

Vantalect

AWS INCIDENT RESPONSE RETAINER · SAMPLE DELIVERABLE

Log-Readiness Check

DISTRIBUTION: OPERATIONAL

Week 2 of the Retainer: Log readiness · prepared for Wrenfield Bancorp, Inc.

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

August 21, 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

The finding in one table 3

The log sources 5

The gaps, their fixes, and monthly costs 7

Pursuit's watch 10

Next steps 11

Notice 12

What this report is

Today the bank's logs would answer most of what the next investigation needs, and 10 gaps remain: 9 that the four attack patterns need, with a combined estimate of $116 a month, and one optional. Mireille Danvers and Imani Castell: this is the result of the check we ran from Monday, August 17, 2026 to Friday, August 21, 2026. It asks one question: if a ransomware actor, a deleter, a copier, or a persistence builder showed up tomorrow, would the evidence exist, and would anyone be told?

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 bank's log sources in the organization's 22 accounts, measured against four patterns drawn from the July incident and from how this kind of attack is usually carried out. It does not cover application logs, host logs, or the bank's own SIEM, and it does not estimate what a logging change costs the bank's staff time. It holds no legal analysis, and it says nothing about what the bank must retain for any regulator; counsel and the bank decide that.

Prices are estimates for the sample

All prices below are estimates for this sample, built from list prices as we understood them in August 2026 and rounded up to whole dollars. Check them against the AWS pricing pages and the bank's own volumes before you budget.

Method: Sonde and a log-source script. Sonde read the organization trail's configuration, the data event selectors, the EventBridge rules, the Config and GuardDuty settings, and the retention and lock settings of each log bucket in every account. The log-source script then tested each source with one harmless event and looked for it. Nothing was changed.

The finding in one table

All four patterns leave evidence in the trail today; what is thin is how long it stays, what it records about reads, and how fast we can query it.

The four patterns, what each leaves in the logs, and where the bank stands today. The alert identifiers are Pursuit's catalog identifiers.

Pattern	What we need to see	Watch alerts	Gaps	Today
P-A Key-based ransomware with imported key material	`CreateKey` with origin `EXTERNAL`, `ImportKeyMaterial` with an expiry, `PutKeyPolicy`, `CreateGrant`; S3 Batch `CreateJob`; bulk object writes under the new key; SSE-C requests and their denials; the count of objects under each key	PU-01, PU-02, PU-03, PU-04, PU-05, PU-12	G-3, G-5, G-8	Visible. The July 3 events were all in the trail; the watch is installed for them. The share of objects under each key can be read from the imaging bucket's S3 Metadata live inventory table (its `kms_key_arn` column), which the Recovery turned on July 5 and queried on July 7, with query results that were not independently preserved; an S3 Inventory report is a scheduled snapshot of encryption type, not key identity, and none is scheduled.
P-B Deletion of snapshots and object versions	`DeleteSnapshot`, `DeleteDBSnapshot`, `DeleteRecoveryPoint`; lifecycle and versioning changes; `DeleteObject` with a version; deletion protection turned off; the trail itself stopped or changed	PU-06, PU-07, PU-09, PU-10	G-1, G-3, G-6	Visible for the control plane and for the imaging and data lake buckets. Not visible: configuration history in the two accounts created July 4, and anything older than the trail's 90 days.
P-C Exfiltration by snapshot sharing	`ModifySnapshotAttribute` and `ModifyDBSnapshotAttribute` naming an outside account; a key policy or grant adding an outside principal; `Decrypt` and `ReEncrypt` from an outside account in the key owner's trail, including a call that is denied; reads of the data itself	PU-03, PU-05, PU-08, PU-15	G-2, G-4, G-8	Visible for sharing and for cross-account key use, which the key owner's trail records. Reads are visible on the imaging and lending buckets since July 31, and not on the data lake.

Pattern	What we need to see	Watch alerts	Gaps	Today
P-D Persistence by users, keys, roles, and sign-in permissions	`CreateUser`, `CreateAccessKey`, `CreateRole` or `UpdateAssumeRolePolicy` with an outside trust; Identity Center permission-set and assignment changes; changes to the organization's guardrails	PU-11, PU-13, PU-14, PU-15	G-1, G-6, G-7, G-9	Visible for IAM. Identity Center changes reach the trail but no alert covers them yet. The organization analyzer has flagged outside trusts since at least July 4, but its findings reach no alert.

The log sources

15 sources were checked; 5 are as they should be and 10 fall short. The table gives each source as found on August 17, which patterns it serves, and the gap that closes the shortfall.

The 15 log sources checked, with their state and the gap each shortfall maps to.

ID	Source	Where	State as found	Patterns	Gap
S-1	Organization trail, management events, all Regions	wf-log-archive	Present. Log file validation on. Files kept 90 days, then expired.	P-A, P-B, P-C, P-D	G-1
S-2	S3 data events, writes: imaging archive and data lake	wf-log-archive	Present (since before July 3).	P-A, P-B	None
S-3	S3 data events, reads: imaging archive and lending documents	wf-log-archive	Present since July 31 (RC-5).	P-C	None
S-4	S3 data events, reads: data lake	wf-log-archive	Not collected.	P-C	G-2
S-5	EventBridge, all management events, to the watch and the provider	every account to wf-audit	Present since July 31 (RC-5). Standing form installed August 19.	P-A, P-B, P-C, P-D	None

ID	Source	Where	State as found	Patterns	Gap
S-6	Query path over the trail (a standing CloudTrail Lake store, or an Athena table on the trail files)	wf-log-archive	None standing. The Investigation's store was closed at hand-over. CloudTrail Lake has been closed to new customers since May 31, 2026, so the plan does not depend on a new store.	P-A, P-B, P-C, P-D	G-3
S-7	S3 server access logs	imaging, lending, data lake	Not enabled.	P-B, P-C	G-4
S-8	S3 Inventory with encryption status (encryption type, not key identity)	wf-prod-imaging	No standing schedule. An inventory report is a delivered snapshot (daily or weekly), not a listing run on demand, so it cannot check a rewrite as it finishes. The Recovery checked the July 5 to July 7 rewrite against the completion reports of its 31 slice jobs and two Athena queries of the imaging bucket's S3 Metadata live inventory table (July 7, 13:52 and 13:55); a scheduled report would later confirm encryption-type coverage, not which KMS key encrypted each object.	P-A	G-5
S-9	AWS Config recorder and delegated aggregator	wf-audit	Present in 20 accounts. Not in the two created July 4.	P-B, P-D	G-6
S-10	IAM Access Analyzer, external access, organization	wf-audit	Present since at least July 4 (the organization analyzer `wf-org-external-access`, used on July 4 to list the outside trusts). Its findings are not routed to the watch.	P-D	G-7
S-11	Trail integrity validation, checked	wf-log-archive	Validation is on. No one runs the check.	P-A, P-B, P-C, P-D	G-8
S-12	Alert rule for Identity Center changes	wf-audit	No rule.	P-D	G-9
S-13	GuardDuty and Security Hub, delegated	wf-audit	Present. Findings go to the provider; since August 19 the watch also routes to on-call.	P-A, P-C, P-D	None

ID	Source	Where	State as found	Patterns	Gap
S-14	Evidence bucket under Object Lock	wf-ir-forensics	Present (created July 4).	P-A, P-B, P-C, P-D	None
S-15	VPC Flow Logs	wf-network only	Transit gateway only. Workload VPCs have none.	Context	G-10

Two things the table does not show. First, the organization trail has held what we need since before July 3, which is why the Investigation could reconstruct 4 days, 17 hours, 50 minutes of dwell time. Second, S3 object reads from the imaging archive stayed unknown for the July incident because read events were not collected; that gap was closed on July 31, 2026 (RC-5), and it cannot be closed backward. Nothing in this report changes what we could say about July.

The gaps, their fixes, and monthly costs

The 9 gaps the patterns need cost an estimated $116 a month in total, about $1,392 a year. The optional one adds $60 a month. Of the 9, 2 cost nothing. The costs are our estimates for the sample, each with its one-line basis.

Each gap, its fix, and its estimated monthly cost. Prices are estimates for the sample.

Gap	The shortfall	The fix	Monthly	Basis for the estimate	Owner
G-1	The trail's files expire after 90 days and the bucket is not locked	Keep trail files 400 days: Standard for 90 days, then Glacier Instant Retrieval. Set Object Lock in governance mode with a 400-day default.	$34	About 90 GB of new trail files a month across 22 accounts, stored at S3 and Glacier Instant Retrieval list prices.	Mireille Danvers
G-2	Read events are not collected on the data lake	Add read data events for the data lake bucket `wf-datalake-prod` to the organization trail.	$60	About 60 million read requests a month at $0.10 per 100,000 events.	Mireille Danvers
G-3	No standing query path over the trail	Create an Athena table over the organization trail files in wf-log-archive (with partition projection by account, Region, and date), with a saved set of the investigation queries, so a query takes minutes and not a day of loading. CloudTrail Lake has been closed to new customers since May 31, 2026, so this plan uses the trail files themselves.	$6	About 1.2 TB of trail files (400 days) scanned once a month by Athena at $5 per TB; the table definition has no charge.	Imani Castell
G-4	No S3 server access logs on the three buckets that matter	Turn on server access logging for the imaging, lending documents, and data lake buckets, each delivered to a log bucket in the same account and Region as the bucket it logs (S3 requires that), then replicate those logs to wf-log-archive if the bank wants one place for them.	$6	About 40 GB of log files a month at S3 Standard list price, stored in the source account and again after replication to wf-log-archive, plus request charges.	Imani Castell
G-5	No scheduled inventory of the imaging archive's encryption type	Schedule a weekly S3 Inventory of `wf-imaging-archive-prod` with the encryption status field, delivered to the evidence bucket. It confirms the encryption type of each object (SSE-KMS or not), not which KMS key was used. Read the key identity from the bucket's S3 Metadata live inventory table (the `kms_key_arn` column) and keep the saved query results.	$3	286 million objects at $0.0025 per million objects listed, four runs a month.	Imani Castell

Gap	The shortfall	The fix	Monthly	Basis for the estimate	Owner
G-6	No Config recorder in the two accounts created July 4	Record configuration in wf-ir-forensics and wf-recovery-vault and add both to the delegated aggregator.	$4	About 1,200 configuration items a month at $0.003 each.	Imani Castell
G-7	Analyzer findings do not reach the watch	Add a watch rule for new Access Analyzer external-access findings from the organization analyzer in wf-audit, on the bus already in place, so a new outside trust pages on-call and Vantalect.	$0	External access findings carry no charge, and a rule on the existing bus adds no new AWS charge.	Mireille Danvers
G-8	Trail integrity is validated but never checked	Run the trail's digest validation weekly from a scheduled function and send a failure to on-call.	$3	One scheduled function a week reading digest files: request and compute charges only.	Imani Castell
G-9	No alert for Identity Center changes	Add a watch rule for permission-set, assignment, and user-store changes in IAM Identity Center, on the bus already in place.	$0	A rule on the existing bus; no new AWS charge.	Imani Castell
G-10 (optional)	No flow logs on the workload VPCs	Optional. Flow logs for the five production VPCs, to S3 in wf-log-archive. They give context for network movement; none of the four patterns needs them.	$60	About 120 GB of flow logs a month at an assumed $0.50 per GB ingested.	Imani Castell
	Required total		**$116**	The 9 gaps the patterns need	
	With the optional gap		**$176**	Adds G-10	

What we recommend first. Closing G-1 (retention and lock) and G-9 (the Identity Center alert) costs little and removes the largest risks: an actor who waits longer than 90 days, and a hijacked administrator session nobody sees. Then G-2, the biggest line item, and G-3, which shortens the next investigation most. Whether to spend $60 a month on the flow logs is a judgment about network movement, not about the four patterns; we have no case for or against it in this incident, where no host access was found.

What we need from the bank. A decision on each gap by Friday, August 28, 2026, the readout, and an owner's date for each one accepted. A gap the bank chooses not to close is accepted in writing, like RC-6, and the readout lists it.

Pursuit's watch

Pursuit's watch was installed on Wednesday, August 19, 2026 in wf-audit, and it carries the same two controls that closed RC-5: all management events through EventBridge, and read data events on the imaging and lending buckets. The forwarding rules were deployed to every account by the StackSet, and they deliver to a central queue in the audit account. Alerts go to the bank's on-call pager and Vantalect.

The watch is the way a pattern becomes a page; the gaps above are what the watch cannot see. The alert catalog and its coverage are Pursuit's. Replayed over the July trail, the catalog raised 61,573 alerts in 59 alert groups; the last column shows which rules raised them.

Pursuit's alert catalog, grouped by the four patterns, with the alerts each rule raised when Pursuit replayed the July trail. A rule can sit in two patterns, so the columns do not add to the total.

Pattern	Alerts	What they cover	Raised on the July trail
P-A	PU-01, PU-02, PU-03, PU-04, PU-05, PU-12	New or imported keys, key policy and grant changes, SSE-C, writes under another account's key, and S3 Batch jobs	PU-01: 4; PU-02: 5; PU-03: 1; PU-04: 215; PU-05: 1; PU-12: 2
P-B	PU-06, PU-07, PU-09, PU-10	Lifecycle and versioning changes, bursts of snapshot and recovery-point deletes, deletion protection off, and trail changes	PU-06: 2; PU-07: 3; PU-09: 2; PU-10: 3
P-C	PU-03, PU-05, PU-08, PU-15	Sharing outside the organization, outside principals added to a key, and an outside account's use of a key a followed session created, denied or not (on July 5 this was PU-15, scenario name PU-outside-key-use)	PU-03: 1; PU-05: 1; PU-08: 2; PU-15: 8
P-D	PU-11, PU-13, PU-14, PU-15	New users, keys, and roles, outside trust, guardrail removal, a role or key made by a followed session and then used from outside the organization, and any action by a principal the watch has marked	PU-11: 15; PU-13: 1; PU-14: 61,309; PU-15: 8

Two limits. The watch has no rule for Identity Center changes yet (G-9), so a permission set or an assignment created by a hijacked administrator would reach the trail and not the pager. And the watch depends on the events arriving: a trail or a rule that someone disables raises an alert, but only if the rule that raises it is still in place.

What this report does not give. It gives no count of the events the watch forwarded since August 19, no count of alerts it raised, and no test result. Those are Pursuit's figures, and they belong in the readout once the watch has run long enough to measure.

Next steps

1. The bank decides each gap and names an owner and a date. The readout on Friday, August 28, 2026 lists the decisions.
2. Vantalect adds G-9 to the watch on request, as part of the watch, the same week.
3. The tabletop on Tuesday, September 15, 2026 tests the watch and the logs together on a different scenario.
4. We re-run the check in the last 60 days of the term if the bank wants it; that is one of the uses of unused prepaid hours.

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.