

Vantalect

AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Root Cause and Vulnerable Infrastructure

DISTRIBUTION: COUNSEL ONLY

Week 2 of 4: Trace · prepared for Wrenfield Bancorp, Inc.

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

July 24, 2026 · AWS Breach Forensics & Recovery: The Investigation and the Recovery (four weeks)

SAMPLE DELIVERABLE

Privileged and confidential. Prepared at the direction of counsel. Sample. Wrenfield is fictional.

This is a sample deliverable. Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

Contents

What this report is 2

The causal chain 4

The six root causes 5

RC-1: A long-lived access key for a service user, never rotated, on an unmanaged machine 5

RC-2: An administrator deploy role trusted by a whole account with no conditions 5

RC-3: No organization guardrails on key origin, imported material, snapshot sharing, lifecycle and versioning changes, or S3 Batch jobs 5

RC-4: Versioning without Object Lock or MFA Delete on the imaging archive 5

RC-5: Detection gaps: read-only events not alerting, write-only data events, a 34–minute holiday page 6

RC-6: Month-end snapshots in the workload account itself, the central copy in governance mode 6

The same weaknesses elsewhere 7

Detection and response gaps 9

What the first hour should have held 10

Control Gaps and Fix Plan 11

What critical means here 11

Controls by root cause 12

Controls for the same weaknesses elsewhere 15

Controls for the detection and response gaps 16

The prioritized fix list 16

Notice 19

What this report is

This report says why the attack worked at each step, and what else in Wrenfield's estate would have let it work. A detachable appendix, "Control Gaps and Fix Plan," holds the fixes. The causal sections do not carry fix text. The report is for Diane Whitcombe, Harold Penwick, and Mireille Danvers, as of Friday, July 24, 2026. Its distribution line is Counsel only: it was prepared at the direction of counsel, and counsel decides who else reads it. **Privileged and confidential. Prepared at the direction of counsel.** The label does not protect a document by itself: privilege depends on how and why the work was commissioned, and counsel decides whether it applies. Vantalect makes no determination about privilege.

What it rests on. The attacker's record in the organization trail (the 519 attacker events and the 1,709 in all), the estate configuration we exported in week one, and a read-only configuration review of the 22 accounts in week two. Interim controls are shown, in the appendix, as they stood on July 24. The closed dates belong to week three and are not in this report.

What it does not cover. It does not test the estate. It makes no finding about the core banking service bureau, which is outside AWS, or about the contractor's laptop, which is outside the evidence: counsel's interview is the only source for how the key left the bank. It does not say whether any law or rule applies; that is for the bank and counsel. It states no hours beyond the Response's 56.

How we rate and sort

Severity. Critical means the weakness alone let an attacker holding one stolen credential change or copy production data. High means it made the harm larger, longer, or harder to undo or to notice. Medium means it narrowed the bank's options without enabling the attack.

Sort. Root causes are listed in the order the attacker met them, which is also severity order. Other weaknesses are sorted by severity, then by the number of accounts they reach.

The causal chain

Six weaknesses made the attack possible, and 3 of them were critical: removing any one of the first three would have stopped it or made it far smaller. The links run in the order the attacker met them. What each let the attacker do is in the sections that follow, and the controls that break each link are in the appendix.

The six root causes, in the attacker's order, with the evidence for each.

Link	Root cause	Evidence	Severity
RC-1: Entry	A long-lived access key for a service user, never rotated, on an unmanaged machine	EV-00003 (first use, June 29, 03:14 EDT, 198.51.100.23); the credential report for wf-tools (key created March 14, 2023, last rotated never)	Critical
RC-2: Privilege	An administrator deploy role trusted by a whole account with no conditions	EV-00051 (July 1 test into wf-nonprod-data); EV-00083 (July 3, 21:04, first production write session); 37 sessions in 10 accounts	Critical
RC-3: Impact	No organization guardrails on key origin, imported material, snapshot sharing, lifecycle and versioning changes, or S3 Batch jobs	EV-00084 (CreateKey, Origin EXTERNAL); EV-00087 (ImportKeyMaterial); EV-00312 (lifecycle rule); EV-00393 (S3 Batch job); EV-00520 (snapshot share)	Critical
RC-4: Recovery of the archive	Versioning without Object Lock or MFA Delete on the imaging archive	EV-00312 (the attacker's rule to expire noncurrent versions after one day, removed July 4 at 01:35)	High
RC-5: Detection	Detection gaps: read-only events not alerting, write-only data events, a 34-minute holiday page	Discovery calls June 29 to July 2 with no alert (the narrative lists them); EV-00098 to EV-00311 (214 SSE-C denials, 40 seconds); GuardDuty finding 22:44, page 23:18	High
RC-6: Recovery of the database	Month-end snapshots in the workload account itself, the central copy in governance mode	EV-00444 to EV-00452 (nine DeleteDBSnapshot calls, 22:05); the copies in wf-backup under Vault Lock in governance mode	Medium

The six root causes

RC-1: A long-lived access key for a service user, never rotated, on an unmanaged machine

Anyone holding the key was svc-artifact-sync from any address, at any hour, with no second factor and no expiry. Severity: critical. svc-artifact-sync's key AKIAWRFNEXAMPLE00001, created March 14, 2023 and never rotated, taken from a contractor's personal laptop (counsel's interview). The evidence pointers are EV-00003 (first use, June 29, 03:14 EDT, 198.51.100.23); the credential report for wf-tools (key created March 14, 2023, last rotated never).

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-1.

RC-2: An administrator deploy role trusted by a whole account with no conditions

One session in wf-tools became an administrator in all ten workload accounts, production and nonprod alike. Severity: critical. wf-deploy-pipeline in ten workload accounts: AdministratorAccess, trusts the wf-tools account with no conditions. The evidence pointers are EV-00051 (July 1 test into wf-nonprod-data); EV-00083 (July 3, 21:04, first production write session); 37 sessions in 10 accounts.

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-2.

RC-3: No organization guardrails on key origin, imported material, snapshot sharing, lifecycle and versioning changes, or S3 Batch jobs

The attacker created keys with their own material, shared a database snapshot with an outside account, changed lifecycle rules, and started a 61.3 million object job. Nothing refused any of it. Severity: critical. No SCP on KMS key origin, imported key material, snapshot sharing, or lifecycle changes. The evidence pointers are EV-00084 (CreateKey, Origin EXTERNAL); EV-00087 (ImportKeyMaterial); EV-00312 (lifecycle rule); EV-00393 (S3 Batch job); EV-00520 (snapshot share).

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-3.

RC-4: Versioning without Object Lock or MFA Delete on the imaging archive

Versioning kept the bank's earlier versions, which saved the archive, but nothing stopped a principal from deleting versions or expiring them. Severity: high. wf-imaging-archive-prod: 286 million objects, 412 TB, versioning on, no Object Lock. The evidence pointers are EV-00312 (the attacker's rule to expire noncurrent versions after one day, removed July 4 at 01:35).

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-4.

RC-5: Detection gaps: read-only events not alerting, write-only data events, a 34-minute holiday page

Four days of discovery raised no alert, the first write-capable session was seen only by a later finding, and the page took 34 minutes. Severity: high. Read-only management events reached the organization trail with no alert path; S3 data events logged for writes only; the provider paged 34 minutes after the finding. The evidence pointers are Discovery calls June 29 to July 2 with no alert (the narrative lists them); EV-00098 to EV-00311 (214 SSE-C denials, 40 seconds); GuardDuty finding 22:44, page 23:18.

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-5.

RC-6: Month-end snapshots in the workload account itself, the central copy in governance mode

The attacker deleted nine month-end snapshots in the workload account in one call batch. The copies in wf-backup were out of their reach. Severity: medium. Nine month-end RDS snapshots in wf-prod-lending, with copies in wf-backup under Vault Lock in governance mode. The evidence pointers are EV-00444 to EV-00452 (nine DeleteDBSnapshot calls, 22:05); the copies in wf-backup under Vault Lock in governance mode.

The control for this link, its interim state on July 24, and its plan are in the appendix, under RC-6.

The same weaknesses elsewhere

The attacker used one path through the estate. Eight more weaknesses of the same kinds were open on July 24. Four of them (W-1, W-2, W-3, and W-8) are other doors into the same rooms, and the attacker did not use them. The rest match single calls the attacker made in one account and could repeat in others. We found all eight by reading configuration, not by testing, so each row says what we saw and what an attacker could do.

Eight weaknesses in the rest of the estate, found by configuration review in week two. Their fixes are in the appendix.

ID	Weakness and severity	What we found	Why it matters
W-1	Other IAM users with long-lived keys (high)	9 IAM users hold 11 active access keys in 6 accounts (wf-tools, wf-shared-services, wf-network, wf-backup, wf-sandbox-1, wf-sandbox-2). 8 of the keys are older than 365 days, the oldest from 2022. 3 of the users have no MFA.	The same entry as RC-1. The attacker found svc-artifact-sync first; any of these keys, taken from a laptop or a build log, starts the same walk.
W-2	Other roles that trust a whole account with no condition (high)	5 roles in 4 accounts trust the wf-tools account (or an account root) with no condition: 2 in wf-shared-services, 1 in wf-network, 1 in wf-backup, and 1 in wf-log-archive. Two of the five can write: wf-backup-copy-admin in wf-backup can delete recovery points, and wf-net-config-deploy in wf-network can change routes.	The attacker assumed wf-deploy-pipeline only. The trail shows no AssumeRole of any of these five. The same stolen key could have assumed them.
W-3	KMS key policies that hand the keys to the account's administrators (high)	14 customer managed keys in the 5 production accounts use the default key policy, which delegates to IAM. Any principal with AdministratorAccess in the account can edit the policy, create grants, and name an outside account. No policy carries an organization condition.	The attacker used this on their own keys. The same hand can add an outside account to a bank key, or schedule a bank key for deletion. No attacker call of this kind touched the 14 bank keys.
W-4	The nonprod accounts (medium)	The 5 nonprod accounts carry the same administrator deploy role and the same trust as production. They have no EBS Recycle Bin rule, no data events, and no backup plan for their snapshots. The attacker opened sessions in all five on July 3.	The attacker looked around in nonprod (ListBuckets, DescribeDBInstances, ListKeys) and left. A deleted snapshot in nonprod is gone at once.
W-5	EBS Recycle Bin retention of 10 days, with the rule unlocked (high)	The prod accounts keep deleted EBS snapshots 10 days. The retention rule is not locked, so an administrator can shorten it or delete it.	The attacker deleted 46 snapshots and did not look in the Recycle Bin. The bank restored all 46 on July 4 at 07:40. An attacker who deleted the rule first, or who waited 10 days, would have won this exchange.

ID	Weakness and severity	What we found	Why it matters
W-6	Snapshot and image sharing allowed everywhere (high)	No policy limits who can share an EBS snapshot, an RDS snapshot, or an image. The setting that blocks public sharing of EBS snapshots is off in all 20 accounts that existed on July 3.	The attacker used this once, on the loan database snapshot (EV-00520). The same call works on the 46 EBS snapshots, on the data lake's snapshots, and on any image.
W-7	Per-account trails that an account administrator can delete (medium)	The attacker deleted wf-lending-legacy-trail (EV-00501). The organization trail held, because member accounts cannot change it. Nothing prevents the same deletion of any other account trail, and the lending documents bucket has no data events at all.	The deletion removed the legacy trail's configuration and stopped its delivery; files it had already delivered remain unless separately deleted. A trail that is the only record in an account would stop recording the same way.
W-8	Credentials on devices the bank does not manage (high)	The credential report shows long-lived keys for people and for pipelines, but the bank has no record of where each key is stored. The stolen key sat in a contractor's personal laptop profile. Contractors reach the tools account by key, not through IAM Identity Center.	This is how RC-1 began. It is outside AWS, so no AWS control finds it. Counsel's interview is the only evidence of where the key lay.

Two of the eight deserve the board's attention first. W-5 is the Recycle Bin: the 46 EBS snapshots came back only because the attacker did not look there and the retention was still running. W-2 is the five unconditioned roles, two of which can write to backups or to the network. Both would have turned a bad night into a worse one with the same key. The fixes are in the appendix.

Detection and response gaps

The bank saw the attack late because three things were not in place: an alert on read-only discovery, a log of reads, and a fast, redundant page. The numbers below are from the record.

Detection and response gaps, with the measure from the record. Their fixes are in the appendix.

ID	Gap	What the record shows	Bears on
D-1	Read-only events did not alert	The attacker's discovery ran from June 29 to July 2, between 02:00 and 11:00 EDT each day. Read-only management events reached the organization trail and no alert path. A key used from a new address, listing roles and accounts, raised nothing.	RC-5
D-2	Data events logged writes only	The organization trail records S3 data events for writes on the imaging and data lake buckets. Reads were not logged, so whether anyone read an object in the imaging archive is unknown. The lending documents bucket has no data events: the ransom note written there at 23:30 never reached the trail.	RC-5
D-3	The page took 34 minutes on a holiday	GuardDuty raised the finding at 22:44; the provider paged one on-call engineer at 23:18. There was no second person to page and no rule that sent a high-severity persistence finding to a phone at once.	RC-5
D-4	No detection of the first write steps	The first write was at 21:04. The calls that mattered most, CreateKey with an external origin (21:06) and ImportKeyMaterial, raised no alert of their own. GuardDuty's finding came from the later user and key creation.	RC-5
D-5	Incident access did not exist in advance	The bank signed the activation at 00:52 and the incident role reached the accounts 42 minutes after Charles joined the bridge. The first containment policy was drafted that night and approved on the bridge.	RC-3

The timings behind the gaps, from the record.

Measure	Value
First use of the stolen key to the first write-capable session (the dwell)	4 days, 17 hours, 50 minutes
Discovery-phase calls in the attacker's record, June 29 to July 4	79
First write (21:04 EDT) to the GuardDuty finding (22:44 EDT)	1 hour 40 minutes
GuardDuty finding to the page (23:18 EDT)	34 minutes
First write to the containment SCP (01:22 EDT)	4 hours 18 minutes
Bridge joined (00:58 EDT) to the incident role deployed	42 minutes
Loan origination offline	110 hours 10 minutes

What the first hour should have held

The attacker kept two ways in after the containment SCP of 01:22 EDT, and used them until the deny-by-ARN update of 02:58 EDT, 1 hour 36 minutes later. The SCP stopped what it named: the attacker's account assumed `OrgAccessBackup` at 01:36 and held an administrator session, and the SCP stopped only the 01:39 `DeleteDBInstance`. The persistence user was used again from 02:47 to 02:50, and its first calls after the 02:58 EDT update were denied. Three steps in the first hour would have closed both ways sooner. They are lessons from this night, not a finding about any person.

The first-hour lesson, from the times in the organization trail. The standing runbook that carries it is gap D-5 in the appendix.

Step	What the record shows	What to hold ready
1. Ask the IAM and STS write question in the first hour	The attacker's user `aws-support-sync` (created 22:31 on July 3) and role `OrgAccessBackup` (22:36) were in the organization trail from the moment they were made. The bank's list of attacker principals reached a policy at 02:58.	A saved query for IAM and STS write events (`CreateUser`, `CreateAccessKey`, `CreateRole`, `AssumeRole`, `GetSessionToken`) by every principal the stolen key reached, run when containment starts.
2. Deny the principals by ARN in the same change as the SCP	The SCP of 01:22 denied actions and did not name principals. The deny-by-ARN statement was added at 02:58. The attacker used `aws-support-sync` at 01:31 (denied) and from 02:47 to 02:50 (reads and a `GetSessionToken`), and its first calls after the update were denied (02:59 and 03:00).	A statement in the first SCP that denies the named attacker principals every action, with the ARNs filled in from step 1.
3. Put a deny-all trust policy on a captured role	`OrgAccessBackup` trusted the attacker's account until it was deleted on July 8. At 01:36 the attacker's account assumed it and held an administrator session. The SCP stopped only the 01:39 `DeleteDBInstance`.	A deny-all trust policy on any role the attacker made or can assume, so the role stays in place for capture and cannot be assumed. The break-glass role is exempt from the SCP and can make the change.

Control Gaps and Fix Plan

Distribution of this appendix: operational, for the bank's security team as counsel directs. It is written so that counsel can detach it from the causal analysis above: it holds every fix, interim control, and plan in this report, and it adds no causal finding. It states no legal conclusion, and counsel decides whether it is separated from the report and who receives it. Detaching it does not change the report's Counsel only label; counsel decides what travels with it.

What critical means here

In this report and in the Recovery's exit gate, critical has one meaning: the weakness alone let an attacker holding one stolen credential change or copy production data. The 3 critical root causes are RC-1, RC-2, and RC-3. The gate (criterion G-1 in the Closure Sweep) requires those three closed as code: a merged pull request with a reviewer who is not the author, and a verification. High and medium causes do not hold the gate in the same way. RC-4 is reported by what each fix closes: closed for new object versions of the imaging archive when F-5 is done, and open for the 286,000,000 objects that exist, planned under F-11, as the next section sets out.

Controls by root cause

On July 24 each critical link had an interim control, and none of the three had been written as code. The high and medium links had no control in the production estate yet; the table shows what stood in their place. Owners propose and approvers sign.

Controls and interim controls on July 24. Closure dates are not shown because no root cause is closed yet.

Root cause	Control that breaks the link	Interim date	Interim control, as it stood	Week-three plan	Owner, approver
RC-1 (critical)	Short-lived credentials from OIDC for the build	July 8	Key deactivated July 4 at 01:24 (RE-004). On July 8 at 10:10 the user and its key were deleted and an OpenID Connect provider created in wf-tools (RE-180 to RE-182). The build was moved by hand, not yet as code.	The build authenticates with OIDC web identity through a role; no IAM user in wf-tools holds a key.	Imani Castell, Mireille Danvers
RC-2 (critical)	Trust narrowed to the Jenkins role with a source identity condition	July 8	Active sessions revoked July 4 at 01:26 (RE-005 to RE-014). On July 8 the trust was narrowed by hand in all ten accounts to the Jenkins role with a source identity condition (RE-170 to RE-179).	The narrowed trust is defined in code and deployed to the ten accounts as one stack set, with drift detection.	Imani Castell, Mireille Danvers
RC-3 (critical)	The guardrail service control policy and resource control policy at the organization, proven in a staging OU first	July 4	The containment SCP on Workloads at 01:22 on July 4 (RE-003) and the RCP `wf-deny-outside-access` on Workloads at 03:20 (RE-072), after resource control policies were enabled at the root at 03:15 and the outside trusts the RCP would cut were listed at 03:16. The exfiltration path closed at 02:08 to 02:10 on July 4 (share removed, outside statement dropped from the three attacker key policies, grant revoked). The policies are the Response's, written for the night, with exceptions for the incident role and the break-glass role. Neither is code, and neither was tested in a staging OU.	The guardrail SCP and RCP are written as code, proven in a staging OU, and then attached at the organization root.	Imani Castell, Mireille Danvers
RC-4 (high)	Object Lock in governance mode for 30 days on new versions, by the bank's choice	None in the estate	No control in the production bucket. The attacker's lifecycle rule was removed July 4 at 01:35 (RE-017). A replication rule from the archive to an Object Lock bucket in wf-recovery-vault was set July 8 at 17:05 (EV-01094); a rule alone copies only objects created after it is set. The bank then created an S3 Batch Replication job over the 286 million current versions under its own key, at 18:25 (EV-01101). The job finished July 12 at 21:40, 99 hours 15 minutes later, with 1,206 tasks failed (SrcVersionNotFound: the source version was already gone). The 122.6 million noncurrent versions were not in its manifest: 61.3 million under the attacker keys, whose key material has expired, and 61.3 million original bank-key versions. The copy puts no retention on the production objects.	Object Lock in governance mode, 30 days, on new versions of the production archive, by the bank's choice. Default retention does not reach the objects that already exist, so the existing versions stay a residual risk until the bank runs a retention job over them or accepts the risk in writing (F-11).	Rafael Quintero, Mireille Danvers

Root cause	Control that breaks the link	Interim date	Interim control, as it stood	Week-three plan	Owner, approver
RC-5 (high)	EventBridge with all management events to Interceptor's watch and the provider; read data events on the imaging and lending buckets	None in the estate	Interceptor has followed the attacker's principals since July 4 at 02:20. It is not an estate-wide alert path.	EventBridge carries all management events to Interceptor's watch and to the provider, and read data events cover the imaging and lending buckets.	Imani Castell, Mireille Danvers
RC-6 (medium)	Move the backup vault to compliance mode in the next quarter	None in the estate	In wf-recovery-vault, the 46 EBS snapshot copies were under LockSnapshot in compliance mode for 14 days (cool-off 72 hours, set July 6 at 05:45), which ended July 20; no extension is evidenced. The ten RDS snapshot copies (the nine month-end snapshots and one of the live database) are plain snapshots, not under any lock. The vault OU's SCP and keys the bank holds protect them; the SCP denies deletion, sharing, and key changes to everyone. The weakest link is a person with Organizations rights in the management account who could change that SCP. AWS Backup Vault Lock (July 6, 19:30; RE-139) covers one recovery point of the live database.	The bank accepts the risk in writing until the central backup vault moves to compliance mode next quarter.	Mireille Danvers, Mireille Danvers

Controls for the same weaknesses elsewhere

The fix for each of the eight weaknesses in the rest of the estate, with owner and target date.

ID	Weakness	Fix	Owner, target
W-1	Other IAM users with long-lived keys (high)	Replace each key with a role or an OIDC identity, then delete the user. Until then, deactivate any key unused for 90 days.	Imani Castell, July 31
W-2	Other roles that trust a whole account with no condition (high)	Narrow each trust to a named role with a source identity condition, as RC-2 does, and put a deny on recovery point deletion in the role wf-backup-copy-admin.	Imani Castell, July 31
W-3	KMS key policies that hand the keys to the account's administrators (high)	Separate key administrators from key users, add an organization condition to cross-account use, and deny key deletion scheduling except from the break-glass role. The guardrails in RC-3 cover the organization-wide deny first.	Imani Castell, September 30
W-4	The nonprod accounts (medium)	Add a Recycle Bin rule, narrow the deploy role to what nonprod pipelines call (using Access Analyzer's generated policy), and cover nonprod with the same guardrails.	Rafael Quintero, September 15
W-5	EBS Recycle Bin retention of 10 days, with the rule unlocked (high)	Raise retention to 30 days, lock the rule with an unlock delay of 7 days, and deny changes to Recycle Bin rules except from the break-glass role.	Imani Castell, August 14
W-6	Snapshot and image sharing allowed everywhere (high)	Deny sharing to any account outside the organization except from the backup roles, and turn on block public access for snapshots in every account.	Imani Castell, July 29
W-7	Per-account trails that an account administrator can delete (medium)	Deny trail deletion and stop-logging in every account except the break-glass role, and retire the legacy trails after their contents are in the organization trail.	Mireille Danvers, July 29
W-8	Credentials on devices the bank does not manage (high)	Contractors sign in through IAM Identity Center on a device the bank manages, or not at all. Counsel and the CISO decide the contract terms.	Mireille Danvers, September 30

Controls for the detection and response gaps

The fix for each detection and response gap.

ID	Gap	Fix	Bears on
D-1	Read-only events did not alert	All management events go to Interceptor's watch and the provider; Interceptor's rules alert on a new address for any long-lived key.	RC-5
D-2	Data events logged writes only	Read data events on the imaging and lending buckets; write events on the lending bucket.	RC-5
D-3	The page took 34 minutes on a holiday	Page two people on a high-severity finding, within 5 minutes, in the provider's runbook, and test it on a holiday schedule.	RC-5
D-4	No detection of the first write steps	Alert on CreateKey with Origin EXTERNAL, ImportKeyMaterial, lifecycle changes on the archive, and snapshot sharing, at once.	RC-5
D-5	Incident access did not exist in advance	A pre-approved containment SCP and a pre-deployed read role, tested twice a year, with the first-hour runbook in the lesson section (the IAM and STS write query, deny by ARN, deny-all trust on a captured role). The CISO sets the cadence.	RC-3

The prioritized fix list

The fix list is sorted by severity of what it closes, then by how many attack steps it breaks, then by how little work it takes.

The fix list in priority order. F-1 to F-7 are week three of the Recovery, July 27 to July 31.

No.	Fix	Closes	Owner	Target	Why in this place
1. F-1	Replace the build's static key with OIDC; delete nothing else yet	RC-1	Imani Castell	July 28	It removes the entry. Everything else assumes it is done.
2. F-2	Put the narrowed wf-deploy-pipeline trust in code, ten accounts, one stack set	RC-2	Imani Castell	July 28	It breaks the privilege link even if another key leaks.
3. F-3	Write the guardrail SCP and RCP as code, prove them in a staging OU, attach at the root	RC-3, W-6, W-7	Imani Castell	July 29	It breaks five of the attacker's steps at once and closes two other weaknesses.
4. F-4	Delete or replace the 11 other keys; narrow the 5 other trusts	W-1, W-2	Imani Castell	July 31	The same entry and the same privilege, through paths not yet used.
5. F-5	Object Lock, governance mode, 30 days, on new versions of the imaging archive	RC-4, new versions only	Rafael Quintero	July 30	It stops a misused credential from deleting the protected versions during retention (governance mode can be bypassed by those with the permission). It does not stop a new current version from being written under the same key, so the write and key guardrails in RC-3 are still needed.
6. F-6	All management events to Interceptor's watch and the provider; read data events on the imaging and lending buckets; new page rule	RC-5, D-1 to D-4	Imani Castell	July 31	It shortens the next attack's dwell. It starts the seven-day watch.
7. F-7	Accept RC-6 in writing; plan the vault's move to compliance mode	RC-6	Mireille Danvers	July 31	The risk is medium and the move needs a quarter; a dated, owned acceptance is the honest state.
8. F-8	Recycle Bin: 30 days, locked, in the prod accounts	W-5	Imani Castell	August 14	It protects the one thing that saved the EBS snapshots.
9. F-9	Right-size the nonprod accounts; Recycle Bin rules there	W-4	Rafael Quintero	September 15	Medium; it follows the guardrails.

No.	Fix	Closes	Owner	Target	Why in this place
10. F-10	Rewrite the KMS key policies; contractors through Identity Center	W-3, W-8	Mireille Danvers	September 30	They need the bank's decisions.
11. F-11	Apply retention to the existing current versions of the imaging archive with an S3 Batch Operations Object Lock retention job, or accept the gap in writing	RC-4, existing objects	Rafael Quintero	September 30	The 286 million existing objects are the population this attack targeted, and default retention does not cover them. A bulk job is the bank's choice (cost, and the governance-mode bypass role).

11 fixes, in this order, make up the plan; F-1 to F-7 are week three of the Recovery. Targets are plan dates, not closures. F-5 locks new versions only, so RC-4 is closed for new object versions when F-5 is done. F-11 covers the existing objects of RC-4, is owned by Rafael Quintero, and is dated September 30, so RC-4 stays open for the existing objects until F-11 is done or the gap is accepted in writing.

Decisions that are the bank's. Mireille Danvers approves the plan and signs the written acceptance in F-7. Rafael Quintero decides F-5 and F-11, because the imaging archive is his and Object Lock changes how it is managed. Counsel decides what the contractor terms in W-8 may say. Vantalect makes no determination on any legal matter in this list.

Notice

Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

© 2026 Vantalect, LLC. Sample deliverable; Wrenfield Bancorp, Inc. is fictional.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. MITRE ATT&CK is a registered trademark of The MITRE Corporation. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Other product names are trademarks of their owners. Vantalect is not affiliated with or endorsed by any of them. Wrenfield Bancorp, Inc. is fictional.