Vantalect



AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Compromise Inventory

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

About this report 2

The register in numbers 3

The register 5

- Principals used 5
- Credentials and principals created 5
- KMS keys created or changed 6
- Data stores re-encrypted, copied, shared, or read 8
- Data stores deleted, and what the attacker left behind 11
- Configurations changed 12
- Logging tampered with 13
- Compute touched 13

What we checked and excluded 14

What closes the open rows 15

Notice 16

About this report

This register lists 31 things the attacker used, created, changed, copied, or touched, and for each one it gives the account, the action, the time, the evidence, the status on July 24, and how sure we are. It is Vantalect's finding as of Friday, July 24, 2026.

Distribution: Counsel only

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. We send this report to Diane Whitcombe of Tessaly & Brook LLP, outside counsel, who decides who else reads it. Parts of it can later become the factual summary for regulators, insurers, and auditors; counsel decides what is released, to whom, and when.

What the status means on this date. The status column shows what the organization trail records on or before July 24. A row shows Removed, Isolated, or Restored only where the trail has the change, and the evidence number is beside it. Where the register's end state depends on work that is not yet recorded, the row shows **Open, planned for week 3**, and the next column gives the end state the register will hold when that work is done. 11 of the 31 rows are open on July 24. Week three of the Recovery (July 27 to July 31) is where they close. The rest were removed, isolated, or restored in the Response, between July 4 and July 8, or are accepted or closed, and each row gives its evidence and date.

Confidence. Confirmed means the trail records the action. Probable means the action is inferred from records we hold, and the report says what the inference is. Possible means we cannot exclude it and cannot show it. Ruled out means we checked and the evidence excludes it, and the evidence is in the table. Not observed means the records we reviewed show nothing, and we do not claim they could.

What it does not cover. It lists what the attacker did in AWS. The theft of the key outside AWS is not in it. It does not list what the bank did, except as the status of an attacker item. It does not say whether any regime applies or whether any notice is due: those are decisions for the bank and counsel. Counts of records come from the bank. Two rows are about what we cannot see: the copy-out of the database snapshot is **probable, with high confidence**, and not confirmed; and **object reads from the imaging archive are unknown, because reads were not logged**. We found no host access.

The register in numbers

31 rows in seven groups: 28 confirmed, one probable, one possible, and one with no host access observed (`CI-030`, which does not rule out host compromise). The row IDs (`CI-001` to `CI-031`) are the register's own and are the same in every report. Principals used (`PU-1` to `PU-3`) are listed with them but are not register rows: they were used, not created or changed.

The register by group and by status on July 24. Every row of the register is in exactly one group.

Group	Rows	Removed	Isolated	Restored	Accepted	Closed	Open
Credentials and principals created	4	4	0	0	0	0	0
KMS keys created or changed	7	1	6	0	0	0	0
Data stores re-encrypted, copied, shared, or read	10	2	0	0	2	0	6
Data stores deleted, and what the attacker left behind	6	0	0	3	0	0	3
Configurations changed	2	1	0	0	0	0	1
Logging tampered with	1	0	0	0	0	0	1
Compute touched	1	0	0	0	0	0	1

What is open. `CI-008`, `CI-009`, `CI-010`, `CI-013`, `CI-014`, `CI-015`, `CI-019`, `CI-023`, `CI-024`, `CI-025`, `CI-028`. Each is something the attacker made or changed that the trail does not yet show as removed or restored, or, for the legacy trail (`CI-019`), whose configuration was deleted and is not recreated, and which awaits the bank's acceptance. None of them lets the attacker act inside the bank's accounts: the attacker's user, key, and roles are deleted, the three keys' material has expired and the keys are in PendingImport (the bank's three `DisableKey` calls of July 8 were rejected, `EV-01052`, `EV-01054`, and `EV-01056`), and the containment SCP denies new keys, shares, and deletions. The exfiltration path closed in stage 1 of the Response, on Saturday, July 4, 2026: after we captured the share's attribute state, the key policies, and the grant (`EV-00625` to `EV-00631`, 02:03 to 02:05), the bank's break-glass role removed the share (`CI-026`, 02:08:20 EDT, `EV-00632`), dropped the outside statement from the three attacker keys' policies (`CI-001`, `CI-003`, and `CI-005`, 02:09:05 EDT to 02:09:45 EDT), and revoked the attacker's grant (`CI-027`, 02:10:30 EDT). The share had been open 137 minutes. Those five changes are in the register as closed, with the event that closed each. The deletion protection of `wf-los-prod` (`CI-028`) is still off; the containment SCP is the compensating control until week three. The rows are open because the register should not call an item closed without the record that closes it.

The register

The register has seven groups of rows, and a table of the principals used. Wide tables are on landscape pages.

Principals used

The attacker used three identities that were not created that night: one stolen key, the bank's own deploy role, and a role in the attacker's own account. The first two are the bank's. They were abused, and the bank has narrowed them. The third is outside the organization.

The principals the attacker used. Times are MM-DD HH:MM:SS EDT, from the first to the last use.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
PU-1	wf-tools	IAM user `svc-artifact-sync` and key `AKIAWRFNEXAMPLE00001`	Stolen key: discovery, then 37 AssumeRole calls into `wf-deploy-pipeline`	06-29 03:14:02 to 07-04 01:24:05	`EV-00003` to `EV-00542`	Removed: key deactivated July 4, 01:24 (`EV-00543`); key and user deleted July 8, 10:10 (`EV-01075`, `EV-01076`); an OIDC provider replaced them (`EV-01077`)	Removed	Confirmed
PU-2	10 workload accounts	Role `wf-deploy-pipeline` and its 37 sessions	Assumed 37 times with administrator access; the role is the bank's own and is still in use by its pipeline	07-01 10:21:14 to 07-04 01:24:05	`EV-00051`, `EV-00083` to `EV-00542`	Isolated: sessions revoked in all ten accounts July 4, 01:26 (`EV-00555` to `EV-00564`); trust narrowed July 8, 10:05 to 10:08 (`EV-01058` to `EV-01074`)	Isolated	Confirmed
PU-3	`777788889999` (outside the organization)	Role `exfil-runner`, session `s-9172`	Seven KMS calls on the prod-lending key (00:06 to 00:51 on July 4); a successful AssumeRole of `OrgAccessBackup` at 01:36 on July 4 (administrator session)	07-04 00:06:09 to 07-04 02:59:30	`EV-00522` to `EV-00525`, `EV-00528`, `EV-00530`, `EV-00531`, `EV-00569`	Accepted: outside the bank's reach. The resource control policy of July 4, 03:20 (`EV-00654`) denies the account's use of the bank's keys and its AssumeRole into the organization	Accepted	Confirmed

Credentials and principals created

The attacker made one user, one access key, and two roles. All four are gone from IAM; the evidence of their creation is in the trail.

Credentials and principals created: 4 rows. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-020	wf-prod-data	user/aws-support-sync	Created with AdministratorAccess; imitates a vendor support account	07-03 22:31:06	EV-00510	Removed: deleted July 8, 10:01 (EV-01047)	Removed	Confirmed
CI-021	wf-prod-data	AKIAWRFNEXAMPLE00002, key of aws-support-sync	Created for the attacker's user; first used 01:31 on July 4	07-03 22:31:58	EV-00512	Removed: deactivated July 4, 03:01 (EV-00646); deleted July 8, 10:00 (EV-01046)	Removed	Confirmed
CI-022	wf-prod-lending	role/OrgAccessBackup	Created, trusting the root of account 777788889999	07-03 22:36:14	EV-00513	Removed: deleted July 8, 10:02 (EV-01049)	Removed	Confirmed
CI-011	wf-prod-imaging	role/s3-batch-replication	Created, trusting S3 Batch Operations; passed to the copy job	07-03 21:39:12	EV-00391	Removed: deleted July 8, 10:03 (EV-01051)	Removed	Confirmed

KMS keys created or changed

Three keys with imported material, an alias on each, and one grant. The outside statement was dropped from each key policy and the grant revoked on July 4; the material expired on July 7, which put the keys in the PendingImport state, and the bank's DisableKey calls of July 8 were rejected for that reason. Nothing the bank needs is under them.

KMS keys created or changed: 7 rows. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-001	wf-prod-lending	key/b9885f41-4ff8-5cbf-9f54-7753a6180289	Created with origin EXTERNAL; material imported, expiring on the ransom deadline	07-03 21:06:08	EV-00084	Isolated: outside statement dropped from the key policy July 4, 02:09:05 EDT (EV-00633); material expired July 7, 18:00 (EV-01037), so the key is in PendingImport; the bank's DisableKey on July 8 at 10:03 was rejected with KMSInvalidStateException (EV-01052) and DescribeKey returned PendingImport (EV-01053); kept as it is for counsel	Isolated	Confirmed
CI-002	wf-prod-lending	alias/wf-backup-2026, on the prod-lending key	Alias created on the attacker key, imitating a backup key	07-03 21:06:15	EV-00085	Isolated: on a key in PendingImport (material expired, EV-01037); the alias itself is not deleted	Isolated	Confirmed
CI-003	wf-prod-imaging	key/6d9bd1af-48a0-5150-b619-9ab79ca2b680	Created with origin EXTERNAL; material imported, expiring on the ransom deadline	07-03 21:09:21	EV-00089	Isolated: outside statement dropped from the key policy July 4, 02:09:25 EDT (EV-00634); material expired July 7, 18:00 (EV-01038), so the key is in PendingImport; the bank's DisableKey on July 8 at 10:03 was rejected with KMSInvalidStateException (EV-01054) and DescribeKey returned PendingImport (EV-01055); kept as it is for counsel	Isolated	Confirmed
CI-004	wf-prod-imaging	alias/wf-backup-2026, on the prod-imaging key	Alias created on the attacker key	07-03 21:09:28	EV-00090	Isolated: on a key in PendingImport (material expired, EV-01038); the alias itself is not deleted	Isolated	Confirmed
CI-005	wf-prod-data	key/33767b29-2aaa-5253-83bf-0d1d670c1e43	Created with origin EXTERNAL; material imported, expiring on the ransom deadline	07-03 21:09:55	EV-00093	Isolated: outside statement dropped from the key policy July 4, 02:09:45 EDT (EV-00635); material expired July 7, 18:00 (EV-01039), so the key is in PendingImport; the bank's DisableKey on July 8 at 10:04 was rejected with KMSInvalidStateException (EV-01056) and DescribeKey returned PendingImport (EV-01057); kept as it is for counsel	Isolated	Confirmed
CI-006	wf-prod-data	alias/wf-backup-2026, on the prod-data key	Alias created on the attacker key	07-03 21:10:02	EV-00094	Isolated: on a key in PendingImport (material expired, EV-01039); the alias itself is not deleted	Isolated	Confirmed

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-027	`wf-prod-lending`	Grant on the prod-lending attacker key	Created by the attacker's account at 00:06 on July 4, the first of its KMS calls	07-04 00:06:09	`EV-00522`	Removed: grant revoked July 4, 02:10:30 EDT (`EV-00636`); its state was captured first (`EV-00629`, 02:04:30)	Removed	Confirmed

Data stores re-encrypted, copied, shared, or read

The imaging archive was re-encrypted in part; snapshots were copied under the attacker keys; one database snapshot copy was shared with the attacker's account until July 4. Two rows are about data we cannot see: the copy-out and any reads.

Data stores re-encrypted, copied, shared, or read: 10 rows. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-012	wf-prod-imaging	S3 Batch job on wf-imaging-archive-prod	Copied objects in place under the imaging attacker key (the bank's version became noncurrent)	07-03 21:41:00	EV-00393	Removed: canceled July 4, 01:28 (EV-00565). The bank's rewrite ran as 31 sequential slice jobs and finished July 7, 12:40. At 14:00 the slice jobs' completion reports showed no failed task, and the bank's two Athena queries of the bucket's live inventory table (13:52 and 13:55, EV-01035, EV-01036) found no current business-data version under an attacker key (the preserved ransom-note versions, rows CI-023 and CI-024, were outside that population and stayed until July 28); a scheduled S3 Inventory report corroborates that later and is not the basis	Removed	Confirmed
CI-008	wf-prod-lending	wf-los-prod-manual-20260703-2122	Snapshot of the production loan database taken by the attacker	07-03 21:22:17	EV-00317	Open, planned for week 3	Removed	Confirmed
CI-015	wf-prod-lending	wf-los-prod-bk-20260703	Copy of the database snapshot under the prod-lending attacker key; the one that was shared with the attacker's account until July 4	07-03 21:58:31	EV-00442	Open, planned for week 3	Isolated	Confirmed
CI-026	wf-prod-lending	Share of wf-los-prod-bk-20260703 with account 777788889999	Database snapshot copy shared with the attacker's account at 23:51:12 on July 3; open 137 minutes	07-03 23:51:12	EV-00520	Removed: attribute state captured first (EV-00625, 02:03:10), then the share removed July 4, 02:08:20 EDT (EV-00632)	Removed	Confirmed

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-009	`wf-prod-lending`	EBS snapshots of `wf-prod-lending` volumes (31)	Created by the attacker (one per volume)	07-03 21:35:10	`EV-00344` to `EV-00389`	Open, planned for week 3	Removed	Confirmed
CI-010	`wf-prod-data`	EBS snapshots of `wf-prod-data` volumes (15)	Created by the attacker (one per volume)	07-03 21:35:22	`EV-00351` to `EV-00379`	Open, planned for week 3	Removed	Confirmed
CI-013	`wf-prod-lending`	EBS snapshot copies under the prod-lending attacker key (31)	Copied from the attacker's snapshots, encrypted under the attacker key	07-03 21:47:00	`EV-00395` to `EV-00440`	Open, planned for week 3	Removed	Confirmed
CI-014	`wf-prod-data`	EBS snapshot copies under the prod-data attacker key (15)	Copied from the attacker's snapshots, encrypted under the attacker key	07-03 21:47:01	`EV-00396` to `EV-00424`	Open, planned for week 3	Removed	Confirmed
CI-029	`wf-prod-lending`	Database snapshot copy (412,317 applicant records)	Probably copied out of the organization: after the share, a ReEncrypt to a key in account `777788889999` and a grant with an outside retiring principal, both on the bank's key	July 4, 00:06:09 EDT to 00:51:06 EDT	Seven KMS events on the lending key: `EV-00522` to `EV-00525`, `EV-00528`, `EV-00530`, `EV-00531`	Accepted: the copy happens in the attacker's account, outside our view. Probable, with high confidence; not confirmed	Accepted	Probable, with high confidence

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-031	`wf-prod-imaging`	Objects in `wf-imaging-archive-prod`	No evidence of reads; reads were not logged (S3 data events recorded writes only)	Not applicable	None possible: no read events exist	Accepted: not ruled out. We cannot say whether any object was read	Accepted	Possible

Data stores deleted, and what the attacker left behind

The bank's database and EBS snapshots were deleted, and the three ransom notes were written.

Data stores deleted, and what the attacker left behind: 6 rows. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-016	`wf-prod-lending`	Month-end database snapshots of `wf-los-prod` (9)	Deleted by the attacker	07-03 22:05:03	`EV-00444` to `EV-00452`	Restored: copied back from `wf-backup` July 5, 05:10 to 07:50 (`EV-00722` to `EV-00732`)	Restored	Confirmed
CI-017	`wf-prod-lending`	EBS snapshots in `wf-prod-lending` (31)	Deleted by the attacker (into the Recycle Bin)	07-03 22:09:04	`EV-00454` to `EV-00485`	Restored: from the Recycle Bin July 4, 07:40 (`EV-00673` to `EV-00719`, with the 15 in the data account)	Restored	Confirmed
CI-018	`wf-prod-data`	EBS snapshots in `wf-prod-data` (15)	Deleted by the attacker (into the Recycle Bin)	07-03 22:09:40	`EV-00486` to `EV-00500`	Restored: from the Recycle Bin July 4, 07:40 (`EV-00673` to `EV-00719`, with the 31 in the lending account)	Restored	Confirmed
CI-023	`wf-prod-imaging`	`RESTORE-INSTRUCTIONS.txt` in `wf-imaging-archive-prod`	Ransom note written, encrypted under the imaging attacker key	07-03 23:30:11	`EV-00518`	Open, planned for week 3	Removed	Confirmed
CI-024	`wf-prod-data`	`RESTORE-INSTRUCTIONS.txt` in `wf-datalake-prod`	Ransom note written, encrypted under the data attacker key	07-03 23:30:36	`EV-00519`	Open, planned for week 3	Removed	Confirmed
CI-025	`wf-prod-lending`	`RESTORE-INSTRUCTIONS.txt` in `wf-lending-docs-prod`	Ransom note written. Not in the trail: that bucket has no data events; known from the object listing	07-03 23:30:50	S3 object listing (no `EV` number)	Open, planned for week 3	Removed	Confirmed

Configurations changed

A lifecycle rule on the imaging archive and the deletion protection of the production database.

Configurations changed: 2 rows. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-007	wf-prod-imaging	Lifecycle rule on wf-imaging-archive-prod	Set to expire noncurrent versions after one day	07-03 21:14:26	EV-00312	Removed: rule deleted July 4, 01:35 (EV-00568), before any version was eligible	Removed	Confirmed
CI-028	wf-prod-lending	Deletion protection of wf-los-prod	Turned off by the attacker at 00:47 on July 4	07-04 00:47:09	EV-00529	Open, planned for week 3	Restored	Confirmed

Logging tampered with

One legacy trail deleted. The organization trail, which the attacker also tried to stop, was never interrupted.

Logging tampered with: 1 row. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-019	wf-prod-lending	Legacy trail wf-lending-legacy-trail	Trail configuration deleted by the attacker (succeeded). Log files already delivered remain unless separately deleted; no such deletion is shown. The organization trail records the same activity and was never stopped (EV-00502)	07-03 22:14:18	EV-00501	Open, planned for week 3	Accepted	Confirmed

Compute touched

None. The 46 EBS volumes were snapshotted through the API, and no instance was launched, stopped, modified, or reached.

Compute touched: 1 row. Times are MM-DD HH:MM:SS EDT. The end state is the register's status when week three's work is done.

ID	Account	Resource	Action	Time (EDT)	Evidence	Status on July 24	End state	Confidence
CI-030	wf-prod-lending	EC2 application tier of the loan platform	No host access observed in the reviewed control-plane, application, and load-balancer records. Host compromise cannot be ruled out with the collected evidence	Not applicable	Application and load-balancer logs; the EC2 calls in the trail	Not observed (see the table of things we checked). Not a finding that no host was reached	Accepted	Not observed

What we checked and excluded

We checked eight things the attacker might have done, found no evidence of any, and exclude them for the reasons below. We could not check a ninth, object reads from the imaging archive, because no log of reads exists. An exclusion is only as good as the evidence behind it, so the table says how sure we are in each case.

The things we checked and excluded, and the one we could not.

What we checked	Result	Evidence	How sure
Attacker EC2 control-plane operations on instances, including the loan platform's application tier	Ruled out for the operations checked	The attacker's EC2 calls are `CreateSnapshot`, `CopySnapshot`, and `DeleteSnapshot` only (rows AT-101, AT-102, AT-108, AT-109, AT-115, AT-117). No instance launch, stop, modify, or session call is attributed to the attacker.	High, for those control-plane operations only. Nothing in AWS can show what happens inside a host. Access through an existing operating-system credential, another network path, or an unrecognized source would not appear here, and no host image or host telemetry was collected.
Attacker traffic in the loan platform's application and load-balancer logs we reviewed	Not observed	The application and load-balancer logs show no attacker traffic (register row CI-030). These logs are outside the organization trail and carry no `EV` number.	High that the reviewed logs show no known attacker traffic, for the period they cover. This does not exclude host compromise by a path those logs do not record.
Overwriting data-lake objects with a customer-supplied key (SSE-C)	Ruled out	All 214 requests were denied by the bucket's SSE-C block (row AT-068, `EV-00098` to `EV-00311`). No data-lake object was changed by that attempt.	Confirmed. The data lake was reached in other ways (a key, EBS snapshots, a ransom note), which the register lists.
Any call in the nine accounts that are not in the tables	Ruled out	No attacker row is recorded in the management, log-archive, audit, network, shared-services, identity, backup, or two sandbox accounts.	High. The organization trail records all member accounts.
Writes in the digital, treasury, and five non-production accounts	Ruled out	In these seven accounts the attacker made AssumeRole and discovery calls only (`ListBuckets`, `DescribeDBInstances`, `ListKeys`), rows AT-070 to AT-098.	High.

What we checked	Result	Evidence	How sure
A console sign-in by the attacker	Ruled out	No console sign-in event is attributed to the attacker among its rows. Every call was made through the API with a key or a role session.	High, for the events we attribute.
Stopping or changing the organization trail	Ruled out	`StopLogging` was denied (row AT-119, `EV-00502`): a member account cannot change an organization trail. The trail recorded every later call.	Confirmed.
The bank's central backup copies in `wf-backup`	Ruled out	No attacker call is recorded in that account, and the nine month-end snapshots were copied from it on July 5 (`EV-00722` to `EV-00732`).	High.
Object reads from the imaging archive	**Not ruled out**	S3 data events recorded writes only; no read is logged, and none can be shown or excluded (register row `CI-031`)	Unknown. Carried as possible and accepted

What closes the open rows

Week three of the Recovery (July 27 to July 31) closes the 11 open rows, and each closes with a record. For each, the bank's platform team makes the change under review, Vantalect checks the result against the trail, and the evidence number goes into the register. Where evidence has to be kept first (the attacker's snapshots and the ransom notes are evidence), the copy is preserved and hashed before anything is removed. Counsel decides whether the bank wants any of it kept longer.

The planned dates for two of the rows are these. Deletion protection on `wf-los-prod` (`CI-028`) is to be re-enabled on Tuesday, July 28. The legacy account trail (`CI-019`) had its configuration deleted. Log files it already delivered remain unless separately deleted, and no such deletion is shown. We expect the bank to accept not recreating it on Tuesday, July 28, because the organization trail supplies the coverage. These are plans as of July 24, and the trail does not yet show any of them done.

What will not close. The copy-out (`CI-029`) and the object reads (`CI-031`) stay accepted: no action of the bank's can turn a probable into a confirmed, or an unknown into a known. They remain in the register with their confidence, so that no later report states more than the evidence does.

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.