Vantalect

AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Criticals Closed and Guardrails at the Top

Week 3 of 6: Criticals and guardrails · prepared for StrataForge Robotics, Inc.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

July 31, 2026 · AWS Security, Compliance & Governance Audit: The Hardening (six weeks)

SAMPLE DELIVERABLE

This is a sample deliverable. StrataForge Robotics, Inc. is a fictional company: every account, resource, finding, figure, and person in this report is simulated to show the form and depth of a Vantalect engagement. AWS prices are list prices from the AWS Price List API on October 13, 2026.

Contents

Summary ... 2

What closed this week ... 5

The critical findings, closed as code ... 7

SF-SEC-001: A 1,127–day-old IAM user key can sign and publish firmware to every robot ... 8

SF-SEC-003: 4 GitHub Actions deploy roles can be assumed from any GitHub repository ... 10

SF-SEC-004: Jupyter is open to the internet on 51 research and sandbox instances, some with no token ... 11

SF-SEC-005: 5 EBS snapshots in kestrel-prod are public, and snapshot block public access is off in all 816 account-Regions ... 12

SF-SEC-006: 4 Kestrel dataset buckets are public: 468.8 million objects of labeled images from customer sites ... 14

SF-SEC-007: A Kestrel MySQL snapshot with annotation records is restorable by any AWS account 15

SF-SEC-008: Kestrel's Jenkins controller is open to the internet on 8080 and 22 ... 16

SF-SEC-009: RDP is open to the internet on 32 PLM CAD workstations that hold product designs ... 18

SF-SEC-010: Root users of 3 Kestrel accounts have access keys and no MFA ... 19

The critical we accepted in writing ... 20

The acceptance, as it will be signed ... 21

Guardrails at the top of the organization ... 22

Service control policies ... 24

The resource control policy ... 25

The EC2 declarative policies ... 26

StackSet account defaults ... 28

How we know they work ... 29

Exceptions, and how they are governed ... 30

Pull request ledger ... 31

Summary

In week 3 we closed **9 of the 10 critical findings** as code, and wrote the tenth down as an acceptance the sponsor and the CTO can sign. That is 27 pull requests in all four repositories, merged between July 27, 2026 and July 31, 2026, each read as code in the twice-weekly change

review and approved by the engineer who owns the account. They closed 19 findings in all: 9 critical, 6 high, 1 medium, and 3 low. Nothing was fixed by hand in a console that is not also in a repository or a scripted runbook with a ticket.

The tenth critical, SF-SEC-002, is the one thing we could not finish in a week and will not pretend we did. 3,412 robots in the field run firmware that cannot use the new per-robot policy until the update reaches each customer's maintenance window. We moved every other robot to the new policy and restricted the legacy one to telemetry; the residual risk, its compensating controls, and its expiry on December 15, 2026 are written out in The critical we accepted in writing for signature.

The second half of the week went into **guardrails at the top of the organization** (Deliverable 9): 5 service control policies, 1 resource control policy, 2 EC2 declarative policies, plus the first 2 of 4 StackSet account defaults (the other 2 merge in weeks 4 and 5). They are why what closed this week stays closed, and Guardrails at the top of the organization says, for each one, which findings it protects.

Where the code is. This report says what changed, why, and how we proved it. The complete code for every fix (the CDK, the policies, the commands, and the rollback steps) is in the Audit Report Appendix, the sample report `strataforge-security-2-appendix`, under the same finding ID. Each section below names the ID to open.

Week 3 in numbers. The week-6 re-scan, run the same way as the week-one scan, decides which findings count as closed for the guarantee.

Week 3 at a glance	Result
Critical findings in the register	10
Closed as code this week	9
Accepted in writing, for signature	1
Findings closed this week, all severities	19
Pull requests merged	27
Pull requests in `platform-landing-zone`	12
Pull requests in `fleet-infra`	10
Pull requests in `crucible-infra`	4
Pull requests in `enterprise-infra`	1
Week-3 findings with a pull request merged and a remainder still open	5

Week 3 at a glance	Result
Organization-wide guardrails in place	8 policies, 2 of 4 StackSet defaults

Decision for the sponsor

Marcus Oyelaran, Chief Information Security Officer, and Priya Raman, Chief Technology Officer: read the acceptance in The critical we accepted in writing and tell Elena Vasquez by the end of week 4 whether you intend to sign it; the signatures are due before the week-6 re-scan. If you would rather not, SF-SEC-002 stays open and is not counted as closed under the guarantee, which means the remaining 3,412 robots must be updated before the re-scan. We do not think that can be done safely. A signed acceptance is a decision to carry a known risk for a stated time, with the controls below; it is not a way to make a finding disappear.

What closed this week

Every row is a finding whose fix merged this week and whose original failed checks we re-ran. A finding is closed only when its pull requests have merged and none of the checks that failed in the week-one scan still fails on the resources it named. The week-6 re-scan repeats that test across the whole organization.

The findings closed in week 3, with the pull requests that fixed them and the day the last one merged. SF-SEC-009 counts security groups; its title counts the workstations behind them.

ID	Severity	Finding	Owner	Pull requests	Closed
SF-SEC-001	Critical	A 1,127-day-old IAM user key can sign and publish firmware to every robot	Sam Okafor	`fleet-infra#4323`, `fleet-infra#4328`	Jul 28
SF-SEC-003	Critical	4 GitHub Actions deploy roles can be assumed from any GitHub repository	Elena Vasquez	`fleet-infra#4340`	Jul 27
SF-SEC-004	Critical	Jupyter is open to the internet on 51 research and sandbox instances, some with no token	Hiro Tanaka	`crucible-infra#1987`	Jul 28
SF-SEC-005	Critical	5 EBS snapshots in kestrel-prod are public, and snapshot block public access is off in all 816 account-Regions	Jonah Reyes	`platform-landing-zone#613`	Jul 27
SF-SEC-006	Critical	4 Kestrel dataset buckets are public: 468.8 million objects of labeled images from customer sites	Jonah Reyes	`crucible-infra#1992`	Jul 28
SF-SEC-007	Critical	A Kestrel MySQL snapshot with annotation records is restorable by any AWS account	Jonah Reyes	`crucible-infra#1982`	Jul 27
SF-SEC-008	Critical	Kestrel's Jenkins controller is open to the internet on `8080` and 22	Jonah Reyes	`crucible-infra#1996`	Jul 28
SF-SEC-009	Critical	RDP is open to the internet on 32 PLM CAD workstations that hold product designs (3 security groups)	Mei Chen	`enterprise-infra#905`	Jul 28
SF-SEC-010	Critical	Root users of 3 Kestrel accounts have access keys and no MFA	Grace Liu	`platform-landing-zone#619`	Jul 28

ID	Severity	Finding	Owner	Pull requests	Closed
SF-SEC-011	High	docs-legacy.strataforge.example points at a deleted S3 website bucket that anyone can claim	Elena Vasquez	`platform-landing-zone#620`	Jul 29
SF-SEC-021	High	The staging OTA test key lets the production pipeline sign, and pilot robots still trust it	Sam Okafor	`fleet-infra#4346`	Jul 29
SF-SEC-024	High	S3 Block Public Access is off at the account level in 31 accounts and on 47 buckets	Elena Vasquez	`platform-landing-zone#629`	Jul 29
SF-SEC-026	High	Service control policies stop nothing: only FullAWSAccess and DenyLeaveOrganization are attached	Elena Vasquez	`platform-landing-zone#633`	Jul 29
SF-SEC-027	High	SSH bastions accept connections from the whole internet	Elena Vasquez	`platform-landing-zone#625`	Jul 29
SF-SEC-028	High	SSH is open to the internet on 76 development instances	Sam Okafor	`fleet-infra#4352`	Jul 30
SF-SEC-041	Medium	SSH and RDP are open to the internet on 27 sandbox instances	Elena Vasquez	`platform-landing-zone#649`	Jul 31
SF-SEC-050	Low	Account baseline gaps: no security contact in 42 accounts, no support role in 20, CloudShell full access on 195 identities	Elena Vasquez	`platform-landing-zone#658`	Jul 31
SF-SEC-052	Low	220 buckets accept requests without TLS	Elena Vasquez	`platform-landing-zone#655`	Jul 31
SF-SEC-053	Low	78 customer managed keys do not rotate	Elena Vasquez	`platform-landing-zone#652`	Jul 31

5 more findings had work merged this week and are not yet closed. Each has a remainder that waits on a maintenance window, an upgrade, or a customer, and each has an owner and a date.

Week-3 work that merged but did not close its finding.

ID	Severity	Finding	Pull requests	What remains	Owner	Due
SF-SEC-002	Critical	One IoT policy lets any of 61,400 robots' certificates publish to any robot's command topic	`fleet-infra#4329`, `fleet-infra#4332`, `fleet-infra#4336`	The acceptance in the next section	Sam Okafor	Jul 31
SF-SEC-016	High	All 16 EKS cluster API endpoints accept connections from 0.0.0.0/0	`fleet-infra#4351`	Make the non-production endpoints private once CI runners reach them through the Transit Gateway	Sam Okafor	Sep 30
SF-SEC-030	High	23 robot certificates are shared by 1,840 robots at 3 customer sites	`fleet-infra#4357`	Re-provision the robots at the Bremen and Ota sites during their maintenance windows	Sam Okafor	Sep 30
SF-SEC-014	High	1,631 instances still allow IMDSv1	`platform-landing-zone#639`	Switch the instances that still make IMDSv1 calls after their agents and SDKs are upgraded	Elena Vasquez	Oct 30
SF-SEC-032	Medium	EBS encryption by default is off in 762 account-Regions; 1,245 volumes are unencrypted	`platform-landing-zone#644`	Migrate the remaining unencrypted volumes through encrypted snapshot copies	Elena Vasquez	Dec 18

The critical findings, closed as code

Deliverable 8 is the 9 sections that follow, in the order of the register. Each gives the evidence behind the rating, the pull requests, the order of the change, how we proved it, and how to undo it. The code itself is in the Audit Report Appendix under the finding ID.

We held the same rollout rule for every fix. Where an account has a non-production twin, the change went there first. Policies that apply to many accounts went to the Sandbox OU, then the non-production Fleet OU, and reached the root of the organization only after 24 hours with no denied calls in CloudTrail that a pipeline or a person needed.

SF-SEC-001: A 1,127-day-old IAM user key can sign and publish firmware to every robot

Critical. Owner: Sam Okafor, Director, Fleet Cloud Engineering. Repository: `fleet-infra`. Closed July 28, 2026. Scope: 1 IAM user in 1 account.

Why it is critical. The benchmark rates this Medium (Security Hub CSPM IAM.3 on the key; raised for blast radius and safety). We rated it Critical on exploitability and blast radius: One leaked key is enough: no MFA, source-IP, or VPC-endpoint condition, and the key has been copied to two laptops. A signed image in the distribution bucket reaches all 212,000 connected robots. It can also put a physical robot at risk, which raises the rating by itself.

What we found.

- Credential report: ota-signing-ci, access key created 06/14/2023 (1,127 days), last used the day before the scan (kms:Sign, us-east-1).
- Attached policy allows kms:Sign on alias/ota-firmware-signing-prod (ECC_NIST_P384) and s3:PutObject on sf-ota-ota-images-5117-us-east-1-000/releases/*.
- CloudTrail (90 days): Sign calls from GitHub-hosted runners and from two engineer laptops in June 2026.
- Robots verify the signature only; nothing checks who produced the build or whether a second person approved it.

What merged.

The pull requests behind SF-SEC-001. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`fleet-infra#4323`	OTA: sign releases with ota-release-signer via GitHub OIDC (two-person approval)	Sam Okafor	Jul 27
`fleet-infra#4328`	OTA: alarm on kms:Sign by any principal but the signer; deactivate the ota-signing-ci key	Sam Okafor	Jul 28

How the change was made, in order.

1. Create the GitHub environment `production` on `strataforge/ota-release` with two required reviewers, `prevent_self_review`, and a deployment branch policy that allows only `main`. GitHub needs one approval, and self-review prevention makes the approver a second person, which is the two-person rule.

2. Deploy the CDK stack that creates `ota-release-signer` (kms:Sign only, ECDSA_SHA_384) and `ota-release-publisher` (s3:PutObject on `releases/*` only), both trusting only `repo:strataforge/ota-release:environment:production`.
3. Change the release workflow to assume the signer role for the signing job and the publisher role for the upload job, with `id-token: write` and no stored AWS secrets.
4. Look up the key ID with `describe-key` (`put-key-policy` takes a key ID or key ARN, never an alias) and save the current key policy to the change record. Then apply the new key policy so kms:Sign is denied to everyone except the signer role.
5. Create the EventBridge rule in the key's Region with state `ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS`, because Sign is a read-only management event and an ordinary `ENABLED` rule never sees it, and add the target that pages the security team. Confirm one full release signs and publishes.
6. Deactivate the user's access key, wait one release cycle, then delete the key and the user.

The code. Appendix, SF-SEC-001: "Signer and publisher roles trusted only by the production environment"; "Key policy for alias/ota-firmware-signing-prod: only the signer role may call Sign"; "ota-unexpected-sign-pattern.json: page on any Sign call that did not come from the signer role"; "Require two reviewers, save and apply the key policy, add the Sign alarm, then retire the old key".

How we proved it.

- `aws iam list-access-keys --user-name ota-signing-ci` shows the key Inactive in fleet-ota-prod; after the next clean release the key and the user are deleted (the last step), and `aws iam get-user` then returns NoSuchEntity.
- A release run assumes both roles with no stored AWS secret, and CloudTrail shows every Sign call under `assumed-role/ota-release-signer`.
- A test kms:Sign call from any other role, an administrator included, is denied and raises the EventBridge page (check the rule's `State` is `ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS`).

How to undo it. Until the old key is deleted (after the next clean release), `aws iam update-access-key --user-name ota-signing-ci --access-key-id <key-id> --status Active` restores it, and the pull requests revert cleanly. We recommend neither. If the GitHub environment is unavailable on a release day, the release waits: we deliberately left no second signer, because a second signer is the weakness this finding was about.

SF-SEC-003: 4 GitHub Actions deploy roles can be assumed from any GitHub repository

Critical. Owner: Elena Vasquez, Vice President, Cloud Platform. Repository: `fleet-infra`. Closed July 27, 2026. Scope: 4 IAM roles in 4 accounts.

Why it is critical. The benchmark rates this High (Vantalect baseline; IAM Access Analyzer reports the federated principal as external access). We rated it Critical on exploitability and blast radius: Any GitHub user can mint a token with audience sts.amazonaws.com from their own workflow. gha-artifact-publisher pushes the images every workload account deploys.

What we found.

- Trust policies condition only on token.actions.githubusercontent.com:aud = sts.amazonaws.com.
- Created in 2022 before StrataForge's CDK construct for GitHub roles existed; 33 later roles pin sub correctly.

What merged.

The pull requests behind SF-SEC-003. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`fleet-infra#4340`	CI: pin sub to repository and environment on four GitHub Actions roles	Elena Vasquez	Jul 27

How the change was made, in order.

1. List the repository and environment each role really serves, from 90 days of AssumeRoleWithWebIdentity events.
2. Write one trust policy per role with `aud` equal to `sts.amazonaws.com` and `sub` pinned with StringEquals (no wildcards).
3. Protect each GitHub environment (required reviewers for production) so the `environment` claim means something.
4. The four roles already exist, and CloudFormation cannot create a role whose name is taken, so first bring them under the stack with `cdk import` (the stack sets `RemovalPolicy.RETAIN` on each role, which an import requires); then `cdk deploy` writes the pinned trust policies. Save each role's current trust policy (`aws iam get-role --query Role.AssumeRolePolicyDocument`) before the import. Use the CLI command only for an emergency change, and reconcile the stack afterward.

5. Run each deploy workflow once and confirm it assumes the role; run a workflow from a scratch repository and confirm AccessDenied.

The code. Appendix, SF-SEC-003: “Trust policy for gha-deploy-fleet-api”; “One loop for all four roles, each pinned to its repository and environment”; “Find real callers, import the existing roles, apply an emergency trust change, and read it back”.

How we proved it.

- Every trust policy shows both `:aud` and `:sub` conditions with StringEquals and no `*`.
- A workflow in a repository outside `strataforge` fails with `Not authorized to perform sts:AssumeRoleWithWebIdentity`.
- The production deploy workflow still succeeds, and CloudTrail shows its subject as `repo:strataforge/fleet-api:environment:production`.

How to undo it. Revert the pull request and redeploy the stack. In an emergency, run `aws iam update-assume-role-policy` with the previous document and reconcile the stack afterward. A deploy that fails with AccessDenied after this change means the workflow runs from a repository or environment the role does not name: add that exact name to the role in the CDK app, never a wildcard.

SF-SEC-004: Jupyter is open to the internet on 51 research and sandbox instances, some with no token

Critical. Owner: Hiro Tanaka, Director, Crucible Platform. Repository: `crucible-infra`. Closed July 28, 2026. Scope: 51 instances in 4 accounts.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM EC2.19). We rated it Critical on exploitability and blast radius: Nine instances were launched with an empty notebook token: anyone reaching `8888` runs code. Instance roles read the Crucible sensor-log lake and Kestrel model artifacts over IMDSv1.

What we found.

- 6 security groups admit 0.0.0.0/0 on `8888` (and 22).
- User data on 9 instances sets NotebookApp.token to an empty string.

What merged.

The pull requests behind SF-SEC-004. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`crucible-infra#1987`	Research: close 8888 and 22; notebooks through Session Manager port forwarding	Hiro Tanaka	Jul 28

How the change was made, in order.

1. Revoke the 8888 rules open to the internet in every account and Region.
2. Stop notebook servers that run with an empty token, and check their instance profiles and home directories for credentials; rotate anything found.
3. Review CloudTrail for the instance roles of the open notebooks for activity the researchers did not run.
4. Give researchers a Session Manager port-forwarding command for the servers they must keep.
5. Create a SageMaker AI Studio domain in private subnets for the rest, with an execution role scoped to the research data.

The code. Appendix, SF-SEC-004: “Revoke port 8888 from the internet in a Region”; “Reach a notebook server through Session Manager”; “SageMaker AI Studio domain with no internet-facing access”.

How we proved it.

- `aws ec2 describe-security-groups --filters Name=ip-permission.from-port,Values=8888 Name=ip-permission.cidr,Values=0.0.0.0/0` returns nothing in every account and Region.
- Security Hub CSPM EC2.19 passes after the next evaluation.
- A scan from outside the VPC finds nothing listening on port 8888 at any of the old addresses.

How to undo it. Revert the pull request to bring a port back, and then restrict it to the corporate range with `aws ec2 authorize-security-group-ingress`; never to `0.0.0.0/0`. Researchers who lose a direct connection use a Session Manager port-forwarding session instead.

SF-SEC-005: 5 EBS snapshots in kestrel-prod are public, and snapshot block public access is off in all 816 account-Regions

Critical. Owner: Jonah Reyes, Director, Perception Platform (formerly Kestrel Vision). Repository: `platform-landing-zone`. Closed July 27, 2026. Scope: 5 EBS snapshots in 48 accounts.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM EC2.1 and EC2.182). We rated it Critical on exploitability and blast radius: Any AWS account can create a volume from a public snapshot. Volumes of the Kestrel perception API hosts, including application configuration.

What we found.

- describe-snapshot-attribute createVolumePermission: Group all.
- All of them are unencrypted: AWS does not allow an encrypted snapshot to be shared publicly, so encryption is not what stands between these and the internet.
- get-snapshot-block-public-access-state: unblocked in every Region of every account.

What merged.

The pull requests behind SF-SEC-005. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`platform-landing-zone#613`	EC2 declarative policy: snapshot and AMI block public access; unshare Kestrel snapshots	Jonah Reyes	Jul 27

How the change was made, in order.

1. Find public snapshots in each Region of kestrel-prod and record what each contains.
2. Remove the `all` group from each snapshot's createVolumePermission.
3. Enable snapshot block public access with `block-all-sharing` in each Region; note that switching it back to `block-new-sharing` would make existing public snapshots public again.
4. Enable the declarative policy type, create the EC2 policy, and attach it to the root.
5. Treat the contents as disclosed until the owning team confirms otherwise.

The code. Appendix, SF-SEC-005: "Find and unshare public snapshots, then block sharing per Region"; "sf-ec2-block-public-sharing: no public snapshots, no new public AMIs"; "Enable the policy type, create the policy, and attach it to the root".

How we proved it.

- `aws ec2 describe-snapshots --owner-ids self --restorable-by-user-ids all` returns nothing in every Region of kestrel-prod.
- `aws ec2 get-snapshot-block-public-access-state` returns `block-all-sharing`.
- Security Hub CSPM EC2.182 passes in every account after the next evaluation.

How to undo it. Do not roll this back. Detaching the declarative policy returns each attribute to its previous state, which turns snapshot block public access off in every account. A team that needs to share a snapshot shares it with a named account ID, which block-all-sharing still allows. Re-sharing a snapshot with everyone is exactly the act this control exists to stop.

SF-SEC-006: 4 Kestrel dataset buckets are public: 468.8 million objects of labeled images from customer sites

Critical. Owner: Jonah Reyes, Director, Perception Platform (formerly Kestrel Vision). Repository: `crucible-infra`. Closed July 28, 2026. Scope: 4 S3 buckets in 1 account.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM S3.2). We rated it Critical on exploitability and blast radius: Anyone on the internet can list and download them. 361 TB of images from customer sites; about 4% of a 200-image sample show people or badge IDs.

What we found.

- Bucket policy grants s3:GetObject and s3:ListBucket to "Principal": "*"; bucket and account Block Public Access off.
- Server access logging is off, so the only record of downloads is the organization trail's S3 data events, which cover these buckets only since the Kestrel accounts joined in November 2025.
- The buckets fed a 2024 public benchmark that Kestrel withdrew; public access was never turned off.

What merged.

The pull requests behind SF-SEC-006. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`crucible-infra#1992`	Perception: import the dataset buckets into CDK; private with Block Public Access	Jonah Reyes	Jul 28

How the change was made, in order.

1. Save each bucket's policy, ACL, and public access block settings to the incident folder as evidence before changing anything.
2. Turn on all four S3 Block Public Access settings on each bucket; that stops public reads at once without touching the objects.
3. Delete the public bucket policy, set the bucket ACL to private, and switch object ownership to BucketOwnerEnforced so ACLs stop working.
4. Put the TLS-only policy on each bucket; access for the Crucible training roles comes from their IAM policies, so the bucket policy needs no Allow.

5. Work out the exposure window: the organization trail has recorded S3 data events for these buckets since the Kestrel accounts joined in November 2025; before that, only the bucket creation dates are known. Give Legal the list of datasets and the outside IP addresses that read them.
6. Turn on server access logging for these buckets (see s3-logging) and move them into the crucible-infra CDK app with `cdk import`.

The code. Appendix, SF-SEC-006: "Evidence, then close the public buckets"; "tls-only.json: the TLS-only policy (the only Deny a bucket policy may carry)"; "The bucket as code in crucible-infra".

How we proved it.

- `aws s3api get-public-access-block` shows all four settings true on each of these buckets (Security Hub CSPM S3.1, S3.8).
- An anonymous `curl` of a known object URL returns 403.
- `aws s3api get-bucket-policy-status` reports `IsPublic` false and the ACL grants nothing to AllUsers or AuthenticatedUsers.

How to undo it. The evidence copy of each bucket policy and ACL, saved before the first change, could restore the old state. Doing so would publish labeled images from customer sites again, so we do not recommend it. A researcher who needs a dataset gets an IAM policy on the Crucible training role, or a presigned URL with an expiry.

SF-SEC-007: A Kestrel MySQL snapshot with annotation records is restorable by any AWS account

Critical. Owner: Jonah Reyes, Director, Perception Platform (formerly Kestrel Vision). Repository: `crucible-infra`. Closed July 27, 2026. Scope: 1 DB snapshot in 1 account.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM RDS.1). We rated it Critical on exploitability and blast radius: Any AWS account can restore it into its own database. Annotator identities and customer-site labels for 1.9 million images.

What we found.

- describe-db-snapshot-attributes: restore = all.
- Unencrypted MySQL 5.7 snapshot taken 10/28/2025 before a migration.

What merged.

The pull requests behind SF-SEC-007. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`crucible-infra#1982`	Perception: unshare the annotations snapshot; snapshot-sharing SCP exception list	Jonah Reyes	Jul 27

How the change was made, in order.

1. Remove the `all` value from the snapshot's `restore` attribute in every Region where it exists.
2. Ask the Perception Platform team whether the snapshot is still needed; if so, copy it with a customer managed key and delete the original after a hold.
3. Treat the data as disclosed for the time it was shared, and give Legal the date range from the snapshot creation date.
4. Attach `sf-protect-account-defaults` (see scp-guardrails); its ProtectRdsSnapshotSharing statement lets only the platform roles change snapshot sharing.
5. Deploy the Config rule that reports any public snapshot.

The code. Appendix, SF-SEC-007: "Remove public sharing and read the attribute back"; "sf-protect-account-defaults, statement ProtectRdsSnapshotSharing: only the platform roles may change snapshot sharing (the whole policy is in the guardrail SCPs)"; "Config rule that reports public RDS snapshots (RDS.1)".

How we proved it.

- `describe-db-snapshot-attributes` shows an empty `restore` attribute value list.
- `rds:ModifyDBSnapshotAttribute` from an ordinary administrator role is denied by `sf-protect-account-defaults`.
- Security Hub CSPM RDS.1 passes in kestrel-prod after the next evaluation.

How to undo it. The attribute can be set again only by the platform role. Share the snapshot with a named account with `aws rds modify-db-snapshot-attribute --attribute-name restore --values-to-add <account-id>`, never with `all`.

SF-SEC-008: Kestrel's Jenkins controller is open to the internet on `8080` and 22

Critical. Owner: Jonah Reyes, Director, Perception Platform (formerly Kestrel Vision). Repository: `crucible-infra`. Closed July 28, 2026. Scope: 1 instance in 1 account.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM EC2.19). We rated it Critical on exploitability and blast radius: Jenkins 2.3× with anonymous read of job configuration; the instance allows IMDSv1. Jenkins holds the Kestrel CI keys and a root access key for kestrel-legacy-mgmt.

What we found.

- Security group admits 0.0.0.0/0 on `8080` and 22; public IPv4 address attached.
- Credentials store holds 31 AWS access keys, including the kestrel-legacy-mgmt root key.

What merged.

The pull requests behind SF-SEC-008. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`crucible-infra#1996`	Perception CI: Jenkins behind an internal ALB with Okta sign-in; rotate stored keys	Jonah Reyes	Jul 28

How the change was made, in order.

1. Revoke the 0.0.0.0/0 rules on ports `8080` and 22 today, and require IMDSv2 on the instance.
2. Treat every credential stored in Jenkins as exposed: list the credentials store, the AWS keys, GitHub tokens, and SSH keys, and rotate each one.
3. Check CloudTrail for the Jenkins instance profile and any IAM user keys it holds for unfamiliar activity since the ports were opened.
4. Move the jobs to GitHub Actions with OIDC roles (see oidc-trust-sub), and shut down the controller when the last job has moved.
5. If the controller must stay for a while, put it behind an internal ALB that authenticates with Okta through OIDC, and allow ports only from the ALB.

The code. Appendix, SF-SEC-008: “Close the ports, require IMDSv2, and list the credentials to rotate”; “Internal ALB that signs people in with Okta before reaching Jenkins”.

How we proved it.

- `aws ec2 describe-security-groups --group-ids <jenkins-security-group-id>` shows no rule open to 0.0.0.0/0 or ::/0.
- `aws ec2 describe-instances` shows `HttpTokens` required for `i-0b89690e9c5782dbe` (Security Hub CSPM EC2.8).
- Every credential in the Jenkins credentials store has a rotation record, and the old values are rejected by their services.

How to undo it. Revert the pull request to reach the old address. If Okta sign-in breaks, use a Session Manager port-forwarding session to the controller rather than reopening `8080` to the internet.

SF-SEC-009: RDP is open to the internet on 32 PLM CAD workstations that hold product designs

Critical. Owner: Mei Chen, Director, Enterprise Applications. Repository: `enterprise-infra`. Closed July 28, 2026. Scope: 3 security groups in 1 account (the finding counts security groups, and its title counts the workstations attached to them).

Why it is critical. The benchmark rates this Critical (Security Hub CSPM EC2.19, EC2.53, EC2.54, and EC2.18). We rated it Critical on exploitability and blast radius: RDP brute force and credential stuffing against Windows hosts. Product designs for every robot line.

What we found.

- 3 security groups admit 0.0.0.0/0 on port `3389`; 32 instances attached.
- 0 also admit ::/0.

What merged.

The pull requests behind SF-SEC-009. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`enterprise-infra#905`	Network: remove 0.0.0.0/0 and ::/0 ingress on 22 and `3389` in plm-prod	Mei Chen	Jul 28

How the change was made, in order.

1. Find every security group rule that opens 22 or `3389` to **`0.0.0.0/0`** or **`::/0`** in each account and Region.
2. Attach the Systems Manager managed instance role to the affected instances and confirm each shows as a managed node.
3. Revoke the open rules, IPv4 and IPv6 both, and keep a copy of each rule for rollback.
4. Give engineers `ssm:StartSession` on tagged instances through their permission set, and RDP users a port-forwarding session or Fleet Manager remote desktop.
5. Change the CDK security group constructs so no construct can open an administration port to the internet, then remove the bastion hosts that Session Manager replaces.

The code. Appendix, SF-SEC-009: “Find and revoke the open rules in one Region”; “Instance with the Systems Manager role and no inbound rules”; “Reach SSH and RDP through Session Manager”.

How we proved it.

- `aws ec2 describe-security-groups --filters Name=ip-permission.from-port,Values=22,3389 Name=ip-permission.cidr,Values=0.0.0.0/0` returns nothing in every Region, and the same for `ip-permission.ipv6-cidr` with `::/0`.
- Security Hub CSPM EC2.53, EC2.54, EC2.19, and EC2.18 pass after the next evaluation.
- Engineers reach each instance through Session Manager, and the session appears in the audit log.

How to undo it. Revert the pull request, then add a temporary rule for one named address, expiring the same day. Session Manager and Fleet Manager remote desktop cover every use that needed the open ports, so a rollback should be rare.

SF-SEC-010: Root users of 3 Kestrel accounts have access keys and no MFA

Critical. Owner: Grace Liu, Manager, Identity and Access. Repository: `platform-landing-zone`. Closed July 28, 2026. Scope: 3 root users in 3 accounts.

Why it is critical. The benchmark rates this Critical (Security Hub CSPM IAM.4). We rated it Critical on exploitability and blast radius: A root key used by a Jenkins job last month lives in Jenkins' credential store. Root of kestrel-prod and kestrel-data, which hold the perception APIs and the labeled datasets.

What we found.

- get-account-summary: AccountAccessKeysPresent = 1 and AccountMFAEnabled = 0 in 3 accounts.
- Most recent root key use: 06/30/2026 (kestrel-legacy-mgmt).
- Centralized root access management is not enabled for the organization.

What merged.

The pull requests behind SF-SEC-010. The full ledger, with files and rollout, is in Pull request ledger.

Pull request	Title	Reviewer	Merged
`platform-landing-zone#619`	Root: centralized root access management; delete member root credentials	Grace Liu	Jul 28

How the change was made, in order.

1. From the management account, enable trusted access for IAM, then root credentials management and root sessions.

2. Audit each member account's root credentials with a short root session using the IAMAuditRootUserCredentials task policy.
3. Delete the root login profile, access keys, signing certificates, and MFA devices in each member account with the IAMDeleteRootUserCredentials task policy.
4. Deploy the EventBridge rule for sts:AssumeRoot so every root session pages the security team.
5. Register a FIDO2 hardware key on the management account root user in the console, remove the virtual device, and keep a second key at the second site.
6. Apply the member-account root deny SCP (see scp-guardrails) only after this cleanup finishes.

The code. Appendix, SF-SEC-010: "Enable centralized root access management (management account)"; "Audit, then delete one member account's root credentials"; "Page on every root session started through sts:AssumeRoot".

How we proved it.

- `aws iam list-organizations-features` lists RootCredentialsManagement and RootSessions.
- In each member account, `aws iam get-account-summary` shows AccountAccessKeysPresent 0 (Security Hub CSPM IAM.4) and the root login profile is gone.
- Security Hub CSPM controls IAM.4, IAM.9, and IAM.6 pass in the management account once the hardware key is registered.

How to undo it. Deleted root credentials cannot be restored, and nothing needs them. A member account that someone must open as root can be recovered on demand: lift `sf-deny-member-root` for that account first, start a root session with `aws sts assume-root` and the `IAMCreateRootUserPassword` task policy, and complete the password reset. Starting a root session pages the security team.

The critical we accepted in writing

SF-SEC-002: One IoT policy lets any of 61,400 robots' certificates publish to any robot's command topic

Every robot's certificate used to carry one IoT policy that allowed all actions on all resources, so one stolen certificate could read from, publish to, or command any robot. In week 3 we created `sf-robot-scoped-v2`, which limits each robot to its own client ID, topics, shadow, and jobs, and moved the thing groups to it in waves (`fleet-infra#4329`, `fleet-infra#4332`). Device Defender now audits the policy daily in all four IoT Regions (`fleet-infra#4336`), so a permissive policy is

found again if it returns. The robots we could not move are the ones whose firmware still publishes in the old `sf/v1/<thing>` topic layout and cannot use the new one. Their certificates now carry a restricted legacy policy, `sf-robot-legacy-v1-restricted`, which lets each robot use only its own `sf/v1/<thing>` topics, its shadow, and its jobs (the jobs deliver the firmware update), and denies every command topic. The per-robot policy and the rollout commands are in the Audit Report Appendix under SF-SEC-002.

The acceptance, as it will be signed

Risk acceptance for SF-SEC-002

Accepted by: Marcus Oyelaran, Chief Information Security Officer, and Priya Raman, Chief Technology Officer.

Expires: December 15, 2026. After that date the finding is open again unless the signers renew it in writing.

Scope: 3,412 ForgeArm gen-2 robots on firmware 3.x, at customer sites, that cannot use the v2 topic layout until firmware 4.2 is installed in each customer's maintenance window.

Statement: StrataForge accepts, until December 15, 2026, the residual risk that a certificate taken from one of the 3,412 ForgeArm gen-2 robots still on firmware 3.x can publish and subscribe to that one robot's own telemetry, shadow, and jobs topics in the legacy sf/v1 layout. It cannot reach another robot's topics, and no robot certificate can reach a command topic. Firmware 4.2 will be installed in each customer's scheduled maintenance window, after which the robot moves to sf-robot-scoped-v2 and the legacy policy is deleted.

Compensating controls, all in place now.

- sf-robot-legacy-v1-restricted lets each robot use only its own sf/v1/`<thing>` topics, its shadow, and its jobs (the jobs deliver the firmware update), and denies every cloud command topic to robot certificates.
- Device Defender Detect profile on the legacy thing group alarms on authorization failures and message-volume anomalies to PagerDuty.
- Weekly report to the CISO of robots remaining on firmware 3.x, by customer site.
- Robots on firmware 3.x accept commands only from the site's local controller, which authenticates over a separate channel.

The first of those is the control that matters most: a legacy certificate can connect only as its own robot and use only that robot's own legacy topics, shadow, and jobs, and every command topic is denied outright. Four more facts belong with the signature, because a signer should not have to ask for them.

- **What an attacker gets.** A certificate taken from one of the 3,412 legacy robots can publish and subscribe to that one robot's own telemetry, shadow, and jobs topics in the legacy layout. It can feed false telemetry for that robot to the fleet service. It cannot reach another robot's topics, command a robot, or reach any robot that has moved to the new policy.
- **What closes it.** Firmware 4.2, installed in each customer's maintenance window. When the last robot has moved, the legacy policy is deleted and the finding closes on the next scan. Until then Sam Okafor reports the count remaining, by customer site, to Marcus Oyelaran every week.
- **What we are not accepting.** The shared test key that 1,240 pilot robots trusted was a separate problem (SF-SEC-021). It is fixed in `fleet-infra#4346`, and it is not part of this acceptance.
- **What happens at expiry.** The weekly report either shows no legacy robots, or it shows the ones that remain and the signers decide again, in writing, with the new count in front of them. We recommend a shorter renewal, not a longer one, if the count has not fallen.

This is the only critical accepted. Under the guarantee, a critical accepted in writing counts as closed. We think that is right for this finding, and we would not recommend it for any other critical in the register.

Guardrails at the top of the organization

Deliverable 9 is what keeps the findings closed. Before this week the organization had two service control policies, FullAWSAccess and a deny on leaving the organization, and no resource control policies or declarative policies, so a new account, a new engineer, or a compromised role could undo any fix with one call. Now 5 service control policies, 1 resource control policy, and 2 EC2 declarative policies sit at the root or on the workload OUs, and 4 StackSets put the same defaults into every member account, including the ones created next year, with a self-managed stack in the management account (the last 2 merge in weeks 4 and 5). The full text of every policy is in the Audit Report Appendix (SF-SEC-026 for the service control policies, SF-SEC-052 for the resource control policy, SF-SEC-014 and SF-SEC-005 for the declarative policies, SF-SEC-050 for the account baseline).

Two limits you should know before relying on them. Service control policies and resource control policies do not apply to the management account, so the account that holds the most power gets alarms (a self-managed `security-alarms` stack in `sf-management`) and a hardware MFA root, not a deny. And a service control policy limits what principals in a member account can do; it never grants anything, so every exception below is an Allow somewhere else. Each policy is well inside the AWS limits on size and count.

Service control policies

The service control policies attached this week. The management account is not affected by any of them.

Policy	Attached to	What it denies	Findings it keeps closed
`sf-protect-security-services`	Root	Stopping or deleting CloudTrail trails and event selectors, AWS Config recorders, GuardDuty, Security Hub CSPM, IAM Access Analyzer, and Inspector, except the platform and security roles	Protects the detection services and the trail that week 5 turns on (SF-SEC-022, SF-SEC-023, SF-SEC-025, SF-SEC-038, SF-SEC-042, SF-SEC-044), so a compromised account cannot switch them off
`sf-deny-member-root`	Root	Every action by a member account's root user, except in a root session started with sts:AssumeRoot (the condition `Null: {aws:AssumedRoot: true}`), which is how root tasks run	Root credentials (SF-SEC-010, SF-SEC-029): even a recreated root login cannot act in a member account
`sf-protect-account-defaults`	Root	Turning off EBS default encryption; changing S3, snapshot, or AMI Block Public Access, RDS snapshot sharing, or KMS key rotation outside the platform roles; and creating IAM users, access keys, or console passwords outside the PlatformIdentityAdmin role	Unencrypted volumes, public buckets and public snapshots (SF-SEC-032, SF-SEC-024, SF-SEC-005), and new IAM users, keys, and console passwords (SF-SEC-012, SF-SEC-013): the defaults cannot be turned off, and only one named role can create an identity
`sf-require-workload-boundary`	Root	Creating a role or user, or setting a permissions boundary, without the sf-workload-boundary boundary, and editing, deleting, or removing the boundary itself, outside the platform and identity administrator roles	See the Audit Report Appendix
`sf-deny-unused-regions`	Workloads, Sandbox, Suspended	Every action in the 11 unused Regions, except global services, the security services, and the platform roles	Default VPCs and exposed resources in Regions nobody watches (SF-SEC-043, SF-SEC-022); leaves only the Regions StrataForge works in

The role names in the exception conditions are the roles StrataForge's pipelines already use; the platform team owns them, and Exceptions, and how they are governed says how an exception to any of them is granted. Order mattered. `sf-deny-member-root` was attached only after the root credential cleanup in SF-SEC-010 finished, because it would have denied the cleanup itself. `sf-protect-account-defaults` stops new IAM users, access keys, and console passwords from appearing outside `PlatformIdentityAdmin`; week 4 removes the human and CI users that already exist.

sf-deny-member-root

```JSON
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberRoot",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::*:root"
        },
        "Null": {
          "aws:AssumedRoot": "true"
        }
      }
    }
  ]
}
```

The resource control policy

A resource control policy limits what anyone can do to a resource in your accounts, whoever asks, and so it also stops a request from an outside account. `sf-rcp-enforce-tls` requires TLS for five services, closing the gap that left 220 buckets accepting plain HTTP (SF-SEC-052) and keeping it closed for every service that matters here. It is attached to the root and does not affect resources in the management account; the account-level controls in `account-baseline` cover that gap.

sf-rcp-enforce-tls

```JSON
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTls",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:*",
        "kms:*",
        "sqs:*",
        "secretsmanager:*",
        "sts:*"
      ],
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

The EC2 declarative policies

Declarative policies are enforced by the service itself, not as an API permission check, so they hold for new APIs and for service-linked roles. `sf-ec2-imdsv2-default` makes IMDSv2 the default for new launches (SF-SEC-014). `sf-ec2-block-public-sharing` blocks all public sharing of snapshots (SF-SEC-005, including the 5 public snapshots we removed) and blocks new public sharing of AMIs.

sf-ec2-imdsv2-default

```JSON
{
  "ec2_attributes": {
    "instance_metadata_defaults": {
      "http_tokens": {
        "@@assign": "required"
      },
      "http_put_response_hop_limit": {
        "@@assign": "2"
      }
    }
  }
}
```

sf-ec2-block-public-sharing

```JSON
{
  "ec2_attributes": {
    "snapshot_block_public_access": {
      "state": {
        "@@assign": "block_all_sharing"
      }
    },
    "image_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

The instance metadata default applies to new launches only. The instances that already allow IMDSv1 keep doing so until their owners change them, which is why `SF-SEC-014` is partly open at the end of this week and has a date in the roadmap.

StackSet account defaults

The StackSets that put the same defaults into every member account, existing and new, with the pull requests that merged them. Only the ones merged in week 3 are in force at the end of this week.

StackSet	What it sets	Targets	Merged	Findings it keeps closed
`account-baseline`	S3 account-level Block Public Access, alternate SECURITY contact, AWSSupportAccess role (the password policy is set by CLI, because CloudFormation has no resource for it)	every member account; sf-management gets a self-managed stack	`platform-landing-zone#629`, Jul 29; `platform-landing-zone#658`, Jul 31	SF-SEC-024 and SF-SEC-050: account-level S3 Block Public Access, a security contact, and a support role in every member account, and a password policy set by script
`ebs-default-encryption`	EBS encryption by default with a customer managed key, alias/sf-ebs, that grants the Auto Scaling role and the forensics account (a snapshot under the AWS managed aws/ebs key cannot be shared)	every member account, 17 Regions; sf-management gets a self-managed stack	`platform-landing-zone#644`, Jul 30	SF-SEC-032: new volumes are encrypted in every Region of every account
`security-alarms`	EventBridge rules for root and break-glass sign-in, trail changes, and kms:Sign by anyone but the OTA signer, to PagerDuty	every member account, 17 Regions; sf-management gets a self-managed stack	`platform-landing-zone#679`, Aug 7; `platform-landing-zone#690`, Aug 10	SF-SEC-001, SF-SEC-010, SF-SEC-040: the alarms in every member account and in a self-managed stack in the management account, which no policy can cover
`vpc-baseline`	Flow logs to the log archive; default security groups with no rules	every VPC in a member account; sf-management gets a self-managed stack	`platform-landing-zone#717`, Aug 13	SF-SEC-043: default security groups carry no rules, and flow logs reach the log archive

StackSets deploy with service-managed permissions and automatic deployment, so a member account that joins an OU receives the defaults without anyone remembering to ask. A service-managed StackSet never deploys to the management account, so each default also has a self-managed stack in `sf-management`. Service control policies do not bind that account either, so it is not a test bed for them: the policies were tried in a sandbox account (below), and the management account's guardrails are its alarms and the hardware-MFA root. CloudFormation has no resource for the IAM password policy, so the account baseline sets it with a script run in every account, `sf-management` included. The account baseline's support role is the part most teams forget; its template is in the Audit Report Appendix under SF-SEC-050.

The `security-alarms` StackSet (merged in week 4) and its self-managed twin in `sf-management` carry the EventBridge rules that page when anything but the OTA release signer calls `kms:Sign`, and when a root session starts through `sts:AssumeRoot`. Both patterns are in the appendix under SF-SEC-001 and SF-SEC-010; the rules target an SNS topic that PagerDuty subscribes to, and week 5 completes that routing.

How we know they work

Each guardrail was tested by trying to do the thing it forbids, as an ordinary administrator, in a sandbox account. A guardrail we have not seen deny is a guess.

```bash
# Run as an administrator role in a Sandbox account. Every call must fail with AccessDenied.
aws ec2 disable-ebs-encryption-by-default --region us-east-1
aws s3control delete-public-access-block --account-id <sandbox-account-id>
aws iam create-user --user-name guardrail-test
aws guardduty delete-detector --detector-id <detector-id> --region us-east-1
aws ec2 describe-instances --region sa-east-1        # an unused Region
aws s3api put-object --bucket <test-bucket> --key t --body /dev/null --endpoint-url http://
s3.us-east-1.amazonaws.com
aws ec2 modify-snapshot-attribute --snapshot-id <snapshot-id> --attribute
createVolumePermission \
  --operation-type add --group-names all

# From the management account: confirm what is attached and where.
aws organizations list-policies-for-target --target-id <org-root-id> --filter
SERVICE_CONTROL_POLICY
aws organizations list-policies-for-target --target-id <org-root-id> --filter
RESOURCE_CONTROL_POLICY
aws organizations list-policies-for-target --target-id <org-root-id> --filter
DECLARATIVE_POLICY_EC2
```

Exceptions, and how they are governed

A guardrail with no way around it gets worked around, and a guardrail with an easy way around it is decoration. StrataForge now has three kinds of exception, each with a different owner and a different clock.

The three kinds of exception StrataForge now runs, who may grant each, and when each ends.

Kind	Example	Who approves	Where it lives	Expires
Exception role in a policy	`PlatformIdentityAdmin` in `sf-protect-account-defaults`	Elena Vasquez for the platform, with Marcus Oyelaran copied	The policy's condition, in `platform-landing-zone`	Reviewed quarterly; removed when unused for a quarter
Control parameter or suppression	Config.1 `includeConfigServiceLinkedRoleCheck` set to false; IAM.6 and IAM.9 suppressed where root has no credentials	Jonah Reyes or the account owner, and the security manager	A Security Hub CSPM automation rule or central configuration policy, with the reason in its description	When the reason stops being true, checked at the monthly review
Risk acceptance	SF-SEC-002	Marcus Oyelaran and, for critical findings, Priya Raman	The acceptance log in the findings register, signed and dated	The date written in it; never open-ended

Four rules apply to all three:

1. **Written before it takes effect.** A pull request or a signed record, never a verbal yes. The reviewer is not the requester.
2. **Time-boxed.** Every exception has an end date. No date, no exception.
3. **Narrow.** A named role, a named resource, a named account; never a wildcard to save time.
4. **Counted.** The monthly review reads the list. An exception nobody can explain is removed, and what breaks tells you who needed it.

Pull request ledger

Every pull request merged this week, in the order it merged. Author for every pull request: Charles Sieg of Vantalect. The reviewer is the engineer who owns the account or the system the change touches. A finding is listed under "Closes" only when this was the pull request that closed it.

The week-3 pull requests: repository and number, files, reviewer, merge date, rollout, and the findings each addresses and closes.

Pull request	Title	Files	Reviewer	Merged	Rollout	Addresses	Closes
`crucible-infra#1982`	Perception: unshare the annotations snapshot; snapshot-sharing SCP exception list	`ops/2026-07-27-unshare-annotations-snapshot.sh`; `apps/perception/lib/annotations-db.ts`	Jonah Reyes	Jul 27	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-007	SF-SEC-007
`fleet-infra#4323`	OTA: sign releases with ota-release-signer via GitHub OIDC (two-person approval)	`apps/ota/lib/ota-release-roles.ts`; `apps/ota/lib/ota-signing-key-policy.ts`; `apps/ota/test/ota-release-roles.test.ts`; `.github/workflows/ota-release.yml`	Sam Okafor	Jul 27	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-001	none
`fleet-infra#4329`	IoT: add sf-robot-scoped-v2 with thing-name policy variables	`apps/iot/policies/sf-robot-scoped-v2.json`; `apps/iot/lib/robot-policies.ts`; `apps/iot/test/robot-policies.test.ts`	Sam Okafor	Jul 27	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-002	none
`fleet-infra#4340`	CI: pin sub to repository and environment on four GitHub Actions roles	`lib/constructs/github-oidc-role.ts`; `apps/ci/lib/deploy-roles.ts`; `apps/ci/test/deploy-roles.test.ts`	Elena Vasquez	Jul 27	Deployed to sf-cicd first and verified, then to production.	SF-SEC-003	SF-SEC-003
`platform-landing-zone#613`	EC2 declarative policy: snapshot and AMI block public access; unshare Kestrel snapshots	`policies/declarative/ec2-block-public-sharing.json`; `org/attachments.yaml`; `ops/2026-07-27-unshare-kestrel-snapshots.sh`	Jonah Reyes	Jul 27	Attached to the Sandbox OU first, then Workloads/Fleet/NonProd, then the Root after 24 hours with no denied calls in CloudTrail.	SF-SEC-005	SF-SEC-005

Pull request	Title	Files	Reviewer	Merged	Rollout	Addresses	Closes
`crucible-infra#1987`	Research: close 8888 and 22; notebooks through Session Manager port forwarding	`apps/research/lib/workstation-stack.ts`; `apps/research/lib/notebook-launch-template.ts`; `apps/perception/lib/dev-workstations.ts`	Hiro Tanaka	Jul 28	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-004	SF-SEC-004
`crucible-infra#1992`	Perception: import the dataset buckets into CDK; private with Block Public Access	`apps/perception/lib/datasets-stack.ts`; `apps/perception/test/datasets-stack.test.ts`	Jonah Reyes	Jul 28	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-006	SF-SEC-006
`crucible-infra#1996`	Perception CI: Jenkins behind an internal ALB with Okta sign-in; rotate stored keys	`apps/perception/lib/jenkins-stack.ts`; `apps/perception/lib/jenkins-alb-oidc.ts`; `apps/perception/test/jenkins-stack.test.ts`	Jonah Reyes	Jul 28	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-008	SF-SEC-008
`enterprise-infra#905`	Network: remove 0.0.0.0/0 and ::/0 ingress on 22 and 3389 in plm-prod	`apps/plm/lib/cad-workstations-stack.ts`	Mei Chen	Jul 28	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-009	SF-SEC-009
`fleet-infra#4328`	OTA: alarm on kms:Sign by any principal but the signer; deactivate the ota-signing-ci key	`apps/ota/lib/ota-signing-alarms.ts`; `apps/ota/lib/ota-legacy-user.ts`; `apps/ota/test/ota-signing-alarms.test.ts`	Sam Okafor	Jul 28	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-001	SF-SEC-001
`fleet-infra#4332`	IoT: move thing groups to sf-robot-scoped-v2 in waves; restrict the legacy firmware group	`apps/iot/lib/policy-rollout.ts`; `apps/iot/policies/sf-robot-legacy-v1-restricted.json`; `apps/iot/rollout/waves.yaml`	Sam Okafor	Jul 28	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-002	none
`platform-landing-zone#619`	Root: centralized root access management; delete member root credentials	`org/root-access.yaml`; `ops/delete-member-root-credentials.sh`	Grace Liu	Jul 28	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-010	SF-SEC-010

Pull request	Title	Files	Reviewer	Merged	Rollout	Addresses	Closes
`fleet-infra#4336`	IoT: Device Defender scheduled audits in all four IoT Regions	`apps/iot/lib/device-defender-audit.ts`; `apps/iot/test/device-defender-audit.test.ts`	Sam Okafor	Jul 29	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-002	none
`fleet-infra#4346`	OTA: limit the staging test key to the staging pipeline	`apps/ota/lib/ota-test-key.ts`; `apps/ota/test/ota-test-key.test.ts`	Sam Okafor	Jul 29	Deployed to fleet-ota-staging first and verified, then to production.	SF-SEC-021	SF-SEC-021
`platform-landing-zone#620`	DNS: delete docs-legacy CNAME; weekly dangling-record check	`dns/strataforge.example/records.yaml`; `stacksets/dns-hygiene/template.yaml`	Elena Vasquez	Jul 29	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-011	SF-SEC-011
`platform-landing-zone#625`	Network: remove 0.0.0.0/0 and ::/0 ingress on 22 and `3389` in sf-shared-services	`stacksets/bastion/template.yaml`	Elena Vasquez	Jul 29	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-027	SF-SEC-027
`platform-landing-zone#629`	Account baseline: S3 Block Public Access at the account and bucket level	`stacksets/account-baseline/template.yaml`; `ops/2026-07-29-bucket-level-bpa.sh`	Elena Vasquez	Jul 29	Deployed to sf-shared-services first and verified, then to production.	SF-SEC-024	SF-SEC-024
`platform-landing-zone#633`	SCPs: protect security services and the trail, deny member root, keep account defaults, deny unused Regions	`policies/scp/protect-security-services.json`; `policies/scp/deny-member-root.json`; `policies/scp/protect-account-defaults.json`; `policies/scp/deny-unused-regions.json`; `org/attachments.yaml`	Elena Vasquez	Jul 29	Attached to the Sandbox OU first, then Workloads/Fleet/NonProd, then the Root after 24 hours with no denied calls in CloudTrail.	SF-SEC-026	SF-SEC-026
`fleet-infra#4351`	EKS: private endpoints for production clusters; corporate CIDRs for non-production	`apps/fleet-api/lib/eks-cluster.ts`; `apps/ingest/lib/eks-cluster.ts`; `apps/ci/lib/runner-network.ts`	Sam Okafor	Jul 30	Deployed to fleet-staging first and verified, then to production.	SF-SEC-016	none

Pull request	Title	Files	Reviewer	Merged	Rollout	Addresses	Closes
`fleet-infra#4352`	Network: remove 0.0.0.0/0 and ::/0 ingress on 22 and 3389 in fleet-dev	`apps/dev-environments/lib/network.ts`	Sam Okafor	Jul 30	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-028	SF-SEC-028
`fleet-infra#4357`	IoT: fleet provisioning template for per-device certificates; revoke shared certificates	`apps/iot/lib/fleet-provisioning.ts`; `apps/iot/templates/robot-provisioning.json`; `apps/iot/rollout/shared-cert-revocation.yaml`	Sam Okafor	Jul 30	Proven in fleet-ota-staging and on the Pittsburgh test fleet before production.	SF-SEC-030	none
`platform-landing-zone#639`	EC2 declarative policy: IMDSv2 required for new launches; switch instances without IMDSv1 calls	`policies/declarative/ec2-imdsv2-default.json`; `ssm/automation/require-imdsv2.yaml`; `ops/imdsv2-waves.csv`	Elena Vasquez	Jul 30	Attached to the Sandbox OU first, then Workloads/Fleet/NonProd, then the Root after 24 hours with no denied calls in CloudTrail.	SF-SEC-014	none
`platform-landing-zone#644`	Account baseline: EBS encryption by default in every Region	`stacksets/ebs-default-encryption/template.yaml`; `policies/scp/protect-account-defaults.json`	Elena Vasquez	Jul 30	Deployed to sf-management first and verified, then to production.	SF-SEC-032	none
`platform-landing-zone#649`	Network: remove 0.0.0.0/0 and ::/0 ingress on 22 and 3389 in sandbox-platform	`stacksets/bastion/template.yaml`	Elena Vasquez	Jul 31	Deployed to the account's non-production twin first where one exists, then to production.	SF-SEC-041	SF-SEC-041
`platform-landing-zone#652`	KMS: rotation on every symmetric customer managed key	`ops/2026-07-30-enable-key-rotation.sh`; `lib/constructs/README.md`	Elena Vasquez	Jul 31	Deployed to sf-network-hub first and verified, then to production.	SF-SEC-053	SF-SEC-053
`platform-landing-zone#655`	RCP: enforce TLS for S3, KMS, SQS, Secrets Manager, and STS	`policies/rcp/enforce-tls.json`; `org/attachments.yaml`	Elena Vasquez	Jul 31	Attached to the Sandbox OU first, then Workloads/Fleet/NonProd, then the Root after 24 hours with no denied calls in CloudTrail.	SF-SEC-052	SF-SEC-052

Pull request	Title	Files	Reviewer	Merged	Rollout	Addresses	Closes
`platform-landing-zone#658`	Account baseline: security contact, support role, CloudShell; password policy by script	`stacksets/account-baseline/template.yaml`; `stacksets/account-baseline/parameters/all-accounts.json`	Elena Vasquez	Jul 31	Deployed to sf-management first and verified, then to production.	SF-SEC-050	SF-SEC-050

© 2026 Vantalect, LLC. Sample deliverable; StrataForge Robotics is fictional.

AWS, Amazon Web Services, AWS Graviton, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. Kubernetes is a registered trademark of The Linux Foundation. GitHub is a trademark of GitHub, Inc. NVIDIA and Isaac Sim are trademarks of NVIDIA Corporation. SAP and SAP S/4HANA are trademarks of SAP SE. Okta is a trademark of Okta, Inc. PagerDuty is a trademark of PagerDuty, Inc. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. CIS Benchmarks is a trademark of the Center for Internet Security, Inc. Vantalect is not affiliated with or endorsed by any of them. StrataForge Robotics is fictional.