

Vantalect

AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

# Closure Sweep

**DISTRIBUTION: OPERATIONAL**

Week 4 of 4: Closure sweep and hand over · prepared for Wrenfield Bancorp, Inc.

---

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

August 7, 2026 · AWS Breach Forensics & Recovery: The Investigation and the Recovery (four weeks)

**SAMPLE DELIVERABLE**

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 gate ..... 2

The method ..... 4

The week-one map against week four ..... 5

The indicator searches ..... 8

The seven-day watch ..... 10

The roles removed ..... 14

What stays open after the gate ..... 16

Notice ..... 16


# What this report is

**This is the Recovery's gate: the week-one map and every indicator search, run again the same way in week four, side by side, with the seven-day watch and the roles removed.** It is for Mireille Danvers, Imani Castell, and the bank's platform and incident teams, as of Friday, August 7, 2026. Its distribution line is Operational: This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis.

**What it does not cover.** It does not repeat the closures in the eradication report, and it adds no new finding about the attack. It states no legal conclusion. Hours appear only as totals: the Response used 56, and the Recovery used 104 of its 110. It does not test the estate beyond the map's checks and the indicator list. It cannot see what the logs do not record: reads from the imaging archive before July 31 stay unknown.

# The gate

**The gate is met on Friday, August 7, 2026, at 15:00 EDT, on the trail and the map; the seven-day watch was live, every canary fired and was acknowledged as a test, and no attacker indicator was active (G-7).** Seven criteria are gate criteria. G-8, the hand-off, happens after the gate. Every criterion has a result and a place where it is shown. The gate says the door is closed and that the watch was proven live and found no attacker activity. It does not say the estate is without risk: the residual risks in the eradication report stand, and RC-4 is closed for new versions only (G-2).

**Who signs.** Vantalect's investigator runs the sweep and grades it. Owen Tribble, Senior Cloud Engineer at the bank, reruns the stored queries from the evidence account (`wf-ir-evidence`), compares his results with ours, and signs each criterion in the last column. He did not write or change any query. He authored some of the week-three pull requests, so Mireille Danvers signs the gate as a whole. Half of Vantalect's fee depends on this gate, which is why the bank's own engineer, and not only ours, checks it.

**The gate's criteria, their results on August 7, and the bank's sign-off. G-7 is shown by the watch tables below; G-8 was done after the gate.**

| No. | Criterion | Result | Where it is shown | Bank sign-off |
|---|---|---|---|---|
| **G-1** | The three critical root causes (RC-1, RC-2, RC-3) are closed as code | Met | The pull requests in the eradication report: RC-1 and RC-2 July 28, RC-3 July 29. RC-4 is not counted here | Owen Tribble, August 6 |
| **G-2** | RC-5 is closed, and RC-4 is closed for new versions with the existing-object gap carried as a residual risk with an owner and a date | Met for RC-5. RC-4 is partly closed | RC-5 July 31; RC-4 July 30 for new versions only, with the existing objects carried as R-2 in the eradication report | Owen Tribble, August 6 |
| **G-3** | RC-6 is accepted in writing, with an owner and a date | Met | ACC-1, signed by Mireille Danvers July 31, owner Imani Castell, until December 18, 2026 | Owen Tribble, August 6 |
| **G-4** | Every one of the 31 inventory items is closed, held, or accepted, with a verification | Met | The eradication report, all 31 rows | Owen Tribble, August 6 |
| **G-5** | The week-one map, run again the same way, shows no attacker object or trust that was not there in week one, and every fixed item stays fixed | Met | The map table below: 19 checks; one open by design (M-16), and M-15 closed for new versions only | Owen Tribble, August 6 |
| **G-6** | Every indicator search, run again the same way, shows no new hit since week one | Met | The indicator table below: no new hit on any indicator | Owen Tribble, August 6 |

| No. | Criterion | Result | Where it is shown | Bank sign-off |
|---|---|---|---|---|
| G-7 | The seven-day watch was proven live by planted canaries, has every alert dispositioned, and none open, and shows no attacker indicator active | Met: the watch was live each day, every canary fired and was acknowledged as a test, and no attacker indicator was active | The watch tables below; the watch record, sealed as EVD-029 | Owen Tribble, August 7 |
| G-8 | Vantalect's access to the bank's accounts is removed, and the custody log is closed | Done after the gate, 16:40 to 16:55 EDT | The roles-removed table below; the final custody log | Mireille Danvers, August 7 |

# The method

**Week one and week four are comparable because nothing about the method changed.** The first pass is the week-one map, exported Tuesday, July 14 and delivered Friday, July 17. The second pass is Wednesday, August 5.

- **One list of checks.** The week-one map is the list of estate checks in the estate report, run from the configuration export of July 14 (sealed as EVD-026). The sweep runs each of them again, in the same order, with the same queries, on Wednesday, August 5.
- **One list of indicators.** Every indicator in the indicator appendix is searched the same way each time: the same query against the organization trail, the same fields, the same window start of June 1, only a later window end.
- **One query set, two readers.** The same Vantalect investigator runs both passes, and nothing is added to a query between the runs. The queries are stored, unchanged, in `wf-ir-evidence` with the sealed sweep results, so anyone with access can rerun them. A bank engineer, named in the gate table, reruns the stored queries for the map, the indicators, and the watch, compares his results with ours, and signs each criterion. He does not write or change a query.
- **Results side by side.** Each table below has the week-one result, the week-four result, and what changed. A check that did not change is shown, not dropped.
- **What a hit is.** A hit is an event in the trail with the indicator as the caller, the source address, or the principal. Calls the bank's responders made on an indicator (to delete it, for example) are not hits, and neither is the bank's own nightly sync from 198.51.100.200, which uses the key `svc-artifact-sync` before it was deleted.

## The week-one map against week four

**Of the 19 checks in the week-one map, 11 moved to a better result, 8 stayed the same, and one of those (M-16, the Recycle Bin) is open by design with a date. M-15 (Object Lock) moved for new versions only.** No check got worse.

**The week-one map, run the same way twice.**

| ID | Check | Week one (July 14) | Week four (August 5) | What changed |
|---|---|---|---|---|
| **M-1** | Accounts in the organization | 22 (20 before the incident, 2 added on July 4) | 22 | None. No account was added or removed. |
| **M-2** | IAM users with an active access key | 9 users, 11 keys | 0 users, 0 keys | Closed (W-1): 5 users deleted, 4 moved to roles |
| **M-3** | IAM users, keys, or roles created by the attacker that still exist | 0 (deleted July 8) | 0 | None. They were gone before week one. |
| **M-4** | Roles that trust the attacker's account | 0 | 0 | None |
| **M-5** | wf-deploy-pipeline: trust narrowed to the Jenkins role with a source identity | 10 of 10 (by hand, July 8) | 10 of 10 | None in the result |
| **M-6** | wf-deploy-pipeline: trust defined in code and in sync | 0 of 10 | 10 of 10 | Closed (RC-2) July 28 |
| **M-7** | Other roles that trust a whole account with no condition | 5 roles in 4 accounts | 0 | Closed (W-2) July 31 |
| **M-8** | Build identity | OIDC role, set by hand July 8 | OIDC role, in code | Closed (RC-1) July 28 |
| **M-9** | KMS keys with origin EXTERNAL | 3, in PendingImport, material expired | 3, unchanged | None. A DisableKey on July 8 was rejected for that state; held for counsel. |
| **M-10** | Customer managed key policies that name an account outside the organization | 0 (the outside statement was dropped from the three attacker keys on July 4) | 0 | None. The three keys are held for counsel. |
| **M-11** | Organization policies attached (SCP and RCP) | 4 (3 SCPs, 1 RCP) | 6 (4 SCPs, 2 RCPs) | The guardrail SCP and RCP added at the root July 29 (RC-3). The evidence account's deny-all, `wf-evidence-deny-all`, is in both counts. |

| ID | Check | Week one (July 14) | Week four (August 5) | What changed |
|---|---|---|---|---|
| **M-12** | Accounts with block public access for EBS snapshots on | 0 of 22 | 22 of 22 | Closed (W-6) July 29 |
| **M-13** | Management events with an alert path | GuardDuty findings only | All management events, to Pursuit's watch and the provider | Closed (RC-5) July 31 |
| **M-14** | S3 data events on the imaging, data lake, and lending buckets | Writes on imaging and data lake; nothing on lending | Reads and writes on imaging and lending; writes on data lake | Closed (RC-5) July 31 |
| **M-15** | Object Lock on wf-imaging-archive-prod | None | Governance mode, 30 days, new versions only | Closed for new versions (RC-4) July 30. The 286 million existing objects have no retention: open, planned (R-2). |
| **M-16** | EBS Recycle Bin retention in the prod accounts | 10 days, unlocked | 10 days, unlocked | None. Open: the fix is dated August 14 (W-5). |
| **M-17** | Ransom notes present in the three buckets | 3 | 0 | Removed July 28 after sealing |
| **M-18** | Snapshots made by the attacker that still exist | 92 EBS (46 and 46 copies), 2 database | 0 EBS, 1 database (held for counsel) | Removed July 28; one copy isolated |
| **M-19** | Current business-data object versions under an attacker key, by query of the bucket's live inventory table (the preserved ransom-note versions are excluded) | 0 (July 7 query; the completion reports of the rewrite jobs show no failed task) | 0 | None. A scheduled S3 Inventory report is a later confirmation, not the basis. |

## The indicator searches

**Every indicator returns the same hits in week four as in week one, and none returns a new one.** The history is the attacker's record: the last attacker event in the trail is Saturday, July 4, 02:59 EDT (`EV-00643`). Nothing has come from any indicator since.

The indicator searches, run twice with the same query. A hit is an event with the indicator as caller, source, or principal.

| Indicator | Type | Week one: hits to July 14 | Week four: hits to August 5 | New hits |
|---|---|---|---|---|
| `203.0.113.47` | Source address | 463 | 463 | 0 |
| `198.51.100.41` | Source address | 28 | 28 | 0 |
| `198.51.100.23` | Source address | 24 | 24 | 0 |
| **Account `777788889999` as caller** | Account | 8 | 8 | 0 |
| `AKIAWRFNEXAMPLE00001` **(svc-artifact-sync)** | Access key | 85 | 85 | 0 |
| `AKIAWRFNEXAMPLE00002` **(aws-support-sync)** | Access key | 8 | 8 | 0 |
| **Session names `jenkins-sync-*`** | Session name | 416 | 416 | 0 |
| **Sessions of `wf-deploy-pipeline` by the stolen key** | Session | 37 | 37 | 0 |
| `alias/wf-backup-2026` | KMS alias | 3 | 3 | 0 |
| **KMS keys with origin EXTERNAL created** | KMS key | 3 | 3 | 0 |
| **Roles `OrgAccessBackup` and `s3-batch-replication`, user `aws-support-sync`** | Principal | 0 existing | 0 existing | 0 |
| `RESTORE-INSTRUCTIONS.txt` | Object name | 2 events | 2 events | 0 |
| **All attacker events** | Total | 519 | 519 | 0 |

# The seven-day watch

**The watch ran from Friday, July 31, 09:00 EDT to Friday, August 7, 09:00 EDT, seven days, with the rules below.** Pursuit's watch read every management event and the read and write data events on the imaging and lending buckets, and alerted on:

- Any call by one of the three attacker addresses, by the attacker's account, or by a principal the watch has marked
- Any key created with origin EXTERNAL, or any key material imported
- Any snapshot or image shared outside the organization, and any lifecycle, versioning, or Object Lock change on the archive
- Any new IAM user, access key, or role trust that names an outside account
- Any change to, or removal of, an organization policy or a trail

Every alert gets one of three dispositions:

**The three dispositions an alert can take. The gate cannot be met while any alert is open.**

| Disposition | Meaning |
|---|---|
| **Explained** | A named change by a named person accounts for it |
| **Escalated** | Treated as a real event and handed to the on-call engineer and the CISO |
| **Open** | No disposition yet. The gate cannot be met while any alert is open. |

**The watch was live on every day, every planted canary fired and was acknowledged as a test, and no attacker indicator was active.** Pursuit replayed the watch window from the scenario's records: 14 indicators (the attacker's keys, principals, addresses, account, keys, and sessions), each counted by local day. The watch read 442 events in the window, from the bank's ordinary activity and the sweep's own reads, and every day recorded events. None of them matched an indicator. To prove the detectors worked, the bank's platform engineer planted a canary on 13 of the watch's rules, each a harmless test call from the role `wf-watch-selftest`, and each raised its alert. 13 alerts fired in the window, all 13 were acknowledged as tests by a named person, 0 were unexplained, and none was open when the gate was met.

The seven-day watch, day by day, replayed by Pursuit from the scenario's records. No event matched an indicator, and every alert was a planted canary.

| Day (09:00 to 09:00 EDT) | Events watched | Events matching an indicator | Indicators active | Canary alerts, acknowledged as tests | Unexplained or open at end of day |
|---|---|---|---|---|---|
| **Friday, July 31** | 61 | 0 | 0 | 0 | 0 |
| **Saturday, August 1** | 25 | 0 | 0 | 0 | 0 |
| **Sunday, August 2** | 37 | 0 | 0 | 0 | 0 |
| **Monday, August 3** | 100 | 0 | 0 | 13 | 0 |
| **Tuesday, August 4** | 73 | 0 | 0 | 0 | 0 |
| **Wednesday, August 5** | 73 | 0 | 0 | 0 | 0 |
| **Thursday, August 6** | 73 | 0 | 0 | 0 | 0 |

The canaries. Each is a test call from the watch self-test role, and each alert was acknowledged as a test.

| Rule | What it watches | Fired (UTC) | Caller | Disposition |
|---|---|---|---|---|
| **PU-01** | KMS key created with external key material or an external key store | 2026-08-03T14:02:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-02** | KMS key material imported, deleted, or rotated on demand | 2026-08-03T14:03:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-03** | KMS key deletion scheduled, or key policy opened to an outside principal | 2026-08-03T14:04:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-04** | S3 write with a customer-provided key (SSE-C), or SSE-C unblocked on a bucket | 2026-08-03T14:06:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |

| Rule | What it watches | Fired (UTC) | Caller | Disposition |
|---|---|---|---|---|
| **PU-05** | S3 write encrypted under a KMS key from another account | 2026-08-03T14:08:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-06** | Lifecycle rule expiring versions within 30 days, or versioning suspended | 2026-08-03T14:10:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-07** | Burst of snapshot and recovery-point deletions | 2026-08-03T14:12:45Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-08** | Snapshot or image shared outside the organization | 2026-08-03T14:15:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-09** | Deletion protection turned off | 2026-08-03T14:17:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-10** | Trail stopped, deleted, or its selectors changed | 2026-08-03T14:19:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-11** | IAM user, access key, or role with outside trust created, or trust changed | 2026-08-03T14:21:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-12** | S3 Batch Operations job created | 2026-08-03T14:23:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |
| **PU-13** | Leave organization, close account, or SCP policy type disabled | 2026-08-03T14:26:00Z | `wf-watch-selftest/imani-castell` | Explained: a test by a named engineer, acknowledged |

Two rules were not tested with a canary, on purpose: PU-14 (needs the intruder's own credentials; the bank does not test a closed path by reopening it); PU-15 (needs a successful outside use of a followed key or role, and a denied one is logged only in the caller's account). Their detectors were not proven by a live test in this watch.

**The 14 indicators the watch counted, and when each was last seen. No indicator was active in the window.**

| Indicator | Events before theLast seen before the windowwindow (EDT) | Events in the window |
|---|---|---|
| **access key of svc-artifact-sync** | 90July 4, 01:24 EDT | 0 |
| **access key of aws-support-sync** | 7July 4, 03:00 EDT | 0 |
| **KMS key b9885f41** | 21August 7, 09:59 EDT | 0 |
| **kms grantee exfil-runner** | 8July 4, 01:36 EDT | 0 |
| **KMS key 6d9bd1af** | 13August 7, 10:00 EDT | 0 |
| **KMS key 33767b29** | 14August 7, 10:02 EDT | 0 |
| **role s3-batch-replication** | 61,300July 4, 01:28 EDT | 0 |
| **role OrgAccessBackup** | 1July 4, 01:39 EDT | 0 |
| **iam user aws-support-sync** | 8July 4, 03:00 EDT | 0 |
| **attacker address 198.51.100.23** | 24June 30, 09:51 EDT | 0 |
| **attacker address 198.51.100.41** | 29July 2, 10:17 EDT | 0 |
| **attacker address 203.0.113.47** | 499July 4, 03:00 EDT | 0 |
| **outside account 777788889999** | 8July 4, 01:36 EDT | 0 |
| **the attacker's 41 role sessions** | 61,726July 4, 02:50 EDT | 0 |

The watch record, with its hash, is sealed in `wf-ir-evidence` as EVD-029 and listed in the custody log.

# The roles removed

**Vantalect's access to the bank's accounts was removed on Friday, August 7, 2026, after the gate, the sweep results were sealed, and Vantalect's working copies were destroyed.** The attacker's own roles and users, removed on July 8, are listed with them so one table shows every principal that should be gone. After this removal, any further access to a bank account is a new decision of the bank's.

Every role, trust, and exception removed, with who removed it and how we verified it.

| Role or access | Where | Created | Removed | By | Verified |
|---|---|---|---|---|---|
| **VantalectIncidentResponse (the incident role)** | 20 accounts, the ones that existed on July 4 | July 4, 01:39 EDT; a self-managed stack set run through the `wf-break-glass` execution role (`EV-00567`, `EV-00571`), and in wf-management a separate stack (`EV-00611`) | August 7, 16:40 EDT | Imani Castell | The stack set has no instances left and the wf-management stack is deleted; GetRole returns NoSuchEntity in 20 of 20 accounts (the two accounts added on July 4 never had the role) |
| **The incident role's exception in the guardrail SCP** | wf-org-guardrails and wf-incident-containment | July 4, 01:22 EDT; RE-003 | August 7, 16:48 EDT | Imani Castell | Both policy documents no longer name the role |
| **Trust in the Vantalect account** | Every account, every role | July 4, 01:39 EDT; the same stack set and stack | August 7, 16:55 EDT | Mireille Danvers | Access Analyzer's external access findings list no principal in the Vantalect account |
| **OrgAccessBackup (the attacker's role)** | wf-prod-lending | July 3, 22:36 EDT; EV-00513 | July 8, 10:02 EDT | Imani Castell | Deleted in the Response; still absent in the sweep |
| **s3-batch-replication (the attacker's role)** | wf-prod-imaging | July 3, 21:39 EDT; EV-00391 | July 8, 10:03 EDT | Imani Castell | Deleted in the Response; still absent in the sweep |
| **aws-support-sync (the attacker's user and key)** | wf-prod-data | July 3, 22:31 EDT; EV-00510 | July 8, 10:01 EDT | Imani Castell | Deleted in the Response; still absent in the sweep |
| **svc-artifact-sync (the compromised user and key)** | wf-tools | March 14, 2023; The credential report | July 8, 10:10 EDT | Imani Castell | Deleted in the Response and replaced by an OIDC role; still absent in the sweep |

## What stays open after the gate

**The gate closes the Recovery's work, not the bank's.** Seven residual risks stand, each with an owner and a date, in the eradication report: the accepted RC-6 until Friday, December 18, 2026, the Object Lock coverage of the existing objects (RC-4, planned, not accepted in writing), the management account, the data that probably left and cannot be recalled if it did, the unknown reads before July 31, the Jenkins controller, and the open weaknesses in the root-cause report. The Recycle Bin fix (W-5) is due Friday, August 14, 2026. Whether, when, and to whom the bank discloses any of this is for the bank and counsel.

## 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.