Vantalect



AWS INCIDENT RESPONSE RETAINER · SAMPLE DELIVERABLE

Readiness Readout

DISTRIBUTION: OPERATIONAL

Week 3 of the Retainer: Readout · prepared for Wrenfield Bancorp, Inc.

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

August 28, 2026 · AWS Incident Response Retainer (one year)

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

What the bank is ready for 3

The readiness scorecard 3

The log gaps, one by one 5

What is still exposed 7

The commitments in force 9

The prepaid hours 10

What happens next 10

Notice 11

What this report is

2 of the 6 readiness items are done, 3 are done with open items (four scheduled log changes, the watch's alert test results, and the broker's listing), and 1 is scheduled: the tabletop on Tuesday, September 15, 2026. Mireille Danvers, Imani Castell, and Harold Penwick: this is the readiness status as of Friday, August 28, 2026, 18 days into the Retainer, which began Monday, August 10, 2026. The first 30 days and the tabletop are still ahead, and this readout separates the work completed from the work still scheduled. It says what the bank can count on today, what it is still exposed to, what Vantalect has committed to, and where the prepaid hours stand.

This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis. The report covers the Retainer's readiness work through Friday, August 28, 2026. It does not cover the tabletop's results (the exercise has not been held), any incident after August 28, or any legal question. Nothing in it is a determination that a regime applies to the bank; counsel and the bank decide that.

What the bank is ready for

If an incident began tonight, the bank could activate Vantalect in one call, Vantalect could make its first read in about 9 minutes and read in all 22 accounts, the watch is installed to page the bank's on-call and Vantalect (its alert test results are not yet in this readout), and the containment policies would be attached and not written. Four things stand behind that sentence.

- **The role works.** The drill on Wednesday, August 12, 2026 measured 9 minutes from the activation call to the first read, against the Retainer's target of under 15 minutes. The role read in 22 of 22 accounts after one fix and wrote nowhere except the evidence bucket. On July 4 the role was deployed 42 minutes after Charles joined the bridge.
- **The logs mostly exist.** 4 of the 9 gaps the four attack patterns need are closed and 1 is installed with its verification pending; 4 more are scheduled to close by Friday, September 11, 2026. The bank declined one optional item in writing.
- **The watch is on.** It was installed on Wednesday, August 19, 2026 and carries the controls that closed RC-5. The Identity Center rule was installed on Monday, August 24, 2026; its test alert has not been received. Pursuit's alert counts and test results are not in this readout.
- **The paper is in place, mostly.** The incident statement of work is pre-agreed with outside counsel and is signed by counsel at activation, so each incident is papered new, through counsel. Counsel decides whether the pre-agreed template is enough. The broker's listing of Vantalect is the open item.

The readiness scorecard

Each of the six items the Retainer promises for the first 30 days, and where it stands. The scorecard is a status, not a grade.

The readiness scorecard as of August 28.

Item	Status	Evidence	Still open	Owner	Next
The activation role	**Ready**	Deployed to every account August 11. Drilled August 12; one finding (D-1), fixed the same morning. Report: retainer-1–access.	None	Mireille Danvers	Re-run after any change to the StackSet, the hold, or the root policies.
The log-readiness check	**Ready, four gaps scheduled**	Check run August 17 to 21. Report: retainer-2–log-readiness.	Four scheduled gaps (G-2, G-3, G-4, G-8).	Imani Castell	Last scheduled date: September 11.
Pursuit's watch	**Installed, alert tests pending**	Installed in wf-audit August 19. The Identity Center rule was added August 24. Alert test results: not yet in hand.	Alert test results (Pursuit's figures).	Imani Castell	Confirm that on-call and Vantalect receive the alerts.
The guardrail pack	**Ready**	Containment service control policies and resource control policies stored detached in the bank's policy repository, with a sealed copy under the `guardrail-pack/` prefix of the evidence account's bucket. Described in the call sheet of August 14.	None	Imani Castell	Re-check against the organization's live policies at each quarter.
The tabletop	**Scheduled**	Half-day exercise with the incident team and counsel, scenario chosen: an IAM Identity Center administrator's session hijacked.	Not yet held.	Mireille Danvers	September 15.
The paper	**Ready, one item open**	The incident statement of work was pre-agreed with outside counsel for signature at activation. The call sheet was delivered August 14.	The broker's written listing of Vantalect as a named non-panel provider has been requested and is not in hand.	Harold Penwick	The general counsel to chase; target September 11.

The drill's measure: 9 minutes from activation call to first read, 22 accounts, one finding (D-1). The log check's measure: 10 gaps found, 4 closed, 1 awaiting verification, 4 scheduled, 1 declined.

The watch's alert results are not in this readout. The alert counts, the test change of the Identity Center rule, and the times an alert reached on-call and Vantalect are Pursuit's figures. We will report them when Pursuit's watch output is delivered.

The log gaps, one by one

Of the 9 required gaps, 4 are closed (an estimated $41 a month), 1 is installed and awaiting verification ($0 a month), and 4 are scheduled ($75 a month). The costs are the estimates in the log-readiness report, which are estimates for the sample, not quotes. Together they come to $116 a month. A gap is marked closed only after its result is recorded; G-9 is installed and not yet closed.

The bank's decision on each log-readiness gap. Costs are estimates for the sample.

Gap	Shortfall	State	Date	Monthly	Note
G-1	The trail's files expire after 90 days and the bucket is not locked	Closed	August 25	$34	Retention set to 400 days; Object Lock default on the trail bucket.
G-2	Read events are not collected on the data lake	Scheduled	September 4	$60	Change window agreed with the data lake owner.
G-3	No standing query path over the trail	Scheduled	September 11	$6	Athena table over the trail files to be created after the trail change settles.
G-4	No S3 server access logs on the three buckets that matter	Scheduled	September 11	$6	With the data lake change.
G-5	No scheduled inventory of the imaging archive's encryption type	Closed	August 27	$3	First weekly inventory delivered to the evidence bucket (encryption type only; key identity comes from the live inventory table).
G-6	No Config recorder in the two accounts created July 4	Closed	August 26	$4	Recorder on in both accounts; aggregator updated.
G-7	Analyzer findings do not reach the watch	Closed	August 24	$0	Rule for analyzer findings added to the watch; the organization analyzer itself has run since July 4.
G-8	Trail integrity is validated but never checked	Scheduled	September 4	$3	Function written; test failure path first.
G-9	No alert for Identity Center changes	Pending	August 24	$0	Installed; verification pending. The test alert result is not yet in hand. Owner: platform lead; due September 4.
G-10	No flow logs on the workload VPCs	Declined	August 26	$60	Accepted in writing by the CISO: flow logs are not needed for the four patterns.

What is still exposed

Twelve things remain, and one of them is accepted in writing: RC-6. A readout that listed only what is fixed would mislead you. These are what we would tell a new executive about on their first day.

Residual exposures as of August 28.

ID	What is exposed	Owner	Status	Reference
X-1	The month-end database snapshots (nine in wf-prod-lending) have central copies in wf-backup under Vault Lock in governance mode, which a principal with the right permission can shorten or remove. The bank accepted this in writing (RC-6) until the vault moves to compliance mode next quarter.	Imani Castell	Accepted in writing until the move	RC-6
X-2	Four log gaps are scheduled and not yet closed: read events on the data lake, a standing query path over the trail (an Athena table, since CloudTrail Lake is closed to new customers), server access logs, and the integrity check.	Imani Castell	Scheduled to September 11	G-2, G-3, G-4, G-8
X-3	One responder. A second client's incident at the same time would get the call-back commitment and a 4-hour hands-on commitment, not the 2-hour one.	Mireille Danvers	A named backup responder does not exist yet	Retainer terms
X-4	The team has not yet used the plan under pressure. The drill tested the role, not the people.	Mireille Danvers	Tabletop September 15	Tabletop
X-5	Reads of the imaging archive before July 31 remain unknown because read events were not collected. This cannot be changed.	Mireille Danvers	Permanent	RC-5
X-6	The broker has not confirmed Vantalect as a named non-panel provider in writing.	Harold Penwick	Requested	The paper

ID	What is exposed	Owner	Status	Reference
X-7	The recovery vault holds plain database snapshots, not under any snapshot lock, protected by the vault organizational unit's policy and by keys the bank holds. Someone with Organizations rights in the management account could change that policy. The 14-day lock on the volume snapshot copies ran out on July 20 unless the bank extended it.	Mireille Danvers	Open; the bank decides what to lock	Recovery vault
X-8	The Identity Center watch rule (G-9) is installed, but no test alert has been received, so nobody has shown that an alert reaches on-call or Vantalect.	Imani Castell	Installed; verification pending; a received test alert is due September 4	G-9
X-9	RC-4 is closed for new object versions only. It remains open for the 286 million object versions that existed on July 30, which have no retention; retention for them needs an S3 Batch Operations job the bank has not chosen.	Mireille Danvers	Open; planned for September 30; not accepted in writing	RC-4, closure R-2
X-10	The Jenkins controller is the trust anchor for the build and its disk was never imaged; hardening it is outside the Recovery.	Imani Castell	Open; no closure recorded; date September 15	Closure R-6
X-11	Four weaknesses (W-3, W-4, W-5, and W-8) were open with dates, and the legacy trails in W-7 were to retire by August 14. This readout has no record that any of them closed.	Mireille Danvers	Open or unverified; the carried date is September 30	Closure R-7
X-12	Data probably copied out in July cannot be recalled if it was, and any use made of it is unknown.	Diane Whitcombe	Standing; counsel decides what follows	Closure R-4

RC-6 deserves its own paragraph because it is the root cause the bank accepted in writing rather than closed. RC-6 is accepted pending its cutover; RC-4 is closed only for new versions and remains open for the existing versions (X-9). The nine month-end database snapshots are copied centrally into `wf-backup`, where the backup vault runs Vault Lock in governance mode. Governance mode lets a principal with the right permission shorten or remove the lock; compliance mode lets no one, not even the account's root user. On July 31, 2026 the bank accepted the risk in writing until the vault moves to compliance mode next quarter. The July recovery also copied 46 EBS snapshots into the recovery vault under a snapshot lock in compliance mode on July 6 (14 days, with a 72-hour cool-off). Unless the bank has extended it, which this readout does not show, that

lock period ended on July 20. The 10 database copies in the vault are plain snapshots and are not under any lock; they rest on the vault organizational unit's policy, which also denies deletion and key changes to everyone, and on keys the bank holds. The weakest link is a person with Organizations rights in the management account who could change that policy. The AWS Backup Vault Lock covers one recovery point of the live database, not these copies. Nothing in this readout changes the bank's acceptance. We will list RC-6 in each readout until it closes.

The commitments in force

Vantalect's commitments run from Monday, August 10, 2026 through August 9, 2027. The term is one year, for $36,000, invoiced in advance (WF-INV-5, issued August 10, due August 25). The rate for any incident hour is $450, against the $675 the bank paid for the July Response.

The response commitments, 24 hours a day, 365 days a year. Credits are capped at 30% of the annual fee a year ($10,800).

Commitment	Default	Service credit if missed
Call-back after a page to the incident line, any hour of any day	30 minutes	10% of the annual fee ($3,600)
Hands-on (role assumed, containment proposed) after counsel signs the activation	2 hours	10% of the annual fee ($3,600)
Written situation report	Every 12 hours until containment is declared	None

Four limits are part of the commitments and not footnotes to them.

- **One responder.** The Retainer is one consultant, Charles Sieg. The agents he directs are not billed separately. Until a named backup responder exists, the commitments carry the overlap limit below.
- **Overlap.** When two retained incidents overlap, the second gets the call-back commitment and a 4-hour hands-on commitment, not the 2-hour one. The Retainer is capped at six clients so that overlap stays unlikely, and we cannot make it impossible.
- **Two parts of paper.** The readiness part is a statement of work between the bank and Vantalect. The incident part is the pre-agreed incident statement of work, which outside counsel signs at activation. Counsel decides whether the pre-agreed template is enough and how each incident is papered.
- **What we do not do.** We do not contact, negotiate with, or pay an attacker, advise whether to pay, or make a legal determination. The Response report set says the same.

For comparison: the July Response used 56 hours at $675, for $37,800. At the Retainer's rate, the same hours would have been $25,200. The activation authorization for a retained client is $10,800 (24 hours at $450). It is billed to counsel's matter, and no prepaid hour is drawn for it at activation.

The prepaid hours

The Retainer includes 40 prepaid readiness hours, worth $18,000 at $450, and none has been used. The readiness work is planned at 48 hours in total, which the fee covers; the tabletop and its report on September 15 are the last of it and have not yet been done. The prepaid hours are separate.

Hours in totals, as of August 28.

Item	Hours	Value
Readiness work, covered by the fee	48 (planned total, tabletop included)	Included
Prepaid readiness hours, used so far	0	$0
Prepaid readiness hours, untouched	40	$18,000

What the prepaid hours pay for: further readiness work, such as a second tabletop, a compromise assessment, or a re-run of the log-readiness check. They do not pay for an incident. Each incident is engaged fresh by the bank's outside counsel under its own papers and billed to counsel's matter at the Retainer rate from the first hour, and no prepaid hour is drawn at activation. If counsel directs after containment, Vantalect credits up to the unused prepaid hours against that matter's invoices by a separate credit memo, and the hours so credited are no longer available for readiness work. Unused hours at the end of the term convert to readiness work in the last 60 days. That period begins June 11 for this term. Up to 20 hours roll into a renewal. No cash is refunded except as the master agreement's early-termination clause provides.

What happens next

1. **September 4 and September 11.** The four scheduled log changes, and a received test alert for the Identity Center rule (G-9). Owner: Imani Castell.
2. **By September 11.** The broker's written listing of Vantalect. Owner: Harold Penwick.
3. **September 15.** The tabletop. The after-action report follows.

4. **Next quarter.** The backup vault to compliance mode, which closes RC-6. Owner: Imani Castell.
5. **Once a quarter.** A short re-run of the role drill. The bank decides whether to schedule it.

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.