snap-0bce9aae3d061064e dev-sandbox
snap-cf3f6acf5749fcf27 dev-sandbox

#8 Critical IAM user with an admin-equivalent (Action "*" on Resource "*") policy

4 findings · 4 assets

CIS 1.15 · AWS FSBP IAM.1 · PCI DSS 7.2.1

What to do. Replace the wildcard policy with a least-privilege policy covering only the actions and resources the user needs.

EXAMPLE COMMANDS

```
Replace the wildcard policy on carla.dev-1 with a scoped least-privilege policy covering only the actions/resources actually required.
```

```
Replace the wildcard policy on carla.qa-13 with a scoped least-privilege policy covering only the actions/resources actually required.
```

```
Replace the wildcard policy on gudrun.svc-19 with a scoped least-privilege policy covering only the actions/resources actually required.
```

AFFECTED RESOURCES

arn:aws:iam::101261694243:user/carla.dev-1 staging
arn:aws:iam::101261694243:user/carla.qa-13 staging
arn:aws:iam::101244916624:user/gudrun.svc-19 dev-sandbox
arn:aws:iam::101295249481:user/finn.qa-24 prod-eu

#9 Critical RDS instance publicly accessible

4 findings · 4 assets

CIS 2.2.3 · AWS FSBP RDS.2 · PCI DSS 1.3.1

What to do. Set PubliclyAccessible to false and reach the database through the VPC, a VPN or a bastion.

EXAMPLE COMMANDS

```
aws rds modify-db-instance --db-instance-identifier mobile-notify-dev-db-0 --no-publicly-accessible --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier infra-api-stg-db-1 --no-publicly-accessible --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier ml-web-prod-db-5 --no-publicly-accessible --apply-immediately
```

AFFECTED RESOURCES

mobile-notify-dev-db-0 staging
infra-api-stg-db-1 prod-eu
ml-web-prod-db-5 staging
infra-billing-dev-db-5 staging

#10 Critical SMB/CIFS (port 445) open to the internet

2 findings · 2 assets

CIS 5.1.2 · AWS FSBP EC2.19 · PCI DSS 1.3.1

What to do. Remove internet access to port 445; file sharing belongs behind a VPN or private connectivity.

EXAMPLE COMMANDS

```
Restrict the ingress rule for port 445 on sg-55c8ec43 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-55c8ec43 --protocol tcp --port 445 --cidr 0.0.0.0/0
```

```
Restrict the ingress rule for port 445 on sg-456027f2 to specific trusted CIDR ranges (e.g. a corporate VPN or bastion host IP), or remove it if unused. AWS CLI: aws ec2 revoke-security-group-ingress --group-id sg-456027f2 --protocol tcp --port 445 --cidr 0.0.0.0/0
```

AFFECTED RESOURCES

sg-55c8ec43 staging
sg-456027f2 prod-us

#11 High EC2 instance allows IMDSv1

45 findings · 45 assets

CIS 5.7 · AWS FSBP EC2.8

What to do. Require IMDSv2 (HttpTokens=required) on the instance and in launch templates.

EXAMPLE COMMANDS

```
aws ec2 modify-instance-metadata-options --instance-id i-8c57c195bfa6e35d7 --http-tokens required --http-endpoint enabled --region us-east-1
```

```
aws ec2 modify-instance-metadata-options --instance-id i-38aa9a8141006367c --http-tokens required --http-endpoint enabled --region us-east-2
```

```
aws ec2 modify-instance-metadata-options --instance-id i-f635ef7e0c87169fb --http-tokens required --http-endpoint enabled --region us-east-2
```

AFFECTED RESOURCES

i-8c57c195bfa6e35d7 dev-sandbox
i-38aa9a8141006367c prod-eu
i-f635ef7e0c87169fb dev-sandbox
i-503c0b8b5060037f2 prod-us
i-3aaa9da7c64000bd6 prod-eu
i-1e925ad6678af13ef dev-sandbox
i-78734f8721e5601a0 dev-sandbox
i-e3912b5ef1a23d171 prod-us
i-186eb6d40e7bdeec2 staging
i-196eb8672ccc6e1bf staging
i-4b9291e16c4be0c5e prod-eu
i-fcd62bd3776169abd staging
i-a3760871ba2e65a2b prod-us
i-dce56c9baf6c52bb1 dev-sandbox
i-9589096f64f7c598d staging
i-320f59539920c74a8 prod-us
i-93890649e38c03395 staging
i-eb918e150f4058e88 prod-eu
i-6a38b8fb3a0a2ba2c staging
i-9023936f92b716e7c dev-sandbox
i-95239b4eadf3edb40 dev-sandbox
i-5194d9ea8af0c1b50 prod-eu
i-c91702cdad1a190b7 prod-us
i-2220a7ae913aba33b dev-sandbox
i-899279d475fba9052 prod-us
i-583adb3cc5ca6fc6e staging
i-5c79bdbad2270faf1 dev-sandbox
i-1570abb9e086b16eb prod-us
i-c114b79e8a56641d2 prod-us
i-0a83b17009f650ee6 staging
i-5c7bfc51946b9f67a dev-sandbox
i-c214b9318b0b8bf99 prod-us
i-0e8d8ecaa0c8af6e7 prod-eu
i-8f94c1dd241077f9a prod-us
i-4cea9a195c075fe55 dev-sandbox
i-b5091863a2e23455b prod-eu
i-c514bdeadd810e81d prod-us
i-583d19d3365be4c35 staging
i-1d1e6138742456c9a dev-sandbox
i-f169574570cfcc4c7 staging
i-50eaa065341509d55 dev-sandbox
i-201e65f16fc29e4b7 dev-sandbox
i-1283be08143459cc2 staging
i-bf09282110256ce8c prod-eu
i-708c4f4689e326125 prod-eu

#12 High IAM user with console access but no MFA

21 findings · 21 assets

CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2

What to do. Enrol an MFA device for the user, and enforce MFA account-wide with an IAM policy condition on aws:MultiFactorAuthPresent.

EXAMPLE COMMANDS

```
Enroll an MFA device for dev.qa-1 in the IAM console (Security credentials tab), or enforce it account-wide via an IAM policy condition requiring aws:MultiFactorAuthPresent.
```

```
Enroll an MFA device for carla.dev-1 in the IAM console (Security credentials tab), or enforce it account-wide via an IAM policy condition requiring aws:MultiFactorAuthPresent.
```

```
Enroll an MFA device for bjorn.ops-3 in the IAM console (Security credentials tab), or enforce it account-wide via an IAM policy condition requiring aws:MultiFactorAuthPresent.
```

AFFECTED RESOURCES

arn:aws:iam::101295249481:user/dev.qa-1 prod-eu
arn:aws:iam::101261694243:user/carla.dev-1 staging
arn:aws:iam::101278471862:user/bjorn.ops-3 prod-us
arn:aws:iam::101278471862:user/gudrun.svc-5 prod-us
arn:aws:iam::101278471862:user/alice.svc-9 prod-us
arn:aws:iam::101261694243:user/dev.qa-12 staging
arn:aws:iam::101261694243:user/carla.qa-13 staging
arn:aws:iam::101295249481:user/gudrun.svc-18 prod-eu
arn:aws:iam::101261694243:user/alice.ops-20 staging
arn:aws:iam::101278471862:user/gudrun.qa-21 prod-us
arn:aws:iam::101244916624:user/gudrun.svc-22 dev-sandbox
arn:aws:iam::101244916624:user/eva.ops-24 dev-sandbox
arn:aws:iam::101244916624:user/finn.qa-27 dev-sandbox
arn:aws:iam::101261694243:user/ines.svc-35 staging
arn:aws:iam::101261694243:user/gudrun.qa-37 staging
arn:aws:iam::101295249481:user/bjorn.qa-38 prod-eu
arn:aws:iam::101261694243:user/carla.svc-38 staging
arn:aws:iam::101295249481:user/dev.data-46 prod-eu
arn:aws:iam::101261694243:user/finn.ops-50 staging
arn:aws:iam::101278471862:user/ines.ops-53 prod-us
arn:aws:iam::101295249481:user/carla.qa-59 prod-eu

#13 High RDS instance storage not encrypted

7 findings · 7 assets

CIS 2.2.1 · AWS FSBP RDS.3 · PCI DSS 3.5.1

What to do. Snapshot the instance, copy the snapshot with a KMS key, restore from the encrypted copy and cut over.

EXAMPLE COMMAND

```
Snapshot the instance, copy the snapshot with --kms-key-id to encrypt it, then restore a new instance from the encrypted snapshot and cut over.
```

AFFECTED RESOURCES

platform-report-prod-db-2 staging
infra-api-stg-db-3 prod-eu
growth-billing-dev-db-3 dev-sandbox
growth-ingest-prod-db-4 prod-eu
ml-report-prod-db-4 prod-eu
platform-auth-dev-db-4 dev-sandbox
payments-api-prod-db-5 staging

#14 High SQS queue open to anyone

7 findings · 7 assets

AWS FSBP SQS.3 · PCI DSS 1.3.1

What to do. Restrict the queue policy Principal or add a Condition on aws:SourceArn / aws:SourceAccount.

EXAMPLE COMMANDS

```
Restrict the statement's Principal or add a Condition on aws:SourceArn / aws:SourceAccount, then: aws sqs set-queue-attributes --queue-url https://sqs.us-west-1.amazonaws.com/101261694243/data-sync-prod-queue-0 --attributes file://attributes.json --region us-west-1
```

```
Restrict the statement's Principal or add a Condition on aws:SourceArn / aws:SourceAccount, then: aws sqs set-queue-attributes --queue-url https://sqs.us-west-2.amazonaws.com/101261694243/mobile-api-stg-queue-3 --attributes file://attributes.json --region us-west-2
```

```
Restrict the statement's Principal or add a Condition on aws:SourceArn / aws:SourceAccount, then: aws sqs set-queue-attributes --queue-url https://sqs.us-east-2.amazonaws.com/101278471862/ml-report-dev-queue-4 --attributes file://attributes.json --region us-east-2
```

AFFECTED RESOURCES

arn:aws:sqs:us-west-1:101261694243:data-sync-prod-queue-0 staging
arn:aws:sqs:us-west-2:101261694243:mobile-api-stg-queue-3 staging
arn:aws:sqs:us-east-2:101278471862:ml-report-dev-queue-4 prod-us
arn:aws:sqs:us-west-2:101261694243:core-cache-dev-queue-5 staging
arn:aws:sqs:us-east-2:101278471862:infra-web-prod-queue-9 prod-us
arn:aws:sqs:us-west-2:101244916624:web-billing-prod-queue-9 dev-sandbox
arn:aws:sqs:us-west-1:101244916624:data-worker-prod-queue-10 dev-sandbox

#15 High EKS API endpoint reachable from the internet

6 findings · 6 assets

AWS FSBP EKS.1 · PCI DSS 1.3.1

What to do. Disable public endpoint access and use private access through the VPC or VPN, or at minimum restrict the public CIDRs.

EXAMPLE COMMANDS

```
aws eks update-cluster-config --name data-eks-0 --resources-vpc-config endpointPublicAccess=false,endpointPrivateAccess=true --region us-east-1 (or, as an interim step, restrict publicAccessCidrs to your office and CI egress addresses).
```

```
aws eks update-cluster-config --name ml-eks-0 --resources-vpc-config endpointPublicAccess=false,endpointPrivateAccess=true --region us-west-2 (or, as an interim step, restrict publicAccessCidrs to your office and CI egress addresses).
```

```
aws eks update-cluster-config --name growth-eks-0 --resources-vpc-config endpointPublicAccess=false,endpointPrivateAccess=true --region us-east-2 (or, as an interim step, restrict publicAccessCidrs to your office and CI egress addresses).
```

AFFECTED RESOURCES

arn:aws:eks:us-east-1:101261694243:cluster/data-eks-0 staging
arn:aws:eks:us-west-2:101244916624:cluster/ml-eks-0 dev-sandbox
arn:aws:eks:us-east-2:101244916624:cluster/growth-eks-0 dev-sandbox
arn:aws:eks:us-west-1:101244916624:cluster/data-eks-0 dev-sandbox
arn:aws:eks:us-west-2:101295249481:cluster/ml-eks-0 prod-eu
arn:aws:eks:us-west-1:101261694243:cluster/web-eks-0 staging

#16 High GuardDuty not enabled in every region

4 findings · 4 assets

AWS FSBP GuardDuty.1 · PCI DSS 11.5.1

What to do. Enable GuardDuty in every region, ideally from a delegated administrator account for the organization.

EXAMPLE COMMANDS

```
aws guardduty create-detector --enable --region ap-southeast-1
aws guardduty create-detector --enable --region ap-northeast-3
aws guardduty create-detector --enable --region ap-south-1
```

```
aws guardduty create-detector --enable --region us-east-2
aws guardduty create-detector --enable --region ca-central-1
aws guardduty create-detector --enable --region ap-southeast-1
aws guardduty create-detector --enable --region ap-northeast-3
aws guardduty create-detector --enable --region ap-south-1
… 1 more line (full command in the CSV export)
```

```
aws guardduty create-detector --enable --region us-east-1
aws guardduty create-detector --enable --region us-east-2
aws guardduty create-detector --enable --region us-west-2
aws guardduty create-detector --enable --region eu-west-2
aws guardduty create-detector --enable --region eu-north-1
```

AFFECTED RESOURCES

guardduty prod-eu
guardduty prod-us
guardduty staging
guardduty dev-sandbox

#17 High SNS topic open to anyone

3 findings · 3 assets

AWS FSBP SNS.4 · PCI DSS 1.3.1

What to do. Restrict the topic policy Principal or add a Condition on aws:SourceArn / aws:SourceAccount.

EXAMPLE COMMANDS

```
Restrict the statement's Principal to the accounts or services that need it, or add a Condition (aws:SourceArn / aws:SourceAccount / aws:PrincipalOrgID): aws sns set-topic-attributes --topic-arn arn:aws:sns:us-west-2:101261694243:platform-cache-stg-events-5 --attribute-name Policy --attribute-value file://policy.json --region us-west-2
```

```
Restrict the statement's Principal to the accounts or services that need it, or add a Condition (aws:SourceArn / aws:SourceAccount / aws:PrincipalOrgID): aws sns set-topic-attributes --topic-arn arn:aws:sns:us-east-1:101295249481:growth-web-dev-events-8 --attribute-name Policy --attribute-value file://policy.json --region us-east-1
```

```
Restrict the statement's Principal to the accounts or services that need it, or add a Condition (aws:SourceArn / aws:SourceAccount / aws:PrincipalOrgID): aws sns set-topic-attributes --topic-arn arn:aws:sns:us-west-1:101261694243:mobile-billing-dev-events-7 --attribute-name Policy --attribute-value file://policy.json --region us-west-1
```

AFFECTED RESOURCES

arn:aws:sns:us-west-2:101261694243:platform-cache-stg-events-5 staging
arn:aws:sns:us-east-1:101295249481:growth-web-dev-events-8 prod-eu
arn:aws:sns:us-west-1:101261694243:mobile-billing-dev-events-7 staging

#18 High No multi-region CloudTrail trail logging all management events

2 findings · 2 assets

CIS 3.1 · AWS FSBP CloudTrail.1 · PCI DSS 10.2.1

What to do. Create one multi-region trail (or organization trail) that logs read and write management events to a dedicated bucket.

EXAMPLE COMMAND

```
aws cloudtrail create-trail --name management-events --s3-bucket-name <log-bucket> --is-multi-region-trail --enable-log-file-validation && aws cloudtrail start-logging --name management-events
(or repair the existing trail: update-trail --is-multi-region-trail, start-logging, and put-event-selectors with ReadWriteType=All,IncludeManagementEvents=true)
```

AFFECTED RESOURCES

cloudtrail prod-eu

cloudtrail staging

#19 Medium Access key older than 90 days

58 findings · 56 assets

CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9

What to do. Create a new key, update every place it is used, then delete the old key; prefer roles and short-lived credentials over long-lived keys.

EXAMPLE COMMANDS

```
Rotate the key: aws iam create-access-key --user-name dev.qa-1, update it wherever it's used, then aws iam delete-access-key --user-name dev.qa-1 --access-key-id AKIA8249915B532ECDF2
```

```
Rotate the key: aws iam create-access-key --user-name gudrun.svc-2, update it wherever it's used, then aws iam delete-access-key --user-name gudrun.svc-2 --access-key-id AKIA09F5E39BF6DC9DEC
```

```
Rotate the key: aws iam create-access-key --user-name alice.data-2, update it wherever it's used, then aws iam delete-access-key --user-name alice.data-2 --access-key-id AKIA7367FB976B803FF7
```

AFFECTED RESOURCES

arn:aws:iam::101295249481:user/dev.qa-1 prod-eu
arn:aws:iam::101278471862:user/gudrun.svc-2 prod-us
arn:aws:iam::101261694243:user/alice.data-2 staging
arn:aws:iam::101295249481:user/finn.data-5 prod-eu
arn:aws:iam::101278471862:user/gudrun.svc-5 prod-us
arn:aws:iam::101278471862:user/alice.svc-6 prod-us
arn:aws:iam::101278471862:user/eva.dev-7 prod-us
arn:aws:iam::101261694243:user/jonas.ops-9 staging
arn:aws:iam::101278471862:user/carla.svc-10 prod-us
arn:aws:iam::101278471862:user/hakon.dev-12 prod-us
arn:aws:iam::101244916624:user/alice.data-12 dev-sandbox
arn:aws:iam::101244916624:user/finn.qa-16 dev-sandbox
arn:aws:iam::101295249481:user/eva.ops-17 prod-eu
arn:aws:iam::101278471862:user/carla.ops-17 prod-us
arn:aws:iam::101278471862:user/alice.svc-18 prod-us
arn:aws:iam::101278471862:user/bjorn.ops-19 prod-us
arn:aws:iam::101261694243:user/alice.ops-20 staging
arn:aws:iam::101278471862:user/gudrun.qa-21 prod-us
arn:aws:iam::101261694243:user/bjorn.qa-21 staging
arn:aws:iam::101244916624:user/ines.data-21 dev-sandbox
arn:aws:iam::101278471862:user/bjorn.ops-24 prod-us
arn:aws:iam::101244916624:user/dev.qa-25 dev-sandbox
arn:aws:iam::101295249481:user/hakon.dev-27 prod-eu
arn:aws:iam::101295249481:user/hakon.qa-28 prod-eu
arn:aws:iam::101278471862:user/carla.data-29 prod-us
arn:aws:iam::101261694243:user/eva.dev-29 staging
arn:aws:iam::101261694243:user/ines.dev-30 staging
arn:aws:iam::101295249481:user/ines.svc-33 prod-eu
arn:aws:iam::101261694243:user/eva.dev-33 staging
arn:aws:iam::101244916624:user/gudrun.ops-33 dev-sandbox
arn:aws:iam::101244916624:user/ines.ops-35 dev-sandbox
arn:aws:iam::101244916624:user/eva.data-36 dev-sandbox
arn:aws:iam::101295249481:user/jonas.svc-37 prod-eu
arn:aws:iam::101261694243:user/gudrun.qa-37 staging
arn:aws:iam::101244916624:user/finn.qa-37 dev-sandbox
arn:aws:iam::101261694243:user/carla.svc-38 staging
arn:aws:iam::101244916624:user/hakon.dev-38 dev-sandbox
arn:aws:iam::101244916624:user/jonas.qa-39 dev-sandbox
arn:aws:iam::101261694243:user/gudrun.qa-41 staging
arn:aws:iam::101244916624:user/finn.svc-42 dev-sandbox
arn:aws:iam::101278471862:user/carla.data-44 prod-us
arn:aws:iam::101278471862:user/bjorn.svc-45 prod-us
arn:aws:iam::101261694243:user/eva.ops-46 staging
arn:aws:iam::101244916624:user/carla.ops-47 dev-sandbox
arn:aws:iam::101261694243:user/eva.svc-48 staging
arn:aws:iam::101295249481:user/eva.ops-49 prod-eu
arn:aws:iam::101244916624:user/gudrun.dev-50 dev-sandbox
arn:aws:iam::101295249481:user/jonas.qa-51 prod-eu
arn:aws:iam::101244916624:user/alice.ops-51 dev-sandbox
arn:aws:iam::101261694243:user/dev.dev-52 staging
arn:aws:iam::101278471862:user/ines.ops-53 prod-us
arn:aws:iam::101278471862:user/eva.svc-55 prod-us
arn:aws:iam::101295249481:user/hakon.qa-56 prod-eu
arn:aws:iam::101278471862:user/alice.dev-56 prod-us
arn:aws:iam::101278471862:user/eva.data-58 prod-us
arn:aws:iam::101295249481:user/carla.qa-59 prod-eu

#20 Medium **EBS volume not encrypted** 50 findings · 50 assets

CIS 5.1.1 · AWS FSBP EC2.3 · PCI DSS 3.5.1

What to do. Snapshot the volume, copy the snapshot with encryption, create a new volume from it and swap it in; enable encryption by default for new volumes.

EXAMPLE COMMAND

```
Encryption can't be enabled in place: snapshot the volume, copy the snapshot with encryption, create a new volume from it, and swap the attachment.
```

AFFECTED RESOURCES

vol-ee9a1185ad19a015c dev-sandbox
vol-5a472dea94bc7a3c7 prod-us
vol-ff4e12b98d83eb47a staging
vol-57472931b1507612d prod-us
vol-c8cc2ef4d6e4f918c staging
vol-edd1471874bf92797 dev-sandbox
vol-ecbb4428e8282dd81 prod-eu
vol-f3851a6de8d25bf57 staging
vol-edbb45bbd8b44ef8f prod-eu
vol-4fc477f767d16e292 prod-eu
vol-a272990997191385a staging
vol-8a740fe1edfc604c9 prod-us
vol-4dc474d19800f10c0 prod-eu
vol-f5019d1e7c6bdaef7 prod-eu
vol-7880cf2c672c7e121 staging
vol-1e4329e5fca0cd286 dev-sandbox
vol-5e6766d4feb910d9d prod-us
vol-68e4e27c5e92db7fb staging
vol-ee0adfd9247e67262 prod-us
vol-5cbe9dbf1f69ece67 dev-sandbox
vol-366fb06e658976644 staging
vol-344b6f729cc0f836a prod-eu
vol-73e4f3cddaf480967 staging
vol-067f03456b3a74da9 dev-sandbox
vol-4a49537d6bf31d549 prod-eu
vol-fa6eb003d7e1582e2 prod-us
vol-40bfe32ccc4897cc6 prod-eu
vol-71e72f3ecedbfdec1 staging
vol-3fbfe19981e75a6c6 prod-eu
vol-dc826bfbc10953e5e dev-sandbox
vol-75e7358a3ad3b85e3 staging
vol-78fc5cbc95532c83b prod-eu
vol-63c325f266b91fa5d dev-sandbox
vol-6d72fe6aba3c10fe3 staging
vol-326b2cf431a292d80 staging
vol-6e72fffd1ba650582 staging
vol-7771c30f905ad99d3 staging
vol-8e778a985e149a056 dev-sandbox
vol-2747b53e00ff4628e dev-sandbox
vol-42c26dec078813a7a prod-eu
vol-71fa1320801857ae5 prod-eu
vol-037b8a21590b689a7 prod-us
vol-50c4c28dcd814a0a5 prod-eu
vol-800376ea87f8b4faa prod-us
vol-b64e7aaffddebb4ab prod-eu
vol-faec8417a56fd5bab staging
vol-7175434db88bf157d staging
vol-aa4ac20e847d2fb7e dev-sandbox
vol-027a7fcb07899eb30 dev-sandbox
vol-667531fccab49a7d7 staging

#21 Medium Network ACL allows SSH or RDP from the internet

49 findings · 49 assets

CIS 5.2 · AWS FSBP EC2.21 · PCI DSS 1.3.1

What to do. Add deny entries for TCP 22 and 3389 from 0.0.0.0/0 and ::/0 ahead of the allow-all rule, or delete unused default VPCs.

EXAMPLE COMMANDS

```
The simplest fix closes all of these at once: delete default VPCs in regions you do not use (aws ec2 delete-vpc after removing their subnets and internet gateway — nothing is running in them), or disable the regions themselves in the account settings. Otherwise add deny entries for TCP 22 and 3389 from 0.0.0.0/0 and ::/0 ahead of the allow-all rule in each ACL.
```

```
Add deny entries ahead of the allow for ports 22 and 3389 from 0.0.0.0/0 and ::/0, e.g. aws ec2 create-network-acl-entry --network-acl-id acl-cbe58b01 --ingress --rule-number 90 --protocol tcp --port-range From=22,To=22 --cidr-block 0.0.0.0/0 --rule-action deny --region us-east-1 (repeat for 3389 and ::/0), or narrow the allow entry to trusted ranges.
```

```
Add deny entries ahead of the allow for ports 22 and 3389 from 0.0.0.0/0 and ::/0, e.g. aws ec2 create-network-acl-entry --network-acl-id acl-e31f5fd2 --ingress --rule-number 90 --protocol tcp --port-range From=22,To=22 --cidr-block 0.0.0.0/0 --rule-action deny --region us-east-2 (repeat for 3389 and ::/0), or narrow the allow entry to trusted ranges.
```

AFFECTED RESOURCES

unused-network-acls prod-us
unused-network-acls prod-eu
unused-network-acls staging
unused-network-acls dev-sandbox
acl-cbe58b01 prod-eu
acl-e31f5fd2 prod-eu
acl-4ac6081b prod-eu
acl-7b2760a0 prod-eu
acl-44c4eefa prod-us
acl-da9ba989 prod-us
acl-34f5eaec prod-us
acl-fa481402 staging
acl-35f7a2f1 staging
acl-6c0b4914 staging
acl-85ba1eef staging
acl-f07f1e7b dev-sandbox
acl-caa45580 dev-sandbox
acl-846103e1 dev-sandbox
acl-c2e1d232 dev-sandbox
acl-cae5896e prod-eu
acl-e41f6165 prod-eu
acl-49c60688 prod-eu
acl-7c276233 prod-eu
acl-45c4f08d prod-us
acl-d99ba7f6 prod-us
acl-35f5ec7f prod-us
acl-fb481595 staging
acl-34f7a15e staging
acl-6d0b4aa7 staging
acl-84ba1d5c staging
acl-ef7f1ce8 dev-sandbox
acl-cba45713 dev-sandbox
acl-8361024e dev-sandbox
acl-c3e1d3c5 dev-sandbox
acl-c8e58648 prod-eu
acl-e21f5e3f prod-eu
acl-4bc609ae prod-eu
acl-7e276559 prod-eu
acl-43c4ed67 prod-us
acl-d79ba4d0 prod-us
acl-37f5efa5 prod-us
acl-f948126f staging
acl-32f79e38 staging
acl-6f0b4dcd staging
acl-86ba2082 staging
acl-f17f200e dev-sandbox
acl-cda45a39 dev-sandbox
acl-8160ff28 dev-sandbox
acl-c1e1d09f dev-sandbox

#22 Medium **Customer-managed KMS key without automatic rotation** 33 findings · 33 assets

CIS 3.6 · PCI DSS 3.7.4

What to do. Enable automatic key rotation on the key.

EXAMPLE COMMANDS

```
aws kms enable-key-rotation --key-id 29431c93-769c-1a65-c65c-e0a6877f195b --region us-east-1
```

```
aws kms enable-key-rotation --key-id 695700b1-bc10-a580-b5cd-ac339b122e2c --region us-east-1
```

```
aws kms enable-key-rotation --key-id 0d64f0c7-597c-2c7c-b2e3-618b34c3c247 --region us-west-1
```

AFFECTED RESOURCES

arn:aws:kms:us-east-1:101295249481:key/29431c93-769c-1a65-c65c-e0a6877f195b prod-eu
arn:aws:kms:us-east-1:101278471862:key/695700b1-bc10-a580-b5cd-ac339b122e2c prod-us
arn:aws:kms:us-west-1:101278471862:key/0d64f0c7-597c-2c7c-b2e3-618b34c3c247 prod-us
arn:aws:kms:us-west-2:101261694243:key/be3b4949-3414-627f-3524-9ea024d1b8c8 staging
arn:aws:kms:us-east-1:101295249481:key/83b47ee5-ffc6-d113-f219-e0de20be759d prod-eu
arn:aws:kms:us-west-1:101295249481:key/9e8c24a4-3fd9-114f-b6c5-c23a94441127 prod-eu
arn:aws:kms:us-east-2:101261694243:key/0f79b00b-a66a-708d-83b1-c52dc51d478d staging
arn:aws:kms:us-west-1:101244916624:key/618a0ac7-1942-d969-27ff-8ef63d8da2cd dev-sandbox
arn:aws:kms:us-west-1:101278471862:key/99c8729b-2055-45ba-32d0-4b39508514a2 prod-us
arn:aws:kms:us-east-2:101261694243:key/ed3310ea-c120-8569-feb0-f0472b359744 staging
arn:aws:kms:us-west-2:101261694243:key/2227ede4-c947-fde0-d425-d1091e751d6e staging
arn:aws:kms:us-east-2:101244916624:key/e0cbc725-2a02-e146-6a82-1a0ddb5868bd dev-sandbox
arn:aws:kms:us-west-2:101244916624:key/6b04e0f1-37de-9706-0cfa-ee57b955314e dev-sandbox
arn:aws:kms:us-west-1:101278471862:key/be03af25-3e5b-2e60-2539-ec6fd9bb3452 prod-us
arn:aws:kms:us-west-2:101244916624:key/41231136-48a2-b474-4fe7-847c5d711e1d dev-sandbox
arn:aws:kms:us-west-2:101295249481:key/63101c11-0130-755a-e5f1-db8f08479646 prod-eu
arn:aws:kms:us-west-1:101278471862:key/3dc3f8e5-bae8-75fe-44a1-752b1fcada12 prod-us
arn:aws:kms:us-east-1:101261694243:key/565015d8-f696-4d30-f512-f50c0cb29524 staging
arn:aws:kms:us-east-2:101244916624:key/4f9e02da-302d-1fc5-b6d2-fae2a638e386 dev-sandbox
arn:aws:kms:us-east-1:101295249481:key/0d646f5a-614b-351e-0c57-7b4d6a9c56da prod-eu
arn:aws:kms:us-west-1:101295249481:key/7ed7009c-ff58-e650-993b-a081554878a7 prod-eu
arn:aws:kms:us-west-2:101295249481:key/fec6f4e7-114c-00c5-5069-b54111d4343b prod-eu
arn:aws:kms:us-east-2:101278471862:key/7122d648-6593-6627-466f-ea93d2e537fc prod-us
arn:aws:kms:us-east-1:101261694243:key/2b57f357-19c0-a41c-ccb8-0f37f7acd5fc staging
arn:aws:kms:us-east-2:101244916624:key/7ce00e01-1090-c8c3-ed06-634601310bd9 dev-sandbox
arn:aws:kms:us-west-2:101244916624:key/161d097b-bb5e-7aa7-9b0e-d724d8f7c402 dev-sandbox
arn:aws:kms:us-east-1:101261694243:key/41f70ac1-003f-3115-bbfa-9024f1cc047e staging
arn:aws:kms:us-west-1:101244916624:key/e1e9e55d-8732-49df-0a07-70ace3fa5080 dev-sandbox
arn:aws:kms:us-west-2:101244916624:key/407f15b6-af42-ddc6-69de-e86f83f35fbc dev-sandbox
arn:aws:kms:us-west-2:101261694243:key/f257319c-9db4-ce4b-9403-a2104e338038 staging
arn:aws:kms:us-east-2:101244916624:key/b55fe405-ecd6-edbf-dae5-c30183dde6f9 dev-sandbox
arn:aws:kms:us-west-1:101244916624:key/70e7f2b8-d60c-3258-07a3-be3f0a8b579f dev-sandbox
arn:aws:kms:us-west-2:101244916624:key/7afe5c31-3ef2-bc84-b7c3-265a81d4c88d dev-sandbox

#23 Medium IAM credentials unused for 45 days or more

27 findings · 27 assets

CIS 1.11 · AWS FSBP IAM.8

What to do. Deactivate or delete the unused password or access key; remove users who have left.

EXAMPLE COMMANDS

```
Deactivate what isn't needed: aws iam update-login-profile / delete-login-profile --user-name finn.data-1 for the password, aws iam update-access-key --user-name finn.data-1 --access-key-id <id> --status Inactive for keys — then delete after a grace period.
```

```
Deactivate what isn't needed: aws iam update-login-profile / delete-login-profile --user-name bjorn.ops-3 for the password, aws iam update-access-key --user-name bjorn.ops-3 --access-key-id <id> --status Inactive for keys — then delete after a grace period.
```

```
Deactivate what isn't needed: aws iam update-login-profile / delete-login-profile --user-name eva.data-8 for the password, aws iam update-access-key --user-name eva.data-8 --access-key-id <id> --status Inactive for keys — then delete after a grace period.
```

AFFECTED RESOURCES

arn:aws:iam::101278471862:user/finn.data-1 prod-us
arn:aws:iam::101278471862:user/bjorn.ops-3 prod-us
arn:aws:iam::101278471862:user/eva.data-8 prod-us
arn:aws:iam::101295249481:user/carla.svc-9 prod-eu
arn:aws:iam::101278471862:user/hakon.dev-12 prod-us
arn:aws:iam::101261694243:user/dev.qa-12 staging
arn:aws:iam::101295249481:user/finn.dev-13 prod-eu
arn:aws:iam::101261694243:user/carla.qa-13 staging
arn:aws:iam::101295249481:user/finn.data-16 prod-eu
arn:aws:iam::101261694243:user/hakon.ops-16 staging
arn:aws:iam::101278471862:user/carla.ops-17 prod-us
arn:aws:iam::101261694243:user/carla.ops-18 staging
arn:aws:iam::101261694243:user/alice.ops-20 staging
arn:aws:iam::101261694243:user/bjorn.qa-21 staging
arn:aws:iam::101244916624:user/gudrun.svc-22 dev-sandbox
arn:aws:iam::101244916624:user/dev.qa-25 dev-sandbox
arn:aws:iam::101295249481:user/hakon.dev-27 prod-eu
arn:aws:iam::101244916624:user/finn.qa-27 dev-sandbox
arn:aws:iam::101295249481:user/hakon.qa-28 prod-eu
arn:aws:iam::101295249481:user/alice.svc-29 prod-eu
arn:aws:iam::101295249481:user/dev.svc-41 prod-eu
arn:aws:iam::101278471862:user/jonas.dev-48 prod-us
arn:aws:iam::101261694243:user/eva.data-49 staging
arn:aws:iam::101278471862:user/ines.ops-53 prod-us
arn:aws:iam::101278471862:user/eva.svc-55 prod-us
arn:aws:iam::101295249481:user/hakon.qa-56 prod-eu
arn:aws:iam::101295249481:user/carla.qa-59 prod-eu

#24 Medium S3 bucket without full Block Public Access

26 findings · 26 assets

CIS 2.1.4 · AWS FSBP S3.8 · PCI DSS 1.3.1

What to do. Enable all four Block Public Access settings on the bucket.

EXAMPLE COMMANDS

```
aws s3api put-public-access-block --bucket platform-cache-stg-uploads-6624-9 --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

```
aws s3api put-public-access-block --bucket infra-worker-stg-logs-1862-13 --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

```
aws s3api put-public-access-block --bucket mobile-notify-prod-assets-9481-16 --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

AFFECTED RESOURCES

platform-cache-stg-uploads-6624-9 dev-sandbox
infra-worker-stg-logs-1862-13 prod-us
mobile-notify-prod-assets-9481-16 prod-eu
ml-api-dev-uploads-1862-17 prod-us
ml-notify-stg-assets-6624-17 dev-sandbox
infra-sync-dev-logs-6624-20 dev-sandbox
data-notify-prod-assets-9481-24 prod-eu
infra-auth-prod-data-1862-25 prod-us
ops-billing-prod-exports-1862-26 prod-us
infra-search-dev-exports-9481-27 prod-eu
payments-api-prod-backups-9481-31 prod-eu
data-worker-dev-data-4243-33 staging
mobile-web-prod-logs-4243-34 staging
data-sync-dev-exports-1862-36 prod-us
ops-worker-stg-uploads-9481-38 prod-eu
core-notify-stg-assets-1862-44 prod-us
ops-api-stg-exports-9481-47 prod-eu
infra-gateway-prod-data-1862-50 prod-us
ml-cache-stg-assets-4243-56 staging
platform-gateway-prod-exports-1862-58 prod-us
mobile-notify-prod-backups-4243-61 staging
payments-sync-prod-uploads-4243-62 staging
core-notify-stg-logs-6624-66 dev-sandbox
growth-gateway-stg-logs-9481-68 prod-eu
core-auth-dev-exports-9481-78 prod-eu
ops-billing-stg-assets-4243-79 staging

#25 Medium S3 bucket without default encryption

19 findings · 19 assets

What to do. Configure default server-side encryption (SSE-S3 or SSE-KMS) on the bucket.

EXAMPLE COMMANDS

```
aws s3api put-bucket-encryption --bucket core-gateway-dev-uploads-1862-2 --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"AES256"}}]}'
```

```
aws s3api put-bucket-encryption --bucket growth-search-prod-assets-6624-2 --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"AES256"}}]}'
```

```
aws s3api put-bucket-encryption --bucket mobile-notify-dev-backups-4243-6 --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"AES256"}}]}'
```

AFFECTED RESOURCES

core-gateway-dev-uploads-1862-2 prod-us
growth-search-prod-assets-6624-2 dev-sandbox
mobile-notify-dev-backups-4243-6 staging
payments-worker-stg-exports-4243-7 staging
payments-gateway-prod-uploads-9481-9 prod-eu
core-search-stg-uploads-9481-14 prod-eu
ml-auth-stg-assets-1862-15 prod-us
ops-auth-stg-exports-4243-22 staging
data-gateway-stg-assets-4243-35 staging
platform-report-stg-exports-9481-39 prod-eu
mobile-auth-stg-assets-9481-43 prod-eu
infra-gateway-prod-data-1862-50 prod-us
mobile-gateway-dev-assets-1862-52 prod-us
mobile-search-stg-backups-9481-54 prod-eu
platform-gateway-prod-exports-1862-58 prod-us
mobile-report-stg-logs-1862-61 prod-us
payments-web-dev-uploads-1862-66 prod-us
ops-billing-prod-data-6624-68 dev-sandbox
payments-web-prod-backups-1862-70 prod-us

#26 Medium **Application load balancer serving plaintext HTTP** 17 findings · 17 assets

AWS FSBP ELB.1

What to do. Make the HTTP listener redirect to HTTPS and serve everything on a TLS listener.

EXAMPLE COMMANDS

```
Replace the listener's default action with a redirect: aws elbv2 modify-listener --listener-arn <listener-arn> --default-actions 'Type=redirect,RedirectConfig={Protocol=HTTPS,Port=443,StatusCode=HTTP_301}' --region us-west-2
```

```
Replace the listener's default action with a redirect: aws elbv2 modify-listener --listener-arn <listener-arn> --default-actions 'Type=redirect,RedirectConfig={Protocol=HTTPS,Port=443,StatusCode=HTTP_301}' --region us-east-2
```

```
Replace the listener's default action with a redirect: aws elbv2 modify-listener --listener-arn <listener-arn> --default-actions 'Type=redirect,RedirectConfig={Protocol=HTTPS,Port=443,StatusCode=HTTP_301}' --region us-west-1
```

AFFECTED RESOURCES

arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/core-ingest-dev-alb-0/0e719567331c94b3 staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-web-dev-alb-0/692e38ebf4165952 dev-sandbox
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/payments-cache-stg-alb-2/486e68d1db1bd8c7 prod-us
arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/payments-worker-stg-alb-5/f308e0bd625e24e6 staging
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/web-search-dev-alb-0/411d170f38cb82b3 prod-us
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/payments-notify-stg-alb-0/0e9cc68b131e19a7 dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/data-search-dev-alb-0/fdb6cb74740d8038 prod-eu
arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/infra-api-prod-alb-0/4be987aa1b11c2cd dev-sandbox
arn:aws:elasticloadbalancing:us-east-1:101261694243:loadbalancer/app/ops-gateway-stg-alb-2/a60ff3632c906d04 staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/growth-ingest-stg-alb-1/d68aff76aa7066bd dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/core-search-stg-alb-2/3d8009dff5992ea5 dev-sandbox
arn:aws:elasticloadbalancing:us-east-1:101244916624:loadbalancer/app/web-billing-prod-alb-3/d81d008bd0703e18 dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/web-search-stg-alb-3/7ca38159f494ab41 prod-eu
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/payments-worker-stg-alb-3/c05e5208561107ef staging
arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/growth-worker-stg-alb-4/ad5540c8820c6bfe staging
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/infra-billing-dev-alb-5/68a17b243036afff staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-sync-stg-alb-5/1d0ad78e3268db07 dev-sandbox

#27 Medium VPC without flow logs

16 findings · 16 assets

CIS 3.7 · AWS FSBP EC2.6

What to do. Enable VPC flow logs (at least REJECT traffic) to CloudWatch Logs or S3 on every VPC; delete default VPCs in regions you do not use.

EXAMPLE COMMANDS

```
The simplest fix closes all of these at once: delete default VPCs in regions you do not use (aws ec2 delete-vpc after removing their subnets and internet gateway — nothing is running in them), or disable the regions themselves in the account settings. Otherwise enable flow logs per VPC: aws ec2 create-flow-logs --resource-type VPC --resource-ids <vpc-id> --traffic-type REJECT --log-destination-type cloud-watch-logs --log-group-name vpc-flow-logs --deliver-logs-permission-arn <role-arn>.
```

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-15907cbb --traffic-type REJECT --log-destination-type cloud-watch-logs --log-group-name vpc-flow-logs --deliver-logs-permission-arn <role-arn> --region us-east-2 (REJECT-only keeps volume and cost down while still catching scans and blocked exfiltration).
```

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-f4e3b734 --traffic-type REJECT --log-destination-type cloud-watch-logs --log-group-name vpc-flow-logs --deliver-logs-permission-arn <role-arn> --region us-west-1 (REJECT-only keeps volume and cost down while still catching scans and blocked exfiltration).
```

AFFECTED RESOURCES

unused-vpcs prod-us
unused-vpcs prod-eu
unused-vpcs staging
unused-vpcs dev-sandbox
vpc-15907cbb prod-eu
vpc-f4e3b734 prod-eu
vpc-892b02bd prod-eu
vpc-4163aa13 prod-us
vpc-dd1f1ec1 staging
vpc-32d93394 dev-sandbox
vpc-1a72f99b dev-sandbox
vpc-5b7fbd51 prod-eu
vpc-fc71e7d6 prod-us
vpc-07fec738 staging
vpc-dc1f1d2e staging
vpc-33d93527 dev-sandbox

#28 Medium Default security group still allows traffic

14 findings · 14 assets

CIS 5.5 · AWS FSBP EC2.2 · PCI DSS 1.3.1

What to do. Remove every ingress and egress rule from each VPC default security group so nothing launched by omission inherits open rules; delete unused default VPCs.

EXAMPLE COMMANDS

```
The simplest fix closes all of these at once: delete default VPCs in regions you do not use (aws ec2 delete-vpc after removing their subnets and internet gateway — nothing is running in them), or disable the regions themselves in the account settings. Otherwise strip each group's ingress and egress rules with aws ec2 revoke-security-group-ingress / revoke-security-group-egress.
```

```
Remove every rule: aws ec2 revoke-security-group-ingress --group-id sg-e2c2b9d9 --ip-permissions "$(aws ec2 describe-security-groups --group-ids sg-e2c2b9d9 --query 'SecurityGroups[0].IpPermissions' --region us-east-1)" --region us-east-1, and the same with revoke-security-group-egress / IpPermissionsEgress. Move anything that relied on it to a purpose-built group first.
```

```
Remove every rule: aws ec2 revoke-security-group-ingress --group-id sg-8ae89ad6 --ip-permissions "$(aws ec2 describe-security-groups --group-ids sg-8ae89ad6 --query 'SecurityGroups[0].IpPermissions' --region us-east-2)" --region us-east-2, and the same with revoke-security-group-egress / IpPermissionsEgress. Move anything that relied on it to a purpose-built group first.
```

AFFECTED RESOURCES

unused-default-security-groups prod-us
unused-default-security-groups prod-eu
unused-default-security-groups staging
unused-default-security-groups dev-sandbox
sg-e2c2b9d9 prod-eu
sg-8ae89ad6 prod-eu
sg-3ff77e9b prod-eu
sg-5a4a2554 prod-eu
sg-fc4c761e prod-us
sg-55ac6aa8 prod-us
sg-57c8ef69 staging
sg-6f7e0d30 staging
sg-89d697fb dev-sandbox
sg-086a94b6 dev-sandbox

#29 Medium CloudFront distribution serves viewers over plaintext HTTP

10 findings · 10 assets

AWS FSBP CloudFront.3

What to do. Set the viewer protocol policy to redirect-to-https or https-only on every cache behavior.

EXAMPLE COMMANDS

```
Set ViewerProtocolPolicy to redirect-to-https (or https-only) on the default and every additional cache behavior: aws cloudfront get-distribution-config --id E51631B9C1892F > config.json, edit, then aws cloudfront update-distribution --id E51631B9C1892F --if-match <ETag> --distribution-config file://config.json
```

```
Set ViewerProtocolPolicy to redirect-to-https (or https-only) on the default and every additional cache behavior: aws cloudfront get-distribution-config --id EA6CB85CA667EA > config.json, edit, then aws cloudfront update-distribution --id EA6CB85CA667EA --if-match <ETag> --distribution-config file://config.json
```

```
Set ViewerProtocolPolicy to redirect-to-https (or https-only) on the default and every additional cache behavior: aws cloudfront get-distribution-config --id EE94E63B66CAC0 > config.json, edit, then aws cloudfront update-distribution --id EE94E63B66CAC0 --if-match <ETag> --distribution-config file://config.json
```

AFFECTED RESOURCES

arn:aws:cloudfront::101278471862:distribution/E51631B9C1892F prod-us
arn:aws:cloudfront::101261694243:distribution/EA6CB85CA667EA staging
arn:aws:cloudfront::101244916624:distribution/EE94E63B66CAC0 dev-sandbox
arn:aws:cloudfront::101278471862:distribution/EF746157DBC0AA prod-us
arn:aws:cloudfront::101244916624:distribution/EF824E30F2E863 dev-sandbox
arn:aws:cloudfront::101295249481:distribution/E306B6E6CDDE80 prod-eu
arn:aws:cloudfront::101261694243:distribution/EA662C0A165575 staging
arn:aws:cloudfront::101244916624:distribution/E7BD9EFAA0BE16 dev-sandbox
arn:aws:cloudfront::101295249481:distribution/EF55838C3AF30F prod-eu
arn:aws:cloudfront::101244916624:distribution/E9D8DE1947ABFD dev-sandbox

#30 Medium RDS instance with automated backups disabled

10 findings · 10 assets

AWS FSBP RDS.11

What to do. Set a backup retention period of at least 7 days.

EXAMPLE COMMANDS

```
aws rds modify-db-instance --db-instance-identifier payments-api-prod-db-0 --backup-retention-period 7 --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier mobile-report-dev-db-0 --backup-retention-period 7 --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier growth-report-stg-db-0 --backup-retention-period 7 --apply-immediately
```

AFFECTED RESOURCES

payments-api-prod-db-0 prod-eu
mobile-report-dev-db-0 prod-us
growth-report-stg-db-0 dev-sandbox
web-api-stg-db-1 staging
platform-api-stg-db-1 dev-sandbox
ml-api-prod-db-1 dev-sandbox
growth-notify-dev-db-3 staging
growth-notify-dev-db-4 prod-eu
ops-cache-stg-db-4 prod-eu
data-web-stg-db-4 prod-us

#31 Medium EFS file system not encrypted

6 findings · 6 assets

CIS 2.3.1 · AWS FSBP EFS.1

What to do. Create an encrypted file system and migrate the data; encryption cannot be enabled on an existing file system.

EXAMPLE COMMANDS

```
Create an encrypted file system (aws efs create-file-system --encrypted --region us-west-2), copy the data across with AWS DataSync or rsync, repoint the mount targets, then delete fs-94fac1a6.
```

```
Create an encrypted file system (aws efs create-file-system --encrypted --region us-east-2), copy the data across with AWS DataSync or rsync, repoint the mount targets, then delete fs-1e9efef9.
```

```
Create an encrypted file system (aws efs create-file-system --encrypted --region us-west-1), copy the data across with AWS DataSync or rsync, repoint the mount targets, then delete fs-8a79a87a.
```

AFFECTED RESOURCES

- `fs-94fac1a6` prod-eu
- `fs-1e9efef9` prod-us
- `fs-8a79a87a` prod-us
- `fs-2f76d9ff` prod-us
- `fs-576adef7` staging
- `fs-3067a5be` staging

#32 Medium AWS Config not recording in every region

5 findings · 4 assets

CIS 3.3 · AWS FSBP Config.1

What to do. Create and start a configuration recorder in each region, with global resource types included in exactly one.

EXAMPLE COMMANDS

```
In exactly one region, update the recorder with --recording-group allSupported=true,includeGlobalResourceTypes=true (CIS wants global types recorded once, not in every region).
```

```
aws configservice put-configuration-recorder --region eu-west-3 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region eu-west-3 --configuration-recorder-name default
aws configservice put-configuration-recorder --region eu-north-1 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region eu-north-1 --configuration-recorder-name default
aws configservice put-configuration-recorder --region ap-southeast-2 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region ap-southeast-2 --configuration-recorder-name default
aws configservice put-configuration-recorder --region ap-northeast-2 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region ap-northeast-2 --configuration-recorder-name default
aws configservice put-configuration-recorder --region ap-northeast-3 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region ap-northeast-3 --configuration-recorder-name default
```

```
aws configservice put-configuration-recorder --region us-east-1 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region us-east-1 --configuration-recorder-name default
aws configservice put-configuration-recorder --region us-east-2 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region us-east-2 --configuration-recorder-name default
aws configservice put-configuration-recorder --region us-west-2 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region us-west-2 --configuration-recorder-name default
aws configservice put-configuration-recorder --region ca-central-1 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region ca-central-1 --configuration-recorder-name default
aws configservice put-configuration-recorder --region eu-west-2 --configuration-recorder name=default,roleARN=<config-service-linked-role> --recording-group allSupported=true && aws configservice start-configuration-recorder --region eu-west-2 --configuration-recorder-name default
… 5 more lines (full command in the CSV export)
```

AFFECTED RESOURCES

- `config` staging
- `config` prod-eu
- `config` prod-us
- `config` dev-sandbox

#33 Medium EBS encryption by default off in some regions

4 findings · 4 assets

CIS 5.1.1 · AWS FSBP EC2.7

What to do. Enable EBS encryption by default in every region so new volumes and snapshot copies are encrypted without anyone remembering to ask.

EXAMPLE COMMANDS

```
aws ec2 enable-ebs-encryption-by-default --region us-east-2
aws ec2 enable-ebs-encryption-by-default --region ca-central-1
aws ec2 enable-ebs-encryption-by-default --region eu-west-1
aws ec2 enable-ebs-encryption-by-default --region eu-west-3
aws ec2 enable-ebs-encryption-by-default --region eu-central-1
… 4 more lines (full command in the CSV export)
```

```
aws ec2 enable-ebs-encryption-by-default --region us-east-1
aws ec2 enable-ebs-encryption-by-default --region us-west-1
aws ec2 enable-ebs-encryption-by-default --region ca-central-1
aws ec2 enable-ebs-encryption-by-default --region eu-west-3
aws ec2 enable-ebs-encryption-by-default --region eu-central-1
… 3 more lines (full command in the CSV export)
```

```
aws ec2 enable-ebs-encryption-by-default --region us-east-1
aws ec2 enable-ebs-encryption-by-default --region us-east-2
aws ec2 enable-ebs-encryption-by-default --region eu-west-1
aws ec2 enable-ebs-encryption-by-default --region eu-west-2
aws ec2 enable-ebs-encryption-by-default --region eu-central-1
… 6 more lines (full command in the CSV export)
```

AFFECTED RESOURCES

- ebs-default-encryption prod-eu
- ebs-default-encryption prod-us
- ebs-default-encryption staging
- ebs-default-encryption dev-sandbox

#34 Medium IAM Access Analyzer not enabled in every region

4 findings · 4 assets

CIS 1.19

What to do. Create an external-access analyzer in each region (or an organization-wide one) and review its findings.

EXAMPLE COMMANDS

```
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-2
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region ca-central-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region eu-west-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region eu-west-3
… 7 more lines (full command in the CSV export)
```

```
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-2
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-west-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region ca-central-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region eu-west-1
… 7 more lines (full command in the CSV export)
```

```
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-east-2
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region us-west-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region ca-central-1
aws accessanalyzer create-analyzer --analyzer-name external-access --type ACCOUNT --region eu-west-1
… 5 more lines (full command in the CSV export)
```

AFFECTED RESOURCES

- access-analyzer prod-eu
- access-analyzer prod-us
- access-analyzer staging
- access-analyzer dev-sandbox

#35 Medium Account-level S3 Block Public Access not fully enabled

3 findings · 3 assets

CIS 2.1.4 · AWS FSBP S3.1 · PCI DSS 1.3.1

What to do. Enable all four Block Public Access settings at the account level so every current and future bucket is covered.

EXAMPLE COMMANDS

```
aws s3control put-public-access-block --account-id 101295249481 --public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

```
aws s3control put-public-access-block --account-id 101278471862 --public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

```
aws s3control put-public-access-block --account-id 101244916624 --public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
```

AFFECTED RESOURCES

s3-account prod-eu
s3-account dev-sandbox
s3-account prod-us

#36 Medium Password policy does not prevent reuse of the last 24 passwords

3 findings · 3 assets

CIS 1.8 · AWS FSBP IAM.7

What to do. Set password reuse prevention to 24 in the account password policy.

EXAMPLE COMMAND

```
aws iam update-account-password-policy --minimum-password-length 14 --password-reuse-prevention 24
```

AFFECTED RESOURCES

root prod-us
root dev-sandbox
root staging

#37 Low S3 bucket without server access logging

189 findings · 189 assets

AWS FSBP S3.9

What to do. Enable server access logging to a dedicated log bucket, or cover the bucket with CloudTrail S3 data events.

EXAMPLE COMMANDS

```
aws s3api put-bucket-logging --bucket data-gateway-prod-exports-1862-0 --bucket-logging-status '{"LoggingEnabled":{"TargetBucket":"<log-bucket>","TargetPrefix":"data-gateway-prod-exports-1862-0/"}}'
```

```
aws s3api put-bucket-logging --bucket growth-worker-stg-uploads-6624-0 --bucket-logging-status '{"LoggingEnabled":{"TargetBucket":"<log-bucket>","TargetPrefix":"growth-worker-stg-uploads-6624-0/"}}'
```

```
aws s3api put-bucket-logging --bucket mobile-billing-prod-data-9481-1 --bucket-logging-status '{"LoggingEnabled":{"TargetBucket":"<log-bucket>","TargetPrefix":"mobile-billing-prod-data-9481-1/"}}'
```

AFFECTED RESOURCES

data-gateway-prod-exports-1862-0 prod-us
growth-worker-stg-uploads-6624-0 dev-sandbox
mobile-billing-prod-data-9481-1 prod-eu
ml-cache-prod-data-1862-1 prod-us
platform-sync-stg-assets-6624-1 dev-sandbox
core-gateway-dev-uploads-1862-2 prod-us
payments-report-prod-data-9481-3 prod-eu
ml-notify-prod-uploads-1862-3 prod-us
platform-web-prod-uploads-4243-3 staging
ml-web-dev-assets-6624-3 dev-sandbox
payments-sync-prod-exports-9481-4 prod-eu
payments-gateway-stg-logs-1862-4 prod-us
core-notify-prod-exports-6624-4 dev-sandbox
ml-billing-dev-logs-9481-5 prod-eu
growth-ingest-stg-uploads-1862-5 prod-us
data-sync-dev-data-4243-5 staging
payments-gateway-stg-backups-6624-5 dev-sandbox
mobile-billing-dev-logs-9481-6 prod-eu
ops-sync-prod-data-1862-6 prod-us
mobile-notify-dev-backups-4243-6 staging
web-billing-stg-exports-9481-7 prod-eu
payments-sync-stg-exports-1862-7 prod-us
payments-worker-stg-exports-4243-7 staging
platform-sync-stg-logs-4243-8 staging
ops-ingest-dev-backups-6624-8 dev-sandbox
mobile-billing-dev-assets-1862-9 prod-us
platform-cache-stg-uploads-6624-9 dev-sandbox
growth-search-dev-assets-6624-10 dev-sandbox
ops-notify-dev-backups-9481-11 prod-eu
infra-ingest-dev-backups-1862-11 prod-us
infra-sync-stg-data-6624-11 dev-sandbox
data-cache-prod-assets-1862-12 prod-us
infra-auth-prod-logs-4243-12 staging
ml-search-prod-uploads-6624-12 dev-sandbox
ops-search-prod-uploads-9481-13 prod-eu
infra-cache-stg-assets-4243-13 staging
core-search-stg-uploads-9481-14 prod-eu
ops-api-dev-uploads-1862-14 prod-us
mobile-notify-dev-logs-6624-14 dev-sandbox
ml-auth-stg-assets-1862-15 prod-us
mobile-notify-prod-assets-9481-16 prod-eu
mobile-sync-stg-uploads-1862-16 prod-us
platform-web-dev-uploads-4243-16 staging
ml-notify-prod-logs-6624-16 dev-sandbox
ml-api-dev-uploads-1862-17 prod-us
payments-web-prod-data-4243-17 staging
ml-notify-stg-assets-6624-17 dev-sandbox
payments-ingest-prod-data-1862-18 prod-us
web-sync-prod-exports-4243-18 staging
growth-sync-dev-data-4243-19 staging
infra-worker-stg-data-6624-19 dev-sandbox
mobile-sync-prod-assets-9481-20 prod-eu
ops-worker-dev-data-1862-20 prod-us
infra-sync-dev-logs-6624-20 dev-sandbox
platform-gateway-stg-backups-9481-21 prod-eu
payments-gateway-stg-backups-4243-21 staging
ml-notify-stg-uploads-1862-22 prod-us
infra-auth-stg-data-9481-23 prod-eu
platform-gateway-stg-assets-1862-23 prod-us
growth-search-prod-exports-4243-23 staging
and 129 more, listed in the CSV export

#38 Low S3 bucket does not deny plaintext HTTP requests

162 findings · 162 assets

CIS 2.1.1 · AWS FSBP S3.5

What to do. Add a bucket-policy Deny statement for requests where aws:SecureTransport is false.

EXAMPLE COMMANDS

```
Add a Deny statement to the bucket policy: {"Effect":"Deny","Principal":"*","Action":"s3:*","Resource":["arn:aws:s3:::mobile-worker-dev-data-9481-0","arn:aws:s3:::mobile-worker-dev-data-9481-0/*"],"Condition":{"Bool":{"aws:SecureTransport":"false"}}}
```

```
Add a Deny statement to the bucket policy: {"Effect":"Deny","Principal":"*","Action":"s3:*","Resource":["arn:aws:s3:::data-gateway-prod-exports-1862-0","arn:aws:s3:::data-gateway-prod-exports-1862-0/*"],"Condition":{"Bool":{"aws:SecureTransport":"false"}}}
```

```
Add a Deny statement to the bucket policy: {"Effect":"Deny","Principal":"*","Action":"s3:*","Resource":["arn:aws:s3:::platform-api-dev-data-4243-0","arn:aws:s3:::platform-api-dev-data-4243-0/*"],"Condition":{"Bool":{"aws:SecureTransport":"false"}}}
```

AFFECTED RESOURCES

mobile-worker-dev-data-9481-0 prod-eu
data-gateway-prod-exports-1862-0 prod-us
platform-api-dev-data-4243-0 staging
ml-cache-prod-data-1862-1 prod-us
platform-sync-stg-assets-6624-1 dev-sandbox
data-notify-dev-assets-9481-2 prod-eu
core-gateway-dev-uploads-1862-2 prod-us
mobile-auth-stg-backups-4243-2 staging
growth-search-prod-assets-6624-2 dev-sandbox
platform-web-prod-uploads-4243-3 staging
payments-sync-prod-exports-9481-4 prod-eu
core-notify-prod-exports-6624-4 dev-sandbox
mobile-billing-dev-logs-9481-6 prod-eu
ops-sync-prod-data-1862-6 prod-us
payments-sync-prod-exports-6624-6 dev-sandbox
web-billing-stg-exports-9481-7 prod-eu
payments-worker-stg-exports-4243-7 staging
infra-web-stg-data-1862-8 prod-us
ops-ingest-dev-backups-6624-8 dev-sandbox
mobile-billing-dev-assets-1862-9 prod-us
growth-cache-stg-uploads-4243-9 staging
ml-billing-prod-data-1862-10 prod-us
infra-ingest-dev-backups-1862-11 prod-us
ops-billing-prod-logs-4243-11 staging
infra-auth-prod-logs-4243-12 staging
infra-worker-stg-logs-1862-13 prod-us
ops-api-dev-uploads-1862-14 prod-us
mobile-ingest-dev-exports-4243-14 staging
mobile-notify-dev-logs-6624-14 dev-sandbox
ml-notify-stg-uploads-9481-15 prod-eu
ml-auth-stg-assets-1862-15 prod-us
payments-notify-stg-assets-6624-15 dev-sandbox
mobile-notify-prod-assets-9481-16 prod-eu
mobile-sync-stg-uploads-1862-16 prod-us
platform-web-dev-uploads-4243-16 staging
ml-api-dev-uploads-1862-17 prod-us
payments-ingest-prod-data-1862-18 prod-us
ml-notify-stg-exports-9481-19 prod-eu
mobile-report-stg-data-1862-19 prod-us
growth-sync-dev-data-4243-19 staging
mobile-sync-prod-assets-9481-20 prod-eu
ops-worker-dev-data-1862-20 prod-us
core-api-dev-assets-6624-21 dev-sandbox
ml-notify-stg-uploads-1862-22 prod-us
infra-auth-stg-data-9481-23 prod-eu
core-web-dev-uploads-6624-23 dev-sandbox
web-sync-dev-data-9481-25 prod-eu
infra-auth-prod-data-1862-25 prod-us
core-ingest-prod-assets-4243-25 staging
web-billing-dev-exports-6624-25 dev-sandbox
growth-notify-dev-assets-6624-26 dev-sandbox
infra-search-dev-exports-9481-27 prod-eu
data-sync-prod-uploads-6624-27 dev-sandbox
ml-web-stg-exports-1862-28 prod-us
core-cache-stg-data-9481-29 prod-eu
growth-report-prod-data-1862-29 prod-us
infra-web-stg-logs-1862-30 prod-us
infra-gateway-dev-data-6624-30 dev-sandbox
payments-api-prod-backups-9481-31 prod-eu
growth-cache-prod-exports-6624-31 dev-sandbox
and 102 more, listed in the CSV export

#39 Low Versioned S3 bucket without MFA Delete

121 findings · 121 assets

CIS 2.1.2

What to do. Enable MFA Delete on the bucket versioning configuration (root user with an MFA device).

EXAMPLE COMMANDS

```
Only the root user can enable it, with a hardware/virtual MFA code: aws s3api put-bucket-versioning --bucket data-gateway-prod-exports-1862-0 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "<serial> <code>"
```

```
Only the root user can enable it, with a hardware/virtual MFA code: aws s3api put-bucket-versioning --bucket mobile-billing-prod-data-9481-1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "<serial> <code>"
```

```
Only the root user can enable it, with a hardware/virtual MFA code: aws s3api put-bucket-versioning --bucket ml-cache-prod-data-1862-1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "<serial> <code>"
```

AFFECTED RESOURCES

data-gateway-prod-exports-1862-0 prod-us
mobile-billing-prod-data-9481-1 prod-eu
ml-cache-prod-data-1862-1 prod-us
platform-sync-stg-assets-6624-1 dev-sandbox
data-notify-dev-assets-9481-2 prod-eu
growth-search-prod-assets-6624-2 dev-sandbox
platform-web-prod-uploads-4243-3 staging
growth-ingest-stg-uploads-1862-5 prod-us
data-sync-dev-data-4243-5 staging
payments-gateway-stg-backups-6624-5 dev-sandbox
ops-sync-prod-data-1862-6 prod-us
payments-sync-prod-exports-6624-6 dev-sandbox
payments-sync-stg-exports-1862-7 prod-us
payments-worker-stg-exports-4243-7 staging
infra-web-stg-data-1862-8 prod-us
ops-ingest-dev-backups-6624-8 dev-sandbox
ml-worker-dev-logs-4243-10 staging
infra-sync-stg-data-6624-11 dev-sandbox
data-cache-prod-assets-1862-12 prod-us
infra-cache-stg-assets-4243-13 staging
core-search-stg-uploads-9481-14 prod-eu
ops-api-dev-uploads-1862-14 prod-us
ml-auth-stg-assets-1862-15 prod-us
payments-worker-prod-data-4243-15 staging
payments-notify-stg-assets-6624-15 dev-sandbox
mobile-notify-prod-assets-9481-16 prod-eu
mobile-sync-stg-uploads-1862-16 prod-us
platform-web-dev-uploads-4243-16 staging
growth-auth-stg-assets-9481-17 prod-eu
payments-ingest-prod-data-1862-18 prod-us
core-api-prod-data-6624-18 dev-sandbox
infra-worker-stg-data-6624-19 dev-sandbox
ops-worker-dev-data-1862-20 prod-us
growth-report-prod-uploads-4243-20 staging
core-notify-dev-uploads-1862-21 prod-us
growth-gateway-prod-assets-9481-22 prod-eu
infra-auth-stg-data-9481-23 prod-eu
growth-search-prod-exports-4243-23 staging
core-search-dev-logs-6624-24 dev-sandbox
infra-auth-prod-data-1862-25 prod-us
platform-billing-prod-uploads-9481-26 prod-eu
growth-cache-prod-exports-1862-27 prod-us
data-sync-prod-uploads-6624-27 dev-sandbox
ml-web-stg-exports-1862-28 prod-us
platform-sync-prod-logs-6624-28 dev-sandbox
payments-auth-stg-logs-4243-29 staging
ml-notify-stg-logs-6624-29 dev-sandbox
infra-gateway-stg-assets-1862-31 prod-us
growth-cache-prod-exports-6624-31 dev-sandbox
core-auth-dev-data-4243-32 staging
mobile-auth-dev-exports-9481-33 prod-eu
ml-gateway-dev-data-6624-33 dev-sandbox
ops-web-dev-data-1862-34 prod-us
platform-ingest-prod-backups-9481-35 prod-eu
mobile-auth-dev-assets-1862-35 prod-us
data-gateway-stg-assets-4243-35 staging
web-gateway-dev-exports-6624-36 dev-sandbox
ops-gateway-dev-uploads-4243-37 staging
ops-api-dev-exports-1862-38 prod-us
infra-report-prod-assets-4243-38 staging
and 61 more, listed in the CSV export

#40 Low EC2 instance without an IAM instance profile

111 findings · 111 assets

CIS 1.17

What to do. Attach an instance profile with the role the software needs and remove any static access keys from the instance.

EXAMPLE COMMANDS

```
aws ec2 associate-iam-instance-profile --instance-id i-37aa98ee95e47586c --iam-instance-profile Name=<profile> --region us-east-2, then remove any static keys from the instance.
```

```
aws ec2 associate-iam-instance-profile --instance-id i-75734ace7dc6cbeb8 --iam-instance-profile Name=<profile> --region us-west-2, then remove any static keys from the instance.
```

```
aws ec2 associate-iam-instance-profile --instance-id i-40bb1fa200154b843 --iam-instance-profile Name=<profile> --region us-west-1, then remove any static keys from the instance.
```

AFFECTED RESOURCES

i-37aa98ee95e47586c prod-eu
i-75734ace7dc6cbeb8 dev-sandbox
i-40bb1fa200154b843 prod-eu
i-00992174821304739 prod-us
i-543c11d70dab9ea1d prod-us
i-35aa95c8f7fb54610 prod-eu
i-3fbb1e0f023d78584 prod-eu
i-126ead620a15b5a1f staging
i-9d022af2f8754c85d staging
i-4f3c09f8a79aa758c prod-us
i-3cbb1956b9313af2f prod-eu
i-e09126a5a001e8258 prod-us
i-970221807d0ce0fab staging
i-8757b9b661c918afb dev-sandbox
i-1c9257b09fc85a962 dev-sandbox
i-dd9121ecc4342b63c prod-us
i-fa35f5cabf40241b0 dev-sandbox
i-3aaa9da7c64000bd6 prod-eu
i-3abb1630652c087f5 prod-eu
i-5ee49817efe892f79 staging
i-0f6ea8a94e0e1b38c staging
i-e3912b5ef1a23d171 prod-us
i-4b3c03ac8a8c7922c prod-us
i-a40235f7cb870e348 staging
i-186eb6d40e7bdeec2 staging
i-ec35dfc0eb2b40826 dev-sandbox
i-229a0a733a23913ce prod-eu
i-196eb8672ccc6e1bf staging
i-0064f1b4f12c696ef staging
i-c8812383aa2764448 dev-sandbox
i-4b03f457dd11f988a prod-eu
i-6f38c0daba5b29733 staging
i-97890c95754526c4a staging
i-6e38bf47c35ef4442 staging
i-dce56c9baf6c52bb1 dev-sandbox
i-ca8126a9742ad1d38 dev-sandbox
i-8c238d233cac997c1 dev-sandbox
i-c981251673f20bd5c dev-sandbox
i-4603ec7884e41a735 prod-eu
i-7d9028595cf4b9188 prod-us
i-00d6321fbd9e1cb3f staging
i-4703ee0ba8f1e20ca prod-eu
i-6a38b8fb3a0a2ba2c staging
i-8f2391dcac7a3529e dev-sandbox
i-e0e572e708ef875b6 dev-sandbox
i-7b92b78f837306cd4 prod-eu
i-cd812b6240a68911a dev-sandbox
i-9e89179afc1cd454d staging
i-ec918fa83ab421347 prod-eu
i-8192c1013c12d03f1 prod-eu
i-5194d9ea8af0c1b50 prod-eu
i-5779b5db9bd0c4416 dev-sandbox
i-116e66d623a1818c6 prod-us
i-5879b76e163457a74 dev-sandbox
i-bd0b63921b8e1b9bd prod-eu
i-768a1a21ece930dc6 prod-eu
i-c316f95b20b09f513 prod-us
i-6e6c5aa367a87feb3 staging
i-5a3ade62462a24c82 staging
i-5a79ba941b2955972 dev-sandbox
and 51 more, listed in the CSV export

#41 Low Secret without automatic rotation

104 findings · 104 assets

AWS FSBP SecretsManager.1

What to do. Attach a rotation function and schedule, or document and perform manual rotation on a schedule.

EXAMPLE COMMANDS

```
Attach a rotation function and schedule: aws secretsmanager rotate-secret --secret-id arn:aws:secretsmanager:us-east-1:101295249481:secret:prod/notify/db-password-0-1b6ef5 --rotation-lambda-arn <function-arn> --rotation-rules AutomaticallyAfterDays=90 --region us-east-1. Secrets that cannot be rotated automatically should be rotated by hand on a schedule and tagged accordingly.
```

```
Attach a rotation function and schedule: aws secretsmanager rotate-secret --secret-id arn:aws:secretsmanager:us-west-1:101295249481:secret:prod/search/api-key-0-050b76 --rotation-lambda-arn <function-arn> --rotation-rules AutomaticallyAfterDays=90 --region us-west-1. Secrets that cannot be rotated automatically should be rotated by hand on a schedule and tagged accordingly.
```

```
Attach a rotation function and schedule: aws secretsmanager rotate-secret --secret-id arn:aws:secretsmanager:us-west-1:101278471862:secret:prod/web/db-password-0-0924f2 --rotation-lambda-arn <function-arn> --rotation-rules AutomaticallyAfterDays=90 --region us-west-1. Secrets that cannot be rotated automatically should be rotated by hand on a schedule and tagged accordingly.
```

AFFECTED RESOURCES

arn:aws:secretsmanager:us-east-1:101295249481:secret:prod/notify/db-password-0-1b6ef5 prod-eu
arn:aws:secretsmanager:us-west-1:101295249481:secret:prod/search/api-key-0-050b76 prod-eu
arn:aws:secretsmanager:us-west-1:101278471862:secret:prod/web/db-password-0-0924f2 prod-us
arn:aws:secretsmanager:us-east-2:101261694243:secret:prod/cache/api-key-0-70ca49 staging
arn:aws:secretsmanager:us-west-2:101261694243:secret:dev/api/oauth-client-0-7d76ca staging
arn:aws:secretsmanager:us-east-1:101295249481:secret:prod/api/api-key-1-3de6de prod-eu
arn:aws:secretsmanager:us-east-2:101295249481:secret:staging/cache/db-password-1-8ca0b2 prod-eu
arn:aws:secretsmanager:us-west-2:101295249481:secret:dev/ingest/api-key-0-4e60de prod-eu
arn:aws:secretsmanager:us-west-1:101278471862:secret:staging/report/oauth-client-1-f1b78a prod-us
arn:aws:secretsmanager:us-east-2:101244916624:secret:prod/gateway/db-password-0-c1a750 dev-sandbox
arn:aws:secretsmanager:us-west-2:101244916624:secret:dev/report/smtp-1-3bf8c5 dev-sandbox
arn:aws:secretsmanager:us-east-1:101278471862:secret:prod/ingest/smtp-1-ce02ca prod-us
arn:aws:secretsmanager:us-east-2:101278471862:secret:staging/billing/smtp-2-16cee7 prod-us
arn:aws:secretsmanager:us-west-1:101278471862:secret:dev/report/smtp-2-27ba3b prod-us
arn:aws:secretsmanager:us-east-1:101261694243:secret:prod/notify/oauth-client-2-58d992 staging
arn:aws:secretsmanager:us-east-2:101261694243:secret:prod/search/api-key-2-3eadd2 staging
arn:aws:secretsmanager:us-east-1:101244916624:secret:staging/api/smtp-2-d04b19 dev-sandbox
arn:aws:secretsmanager:us-east-2:101244916624:secret:staging/search/oauth-client-1-844a4f dev-sandbox
arn:aws:secretsmanager:us-west-2:101244916624:secret:prod/report/oauth-client-2-3fc769 dev-sandbox
arn:aws:secretsmanager:us-east-1:101295249481:secret:prod/notify/smtp-3-bd672d prod-eu
arn:aws:secretsmanager:us-east-2:101295249481:secret:staging/search/api-key-3-fd6732 prod-eu
arn:aws:secretsmanager:us-west-1:101295249481:secret:staging/worker/oauth-client-3-107fb0 prod-eu
arn:aws:secretsmanager:us-west-2:101295249481:secret:prod/web/api-key-2-38c2cf prod-eu
arn:aws:secretsmanager:us-east-1:101278471862:secret:prod/worker/db-password-2-487e61 prod-us
arn:aws:secretsmanager:us-east-2:101278471862:secret:dev/sync/api-key-3-7a6daa prod-us
arn:aws:secretsmanager:us-east-2:101261694243:secret:prod/billing/smtp-3-e6d8e7 staging
arn:aws:secretsmanager:us-west-2:101261694243:secret:dev/billing/oauth-client-3-10369e staging
arn:aws:secretsmanager:us-east-1:101244916624:secret:staging/auth/api-key-3-5c1607 dev-sandbox
arn:aws:secretsmanager:us-west-1:101244916624:secret:dev/ingest/smtp-2-90c87b dev-sandbox
arn:aws:secretsmanager:us-west-2:101244916624:secret:dev/worker/smtp-3-a35a54 dev-sandbox
arn:aws:secretsmanager:us-east-1:101295249481:secret:dev/worker/oauth-client-4-434554 prod-eu
arn:aws:secretsmanager:us-east-1:101278471862:secret:dev/cache/oauth-client-3-a8ebbb prod-us
arn:aws:secretsmanager:us-east-2:101278471862:secret:dev/ingest/db-password-4-64061b prod-us
arn:aws:secretsmanager:us-east-1:101261694243:secret:prod/auth/oauth-client-4-7691ee staging
arn:aws:secretsmanager:us-east-2:101261694243:secret:staging/cache/db-password-4-a13bd8 staging
arn:aws:secretsmanager:us-west-1:101261694243:secret:dev/cache/smtp-3-34399e staging
arn:aws:secretsmanager:us-west-2:101261694243:secret:dev/notify/oauth-client-4-275063 staging
arn:aws:secretsmanager:us-east-1:101244916624:secret:prod/billing/oauth-client-4-85e935 dev-sandbox
arn:aws:secretsmanager:us-west-1:101244916624:secret:dev/sync/api-key-3-f18d7f dev-sandbox
arn:aws:secretsmanager:us-west-2:101244916624:secret:staging/ingest/api-key-4-1264e0 dev-sandbox
arn:aws:secretsmanager:us-east-1:101295249481:secret:prod/billing/api-key-5-ea2f0e prod-eu
arn:aws:secretsmanager:us-west-1:101295249481:secret:staging/sync/oauth-client-5-f35c6b prod-eu
arn:aws:secretsmanager:us-west-2:101295249481:secret:dev/web/api-key-4-d4f087 prod-eu
arn:aws:secretsmanager:us-east-2:101278471862:secret:prod/search/oauth-client-5-02ab36 prod-us
arn:aws:secretsmanager:us-west-1:101278471862:secret:prod/cache/api-key-5-32bcb7 prod-us
arn:aws:secretsmanager:us-east-2:101261694243:secret:staging/sync/smtp-5-7eebce staging

arn:aws:secretsmanager:us-west-1:101261694243:secret:staging/cache/smtp-4-6f1b38 staging
arn:aws:secretsmanager:us-west-2:101261694243:secret:staging/ingest/db-password-5-e4d647 staging
arn:aws:secretsmanager:us-east-2:101295249481:secret:prod/gateway/db-password-6-de5de1 prod-eu
arn:aws:secretsmanager:us-east-1:101278471862:secret:prod/report/db-password-5-260664 prod-us
arn:aws:secretsmanager:us-east-2:101261694243:secret:staging/gateway/oauth-client-6-521bf5 staging
arn:aws:secretsmanager:us-west-1:101261694243:secret:dev/worker/db-password-5-ea5c2f staging
arn:aws:secretsmanager:us-east-1:101244916624:secret:dev/api/db-password-6-d1b8b8 dev-sandbox
arn:aws:secretsmanager:us-west-2:101244916624:secret:prod/report/smtp-6-b189b2 dev-sandbox
arn:aws:secretsmanager:us-east-1:101295249481:secret:staging/cache/smtp-7-8a5f1f prod-eu
arn:aws:secretsmanager:us-east-1:101278471862:secret:prod/auth/db-password-6-c9bc08 prod-us
arn:aws:secretsmanager:us-east-2:101278471862:secret:staging/notify/oauth-client-7-f44156 prod-us
arn:aws:secretsmanager:us-east-1:101261694243:secret:dev/api/api-key-7-a5ab2a staging
arn:aws:secretsmanager:us-east-2:101261694243:secret:dev/ingest/smtp-7-e5015e staging
arn:aws:secretsmanager:us-west-1:101261694243:secret:dev/billing/smtp-6-1092b2 staging
and 44 more, listed in the CSV export

#42 Low DynamoDB table without point-in-time recovery

87 findings · 87 assets

AWS FSBP DynamoDB.2

What to do. Enable point-in-time recovery on the table.

EXAMPLE COMMANDS

```
aws dynamodb update-continuous-backups --table-name growth-billing-prod-users-0 --point-in-time-recovery-specification PointInTimeRecoveryEnabled=true --region us-east-2
```

```
aws dynamodb update-continuous-backups --table-name data-auth-stg-orders-0 --point-in-time-recovery-specification PointInTimeRecoveryEnabled=true --region us-west-1
```

```
aws dynamodb update-continuous-backups --table-name mobile-sync-dev-events-0 --point-in-time-recovery-specification PointInTimeRecoveryEnabled=true --region us-east-2
```

AFFECTED RESOURCES

arn:aws:dynamodb:us-east-2:101295249481:table/growth-billing-prod-users-0 prod-eu
arn:aws:dynamodb:us-west-1:101295249481:table/data-auth-stg-orders-0 prod-eu
arn:aws:dynamodb:us-east-2:101278471862:table/mobile-sync-dev-events-0 prod-us
arn:aws:dynamodb:us-west-1:101278471862:table/infra-gateway-stg-events-0 prod-us
arn:aws:dynamodb:us-east-1:101261694243:table/ops-ingest-prod-sessions-0 staging
arn:aws:dynamodb:us-west-2:101261694243:table/infra-sync-dev-cache-0 staging
arn:aws:dynamodb:us-east-1:101244916624:table/ml-auth-stg-events-0 dev-sandbox
arn:aws:dynamodb:us-east-1:101295249481:table/data-sync-dev-users-1 prod-eu
arn:aws:dynamodb:us-east-2:101295249481:table/payments-auth-dev-sessions-1 prod-eu
arn:aws:dynamodb:us-west-1:101295249481:table/data-worker-prod-orders-1 prod-eu
arn:aws:dynamodb:us-west-2:101295249481:table/mobile-web-stg-cache-0 prod-eu
arn:aws:dynamodb:us-east-2:101278471862:table/ml-cache-stg-cache-1 prod-us
arn:aws:dynamodb:us-west-2:101261694243:table/ops-notify-dev-events-1 staging
arn:aws:dynamodb:us-east-2:101244916624:table/core-ingest-dev-orders-0 dev-sandbox
arn:aws:dynamodb:us-west-1:101244916624:table/core-web-prod-users-0 dev-sandbox
arn:aws:dynamodb:us-west-2:101244916624:table/data-notify-prod-orders-1 dev-sandbox
arn:aws:dynamodb:us-west-2:101295249481:table/ops-api-stg-sessions-1 prod-eu
arn:aws:dynamodb:us-east-2:101278471862:table/payments-cache-stg-orders-2 prod-us
arn:aws:dynamodb:us-east-1:101261694243:table/platform-search-dev-orders-2 staging
arn:aws:dynamodb:us-east-2:101261694243:table/ml-notify-prod-users-2 staging
arn:aws:dynamodb:us-west-1:101261694243:table/ops-notify-dev-orders-1 staging
arn:aws:dynamodb:us-east-1:101244916624:table/ops-ingest-prod-sessions-2 dev-sandbox
arn:aws:dynamodb:us-east-2:101244916624:table/ml-worker-prod-orders-1 dev-sandbox
arn:aws:dynamodb:us-west-2:101244916624:table/ops-worker-dev-users-2 dev-sandbox
arn:aws:dynamodb:us-east-1:101295249481:table/mobile-search-stg-events-3 prod-eu
arn:aws:dynamodb:us-west-2:101295249481:table/core-ingest-prod-events-2 prod-eu
arn:aws:dynamodb:us-east-2:101278471862:table/growth-notify-dev-events-3 prod-us
arn:aws:dynamodb:us-west-1:101278471862:table/mobile-api-dev-orders-3 prod-us
arn:aws:dynamodb:us-east-1:101261694243:table/data-worker-dev-events-3 staging
arn:aws:dynamodb:us-east-2:101261694243:table/data-gateway-dev-events-3 staging
arn:aws:dynamodb:us-west-1:101261694243:table/infra-web-prod-orders-2 staging
arn:aws:dynamodb:us-west-2:101261694243:table/core-ingest-prod-events-3 staging
arn:aws:dynamodb:us-east-2:101244916624:table/infra-web-stg-cache-2 dev-sandbox
arn:aws:dynamodb:us-west-2:101244916624:table/web-worker-prod-cache-3 dev-sandbox
arn:aws:dynamodb:us-east-1:101295249481:table/web-cache-prod-events-4 prod-eu
arn:aws:dynamodb:us-west-1:101295249481:table/ml-ingest-stg-sessions-4 prod-eu
arn:aws:dynamodb:us-west-2:101295249481:table/data-search-stg-cache-3 prod-eu
arn:aws:dynamodb:us-east-1:101278471862:table/infra-gateway-dev-users-3 prod-us
arn:aws:dynamodb:us-east-1:101261694243:table/infra-search-prod-events-4 staging
arn:aws:dynamodb:us-east-2:101261694243:table/growth-notify-stg-cache-4 staging
arn:aws:dynamodb:us-west-1:101261694243:table/core-notify-dev-events-3 staging
arn:aws:dynamodb:us-west-2:101261694243:table/infra-auth-prod-cache-4 staging
arn:aws:dynamodb:us-east-2:101244916624:table/ml-notify-prod-events-3 dev-sandbox
arn:aws:dynamodb:us-east-1:101295249481:table/growth-ingest-prod-events-5 prod-eu
arn:aws:dynamodb:us-west-1:101295249481:table/platform-worker-prod-cache-5 prod-eu
arn:aws:dynamodb:us-west-2:101295249481:table/core-cache-dev-events-4 prod-eu
arn:aws:dynamodb:us-east-1:101278471862:table/growth-web-stg-cache-4 prod-us
arn:aws:dynamodb:us-east-2:101278471862:table/ml-web-stg-orders-5 prod-us
arn:aws:dynamodb:us-east-2:101261694243:table/infra-report-stg-orders-5 staging
arn:aws:dynamodb:us-east-2:101244916624:table/payments-gateway-stg-events-4 dev-sandbox
arn:aws:dynamodb:us-west-1:101244916624:table/data-billing-stg-orders-4 dev-sandbox
arn:aws:dynamodb:us-west-2:101244916624:table/payments-report-dev-sessions-5 dev-sandbox

arn:aws:dynamodb:us-east-1:101295249481:table/core-report-prod-sessions-6 prod-eu
arn:aws:dynamodb:us-west-1:101295249481:table/ops-search-stg-sessions-6 prod-eu
arn:aws:dynamodb:us-west-2:101295249481:table/core-api-prod-users-5 prod-eu
arn:aws:dynamodb:us-east-1:101278471862:table/data-web-stg-users-5 prod-us
arn:aws:dynamodb:us-west-1:101278471862:table/payments-ingest-stg-events-6 prod-us
arn:aws:dynamodb:us-west-1:101261694243:table/growth-billing-prod-users-5 staging
arn:aws:dynamodb:us-east-1:101244916624:table/payments-auth-stg-orders-6 dev-sandbox
arn:aws:dynamodb:us-west-2:101244916624:table/ml-worker-dev-users-6 dev-sandbox
and 27 more, listed in the CSV export

#43 Low IAM user with policies attached directly

71 findings · 71 assets

CIS 1.14 · AWS FSBP IAM.2

What to do. Attach permissions to groups and put users in groups; remove policies attached directly to users.

EXAMPLE COMMAND

```
Move the permissions to a group (aws iam create-group / attach-group-policy / add-user-to-group) and detach them from the user (aws iam detach-user-policy, aws iam delete-user-policy).
```

AFFECTED RESOURCES

arn:aws:iam::101295249481:user/jonas.qa-0 prod-eu
arn:aws:iam::101244916624:user/alice.svc-0 dev-sandbox
arn:aws:iam::101261694243:user/alice.svc-3 staging
arn:aws:iam::101278471862:user/alice.svc-6 prod-us
arn:aws:iam::101244916624:user/eva.svc-6 dev-sandbox
arn:aws:iam::101295249481:user/finn.dev-7 prod-eu
arn:aws:iam::101278471862:user/eva.dev-7 prod-us
arn:aws:iam::101244916624:user/hakon.dev-8 dev-sandbox
arn:aws:iam::101278471862:user/carla.svc-10 prod-us
arn:aws:iam::101244916624:user/alice.dev-11 dev-sandbox
arn:aws:iam::101278471862:user/hakon.dev-12 prod-us
arn:aws:iam::101295249481:user/finn.dev-13 prod-eu
arn:aws:iam::101278471862:user/bjorn.ops-13 prod-us
arn:aws:iam::101295249481:user/carla.dev-15 prod-eu
arn:aws:iam::101278471862:user/carla.dev-15 prod-us
arn:aws:iam::101244916624:user/finn.qa-16 dev-sandbox
arn:aws:iam::101295249481:user/eva.ops-17 prod-eu
arn:aws:iam::101278471862:user/carla.ops-17 prod-us
arn:aws:iam::101244916624:user/hakon.ops-17 dev-sandbox
arn:aws:iam::101278471862:user/alice.svc-18 prod-us
arn:aws:iam::101261694243:user/carla.ops-18 staging
arn:aws:iam::101244916624:user/bjorn.dev-18 dev-sandbox
arn:aws:iam::101278471862:user/bjorn.ops-19 prod-us
arn:aws:iam::101261694243:user/bjorn.dev-19 staging
arn:aws:iam::101295249481:user/alice.dev-20 prod-eu
arn:aws:iam::101261694243:user/alice.ops-20 staging
arn:aws:iam::101244916624:user/ines.data-21 dev-sandbox
arn:aws:iam::101278471862:user/bjorn.ops-24 prod-us
arn:aws:iam::101295249481:user/hakon.ops-26 prod-eu
arn:aws:iam::101278471862:user/carla.qa-26 prod-us
arn:aws:iam::101244916624:user/gudrun.ops-26 dev-sandbox
arn:aws:iam::101295249481:user/hakon.dev-27 prod-eu
arn:aws:iam::101261694243:user/eva.svc-27 staging
arn:aws:iam::101261694243:user/eva.dev-29 staging
arn:aws:iam::101295249481:user/hakon.qa-30 prod-eu
arn:aws:iam::101244916624:user/finn.dev-31 dev-sandbox
arn:aws:iam::101295249481:user/eva.dev-32 prod-eu
arn:aws:iam::101261694243:user/hakon.ops-32 staging
arn:aws:iam::101244916624:user/hakon.ops-34 dev-sandbox
arn:aws:iam::101295249481:user/bjorn.data-35 prod-eu
arn:aws:iam::101261694243:user/ines.svc-35 staging
arn:aws:iam::101295249481:user/bjorn.qa-38 prod-eu
arn:aws:iam::101244916624:user/hakon.dev-38 dev-sandbox
arn:aws:iam::101261694243:user/bjorn.qa-39 staging
arn:aws:iam::101244916624:user/jonas.qa-39 dev-sandbox
arn:aws:iam::101278471862:user/carla.qa-40 prod-us
arn:aws:iam::101261694243:user/dev.svc-40 staging
arn:aws:iam::101295249481:user/dev.svc-41 prod-eu
arn:aws:iam::101244916624:user/hakon.qa-43 dev-sandbox
arn:aws:iam::101295249481:user/hakon.svc-44 prod-eu
arn:aws:iam::101261694243:user/hakon.dev-45 staging
arn:aws:iam::101244916624:user/finn.svc-45 dev-sandbox
arn:aws:iam::101244916624:user/carla.ops-47 dev-sandbox
arn:aws:iam::101261694243:user/eva.svc-48 staging
arn:aws:iam::101295249481:user/eva.ops-49 prod-eu
arn:aws:iam::101261694243:user/eva.data-49 staging
arn:aws:iam::101244916624:user/finn.qa-49 dev-sandbox
arn:aws:iam::101295249481:user/ines.qa-50 prod-eu
arn:aws:iam::101278471862:user/alice.svc-52 prod-us
arn:aws:iam::101278471862:user/carla.ops-54 prod-us
and 11 more, listed in the CSV export

#44 Low EBS volume not attached to any instance

70 findings · 70 assets

What to do. Snapshot if the data matters, then delete the volume to stop paying for and exposing it.

EXAMPLE COMMANDS

```
Confirm it's no longer needed, then snapshot for safety and delete: aws ec2 delete-volume --volume-id vol-ee9a1185ad19a015c
```

```
Confirm it's no longer needed, then snapshot for safety and delete: aws ec2 delete-volume --volume-id vol-2c1b90db4b6bd2788
```

```
Confirm it's no longer needed, then snapshot for safety and delete: aws ec2 delete-volume --volume-id vol-e8995de33e516b61a
```

AFFECTED RESOURCES

vol-ee9a1185ad19a015c dev-sandbox
vol-2c1b90db4b6bd2788 prod-us
vol-e8995de33e516b61a prod-us
vol-edd1471874bf92797 dev-sandbox
vol-e48502d03fd5a73ef staging
vol-534722e57bb3e47a0 prod-us
vol-f80d2e2e7ea271527 prod-us
vol-077961848e13b8bf9 staging
vol-92845cd7179be78e7 dev-sandbox
vol-b7bad756ab984dfce prod-eu
vol-8a740fe1edfc604c9 prod-us
vol-1540dd2366edbefac dev-sandbox
vol-bcbadf357e541d9de prod-eu
vol-8d8454f8fa95f4256 dev-sandbox
vol-5c6525179d243a29b prod-us
vol-fa0d3154d674dbed0 prod-us
vol-66e2a0bfac48a86d4 staging
vol-ecb731aa787a9f59e dev-sandbox
vol-cd86d18cbe1c5e1e8 dev-sandbox
vol-c444035dbb9ec2988 prod-eu
vol-b543ebc0f645f42fa prod-eu
vol-f00d219678f942863 prod-us
vol-deb71ba02acf13e29 dev-sandbox
vol-bebd20f27c31ff5f9 prod-eu
vol-2e4b6600ca13993cb prod-eu
vol-7880cf2c672c7e121 staging
vol-f00ae2fff2a5d6c92 prod-us
vol-bdbd1f5f8f9abc63c prod-eu
vol-037cbff51209fbc90 dev-sandbox
vol-e284b40436a0a16f7 dev-sandbox
vol-1c4326bfc5a509390 dev-sandbox
vol-5c6763aef070d7e7b prod-us
vol-6963ed948b454f68c staging
vol-194322065cd6220c5 dev-sandbox
vol-5ebea0e5ae29fe041 dev-sandbox
vol-eb0adb20e42632bc3 prod-us
vol-5dbe9f520959c14c2 dev-sandbox
vol-ed089faf40cca8b5d prod-us
vol-366d71d7c26a04c89 staging
vol-22456ec84bfe6a79f dev-sandbox
vol-346d6eb1500778b5d staging
vol-78fc5cbc95532c83b prod-eu
vol-046ebfc1337406e3b prod-us
vol-d782641c281f54a27 dev-sandbox
vol-67e71f8099e62de60 staging
vol-0d7f0e4ae54becba4 dev-sandbox
vol-bb50c125c657afae1 prod-eu
vol-6772f4f8fd51beb36 staging
vol-7efa2797afe363dee prod-eu
vol-46c27438ec822e843 prod-eu
vol-ceb873f1c674e5d65 prod-eu
vol-b450b620fdc8acb9b prod-eu
vol-6b0594720a33c9bc2 prod-us
vol-71fa1320801857ae5 prod-eu
vol-6d05979860aeb3ef2 prod-us
vol-6bc3328a86636c46e dev-sandbox
vol-800376ea87f8b4faa prod-us
vol-fa7a733350168e83b dev-sandbox
vol-b74e7c4275d2b4231 prod-eu
vol-b9ba91797fe033118 prod-eu
and 10 more, listed in the CSV export

#45 Low Application load balancer forwards invalid HTTP headers

43 findings · 43 assets

AWS FSBP ELB.4

What to do. Enable routing.http.drop_invalid_header_fields.enabled on the load balancer.

EXAMPLE COMMANDS

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/core-ingest-stg-alb-0/708d236c689e73c3 --attributes Key=routing.http.drop_invalid_header_fields.enabled,Value=true --region us-east-1
```

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/web-search-dev-alb-0/411d170f38cb82b3 --attributes Key=routing.http.drop_invalid_header_fields.enabled,Value=true --region us-east-2
```

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:101261694243:loadbalancer/app/infra-notify-dev-alb-0/fed9c543dbf2d535 --attributes Key=routing.http.drop_invalid_header_fields.enabled,Value=true --region us-east-1
```

AFFECTED RESOURCES

arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/core-ingest-stg-alb-0/708d236c689e73c3 prod-eu
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/web-search-dev-alb-0/411d170f38cb82b3 prod-us
arn:aws:elasticloadbalancing:us-east-1:101261694243:loadbalancer/app/infra-notify-dev-alb-0/fed9c543dbf2d535 staging
arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/payments-notify-stg-alb-0/a3662f63ae5ee252 staging
arn:aws:elasticloadbalancing:us-east-1:101244916624:loadbalancer/app/data-auth-stg-alb-0/b8cce11b3272b3ec dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/data-search-dev-alb-0/fdb6cb74740d8038 prod-eu
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/core-web-stg-alb-0/8643827ed7d324cb staging
arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/core-gateway-stg-alb-1/f011bc42805daa9e staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-web-dev-alb-0/692e38ebf4165952 dev-sandbox
arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/infra-api-prod-alb-0/4be987aa1b11c2cd dev-sandbox
arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/growth-report-stg-alb-2/09eb184ff99679a7 prod-eu
arn:aws:elasticloadbalancing:us-east-2:101295249481:loadbalancer/app/mobile-billing-prod-alb-2/9c82caab0e03dd46 prod-eu
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/payments-cache-stg-alb-2/486e68d1db1bd8c7 prod-us
arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/growth-search-stg-alb-2/2d2d77991475915e prod-us
arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/web-ingest-prod-alb-2/e51804186ec752a5 staging
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/core-search-stg-alb-2/3d8009dff5992ea5 dev-sandbox
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/platform-search-stg-alb-3/17527b7e045b9a1b prod-us
arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/infra-gateway-stg-alb-3/017583e6fa0cf4a4 prod-us
arn:aws:elasticloadbalancing:us-east-1:101261694243:loadbalancer/app/ops-web-stg-alb-3/386955e9d30a04f6 staging
arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/web-search-stg-alb-3/a35dc0c78ad5943a staging
arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/payments-ingest-prod-alb-3/e2125fb105eaeb78 staging
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/growth-billing-stg-alb-3/7e8e9456dbc3af19 dev-sandbox
arn:aws:elasticloadbalancing:us-west-1:101295249481:loadbalancer/app/web-cache-dev-alb-4/9e1dc5b1c725cca4 prod-eu
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/platform-cache-dev-alb-4/cb57d81fa8047666 prod-us
arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/data-gateway-dev-alb-4/a71597ed3b6c3891 prod-us
arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/core-gateway-dev-alb-4/8145d8afe65f3987 staging
arn:aws:elasticloadbalancing:us-east-1:101244916624:loadbalancer/app/web-billing-stg-alb-4/3efd153ca54db031 dev-sandbox
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/ml-web-stg-alb-3/22ee1944be95e581 dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/payments-search-dev-alb-4/e7d6826536ded246 dev-sandbox
arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/web-gateway-prod-alb-5/262cce8ea0deda6a prod-eu
arn:aws:elasticloadbalancing:us-west-1:101295249481:loadbalancer/app/core-auth-prod-alb-5/729eea15e3b970cb prod-eu
arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/mobile-report-prod-alb-4/c424c9e6926d4f3a prod-eu
arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/platform-report-dev-alb-5/d92bf25cccf117e8 prod-us
arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/ops-cache-prod-alb-5/536972fcab5ed534 prod-us
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/infra-gateway-prod-alb-4/08374e796d856274 staging

arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/payments-worker-stg-alb-5/f308e0bd625e24e6 staging
arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/mobile-ingest-dev-alb-4/ddb2c36e6675b84f dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/platform-sync-prod-alb-5/d372d95df5ae1cda dev-sandbox
arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/platform-web-stg-alb-5/6d30ebfb11e37e63 prod-eu
arn:aws:elasticloadbalancing:us-east-1:101278471862:loadbalancer/app/core-auth-dev-alb-5/0304ae2145f85313 prod-us
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/infra-billing-dev-alb-5/68a17b243036afff staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-sync-stg-alb-5/1d0ad78e3268db07 dev-sandbox
arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/growth-worker-stg-alb-5/b604f53ef50bb231 dev-sandbox

#46 Low ECR repository without image scanning

39 findings · 39 assets

AWS FSBP ECR.1

What to do. Enable scan-on-push on the repository or enhanced scanning for the whole registry.

EXAMPLE COMMANDS

```
aws ecr put-image-scanning-configuration --repository-name infra/notify-0 --image-scanning-configuration scanOnPush=true --region us-east-2 (or enable enhanced scanning for the whole registry: aws ecr put-registry-scanning-configuration --scan-type ENHANCED --rules '[{"scanFrequency":"SCAN_ON_PUSH","repositoryFilters":[{"filter":"*","filterType":"WILDCARD"}]}]' --region us-east-2)
```

```
aws ecr put-image-scanning-configuration --repository-name mobile/cache-0 --image-scanning-configuration scanOnPush=true --region us-east-1 (or enable enhanced scanning for the whole registry: aws ecr put-registry-scanning-configuration --scan-type ENHANCED --rules '[{"scanFrequency":"SCAN_ON_PUSH","repositoryFilters":[{"filter":"*","filterType":"WILDCARD"}]}]' --region us-east-1)
```

```
aws ecr put-image-scanning-configuration --repository-name infra/cache-0 --image-scanning-configuration scanOnPush=true --region us-east-1 (or enable enhanced scanning for the whole registry: aws ecr put-registry-scanning-configuration --scan-type ENHANCED --rules '[{"scanFrequency":"SCAN_ON_PUSH","repositoryFilters":[{"filter":"*","filterType":"WILDCARD"}]}]' --region us-east-1)
```

AFFECTED RESOURCES

arn:aws:ecr:us-east-2:101278471862:repository/infra/notify-0 prod-us
arn:aws:ecr:us-east-1:101261694243:repository/mobile/cache-0 staging
arn:aws:ecr:us-east-1:101244916624:repository/infra/cache-0 dev-sandbox
arn:aws:ecr:us-east-1:101278471862:repository/infra/cache-0 prod-us
arn:aws:ecr:us-east-2:101278471862:repository/ops/sync-1 prod-us
arn:aws:ecr:us-east-1:101244916624:repository/mobile/api-1 dev-sandbox
arn:aws:ecr:us-west-2:101295249481:repository/core/report-1 prod-eu
arn:aws:ecr:us-east-1:101278471862:repository/web/api-1 prod-us
arn:aws:ecr:us-west-1:101278471862:repository/infra/web-2 prod-us
arn:aws:ecr:us-east-2:101244916624:repository/web/cache-1 dev-sandbox
arn:aws:ecr:us-west-1:101295249481:repository/ml/search-3 prod-eu
arn:aws:ecr:us-east-1:101278471862:repository/mobile/billing-2 prod-us
arn:aws:ecr:us-east-2:101278471862:repository/platform/worker-3 prod-us
arn:aws:ecr:us-west-1:101278471862:repository/web/web-3 prod-us
arn:aws:ecr:us-east-1:101261694243:repository/data/notify-3 staging
arn:aws:ecr:us-west-1:101261694243:repository/growth/billing-2 staging
arn:aws:ecr:us-east-2:101244916624:repository/web/gateway-2 dev-sandbox
arn:aws:ecr:us-west-1:101244916624:repository/payments/sync-2 dev-sandbox
arn:aws:ecr:us-west-1:101278471862:repository/ops/gateway-4 prod-us
arn:aws:ecr:us-east-1:101261694243:repository/infra/cache-4 staging
arn:aws:ecr:us-west-1:101261694243:repository/mobile/sync-3 staging
arn:aws:ecr:us-east-1:101244916624:repository/ml/billing-4 dev-sandbox
arn:aws:ecr:us-west-2:101295249481:repository/ops/worker-4 prod-eu
arn:aws:ecr:us-east-1:101278471862:repository/payments/ingest-4 prod-us
arn:aws:ecr:us-east-1:101261694243:repository/platform/billing-5 staging
arn:aws:ecr:us-west-2:101295249481:repository/infra/gateway-5 prod-eu
arn:aws:ecr:us-east-2:101278471862:repository/payments/api-6 prod-us
arn:aws:ecr:us-east-1:101244916624:repository/core/search-6 dev-sandbox
arn:aws:ecr:us-east-2:101244916624:repository/infra/notify-5 dev-sandbox
arn:aws:ecr:us-west-1:101295249481:repository/infra/search-7 prod-eu
arn:aws:ecr:us-west-2:101295249481:repository/web/web-6 prod-eu
arn:aws:ecr:us-east-1:101278471862:repository/infra/web-6 prod-us
arn:aws:ecr:us-west-1:101278471862:repository/ops/web-7 prod-us
arn:aws:ecr:us-east-1:101261694243:repository/platform/web-7 staging
arn:aws:ecr:us-east-2:101244916624:repository/platform/sync-6 dev-sandbox
arn:aws:ecr:us-west-1:101244916624:repository/core/billing-6 dev-sandbox
arn:aws:ecr:us-west-2:101295249481:repository/mobile/web-7 prod-eu
arn:aws:ecr:us-east-1:101278471862:repository/infra/ingest-7 prod-us
arn:aws:ecr:us-east-2:101244916624:repository/platform/billing-7 dev-sandbox

#47 Low Load balancer without access logs

37 findings · 37 assets

AWS FSBP ELB.5

What to do. Enable access logging to an S3 log bucket.

EXAMPLE COMMANDS

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/data-worker-dev-alb-0/87e59e31e6a80116 --attributes Key=access_logs.s3.enabled,Value=true Key=access_logs.s3.bucket,Value=<log-bucket> Key=access_logs.s3.prefix,Value=data-worker-dev-alb-0 --region us-west-1
```

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/core-ingest-dev-alb-0/0e719567331c94b3 --attributes Key=access_logs.s3.enabled,Value=true Key=access_logs.s3.bucket,Value=<log-bucket> Key=access_logs.s3.prefix,Value=core-ingest-dev-alb-0 --region us-west-2
```

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/web-cache-stg-alb-1/db5f763b7ab07e05 --attributes Key=access_logs.s3.enabled,Value=true Key=access_logs.s3.bucket,Value=<log-bucket> Key=access_logs.s3.prefix,Value=web-cache-stg-alb-1 --region us-east-1
```

AFFECTED RESOURCES

arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/data-worker-dev-alb-0/87e59e31e6a80116 prod-us

arn:aws:elasticloadbalancing:us-west-2:101261694243:loadbalancer/app/core-ingest-dev-alb-0/0e719567331c94b3 staging

arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/web-cache-stg-alb-1/db5f763b7ab07e05 prod-eu

arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/data-search-dev-alb-0/fdb6cb74740d8038 prod-eu

arn:aws:elasticloadbalancing:us-west-1:101278471862:loadbalancer/app/web-notify-prod-alb-1/fe87b78dbd24eb59 prod-us

arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/core-web-stg-alb-0/8643827ed7d324cb staging

arn:aws:elasticloadbalancing:us-east-1:101244916624:loadbalancer/app/ml-ingest-dev-alb-1/48fc9f38df413688 dev-sandbox

arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-web-dev-alb-0/692e38ebf4165952 dev-sandbox

arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/infra-api-prod-alb-0/4be987aa1b11c2cd dev-sandbox

arn:aws:elasticloadbalancing:us-west-1:101295249481:loadbalancer/app/payments-sync-prod-alb-2/95c0fb66cbdb91f1 prod-eu

arn:aws:elasticloadbalancing:us-east-1:101278471862:loadbalancer/app/platform-sync-stg-alb-1/16329dee81af2052 prod-us

arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/payments-cache-stg-alb-2/486e68d1db1bd8c7 prod-us

arn:aws:elasticloadbalancing:us-east-1:101261694243:loadbalancer/app/ops-gateway-stg-alb-2/a60ff3632c906d04 staging

arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/growth-ingest-stg-alb-1/d68aff76aa7066bd dev-sandbox

arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/core-search-stg-alb-2/3d8009dff5992ea5 dev-sandbox

arn:aws:elasticloadbalancing:us-east-1:101295249481:loadbalancer/app/data-report-prod-alb-3/2337287fe1123b76 prod-eu

arn:aws:elasticloadbalancing:us-east-2:101295249481:loadbalancer/app/payments-report-prod-alb-3/fbfe08ba8697768f prod-eu

arn:aws:elasticloadbalancing:us-east-1:101278471862:loadbalancer/app/ops-cache-stg-alb-2/00dd4b5c2d836cd4 prod-us

arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/web-search-stg-alb-3/a35dc0c78ad5943a staging

arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/data-auth-stg-alb-2/fba21f047754b7a5 staging

arn:aws:elasticloadbalancing:us-east-1:101244916624:loadbalancer/app/web-billing-prod-alb-3/d81d008bd0703e18 dev-sandbox

arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/payments-search-dev-alb-2/8948773439b2a16a dev-sandbox

arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/web-search-stg-alb-3/7ca38159f494ab41 prod-eu

arn:aws:elasticloadbalancing:us-east-1:101278471862:loadbalancer/app/growth-cache-dev-alb-3/2dd5d97e55e8fc64 prod-us

arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/platform-cache-dev-alb-4/cb57d81fa8047666 prod-us

arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/core-gateway-dev-alb-4/8145d8afe65f3987 staging

arn:aws:elasticloadbalancing:us-west-2:101244916624:loadbalancer/app/payments-search-dev-alb-4/e7d6826536ded246 dev-sandbox

arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/mobile-report-prod-alb-4/c424c9e6926d4f3a prod-eu

arn:aws:elasticloadbalancing:us-east-2:101278471862:loadbalancer/app/platform-report-dev-alb-5/d92bf25cccf117e8 prod-us

arn:aws:elasticloadbalancing:us-east-2:101261694243:loadbalancer/app/ops-search-dev-alb-5/892dd2a786a73d97 staging

arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-sync-stg-alb-4/723e93048490f5d9 dev-sandbox

arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/mobile-ingest-dev-alb-4/ddb2c36e6675b84f dev-sandbox

arn:aws:elasticloadbalancing:us-west-2:101295249481:loadbalancer/app/platform-web-stg-alb-5/6d30ebfb11e37e63 prod-eu

arn:aws:elasticloadbalancing:us-east-1:101278471862:loadbalancer/app/core-auth-dev-alb-5/0304ae2145f85313 prod-us
arn:aws:elasticloadbalancing:us-west-1:101261694243:loadbalancer/app/infra-billing-dev-alb-5/68a17b243036afff staging
arn:aws:elasticloadbalancing:us-east-2:101244916624:loadbalancer/app/core-sync-stg-alb-5/1d0ad78e3268db07 dev-sandbox
arn:aws:elasticloadbalancing:us-west-1:101244916624:loadbalancer/app/growth-worker-stg-alb-5/b604f53ef50bb231 dev-sandbox

#48 Low RDS instance not applying minor engine upgrades automatically

33 findings · 33 assets

CIS 2.2.2 · AWS FSBP RDS.13

What to do. Enable Auto Minor Version Upgrade so engine security patches are applied in the maintenance window.

EXAMPLE COMMANDS

```
aws rds modify-db-instance --db-instance-identifier payments-api-prod-db-0 --auto-minor-version-upgrade --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier platform-billing-prod-db-0 --auto-minor-version-upgrade --apply-immediately
```

```
aws rds modify-db-instance --db-instance-identifier ops-worker-prod-db-0 --auto-minor-version-upgrade --apply-immediately
```

AFFECTED RESOURCES

payments-api-prod-db-0 prod-eu
platform-billing-prod-db-0 prod-eu
ops-worker-prod-db-0 prod-us
web-web-dev-db-0 staging
growth-billing-stg-db-1 prod-us
platform-api-stg-db-1 dev-sandbox
ml-api-prod-db-1 dev-sandbox
infra-report-dev-db-1 dev-sandbox
data-web-stg-db-2 prod-eu
core-cache-prod-db-2 staging
mobile-report-stg-db-2 staging
web-gateway-prod-db-2 dev-sandbox
data-sync-prod-db-2 dev-sandbox
mobile-sync-stg-db-3 prod-us
platform-report-dev-db-3 prod-us
data-worker-dev-db-3 prod-us
ops-search-stg-db-3 staging
ops-notify-stg-db-3 staging
growth-notify-dev-db-3 staging
web-cache-prod-db-3 staging
mobile-ingest-stg-db-3 dev-sandbox
growth-billing-dev-db-3 dev-sandbox
ops-cache-stg-db-4 prod-eu
ml-report-prod-db-4 prod-eu
payments-gateway-prod-db-4 staging
mobile-api-dev-db-4 dev-sandbox
ml-auth-stg-db-4 dev-sandbox
platform-auth-dev-db-4 dev-sandbox
payments-cache-stg-db-5 prod-eu
payments-api-prod-db-5 staging
infra-billing-dev-db-5 staging
platform-ingest-prod-db-5 dev-sandbox
platform-notify-stg-db-5 dev-sandbox

#49 Low RDS instance in a single Availability Zone

27 findings · 27 assets

CIS 2.2.4 · AWS FSBP RDS.5

What to do. Enable Multi-AZ for production databases; tag non-production ones so the score weights them accordingly.

EXAMPLE COMMANDS

```
aws rds modify-db-instance --db-instance-identifier payments-api-prod-db-0 --multi-az --apply-immediately (doubles the instance cost — tag non-production databases with Environment=dev to weight this accordingly).
```

```
aws rds modify-db-instance --db-instance-identifier platform-billing-prod-db-0 --multi-az --apply-immediately (doubles the instance cost — tag non-production databases with Environment=dev to weight this accordingly).
```

```
aws rds modify-db-instance --db-instance-identifier infra-report-stg-db-0 --multi-az --apply-immediately (doubles the instance cost — tag non-production databases with Environment=dev to weight this accordingly).
```

AFFECTED RESOURCES

payments-api-prod-db-0 prod-eu
platform-billing-prod-db-0 prod-eu
infra-report-stg-db-0 staging
web-web-dev-db-0 staging
mobile-report-prod-db-0 dev-sandbox
data-api-stg-db-0 dev-sandbox
infra-api-stg-db-1 prod-eu
platform-api-stg-db-1 dev-sandbox
ml-api-prod-db-1 dev-sandbox
infra-report-dev-db-1 dev-sandbox
core-cache-stg-db-2 prod-eu
mobile-notify-prod-db-2 prod-us
platform-billing-dev-db-2 staging
mobile-report-stg-db-2 staging
infra-ingest-dev-db-2 dev-sandbox
data-sync-prod-db-2 dev-sandbox
payments-sync-dev-db-3 prod-eu
data-notify-prod-db-3 prod-eu
ops-web-prod-db-3 prod-eu
growth-billing-dev-db-3 dev-sandbox
ml-cache-stg-db-3 dev-sandbox
growth-ingest-prod-db-4 prod-eu
growth-notify-dev-db-4 prod-eu
ops-cache-stg-db-4 prod-eu
growth-api-stg-db-5 prod-eu
platform-ingest-prod-db-5 dev-sandbox
platform-auth-stg-db-5 dev-sandbox

#50 Low Elastic IP not associated with anything

14 findings · 14 assets

What to do. Release the address if it is no longer needed.

EXAMPLE COMMANDS

```
Release it if unused: aws ec2 release-address --allocation-id eipalloc-649b9d4a
```

```
Release it if unused: aws ec2 release-address --allocation-id eipalloc-9982c2fe
```

```
Release it if unused: aws ec2 release-address --allocation-id eipalloc-c6934334
```

AFFECTED RESOURCES

eipalloc-649b9d4a dev-sandbox
eipalloc-9982c2fe prod-us
eipalloc-c6934334 staging
eipalloc-50e98073 staging
eipalloc-1e82679f dev-sandbox
eipalloc-46838e8c dev-sandbox
eipalloc-e8742f1a prod-us
eipalloc-700c1d4c dev-sandbox
eipalloc-89a3499f prod-us
eipalloc-86a344e6 prod-us
eipalloc-a7bffd8c staging
eipalloc-55e98852 staging
eipalloc-dc8ce4f3 prod-eu
eipalloc-87a34679 prod-us

#51 Low IAM user with two active access keys

10 findings · 10 assets

CIS 1.12

What to do. Keep one active key per user; the second key exists only for rotation and should be deleted afterwards.

EXAMPLE COMMANDS

```
Finish the rotation: aws iam update-access-key --user-name alice.data-2 --access-key-id <old-key> --status
Inactive, then delete it once nothing uses it.
```

```
Finish the rotation: aws iam update-access-key --user-name hakon.dev-12 --access-key-id <old-key> --status
Inactive, then delete it once nothing uses it.
```

```
Finish the rotation: aws iam update-access-key --user-name hakon.dev-27 --access-key-id <old-key> --status
Inactive, then delete it once nothing uses it.
```

AFFECTED RESOURCES

arn:aws:iam::101261694243:user/alice.data-2 staging
arn:aws:iam::101278471862:user/hakon.dev-12 prod-us
arn:aws:iam::101295249481:user/hakon.dev-27 prod-eu
arn:aws:iam::101278471862:user/carla.data-29 prod-us
arn:aws:iam::101295249481:user/ines.svc-33 prod-eu
arn:aws:iam::101295249481:user/ines.dev-36 prod-eu
arn:aws:iam::101244916624:user/hakon.dev-38 dev-sandbox
arn:aws:iam::101261694243:user/eva.svc-48 staging
arn:aws:iam::101244916624:user/gudrun.dev-50 dev-sandbox
arn:aws:iam::101295249481:user/carla.qa-59 prod-eu

#52 Low EKS cluster without audit logging

9 findings · 9 assets

AWS FSBP EKS.8

What to do. Enable the audit and authenticator control-plane log types on the cluster.

EXAMPLE COMMANDS

```
aws eks update-cluster-config --name platform-eks-0 --logging '{"clusterLogging":[{"types":
["audit","authenticator"],"enabled":true}]}' --region us-east-2
```

```
aws eks update-cluster-config --name core-eks-0 --logging '{"clusterLogging":[{"types":
["audit","authenticator"],"enabled":true}]}' --region us-west-1
```

```
aws eks update-cluster-config --name data-eks-0 --logging '{"clusterLogging":[{"types":
["audit","authenticator"],"enabled":true}]}' --region us-east-1
```

AFFECTED RESOURCES

arn:aws:eks:us-east-2:101295249481:cluster/platform-eks-0 prod-eu
arn:aws:eks:us-west-1:101278471862:cluster/core-eks-0 prod-us
arn:aws:eks:us-east-1:101261694243:cluster/data-eks-0 staging
arn:aws:eks:us-east-2:101261694243:cluster/infra-eks-0 staging
arn:aws:eks:us-west-2:101244916624:cluster/ml-eks-0 dev-sandbox
arn:aws:eks:us-west-2:101295249481:cluster/ml-eks-0 prod-eu
arn:aws:eks:us-east-1:101278471862:cluster/mobile-eks-0 prod-us
arn:aws:eks:us-west-1:101261694243:cluster/web-eks-0 staging
arn:aws:eks:us-east-2:101244916624:cluster/growth-eks-0 dev-sandbox

#53 Low RDS cluster without instances in a second Availability Zone

9 findings · 9 assets

CIS 2.2.4 · AWS FSBP RDS.15

What to do. Add a reader instance in another Availability Zone.

EXAMPLE COMMANDS

```
Add a reader in another AZ: aws rds create-db-instance --db-cluster-identifier core-cache-prod-cluster-0 --db-instance-identifier core-cache-prod-cluster-0-reader-b --engine aurora-postgresql --db-instance-class <class> --availability-zone <other-az>
```

```
Add a reader in another AZ: aws rds create-db-instance --db-cluster-identifier growth-worker-stg-cluster-0 --db-instance-identifier growth-worker-stg-cluster-0-reader-b --engine aurora-mysql --db-instance-class <class> --availability-zone <other-az>
```

```
Add a reader in another AZ: aws rds create-db-instance --db-cluster-identifier web-gateway-prod-cluster-0 --db-instance-identifier web-gateway-prod-cluster-0-reader-b --engine aurora-postgresql --db-instance-class <class> --availability-zone <other-az>
```

AFFECTED RESOURCES

core-cache-prod-cluster-0 prod-eu
growth-worker-stg-cluster-0 prod-eu
web-gateway-prod-cluster-0 prod-eu
infra-web-stg-cluster-0 staging
web-api-prod-cluster-0 staging
ops-sync-prod-cluster-0 dev-sandbox
infra-auth-stg-cluster-1 prod-us
infra-cache-prod-cluster-1 staging
ops-gateway-prod-cluster-1 dev-sandbox

#54 Low Block public access for EBS snapshots off in some regions

4 findings · 4 assets

AWS FSBP EC2.182

What to do. Enable snapshot block public access (block-all-sharing) in every region.

EXAMPLE COMMANDS

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-west-2
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region ca-central-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region eu-west-3
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region eu-central-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region eu-north-1
… 6 more lines (full command in the CSV export)
```

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-east-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-east-2
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-west-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-west-2
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region ca-central-1
… 10 more lines (full command in the CSV export)
```

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-east-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-east-2
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region us-west-2
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region ca-central-1
aws ec2 enable-snapshot-block-public-access --state block-all-sharing --region eu-west-1
… 11 more lines (full command in the CSV export)
```

AFFECTED RESOURCES

ebs-snapshot-block-public-access prod-eu
ebs-snapshot-block-public-access prod-us
ebs-snapshot-block-public-access staging
ebs-snapshot-block-public-access dev-sandbox

#55 Low CloudTrail logs not encrypted with a KMS key

4 findings · 4 assets

CIS 3.5 · AWS FSBP CloudTrail.2

What to do. Configure the trail with a customer-managed KMS key.

EXAMPLE COMMANDS

```
aws cloudtrail update-trail --name arn:aws:cloudtrail:us-east-1:101295249481:trail/org-trail --kms-key-id <key-id>
--region us-east-1 (the key policy must allow CloudTrail to encrypt and log readers to decrypt). Run this from the
organization account that owns the trail.
```

```
aws cloudtrail update-trail --name arn:aws:cloudtrail:us-east-1:101278471862:trail/org-trail --kms-key-id <key-id>
--region us-east-1 (the key policy must allow CloudTrail to encrypt and log readers to decrypt).
```

```
aws cloudtrail update-trail --name arn:aws:cloudtrail:us-east-1:101261694243:trail/org-trail --kms-key-id <key-id>
--region us-east-1 (the key policy must allow CloudTrail to encrypt and log readers to decrypt). Run this from the
organization account that owns the trail.
```

AFFECTED RESOURCES

- arn:aws:cloudtrail:us-east-1:101295249481:trail/org-trail prod-eu
- arn:aws:cloudtrail:us-east-1:101278471862:trail/org-trail prod-us
- arn:aws:cloudtrail:us-east-1:101261694243:trail/org-trail staging
- arn:aws:cloudtrail:us-east-1:101244916624:trail/org-trail dev-sandbox

#56 Low No CloudWatch alarm for AWS Config configuration changes

4 findings · 4 assets

CIS 4.9

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.9 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-config-changes --filter-pattern '{
($.eventSource = config.amazonaws.com) && (($.eventName = StopConfigurationRecorder) || ($.eventName =
DeleteDeliveryChannel) || ($.eventName = PutDeliveryChannel) || ($.eventName = PutConfigurationRecorder)) }' --
metric-transformations metricName=CIS-config-changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-config-changes --metric-name CIS-config-changes --namespace
CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --
evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

- monitoring prod-eu
- monitoring prod-us
- monitoring staging
- monitoring dev-sandbox

#57 Low No CloudWatch alarm for CloudTrail configuration changes

4 findings · 4 assets

CIS 4.5

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.5 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-cloudtrail-config-changes --filter-pattern
'{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName =
StartLogging) || ($.eventName = StopLogging) }' --metric-transformations metricName=CIS-cloudtrail-config-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-cloudtrail-config-changes --metric-name CIS-cloudtrail-config-
changes --namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

- monitoring prod-eu
- monitoring prod-us
- monitoring staging
- monitoring dev-sandbox

#58 Low S3 object-level write events not logged

4 findings · 4 assets

CIS 3.8

What to do. Add a data event selector for S3 object write events to a trail.

EXAMPLE COMMAND

```
aws cloudtrail put-event-selectors --trail-name <trail> --advanced-event-selectors '[{"Name":"S3
writes","FieldSelectors":[{"Field":"eventCategory","Equals":["Data"]},{"Field":"resources.type","Equals":
["AWS::S3::Object"]},{"Field":"readOnly","Equals":["false"]}]}]'
```

AFFECTED RESOURCES

- cloudtrail prod-eu
- cloudtrail prod-us
- cloudtrail staging
- cloudtrail dev-sandbox

#59 Low Security Hub not enabled in every region

4 findings · 4 assets

CIS 4.16

What to do. Enable Security Hub with the default standards in each region, or delegate it to a security account across the organization.

EXAMPLE COMMANDS

```
aws securityhub enable-security-hub --enable-default-standards --region us-east-1
aws securityhub enable-security-hub --enable-default-standards --region us-east-2
aws securityhub enable-security-hub --enable-default-standards --region us-west-1
aws securityhub enable-security-hub --enable-default-standards --region eu-west-2
aws securityhub enable-security-hub --enable-default-standards --region eu-north-1
… 4 more lines (full command in the CSV export)
```

```
aws securityhub enable-security-hub --enable-default-standards --region us-east-1
aws securityhub enable-security-hub --enable-default-standards --region us-west-2
aws securityhub enable-security-hub --enable-default-standards --region eu-west-1
aws securityhub enable-security-hub --enable-default-standards --region eu-west-2
aws securityhub enable-security-hub --enable-default-standards --region ap-southeast-2
… 2 more lines (full command in the CSV export)
```

```
aws securityhub enable-security-hub --enable-default-standards --region us-east-1
aws securityhub enable-security-hub --enable-default-standards --region us-east-2
aws securityhub enable-security-hub --enable-default-standards --region ca-central-1
aws securityhub enable-security-hub --enable-default-standards --region eu-west-3
aws securityhub enable-security-hub --enable-default-standards --region ap-southeast-1
… 3 more lines (full command in the CSV export)
```

AFFECTED RESOURCES

- securityhub prod-eu
- securityhub prod-us
- securityhub staging
- securityhub dev-sandbox

#60 Low No CloudWatch alarm for console authentication failures

3 findings · 3 assets

CIS 4.6

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.6 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-console-auth-failures --filter-pattern '{
($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }' --metric-transformations
metricName=CIS-console-auth-failures,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-console-auth-failures --metric-name CIS-console-auth-failures --
namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

- monitoring prod-eu
- monitoring staging
- monitoring dev-sandbox

#61 Low No CloudWatch alarm for console sign-in without MFA

3 findings · 3 assets

CIS 4.2

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.2 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-console-signin-without-mfa --filter-pattern '{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") }' --metric-transformations metricName=CIS-console-signin-without-mfa,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-console-signin-without-mfa --metric-name CIS-console-signin-without-mfa --namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring prod-us

#62 Low No CloudWatch alarm for disabling or scheduled deletion of customer-managed KMS keys

3 findings · 3 assets

CIS 4.7

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.7 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-kms-key-deletion --filter-pattern '{ ($.eventSource = kms.amazonaws.com) && (($.eventName = DisableKey) || ($.eventName = ScheduleKeyDeletion)) }' --metric-transformations metricName=CIS-kms-key-deletion,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-kms-key-deletion --metric-name CIS-kms-key-deletion --namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring prod-us

#63 Low No CloudWatch alarm for IAM policy changes

3 findings · 3 assets

CIS 4.4

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.4 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-iam-policy-changes --filter-pattern '{ ($.eventName = DeleteGroupPolicy) || ($.eventName = DeleteRolePolicy) || ($.eventName = DeleteUserPolicy) || ($.eventName = PutGroupPolicy) || ($.eventName = PutRolePolicy) || ($.eventName = PutUserPolicy) || ($.eventName = CreatePolicy) || ($.eventName = DeletePolicy) || ($.eventName = CreatePolicyVersion) || ($.eventName = DeletePolicyVersion) || ($.eventName = AttachRolePolicy) || ($.eventName = DetachRolePolicy) || ($.eventName = AttachUserPolicy) || ($.eventName = DetachUserPolicy) || ($.eventName = AttachGroupPolicy) || ($.eventName = DetachGroupPolicy) }' --metric-transformations metricName=CIS-iam-policy-changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-iam-policy-changes --metric-name CIS-iam-policy-changes --namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring prod-us

#64 Low No CloudWatch alarm for network ACL changes

3 findings · 3 assets

CIS 4.11

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.11 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-nacl-changes --filter-pattern '{
($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) ||
($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName =
ReplaceNetworkAclAssociation) }' --metric-transformations metricName=CIS-nacl-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-nacl-changes --metric-name CIS-nacl-changes --namespace
CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --
evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring staging

#65 Low No CloudWatch alarm for security group changes

3 findings · 3 assets

CIS 4.10

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.10 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-security-group-changes --filter-pattern '{
($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName =
RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) ||
($.eventName = DeleteSecurityGroup) }' --metric-transformations metricName=CIS-security-group-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-security-group-changes --metric-name CIS-security-group-changes --
namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring staging

#66 Low No CloudWatch alarm for unauthorized API calls

3 findings · 3 assets

CIS 4.1

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.1 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-unauthorized-api-calls --filter-pattern '{
($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") }' --metric-transformations
metricName=CIS-unauthorized-api-calls,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-unauthorized-api-calls --metric-name CIS-unauthorized-api-calls --
namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring staging

#67 Low No CloudWatch alarm for use of the 'root' account

3 findings · 3 assets

CIS 4.3

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.3 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-root-usage --filter-pattern '{
$.userIdentity.type = "Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent" }' --
metric-transformations metricName=CIS-root-usage,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-root-usage --metric-name CIS-root-usage --namespace CISBenchmark -
-statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods
1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring dev-sandbox
monitoring staging

#68 Low Root user MFA is a virtual device rather than hardware

3 findings · 3 assets

CIS 1.5 · AWS FSBP IAM.6

What to do. Register a hardware MFA device (FIDO security key) for the root user and remove the virtual one.

EXAMPLE COMMAND

```
Register a FIDO2 security key or hardware TOTP token for the root user under My Security Credentials, then
deactivate the virtual device.
```

AFFECTED RESOURCES

root prod-eu
root staging
root prod-us

#69 Low CloudTrail S3 bucket without server access logging

2 findings · 2 assets

CIS 3.4

What to do. Enable server access logging on the bucket that receives CloudTrail logs.

EXAMPLE COMMANDS

```
aws s3api put-bucket-logging --bucket cloudtrail-101295249481 --bucket-logging-status '{"LoggingEnabled":
{"TargetBucket":"<access-log-bucket>","TargetPrefix":"cloudtrail-bucket/"}}'
```

```
aws s3api put-bucket-logging --bucket cloudtrail-101261694243 --bucket-logging-status '{"LoggingEnabled":
{"TargetBucket":"<access-log-bucket>","TargetPrefix":"cloudtrail-bucket/"}}'
```

AFFECTED RESOURCES

arn:aws:cloudtrail:us-east-1:101295249481:trail/org-trail
prod-eu
arn:aws:cloudtrail:us-east-1:101261694243:trail/org-trail
staging

#70 Low No CloudWatch alarm for network gateway changes

2 findings · 2 assets

CIS 4.12

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.12 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-network-gateway-changes --filter-pattern
'{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName =
AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) ||
($.eventName = DetachInternetGateway) }' --metric-transformations metricName=CIS-network-gateway-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-network-gateway-changes --metric-name CIS-network-gateway-changes
--namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu
monitoring staging

#71 Low No CloudWatch alarm for route table changes

2 findings · 2 assets

CIS 4.13

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.13 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-route-table-changes --filter-pattern '{
($.eventSource = ec2.amazonaws.com) && (($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) ||
($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) ||
($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable)) }' --metric-transformations metricName=CIS-
route-table-changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-route-table-changes --metric-name CIS-route-table-changes --
namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-eu

monitoring dev-sandbox

#72 Low No CloudWatch alarm for S3 bucket policy changes

2 findings · 2 assets

CIS 4.8

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.8 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-s3-bucket-policy-changes --filter-pattern
'{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) ||
($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) ||
($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) ||
($.eventName = DeleteBucketReplication)) }' --metric-transformations metricName=CIS-s3-bucket-policy-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-s3-bucket-policy-changes --metric-name CIS-s3-bucket-policy-
changes --namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring staging

monitoring dev-sandbox

#73 Low No CloudWatch alarm for VPC changes

2 findings · 2 assets

CIS 4.14

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.14 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-vpc-changes --filter-pattern '{
($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName =
AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName =
DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc)
|| ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName =
EnableVpcClassicLink) }' --metric-transformations metricName=CIS-vpc-
changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-vpc-changes --metric-name CIS-vpc-changes --namespace CISBenchmark
--statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods
1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

monitoring prod-us

monitoring dev-sandbox

#74 Low S3 object-level read events not logged

2 findings · 2 assets

CIS 3.9

What to do. Add a data event selector for S3 object read events to a trail.

EXAMPLE COMMAND

```
aws cloudtrail put-event-selectors --trail-name <trail> --advanced-event-selectors '[{"Name":"S3
reads","FieldSelectors":[{"Field":"eventCategory","Equals":["Data"]},{"Field":"resources.type","Equals":
["AWS::S3::Object"]},{"Field":"readOnly","Equals":["true"]},{"Field":"resources.ARN","StartsWith":["arn:aws:s3:::
<sensitive-bucket>/"]}]}]'
```

AFFECTED RESOURCES

`cloudtrail` prod-eu

`cloudtrail` dev-sandbox

#75 Low CloudTrail log file validation disabled

1 finding · 1 asset

CIS 3.2 · AWS FSBP CloudTrail.4 · PCI DSS 10.3.2

What to do. Enable log file validation on the trail so tampering with delivered logs is detectable.

EXAMPLE COMMAND

```
aws cloudtrail update-trail --name arn:aws:cloudtrail:us-east-1:101295249481:trail/org-trail --enable-log-file-
validation --region us-east-1 Run this from the organization account that owns the trail.
```

AFFECTED RESOURCES

`arn:aws:cloudtrail:us-east-1:101295249481:trail/org-trail`
prod-eu

#76 Low No CloudWatch alarm for AWS Organizations changes

1 finding · 1 asset

CIS 4.15

What to do. Create a metric filter on the CloudTrail log group matching the CIS 4.15 pattern and an alarm on that metric with an SNS action that reaches someone.

EXAMPLE COMMAND

```
aws logs put-metric-filter --log-group-name cloudtrail --filter-name CIS-organizations-changes --filter-pattern '{
($.eventSource = organizations.amazonaws.com) && (($.eventName = AcceptHandshake) || ($.eventName = AttachPolicy)
|| ($.eventName = CancelHandshake) || ($.eventName = CreateAccount) || ($.eventName = CreateOrganization) ||
($.eventName = CreateOrganizationalUnit) || ($.eventName = CreatePolicy) || ($.eventName = DeclineHandshake) ||
($.eventName = DeleteOrganization) || ($.eventName = DeleteOrganizationalUnit) || ($.eventName = DeletePolicy) ||
($.eventName = EnableAllFeatures) || ($.eventName = EnablePolicyType) || ($.eventName =
InviteAccountToOrganization) || ($.eventName = LeaveOrganization) || ($.eventName = DetachPolicy) || ($.eventName =
DisablePolicyType) || ($.eventName = MoveAccount) || ($.eventName = RemoveAccountFromOrganization) || ($.eventName
= UpdateOrganizationalUnit) || ($.eventName = UpdatePolicy)) }' --metric-transformations metricName=CIS-
organizations-changes,metricNamespace=CISBenchmark,metricValue=1 --region us-east-1
aws cloudwatch put-metric-alarm --alarm-name CIS-organizations-changes --metric-name CIS-organizations-changes --
namespace CISBenchmark --statistic Sum --period 300 --threshold 1 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns-topic-arn> --region us-east-1
```

AFFECTED RESOURCES

`monitoring` prod-us

#77 Low No role holds the AWSSupportAccess policy

1 finding · 1 asset

CIS 1.16

What to do. Create a role with the AWSSupportAccess managed policy so incidents can be raised with AWS Support without admin credentials.

EXAMPLE COMMAND

```
Create a dedicated role: aws iam create-role --role-name aws-support-access --assume-role-policy-document <trust
policy>, then aws iam attach-role-policy --role-name aws-support-access --policy-arn
arn:aws:iam::aws:policy/AWSSupportAccess
```

AFFECTED RESOURCES

`root` dev-sandbox

#78 Low No security contact registered for the account

1 finding · 1 asset

CIS 1.2 · AWS FSBP Account.1

What to do. Register a security alternate contact (a shared mailbox, not a person) so AWS abuse and security notices reach someone.

EXAMPLE COMMAND

```
aws account put-alternate-contact --alternate-contact-type SECURITY --name "Security team" --email-address
security@example.com --phone-number "+354 ..." --title "Security contact"
```

AFFECTED RESOURCES

root prod-us

#79 Info EC2 instance with a public IP address (inventory)

88 findings · 88 assets

AWS FSBP EC2.9

What to do. Confirm the instance needs a public address; otherwise move it to a private subnet behind a load balancer or NAT gateway.

EXAMPLE COMMANDS

```
Confirm i-61500e2fb756e2e3c needs a public IP. If not, move it to a private subnet behind a load balancer or NAT
gateway and release the address.
```

```
Confirm i-8c57c195bfa6e35d7 needs a public IP. If not, move it to a private subnet behind a load balancer or NAT
gateway and release the address.
```

```
Confirm i-21925f8fcd38adc16 needs a public IP. If not, move it to a private subnet behind a load balancer or NAT
gateway and release the address.
```

AFFECTED RESOURCES

i-61500e2fb756e2e3c prod-eu
i-8c57c195bfa6e35d7 dev-sandbox
i-21925f8fcd38adc16 dev-sandbox
i-00992174821304739 prod-us
i-3fbb1e0f023d78584 prod-eu
i-553c136a2f294113b prod-us
i-aa1e30731790693a0 staging
i-7473493b16282469e dev-sandbox
i-4f3c09f8a79aa758c prod-us
i-7973511a9343a0f69 dev-sandbox
i-2e9a1d571715e6128 prod-eu
i-8757b9b661c918afb dev-sandbox
i-1c9257b09fc85a962 dev-sandbox
i-3bbb17c385ec97188 prod-eu
i-5de49684d78a36c8b staging
i-ae1e36bffae0092e7 staging
i-5e5009764b36a025c prod-eu
i-523c0eb14de687ced prod-us
i-ad1e352c1c9d6b65f staging
i-1e925ad6678af13ef dev-sandbox
i-49bb2dcdcab98cfaa prod-eu
i-ec35dfc0eb2b40826 dev-sandbox
i-229a0a733a23913ce prod-eu
i-4b03f457dd11f988a prod-eu
i-97890c95754526c4a staging
i-c78121f01fb65ff1c dev-sandbox
i-948907dc0fe0b9050 staging
i-a27606de0a1019a4a prod-us
i-7d9028595cf4b9188 prod-us
i-928904b63438fc8ed staging
i-91239502524f69fed dev-sandbox
i-0e69a1d88198604c5 dev-sandbox
i-4e92969a21e150637 prod-eu
i-a4760a044533bc099 prod-us
i-ffd6308cab11a412d staging
i-fe64ee8e4659307f3 staging
i-6a38b8fb3a0a2ba2c staging
i-1069a4fe4890521df dev-sandbox
i-340f5c79511c0b1f1 prod-us
i-6938b7684e4b0f124 staging
i-9023936f92b716e7c dev-sandbox
i-dfe571547d4a8b476 dev-sandbox
i-4203e62cd59e7c22e prod-eu
i-6838b5d59a533857b staging
i-0a699b8c94b511e59 dev-sandbox
i-8192c1013c12d03f1 prod-eu
i-563ad816612f41ca3 staging
i-8bcebe2b77cf8a47a staging
i-be0b652539acfa164 prod-eu
i-86711a8509ad725a7 dev-sandbox
i-5879b76e163457a74 dev-sandbox
i-736c62823564aecb5 staging
i-778a1bb43b85f5d01 prod-eu
i-4d94d39eb2a8b5460 prod-eu
i-5b3adff5b2106111f staging
i-4b94d078fa9fa0f90 prod-eu
i-c516fc8101f6112c6 prod-us
i-90cec60a39587fdd0 staging
i-583adb3cc5ca6fc6e staging
i-18860611844d6e5b3 staging
and 28 more, listed in the CSV export

APPENDIX A Critical findings (80)

What each finding is and where. The fix for each check is in the Remediation Plan, referenced by number.

Critical **IAM user "carla.dev-1" has an admin-equivalent policy** Plan #8

`arn:aws:iam::101261694243:user/carla.dev-1 · staging · global · CIS 1.15 · AWS FSBP IAM.1 · PCI DSS 7.2.1`

carla.dev-1 has a policy statement granting Action:"*" on Resource:"*" — effectively unrestricted access to the account.

Critical **IAM user "carla.qa-13" has an admin-equivalent policy** Plan #8

`arn:aws:iam::101261694243:user/carla.qa-13 · staging · global · CIS 1.15 · AWS FSBP IAM.1 · PCI DSS 7.2.1`

carla.qa-13 has a policy statement granting Action:"*" on Resource:"*" — effectively unrestricted access to the account.

Critical **IAM user "gudrun.svc-19" has an admin-equivalent policy** Plan #8

`arn:aws:iam::101244916624:user/gudrun.svc-19 · dev-sandbox · global · CIS 1.15 · AWS FSBP IAM.1 · PCI DSS 7.2.1`

gudrun.svc-19 has a policy statement granting Action:"*" on Resource:"*" — effectively unrestricted access to the account.

Critical **IAM user "finn.qa-24" has an admin-equivalent policy** Plan #8

`arn:aws:iam::101295249481:user/finn.qa-24 · prod-eu · global · CIS 1.15 · AWS FSBP IAM.1 · PCI DSS 7.2.1`

finn.qa-24 has a policy statement granting Action:"*" on Resource:"*" — effectively unrestricted access to the account.

Critical **IAM role "ops-billing-dev-role-17" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101278471862:role/ops-billing-dev-role-17 · prod-us · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101278471862:role/ops-billing-dev-role-17 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **IAM role "infra-api-prod-role-31" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101295249481:role/infra-api-prod-role-31 · prod-eu · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101295249481:role/infra-api-prod-role-31 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **IAM role "payments-cache-prod-role-40" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101295249481:role/payments-cache-prod-role-40 · prod-eu · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101295249481:role/payments-cache-prod-role-40 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **IAM role "ops-auth-dev-role-73" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101244916624:role/ops-auth-dev-role-73 · dev-sandbox · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101244916624:role/ops-auth-dev-role-73 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **IAM role "ops-notify-stg-role-94" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101244916624:role/ops-notify-stg-role-94 · dev-sandbox · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101244916624:role/ops-notify-stg-role-94 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **IAM role "core-api-dev-role-101" can be assumed by any AWS account** Plan #6

`arn:aws:iam::101295249481:role/core-api-dev-role-101 · prod-eu · global · PCI DSS 7.2.1`

The trust policy of arn:aws:iam::101295249481:role/core-api-dev-role-101 (statement (no Sid)) allows sts:AssumeRole for Principal "*" with no Condition, so anyone with an AWS account can obtain this role's credentials and use every permission attached to it.

Critical **S3 bucket "platform-api-dev-data-4243-0" is publicly accessible** Plan #4

`platform-api-dev-data-4243-0 · staging · us-east-1 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

platform-api-dev-data-4243-0 grants access to the internet (AllUsers/AuthenticatedUsers) via its bucket policy.

Critical **S3 bucket "mobile-billing-prod-data-9481-1" is publicly accessible** Plan #4

`mobile-billing-prod-data-9481-1 · prod-eu · us-west-1 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

mobile-billing-prod-data-9481-1 grants access to the internet (AllUsers/AuthenticatedUsers) via its bucket policy.

Critical **S3 bucket "mobile-auth-stg-backups-4243-2" is publicly accessible** Plan #4

`mobile-auth-stg-backups-4243-2 · staging · us-west-2 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

mobile-auth-stg-backups-4243-2 grants access to the internet (AllUsers/AuthenticatedUsers) via its ACL.

Critical **S3 bucket "infra-web-stg-data-1862-8" is publicly accessible** Plan #4

`infra-web-stg-data-1862-8 · prod-us · us-west-1 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

infra-web-stg-data-1862-8 grants access to the internet (AllUsers/AuthenticatedUsers) via its ACL.

Critical **S3 bucket "ops-notify-stg-assets-9481-60" is publicly accessible** Plan #4

`ops-notify-stg-assets-9481-60 · prod-eu · us-east-1 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

ops-notify-stg-assets-9481-60 grants access to the internet (AllUsers/AuthenticatedUsers) via its ACL.

Critical **S3 bucket "web-billing-prod-uploads-6624-60" is publicly accessible** Plan #4

`web-billing-prod-uploads-6624-60 · dev-sandbox · us-west-1 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

web-billing-prod-uploads-6624-60 grants access to the internet (AllUsers/AuthenticatedUsers) via its ACL.

Critical **S3 bucket "mobile-notify-stg-logs-4243-72" is publicly accessible** Plan #4

`mobile-notify-stg-logs-4243-72 · staging · us-west-2 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

mobile-notify-stg-logs-4243-72 grants access to the internet (AllUsers/AuthenticatedUsers) via its bucket policy.

Critical **S3 bucket "core-ingest-dev-data-9481-76" is publicly accessible** Plan #4

`core-ingest-dev-data-9481-76 · prod-eu · us-east-2 · CIS 2.1.4 · AWS FSBP S3.2 · PCI DSS 1.3.1`

core-ingest-dev-data-9481-76 grants access to the internet (AllUsers/AuthenticatedUsers) via its bucket policy.

Critical **MySQL (port 3306) open to the internet** Plan #1

`sg-e1c2b846 · prod-eu · us-east-1 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "payments-api-dev-sg" (sg-e1c2b846) allows inbound traffic to MySQL on port 3306 from 0.0.0.0/0 — the entire IPv4 internet. This is on the AWS list of high-risk ports that should never be reachable from anywhere.

Critical **SSH (port 22) open to the internet** Plan #2

`sg-88d69668 · dev-sandbox · us-east-1 · CIS 5.3 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "ops-report-stg-sg" (sg-88d69668) allows inbound SSH traffic from 0.0.0.0/0, exposing it to the entire IPv4 internet.

Critical **SSH (port 22) open to the internet** Plan #2

`sg-55c8ec43 · staging · us-east-2 · CIS 5.3 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "platform-cache-stg-sg" (sg-55c8ec43) allows inbound SSH traffic from 0.0.0.0/0, exposing it to the entire IPv4 internet.

Critical **RDP (port 3389) open to the internet** Plan #2

`sg-55c8ec43 · staging · us-east-2 · CIS 5.3 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "platform-cache-stg-sg" (sg-55c8ec43) allows inbound RDP traffic from 0.0.0.0/0, exposing it to the entire IPv4 internet.

Critical **SMB/CIFS (port 445) open to the internet** Plan #10

`sg-55c8ec43 · staging · us-east-2 · CIS 5.1.2 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "platform-cache-stg-sg" (sg-55c8ec43) allows inbound SMB/CIFS traffic from 0.0.0.0/0, exposing it to the entire IPv4 internet.

Critical **23 high-risk ports open to the internet (all ports)** Plan #1

`sg-55c8ec43 · staging · us-east-2 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "platform-cache-stg-sg" (sg-55c8ec43) allows inbound all ports from 0.0.0.0/0, which includes FTP data (20), FTP (21), Telnet (23), SMTP (25), POP3 (110), Windows RPC (135), IMAP (143), SQL Server (1433), SQL Server browser (1434), MySQL (3306), mSQL (4333), PostgreSQL (5432), VNC (5500), Kibana (5601), Redis (6379), Elasticsearch (9200), Elasticsearch transport (9300), MongoDB (27017), development web (3000) (3000), development web (5000) (5000), HTTP alternate (8080) (8080), HTTP alternate (8088) (8088), HTTP alternate (8888) (8888). Anything listening on those ports on an attached instance is reachable from the entire IPv4 internet.

Critical **SSH (port 22) open to the internet** Plan #2

`sg-40f7802e · prod-eu · us-west-1 · CIS 5.3 · AWS FSBP EC2.19 · PCI DSS 1.3.1`

Security group "web-billing-dev-sg" (sg-40f7802e) allows inbound SSH traffic from 0.0.0.0/0, exposing it to the entire IPv4 internet.

+55 additional critical finding(s) not listed individually; every affected resource appears in the Remediation Plan and the full list is in the CSV export.

APPENDIX A

High findings (93)

What each finding is and where. The fix for each check is in the Remediation Plan, referenced by number.

High **IAM user "dev.qa-1" has console access without MFA** Plan #12

`arn:aws:iam::101295249481:user/dev.qa-1 · prod-eu · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

dev.qa-1 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "carla.dev-1" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/carla.dev-1 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

carla.dev-1 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "bjorn.ops-3" has console access without MFA** Plan #12

`arn:aws:iam::101278471862:user/bjorn.ops-3 · prod-us · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

bjorn.ops-3 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "gudrun.svc-5" has console access without MFA** Plan #12

`arn:aws:iam::101278471862:user/gudrun.svc-5 · prod-us · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

gudrun.svc-5 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "alice.svc-9" has console access without MFA** Plan #12

`arn:aws:iam::101278471862:user/alice.svc-9 · prod-us · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

alice.svc-9 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "dev.qa-12" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/dev.qa-12 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

dev.qa-12 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "carla.qa-13" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/carla.qa-13 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

carla.qa-13 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "gudrun.svc-18" has console access without MFA** Plan #12

`arn:aws:iam::101295249481:user/gudrun.svc-18 · prod-eu · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

gudrun.svc-18 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "alice.ops-20" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/alice.ops-20 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

alice.ops-20 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "gudrun.qa-21" has console access without MFA** Plan #12

`arn:aws:iam::101278471862:user/gudrun.qa-21 · prod-us · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

gudrun.qa-21 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "gudrun.svc-22" has console access without MFA** Plan #12

`arn:aws:iam::101244916624:user/gudrun.svc-22 · dev-sandbox · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

gudrun.svc-22 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "eva.ops-24" has console access without MFA** Plan #12

`arn:aws:iam::101244916624:user/eva.ops-24 · dev-sandbox · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

eva.ops-24 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "finn.qa-27" has console access without MFA** Plan #12

`arn:aws:iam::101244916624:user/finn.qa-27 · dev-sandbox · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

finn.qa-27 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "ines.svc-35" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/ines.svc-35 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

ines.svc-35 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "gudrun.qa-37" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/gudrun.qa-37 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

gudrun.qa-37 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "bjorn.qa-38" has console access without MFA** Plan #12

`arn:aws:iam::101295249481:user/bjorn.qa-38 · prod-eu · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

bjorn.qa-38 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "carla.svc-38" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/carla.svc-38 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

carla.svc-38 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "dev.data-46" has console access without MFA** Plan #12

`arn:aws:iam::101295249481:user/dev.data-46 · prod-eu · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

dev.data-46 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "finn.ops-50" has console access without MFA** Plan #12

`arn:aws:iam::101261694243:user/finn.ops-50 · staging · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

finn.ops-50 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "ines.ops-53" has console access without MFA** Plan #12

`arn:aws:iam::101278471862:user/ines.ops-53 · prod-us · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

ines.ops-53 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **IAM user "carla.qa-59" has console access without MFA** Plan #12

`arn:aws:iam::101295249481:user/carla.qa-59 · prod-eu · global · CIS 1.9 · AWS FSBP IAM.5 · PCI DSS 8.4.2`

carla.qa-59 can sign in to the AWS Console with just a password — no multi-factor authentication is enrolled.

High **CloudTrail is not recording management events across all regions** Plan #18

`cloudtrail · prod-eu · global · CIS 3.1 · AWS FSBP CloudTrail.1 · PCI DSS 10.2.1`

The account has 1 trail(s), but none is simultaneously multi-region, logging, and capturing all management events (org-trail: does not capture all management events). Without it, API activity in this account cannot be reconstructed after an incident, and most detective controls (GuardDuty, SIEM alerting) have nothing to work from.

High **CloudTrail is not recording management events across all regions** Plan #18

`cloudtrail · staging · global · CIS 3.1 · AWS FSBP CloudTrail.1 · PCI DSS 10.2.1`

The account has 1 trail(s), but none is simultaneously multi-region, logging, and capturing all management events (org-trail: does not capture all management events). Without it, API activity in this account cannot be reconstructed after an incident, and most detective controls (GuardDuty, SIEM alerting) have nothing to work from.

High **GuardDuty is not enabled in 3 of 17 scanned regions** Plan #16

`guardduty · prod-eu · global · AWS FSBP GuardDuty.1 · PCI DSS 11.5.1`

No enabled GuardDuty detector exists in: ap-southeast-1, ap-northeast-3, ap-south-1. Compromised credentials, crypto-mining, and anomalous API activity in those regions go undetected.

High **GuardDuty is not enabled in 6 of 17 scanned regions** Plan #16

`guardduty · prod-us · global · AWS FSBP GuardDuty.1 · PCI DSS 11.5.1`

No enabled GuardDuty detector exists in: us-east-2, ca-central-1, ap-southeast-1, ap-northeast-3, ap-south-1, sa-east-1. Compromised credentials, crypto-mining, and anomalous API activity in those regions go undetected.

+68 additional high finding(s) not listed individually; every affected resource appears in the Remediation Plan and the full list is in the CSV export.

APPENDIX A

Medium findings (357)

What each finding is and where. The fix for each check is in the Remediation Plan, referenced by number.

Medium **IAM password policy does not prevent password reuse** Plan #36

`root · prod-us · global · CIS 1.8 · AWS FSBP IAM.7`

The policy remembers 5 previous passwords; CIS requires 24 so that a rotated password can't simply be set back.

Medium **IAM password policy does not prevent password reuse** Plan #36

`root · staging · global · CIS 1.8 · AWS FSBP IAM.7`

The policy remembers 5 previous passwords; CIS requires 24 so that a rotated password can't simply be set back.

Medium **IAM password policy does not prevent password reuse** Plan #36

`root · dev-sandbox · global · CIS 1.8 · AWS FSBP IAM.7`

The policy remembers 0 previous passwords; CIS requires 24 so that a rotated password can't simply be set back.

Medium **Access key for "dev.qa-1" is 224 days old** Plan #19

`arn:aws:iam::101295249481:user/dev.qa-1 · prod-eu · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA8249915B532ECDF2 on dev.qa-1 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **IAM user "finn.data-1" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101278471862:user/finn.data-1 · prod-us · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **Access key for "gudrun.svc-2" is 229 days old** Plan #19

`arn:aws:iam::101278471862:user/gudrun.svc-2 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA09F5E39BF6DC9DEC on gudrun.svc-2 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "alice.data-2" is 347 days old** Plan #19

`arn:aws:iam::101261694243:user/alice.data-2 · staging · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA7367FB976B803FF7 on alice.data-2 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **IAM user "bjorn.ops-3" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101278471862:user/bjorn.ops-3 · prod-us · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **Access key for "finn.data-5" is 384 days old** Plan #19

`arn:aws:iam::101295249481:user/finn.data-5 · prod-eu · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA98A74247649909EC on finn.data-5 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "gudrun.svc-5" is 443 days old** Plan #19

`arn:aws:iam::101278471862:user/gudrun.svc-5 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA1C70BE5DC4350E26 on gudrun.svc-5 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "alice.svc-6" is 384 days old** Plan #19

`arn:aws:iam::101278471862:user/alice.svc-6 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIAB0E084D5A77E12CD on alice.svc-6 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "eva.dev-7" is 438 days old** Plan #19

`arn:aws:iam::101278471862:user/eva.dev-7 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA3B6966540CC82EA9 on eva.dev-7 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **IAM user "eva.data-8" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101278471862:user/eva.data-8 · prod-us · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **IAM user "carla.svc-9" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101295249481:user/carla.svc-9 · prod-eu · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: access key AKIAE5582BCCDDAB51F4 (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **Access key for "jonas.ops-9" is 359 days old** Plan #19

`arn:aws:iam::101261694243:user/jonas.ops-9 · staging · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIAE188B2FD4B897C2F on jonas.ops-9 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "carla.svc-10" is 334 days old** Plan #19

`arn:aws:iam::101278471862:user/carla.svc-10 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA976805D4F18A2D94 on carla.svc-10 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **Access key for "hakon.dev-12" is 308 days old** Plan #19

`arn:aws:iam::101278471862:user/hakon.dev-12 · prod-us · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA84EA88BF467B672C on hakon.dev-12 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **IAM user "hakon.dev-12" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101278471862:user/hakon.dev-12 · prod-us · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **IAM user "dev.qa-12" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101261694243:user/dev.qa-12 · staging · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **Access key for "alice.data-12" is 98 days old** Plan #19

`arn:aws:iam::101244916624:user/alice.data-12 · dev-sandbox · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA182A2B44F505C55A on alice.data-12 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

Medium **IAM user "finn.dev-13" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101295249481:user/finn.dev-13 · prod-eu · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: access key AKIA9962D4955A9BBAB5 (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **IAM user "carla.qa-13" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101261694243:user/carla.qa-13 · staging · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: access key AKIA5D54B3825232A4EF (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **IAM user "finn.data-16" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101295249481:user/finn.data-16 · prod-eu · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: console password (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **IAM user "hakon.ops-16" has credentials unused for 45+ days** Plan #23

`arn:aws:iam::101261694243:user/hakon.ops-16 · staging · global · CIS 1.11 · AWS FSBP IAM.8`

Unused but still active: access key AKIA7D4E1A65961D8A47 (never used). Dormant credentials are the ones nobody notices when they leak.

Medium **Access key for "finn.qa-16" is 418 days old** Plan #19

`arn:aws:iam::101244916624:user/finn.qa-16 · dev-sandbox · global · CIS 1.13 · AWS FSBP IAM.3 · PCI DSS 8.3.9`

Access key AKIA8822AF0FE058C424 on finn.qa-16 has not been rotated in over 90 days, increasing the blast radius if it has leaked.

+332 additional medium finding(s) not listed individually; every affected resource appears in the Remediation Plan and the full list is in the CSV export.

APPENDIX A Low findings (1220)

What each finding is and where. The fix for each check is in the Remediation Plan, referenced by number.

Low **Root account MFA is a virtual device, not hardware** Plan #68

`root · prod-eu · global · CIS 1.5 · AWS FSBP IAM.6`

The root user's MFA is an app-based virtual device. A phone can be lost, backed up to the cloud, or phished; CIS Level 2 asks for a hardware token for the one identity that can't be permission-limited.

Low **Root account MFA is a virtual device, not hardware** Plan #68

`root · prod-us · global · CIS 1.5 · AWS FSBP IAM.6`

The root user's MFA is an app-based virtual device. A phone can be lost, backed up to the cloud, or phished; CIS Level 2 asks for a hardware token for the one identity that can't be permission-limited.

Low **No security contact is registered for the account** Plan #78

`root · prod-us · global · CIS 1.2 · AWS FSBP Account.1`

AWS sends abuse reports, vulnerability notices and security bulletins to the alternate security contact. Without one, they go to the root email address — often a shared inbox nobody watches.

Low **Root account MFA is a virtual device, not hardware** Plan #68

`root · staging · global · CIS 1.5 · AWS FSBP IAM.6`

The root user's MFA is an app-based virtual device. A phone can be lost, backed up to the cloud, or phished; CIS Level 2 asks for a hardware token for the one identity that can't be permission-limited.

Low **No IAM role or user can open AWS Support cases** Plan #77

`root · dev-sandbox · global · CIS 1.16`

Nothing in the account holds the AWSSupportAccess policy, so during an incident nobody has a ready-made, least-privilege way to engage AWS Support without reaching for root.

Low **IAM user "jonas.qa-0" has policies attached directly** Plan #43

`arn:aws:iam::101295249481:user/jonas.qa-0 · prod-eu · global · CIS 1.14 · AWS FSBP IAM.2`

jonas.qa-0 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "alice.svc-0" has policies attached directly** Plan #43

`arn:aws:iam::101244916624:user/alice.svc-0 · dev-sandbox · global · CIS 1.14 · AWS FSBP IAM.2`

alice.svc-0 carries 1 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "alice.data-2" has 2 active access keys** Plan #51

`arn:aws:iam::101261694243:user/alice.data-2 · staging · global · CIS 1.12`

alice.data-2 holds 2 active access keys (AKIA7367FB976B803FF7, AKIA8FE24EB9B6FC2F72). A second key is meant to exist only briefly, during rotation.

Low **IAM user "alice.svc-3" has policies attached directly** Plan #43

`arn:aws:iam::101261694243:user/alice.svc-3 · staging · global · CIS 1.14 · AWS FSBP IAM.2`

alice.svc-3 carries 2 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "alice.svc-6" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/alice.svc-6 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

alice.svc-6 carries 1 attached and 0 inline policy directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "eva.svc-6" has policies attached directly** Plan #43

`arn:aws:iam::101244916624:user/eva.svc-6 · dev-sandbox · global · CIS 1.14 · AWS FSBP IAM.2`

eva.svc-6 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "finn.dev-7" has policies attached directly** Plan #43

`arn:aws:iam::101295249481:user/finn.dev-7 · prod-eu · global · CIS 1.14 · AWS FSBP IAM.2`

finn.dev-7 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "eva.dev-7" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/eva.dev-7 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

eva.dev-7 carries 1 attached and 0 inline policy directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "hakon.dev-8" has policies attached directly** Plan #43

`arn:aws:iam::101244916624:user/hakon.dev-8 · dev-sandbox · global · CIS 1.14 · AWS FSBP IAM.2`

hakon.dev-8 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "carla.svc-10" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/carla.svc-10 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

carla.svc-10 carries 1 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "alice.dev-11" has policies attached directly** Plan #43

`arn:aws:iam::101244916624:user/alice.dev-11 · dev-sandbox · global · CIS 1.14 · AWS FSBP IAM.2`

alice.dev-11 carries 3 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "hakon.dev-12" has 2 active access keys** Plan #51

`arn:aws:iam::101278471862:user/hakon.dev-12 · prod-us · global · CIS 1.12`

hakon.dev-12 holds 2 active access keys (AKIA6635993C2E21034F, AKIA84EA88BF467B672C). A second key is meant to exist only briefly, during rotation.

Low **IAM user "hakon.dev-12" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/hakon.dev-12 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

hakon.dev-12 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "finn.dev-13" has policies attached directly** Plan #43

`arn:aws:iam::101295249481:user/finn.dev-13 · prod-eu · global · CIS 1.14 · AWS FSBP IAM.2`

finn.dev-13 carries 3 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "bjorn.ops-13" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/bjorn.ops-13 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

bjorn.ops-13 carries 2 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "carla.dev-15" has policies attached directly** Plan #43

`arn:aws:iam::101295249481:user/carla.dev-15 · prod-eu · global · CIS 1.14 · AWS FSBP IAM.2`

carla.dev-15 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "carla.dev-15" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/carla.dev-15 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

carla.dev-15 carries 3 attached and 0 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "finn.qa-16" has policies attached directly** Plan #43

`arn:aws:iam::101244916624:user/finn.qa-16 · dev-sandbox · global · CIS 1.14 · AWS FSBP IAM.2`

finn.qa-16 carries 2 attached and 1 inline policies directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "eva.ops-17" has policies attached directly** Plan #43

`arn:aws:iam::101295249481:user/eva.ops-17 · prod-eu · global · CIS 1.14 · AWS FSBP IAM.2`

eva.ops-17 carries 1 attached and 0 inline policy directly rather than through group membership, which makes permissions harder to review and revoke consistently.

Low **IAM user "carla.ops-17" has policies attached directly** Plan #43

`arn:aws:iam::101278471862:user/carla.ops-17 · prod-us · global · CIS 1.14 · AWS FSBP IAM.2`

carla.ops-17 carries 1 attached and 0 inline policy directly rather than through group membership, which makes permissions harder to review and revoke consistently.

+1195 additional low finding(s) not listed individually; every affected resource appears in the Remediation Plan and the full list is in the CSV export.

APPENDIX A Info findings (88)

What each finding is and where. The fix for each check is in the Remediation Plan, referenced by number.

Info **EC2 instance "web-cache-stg-0 (i-61500e2fb756e2e3c)" has a public IP address** Plan #79

`i-61500e2fb756e2e3c · prod-eu · us-east-1 · AWS FSBP EC2.9`

web-cache-stg-0 (i-61500e2fb756e2e3c) is directly addressable from the internet at 203.0.173.177. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "mobile-api-prod-0 (i-8c57c195bfa6e35d7)" has a public IP address** Plan #79

`i-8c57c195bfa6e35d7 · dev-sandbox · us-east-1 · AWS FSBP EC2.9`

mobile-api-prod-0 (i-8c57c195bfa6e35d7) is directly addressable from the internet at 203.0.66.151. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "core-sync-stg-0 (i-21925f8fcd38adc16)" has a public IP address** Plan #79

`i-21925f8fcd38adc16 · dev-sandbox · us-west-1 · AWS FSBP EC2.9`

core-sync-stg-0 (i-21925f8fcd38adc16) is directly addressable from the internet at 203.0.252.182. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "platform-cache-stg-1 (i-00992174821304739)" has a public IP address** Plan #79

`i-00992174821304739 · prod-us · us-east-2 · AWS FSBP EC2.9`

platform-cache-stg-1 (i-00992174821304739) is directly addressable from the internet at 203.0.215.250. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "web-sync-dev-2 (i-3fbb1e0f023d78584)" has a public IP address** Plan #79

`i-3fbb1e0f023d78584 · prod-eu · us-west-1 · AWS FSBP EC2.9`

web-sync-dev-2 (i-3fbb1e0f023d78584) is directly addressable from the internet at 203.0.63.123. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "data-sync-stg-2 (i-553c136a2f294113b)" has a public IP address** Plan #79

`i-553c136a2f294113b · prod-us · us-west-1 · AWS FSBP EC2.9`

data-sync-stg-2 (i-553c136a2f294113b) is directly addressable from the internet at 203.0.79.162. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "data-worker-stg-2 (i-aa1e30731790693a0)" has a public IP address** Plan #79

`i-aa1e30731790693a0 · staging · us-west-2 · AWS FSBP EC2.9`

data-worker-stg-2 (i-aa1e30731790693a0) is directly addressable from the internet at 203.0.99.173. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "ml-billing-dev-3 (i-7473493b16282469e)" has a public IP address** Plan #79

`i-7473493b16282469e · dev-sandbox · us-west-2 · AWS FSBP EC2.9`

ml-billing-dev-3 (i-7473493b16282469e) is directly addressable from the internet at 203.0.208.215. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "mobile-ingest-dev-4 (i-4f3c09f8a79aa758c)" has a public IP address** Plan #79

`i-4f3c09f8a79aa758c · prod-us · us-west-1 · AWS FSBP EC2.9`

mobile-ingest-dev-4 (i-4f3c09f8a79aa758c) is directly addressable from the internet at 203.0.194.9. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "infra-search-stg-4 (i-7973511a9343a0f69)" has a public IP address** Plan #79

`i-7973511a9343a0f69 · dev-sandbox · us-west-2 · AWS FSBP EC2.9`

infra-search-stg-4 (i-7973511a9343a0f69) is directly addressable from the internet at 203.0.104.205. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "payments-auth-prod-5 (i-2e9a1d571715e6128)" has a public IP address** Plan #79

`i-2e9a1d571715e6128 · prod-eu · us-west-2 · AWS FSBP EC2.9`

payments-auth-prod-5 (i-2e9a1d571715e6128) is directly addressable from the internet at 203.0.52.209. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "ml-ingest-prod-5 (i-8757b9b661c918afb)" has a public IP address** Plan #79

`i-8757b9b661c918afb · dev-sandbox · us-east-1 · AWS FSBP EC2.9`

ml-ingest-prod-5 (i-8757b9b661c918afb) is directly addressable from the internet at 203.0.88.155. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "infra-gateway-stg-5 (i-1c9257b09fc85a962)" has a public IP address** Plan #79

`i-1c9257b09fc85a962 · dev-sandbox · us-west-1 · AWS FSBP EC2.9`

infra-gateway-stg-5 (i-1c9257b09fc85a962) is directly addressable from the internet at 203.0.10.160. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "web-billing-stg-6 (i-3bbb17c385ec97188)" has a public IP address** Plan #79

`i-3bbb17c385ec97188 · prod-eu · us-west-1 · AWS FSBP EC2.9`

web-billing-stg-6 (i-3bbb17c385ec97188) is directly addressable from the internet at 203.0.77.68. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "core-gateway-prod-6 (i-5de49684d78a36c8b)" has a public IP address** Plan #79

`i-5de49684d78a36c8b · staging · us-east-1 · AWS FSBP EC2.9`

core-gateway-prod-6 (i-5de49684d78a36c8b) is directly addressable from the internet at 203.0.162.46. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "payments-ingest-stg-6 (i-ae1e36bffae0092e7)" has a public IP address** Plan #79

`i-ae1e36bffae0092e7 · staging · us-west-2 · AWS FSBP EC2.9`

payments-ingest-stg-6 (i-ae1e36bffae0092e7) is directly addressable from the internet at 203.0.137.12. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "platform-auth-prod-7 (i-5e5009764b36a025c)" has a public IP address** Plan #79

`i-5e5009764b36a025c · prod-eu · us-east-1 · AWS FSBP EC2.9`

platform-auth-prod-7 (i-5e5009764b36a025c) is directly addressable from the internet at 203.0.66.218. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "mobile-web-stg-7 (i-523c0eb14de687ced)" has a public IP address** Plan #79

`i-523c0eb14de687ced · prod-us · us-west-1 · AWS FSBP EC2.9`

mobile-web-stg-7 (i-523c0eb14de687ced) is directly addressable from the internet at 203.0.9.80. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "growth-search-dev-7 (i-ad1e352c1c9d6b65f)" has a public IP address** Plan #79

`i-ad1e352c1c9d6b65f · staging · us-west-2 · AWS FSBP EC2.9`

growth-search-dev-7 (i-ad1e352c1c9d6b65f) is directly addressable from the internet at 203.0.196.160. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "platform-auth-prod-7 (i-1e925ad6678af13ef)" has a public IP address** Plan #79

`i-1e925ad6678af13ef · dev-sandbox · us-west-1 · AWS FSBP EC2.9`

platform-auth-prod-7 (i-1e925ad6678af13ef) is directly addressable from the internet at 203.0.102.212. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "web-billing-prod-8 (i-49bb2dcdcab98cfaa)" has a public IP address** Plan #79

`i-49bb2dcdcab98cfaa · prod-eu · us-west-1 · AWS FSBP EC2.9`

web-billing-prod-8 (i-49bb2dcdcab98cfaa) is directly addressable from the internet at 203.0.151.234. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "payments-notify-dev-8 (i-ec35dfc0eb2b40826)" has a public IP address** Plan #79

`i-ec35dfc0eb2b40826 · dev-sandbox · us-east-2 · AWS FSBP EC2.9`

payments-notify-dev-8 (i-ec35dfc0eb2b40826) is directly addressable from the internet at 203.0.85.160. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "infra-api-stg-9 (i-229a0a733a23913ce)" has a public IP address** Plan #79

`i-229a0a733a23913ce · prod-eu · us-west-2 · AWS FSBP EC2.9`

infra-api-stg-9 (i-229a0a733a23913ce) is directly addressable from the internet at 203.0.200.248. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "ml-cache-dev-11 (i-4b03f457dd11f988a)" has a public IP address** Plan #79

`i-4b03f457dd11f988a · prod-eu · us-east-1 · AWS FSBP EC2.9`

ml-cache-dev-11 (i-4b03f457dd11f988a) is directly addressable from the internet at 203.0.62.7. Inventory only — exposure through its security groups is assessed separately.

Info **EC2 instance "data-worker-prod-11 (i-97890c95754526c4a)" has a public IP address** Plan #79

`i-97890c95754526c4a · staging · us-west-2 · AWS FSBP EC2.9`

data-worker-prod-11 (i-97890c95754526c4a) is directly addressable from the internet at 203.0.16.86. Inventory only — exposure through its security groups is assessed separately.

+63 additional info finding(s) not listed individually; every affected resource appears in the Remediation Plan and the full list is in the CSV export.

APPENDIX B

How the score is calculated

Step 1 — each security property gets its own size-adjusted score

Every finding maps to one or more of Confidentiality, Integrity and Availability; a few "hygiene" findings such as unattached volumes map to none and are handled separately. Within a property, each finding is weighted by severity and expressed as a rate per 100 resources scanned, not a raw count, so the same number of findings scores worse in a small estate than in a large one. The weighted rates are summed, and the property's score is 100 divided by (1 + that sum / 100): a weighted rate of 100 exactly halves the score. This declines gradually as issues accumulate rather than falling off a cliff or letting a couple of findings in a large estate floor the score.

SEVERITY	WEIGHT (POINTS PER 100 RESOURCES SCANNED)
Critical	15
High	8
Medium	3
Low	1
Info	0 (informational only)

Step 2 — the overall score combines the three properties

The headline score is a weighted composite of the three property scores, reduced by a small hygiene penalty for cost and clean-up issues that do not belong to any single property. It is clamped to 0–100 and mapped to a letter grade from A+ to F.

COMPONENT	WEIGHT
Confidentiality score	× 0.40
Integrity score	× 0.35
Availability score	× 0.25
Hygiene penalty (unattached volumes, unassociated IPs and similar)	– points lost, same rate formula

Asset criticality

Each finding's weight is also multiplied by a criticality factor derived from the resource's own AWS tags (Environment, DataClassification) and, for security groups, whether anything is using it: a critical finding on an unattached development security group counts for less than the same finding on a tagged production database. Because this signal is self-reported by the audited account, it is presented separately from the fixed severity weights.

TAG SIGNAL	EFFECT ON WEIGHT
Environment: development, sandbox, demo	× 0.3
Environment: staging, uat, qa, test	× 0.6
Environment: production (or untagged)	× 1.0
Security group not attached to any active network interface	× 0.4 (compounds with environment)
DataClassification: PII, PHI, confidential, sensitive, restricted	× 1.3 (never below neutral)
DataClassification: public	× 0.7

Where a check corresponds to a published control, the finding cites it (CIS AWS Foundations Benchmark v5.0.0 with the v3.0.0 number where it differs, AWS Foundational Security Best Practices, PCI DSS v4.0, and through a documented mapping ISO/IEC 27001:2022, SOC 2, NIST CSF 2.0 and NIS2); checks with no confident published counterpart carry no citation.

APPENDIX C

Scope, method and data handling

Scan type	AWS cloud security posture
Scope	Synthetic organization (4 fabricated account(s), synthetic:12:4x17x1) — demonstration data, not a real AWS environment
Resources audited	4,984
Started	25 September 2026 at 00:09
Completed	25 September 2026 at 00:09
Report generated	25 September 2026 at 00:36

Method

The scan used a read-only set of AWS API calls (Describe, Get and List actions only) with the credentials of the operator who ran it. No AWS resource was modified. Each check evaluated every resource of its type in every scanned region and recorded how many it evaluated and whether it completed, which is the evidence behind the verdicts in section 2.

Data handling

This report was generated by RISKAudit on the machine that ran the scan. The scan results are stored in a local database on that machine and were not transmitted to the vendor or to any third party.

Accounts

ACCOUNT	STATUS	FINDINGS
prod-us 101278471862	Scanned	444
prod-eu 101295249481	Scanned	451
staging 101261694243	Scanned	468
dev-sandbox 101244916624	Scanned	475

APPENDIX D

How to read this report

Finding	One check failing on one resource, with a severity and a recommended fix.
Severity	Critical: exploitable or exposing data now. High: a serious weakness likely to be exploited. Medium: a weakness that needs attention. Low: hygiene or defence-in-depth. Info: inventory only, not scored.
Asset / resource	One AWS object the checks looked at: a bucket, an instance, a user, a security group, an account setting.
Score and grade	A 0–100 posture score derived from the findings, the size of the estate and the criticality of the affected resources (Appendix B), mapped to a letter grade from A+ to F.
Control	One requirement of a published framework, such as CIS recommendation 1.4, "Ensure MFA is enabled for the root user account".
Verdict	The outcome recorded for a control: pass, fail, pass with partial evidence, not evaluated, not applicable, or manual (section 3).
CIS AWS Foundations Benchmark	The most widely used configuration baseline for AWS accounts, published by the Center for Internet Security. Level 1 is the baseline; Level 2 is defence in depth.
AWS Foundational Security Best Practices	AWS's own control set, as used by AWS Security Hub.
ISO/IEC 27001, SOC 2, NIST CSF, NIS2, PCI DSS	Broader security standards and regulations. Only the technical parts of their controls can be evidenced by configuration checks; the mapping used is documented with the product.
Remediation plan	The findings grouped by check, with the generic fix and every affected resource, so one entry fixes one class of problem across the estate.