Vantalect



AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Indicators of Compromise

DISTRIBUTION: RELEASABLE

Week 2 of 4: Trace (appendix) · 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

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

What to do with them 3

The indicators 5

Machine-readable exports 15

CSV 15

STIX 2.1 16

Detection queries 18

CloudTrail Lake (SQL) 18

EventBridge patterns (JSON) 21

Notice 25

About this report

This report lists every indicator of compromise from the attack on Wrenfield's AWS organization, 75 in all, in one table, in two machine-readable forms, and with queries that would have caught the technique. It is Vantalect's finding as of Friday, July 24, 2026.

> **Distribution: Releasable once counsel clears it**
>
> This report holds facts only, in a form counsel may release. Counsel decides whether, when, and to whom. Until counsel (Diane Whitcombe, Tessaly & Brook LLP) clears it, treat it as counsel-only. The indicators are in a form the bank's detection team, its peers, and law enforcement can use. The attack narrative, which is counsel-only, gives the story behind them; this report holds facts and no analysis.

What is in it. Every indicator is a value seen in the bank's organization trail, in an action we attribute to the attacker, or a pattern of such actions. Each row has the first and last time we saw it (UTC), a confidence, and the context a defender needs to use it. The CSV and STIX excerpts show the two export formats. The detection queries are for CloudTrail Lake (SQL) and Amazon EventBridge (JSON).

What is not in it. No address, session, or user agent that belongs to the bank, its build agents, or the responders is listed as an indicator. Temporary session key IDs (those that start with ASIA) are not listed: they change with each session, and the session name carries the same information. The ransom contact and the note's text are withheld. No secret is printed. This report makes no statement about who the attacker is, and the tracking label in the STIX excerpt names a cluster of tooling, not a person, a group, or a country.

What the confidence means. High means we saw the value in the trail in an attacker action and saw no benign use of it. Medium means we saw it, but the value is also used by benign tools or the signal is behavioral, so match it only with another indicator. We use no Low confidence: an indicator we could not tie to the attack is not in the table.

What to do with them

Use the identifiers to search and the patterns to alert, and use the time windows when you block. The table below has 72 high-confidence rows and 3 medium-confidence rows.

- **Identifiers are safe to search on at any time.** The two access key IDs, the account ID `777788889999`, the 37 `jenkins-sync-NNNN` session names, the key ARNs, and the file names are unique to this attack. A hit anywhere in a log is worth a look.
- **Addresses need their windows.** The first address (`198.51.100.23`) is a residential-proxy exit, and proxy and hosting addresses are shared with other customers. Block any address only for the first and last times in the table, and prefer an alert to a block. Treat `203.0.113.47` with the same caution: it was the attacker's during the windows shown, and the next holder of an address may be someone else.
- **The AWS CLI user agent alone proves nothing.** The same build is used by the bank's own build agents and by our responders. The Boto3 string is more distinctive, and it is still only a tool.
- **The patterns are the durable part.** A new address is cheap for an attacker. Keys with imported material that expire on the ransom deadline, a lifecycle rule that expires versions after one day, a snapshot shared with an outside account, and KMS calls from another account on a bank key are the shape of the technique, and they are what the detection queries look for.

The indicators by type.

Indicator type	Rows
Access key ID	2
Session name	41
Principal ARN	5
Role ARN pattern	1
Account ID	1
IP address	4
User agent	2
KMS key ARN	3
KMS alias	1
Object name	3
Snapshot name	2
S3 Batch job ID	1
Tooling pattern	9
Time window	3
All indicators	75

The indicators

Every indicator, in one table. Times are UTC. A value in backticks is exact; a pattern describes a set of calls. The context column says where the indicator came from and how to use it.

All 75 indicators. First and last seen are the earliest and latest attacker events that carry the value, to the minute, in UTC.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-001	Access key ID	`AKIAWRFNEXAMPLE00001`	2026-06-29 07:14	2026-07-04 05:24	High	Long-lived key of IAM user svc-artifact-sync in wf-tools (created March 14, 2023, never rotated). Stolen outside AWS. Deactivated July 4 at 01:24 EDT (EV-00543), deleted July 8 (EV-01075).
IOC-002	Access key ID	`AKIAWRFNEXAMPLE00002`	2026-07-04 02:31	2026-07-04 07:00	High	Created by the attacker for IAM user aws-support-sync in wf-prod-data at 22:31 EDT on July 3 (EV-00512). First used July 4 at 01:31 EDT, after the containment SCP; deactivated at 03:01 EDT (EV-00646), deleted July 8 (EV-01046).
IOC-003	Session name	`jenkins-sync-4440`	2026-07-01 14:21	2026-07-01 14:22	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-data by svc-artifact-sync from 198.51.100.41 (EV-00051); 3 calls made in the session.
IOC-004	Session name	`jenkins-sync-4471`	2026-07-04 01:04	2026-07-04 01:22	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00083); 5 calls made in the session.
IOC-005	Session name	`jenkins-sync-4473`	2026-07-04 01:09	2026-07-04 01:14	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00088); 5 calls made in the session.
IOC-006	Session name	`jenkins-sync-4475`	2026-07-04 01:09	2026-07-04 01:12	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00091); 218 calls made in the session.
IOC-007	Session name	`jenkins-sync-4478`	2026-07-04 01:20	2026-07-04 01:21	High	AssumeRole of wf-deploy-pipeline in wf-prod-digital by svc-artifact-sync from 203.0.113.47 (EV-00313); 3 calls made in the session.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-008	Session name	`jenkins-sync-4480`	2026-07-04 01:22	2026-07-04 01:23	High	AssumeRole of wf-deploy-pipeline in wf-prod-treasury by svc-artifact-sync from 203.0.113.47 (EV-00318); 3 calls made in the session.
IOC-009	Session name	`jenkins-sync-4482`	2026-07-04 01:26	2026-07-04 01:27	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-lending by svc-artifact-sync from 203.0.113.47 (EV-00322); 3 calls made in the session.
IOC-010	Session name	`jenkins-sync-4483`	2026-07-04 01:27	2026-07-04 01:28	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00325); 3 calls made in the session.
IOC-011	Session name	`jenkins-sync-4485`	2026-07-04 01:28	2026-07-04 01:29	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-data by svc-artifact-sync from 203.0.113.47 (EV-00328); 3 calls made in the session.
IOC-012	Session name	`jenkins-sync-4488`	2026-07-04 01:29	2026-07-04 01:30	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-digital by svc-artifact-sync from 203.0.113.47 (EV-00332); 3 calls made in the session.
IOC-013	Session name	`jenkins-sync-4491`	2026-07-04 01:30	2026-07-04 01:31	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-treasury by svc-artifact-sync from 203.0.113.47 (EV-00336); 3 calls made in the session.
IOC-014	Session name	`jenkins-sync-4494`	2026-07-04 01:34	2026-07-04 01:48	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00342); 62 calls made in the session.
IOC-015	Session name	`jenkins-sync-4496`	2026-07-04 01:34	2026-07-04 01:47	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00343); 30 calls made in the session.
IOC-016	Session name	`jenkins-sync-4499`	2026-07-04 01:38	2026-07-04 01:41	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00390); 3 calls made in the session.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-017	Session name	`jenkins-sync-4502`	2026-07-04 01:56	2026-07-04 01:58	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00441); 1 call made in the session.
IOC-018	Session name	`jenkins-sync-4505`	2026-07-04 02:03	2026-07-04 02:36	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00443); 44 calls made in the session.
IOC-019	Session name	`jenkins-sync-4508`	2026-07-04 02:08	2026-07-04 02:08	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00453); 0 calls made in the session.
IOC-020	Session name	`jenkins-sync-4510`	2026-07-04 02:09	2026-07-04 02:31	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00483); 18 calls made in the session.
IOC-021	Session name	`jenkins-sync-4512`	2026-07-04 02:19	2026-07-04 02:19	High	AssumeRole of wf-deploy-pipeline in wf-prod-digital by svc-artifact-sync from 203.0.113.47 (EV-00503); 0 calls made in the session.
IOC-022	Session name	`jenkins-sync-4514`	2026-07-04 02:22	2026-07-04 02:22	High	AssumeRole of wf-deploy-pipeline in wf-prod-treasury by svc-artifact-sync from 203.0.113.47 (EV-00504); 0 calls made in the session.
IOC-023	Session name	`jenkins-sync-4516`	2026-07-04 02:25	2026-07-04 02:25	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-lending by svc-artifact-sync from 203.0.113.47 (EV-00505); 0 calls made in the session.
IOC-024	Session name	`jenkins-sync-4517`	2026-07-04 02:27	2026-07-04 02:27	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00506); 0 calls made in the session.
IOC-025	Session name	`jenkins-sync-4519`	2026-07-04 02:27	2026-07-04 02:27	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-data by svc-artifact-sync from 203.0.113.47 (EV-00507); 0 calls made in the session.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-026	Session name	`jenkins-sync-4522`	2026-07-04 02:28	2026-07-04 02:28	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-digital by svc-artifact-sync from 203.0.113.47 (EV-00508); 0 calls made in the session.
IOC-027	Session name	`jenkins-sync-4525`	2026-07-04 02:29	2026-07-04 02:29	High	AssumeRole of wf-deploy-pipeline in wf-nonprod-treasury by svc-artifact-sync from 203.0.113.47 (EV-00509); 0 calls made in the session.
IOC-028	Session name	`jenkins-sync-4527`	2026-07-04 03:04	2026-07-04 03:51	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00515); 1 call made in the session.
IOC-029	Session name	`jenkins-sync-4530`	2026-07-04 03:09	2026-07-04 03:30	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00516); 1 call made in the session.
IOC-030	Session name	`jenkins-sync-4532`	2026-07-04 03:09	2026-07-04 03:30	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00517); 1 call made in the session.
IOC-031	Session name	`jenkins-sync-4534`	2026-07-04 04:04	2026-07-04 04:47	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00521); 1 call made in the session.
IOC-032	Session name	`jenkins-sync-4536`	2026-07-04 04:08	2026-07-04 04:08	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00526); 0 calls made in the session.
IOC-033	Session name	`jenkins-sync-4538`	2026-07-04 04:09	2026-07-04 04:09	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00527); 0 calls made in the session.
IOC-034	Session name	`jenkins-sync-4541`	2026-07-04 05:04	2026-07-04 05:04	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00532); 0 calls made in the session.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-035	Session name	`jenkins-sync-4542`	2026-07-04 05:09	2026-07-04 05:09	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00533); 0 calls made in the session.
IOC-036	Session name	`jenkins-sync-4544`	2026-07-04 05:09	2026-07-04 05:09	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00534); 0 calls made in the session.
IOC-037	Session name	`jenkins-sync-4547`	2026-07-04 05:23	2026-07-04 05:23	High	AssumeRole of wf-deploy-pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00538); 1 call made in the session.
IOC-038	Session name	`jenkins-sync-4549`	2026-07-04 05:23	2026-07-04 05:23	High	AssumeRole of wf-deploy-pipeline in wf-prod-imaging by svc-artifact-sync from 203.0.113.47 (EV-00540); 0 calls made in the session.
IOC-039	Session name	`jenkins-sync-4550`	2026-07-04 05:24	2026-07-04 05:24	High	AssumeRole of wf-deploy-pipeline in wf-prod-data by svc-artifact-sync from 203.0.113.47 (EV-00542); 1 call made in the session.
IOC-040	Session name	`s3-batch-operations`	2026-07-04 01:41	2026-07-04 05:28	High	Session of role s3-batch-replication assumed by S3 Batch Operations for the attacker's copy job in wf-prod-imaging.
IOC-041	Session name	`s-9172`	2026-07-04 04:05	2026-07-04 05:36	High	exfil-runner role in account 777788889999: 7 KMS calls on the prod-lending key, logged in the bank's account, July 4 00:06 to 00:51 EDT (two CreateGrant, a DescribeKey, a ReEncrypt to a key in the attacker's account, two Decrypt, a RetireGrant). Its AssumeRole of OrgAccessBackup followed at 01:36 and succeeded.
IOC-042	Session name	`ops`	2026-07-04 05:36	2026-07-04 05:39	High	OrgAccessBackup administrator session assumed from the attacker's account at 01:36 EDT; the assume succeeded. Its DeleteDBInstance on wf-los-prod at 01:39 was denied by the SCP.
IOC-044	Principal ARN	`arn:aws:iam::584729103358:user/svc-artifact-sync`	2026-06-29 07:14	2026-07-04 05:24	High	Compromised, not malicious: the bank's own service user in wf-tools whose key was stolen. Look for AssumeRole of wf-deploy-pipeline by this user from outside the bank.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-045	Principal ARN	`arn:aws:iam::584729104423:user/aws-support-sync`	2026-07-04 02:31	2026-07-04 07:00	High	Created by the attacker in wf-prod-data with AdministratorAccess (EV-00510, EV-00511); name imitates a vendor support account. Deleted July 8.
IOC-046	Principal ARN	`arn:aws:iam::584729104402:role/OrgAccessBackup`	2026-07-04 02:36	2026-07-04 05:39	High	Created by the attacker in wf-prod-lending (EV-00513); trusts the root of account `777788889999`. Deleted July 8.
IOC-047	Principal ARN	`arn:aws:iam::584729104415:role/s3-batch-replication`	2026-07-04 01:39	2026-07-04 05:28	High	Created by the attacker in wf-prod-imaging (EV-00391); trusts S3 Batch Operations; used for the copy job (EV-00393). Deleted July 8.
IOC-048	Principal ARN	`arn:aws:iam::777788889999:role/exfil-runner`	2026-07-04 04:06	2026-07-04 07:00	High	Role in the attacker's own account; its session is s-9172. Seen only in the bank's trail as the caller of KMS and STS.
IOC-049	Role ARN pattern	`arn:aws:iam::*:role/wf-deploy-pipeline`	2026-07-01 14:21	2026-07-04 05:24	High	The bank's own role, present in all 10 workload accounts, administrator access, trusting the whole wf-tools account. Abused 37 times; a legitimate role, so alert on the caller, not the role.
IOC-050	Account ID	`777788889999`	2026-07-04 01:06	2026-07-04 07:00	High	The attacker's AWS account (outside the organization). Named in three key policies, the OrgAccessBackup trust, the snapshot share, and the calls in which it is the calling account (7 KMS calls, one of them denied, and one AssumeRole of OrgAccessBackup).
IOC-051	IP address	`198.51.100.23`	2026-06-29 07:14	2026-06-30 13:51	High	Residential-proxy exit; the first use of the stolen key (June 29 to 30), discovery only. Proxies are shared: block only with the time window.
IOC-052	IP address	`198.51.100.41`	2026-07-01 06:00	2026-07-02 14:17	High	Discovery on July 1 and 2, including the test AssumeRole into wf-nonprod-data (EV-00051). A second outside address used the same way; shared hosting is possible, so use the time window.
IOC-053	IP address	`203.0.113.47`	2026-07-04 01:04	2026-07-04 07:00	High	The operation host: 463 events on July 3 and 4, 220 of them denied (214 SSE-C), including the second key's calls after containment.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-055	User agent	`Boto3/1.34.120 md/Botocore#1.34.120 ua/2.0 os/linux#6.1.0-21-amd64 md/arch#x86_64 lang/python#3.11.2 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.34.120`	2026-06-29 07:14	2026-07-04 07:00	High	Python 3.11.2 on Linux; used for all discovery from the three outside addresses and for the exfil-runner session. 67 attacker events and no other actor's.
IOC-056	User agent	`aws-cli/2.17.8 md/awscrt#0.20.11 ua/2.0 os/linux#6.1.0-21-amd64 md/arch#x86_64 lang/python#3.11.8 md/pyimpl#CPython cfg/retry-mode#standard md/installer#exe md/distrib#debian.12 md/prompt#off`	2026-07-04 01:04	2026-07-04 05:24	Medium	AWS CLI 2.17.8 on Debian 12: 449 attacker events on July 3 to 4. The same build is also seen from the bank's own build agents and from our responders, so match it only together with an address or a session name.
IOC-057	KMS key ARN	`arn:aws:kms:us-east-1:584729104402:key/b9885f41-4ff8-5cbf-9f54-7753a6180289`	2026-07-04 01:06	2026-07-04 07:00	High	Origin EXTERNAL key created in wf-prod-lending (EV-00084); policy grants account `777788889999`; material expires 2026-07-07T22:00:00Z; the expiry was logged July 7 at 18:00 EDT, which left the key in PendingImport. The outside statement was dropped from the key policy on July 4 at 02:09 EDT. The bank's DisableKey on the key on July 8 at 10:03 to 10:04 EDT (EV-01052) was rejected with KMSInvalidStateException, because a key in PendingImport cannot be disabled; the key was kept as it is.
IOC-058	KMS key ARN	`arn:aws:kms:us-east-1:584729104415:key/6d9bd1af-48a0-5150-b619-9ab79ca2b680`	2026-07-04 01:09	2026-07-04 05:28	High	Origin EXTERNAL key created in wf-prod-imaging (EV-00089); policy grants account `777788889999`; material expires 2026-07-07T22:00:00Z; the expiry was logged July 7 at 18:00 EDT, which left the key in PendingImport. The outside statement was dropped from the key policy on July 4 at 02:09 EDT. The bank's DisableKey on the key on July 8 at 10:03 to 10:04 EDT (EV-01054) was rejected with KMSInvalidStateException, because a key in PendingImport cannot be disabled; the key was kept as it is.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-059	KMS key ARN	`arn:aws:kms:us-east-1:584729104423:key/33767b29-2aaa-5253-83bf-0d1d670c1e43`	2026-07-04 01:09	2026-07-04 05:31	High	Origin EXTERNAL key created in wf-prod-data (EV-00093); policy grants account `777788889999`; material expires 2026-07-07T22:00:00Z; the expiry was logged July 7 at 18:00 EDT, which left the key in PendingImport. The outside statement was dropped from the key policy on July 4 at 02:09 EDT. The bank's DisableKey on the key on July 8 at 10:03 to 10:04 EDT (EV-01056) was rejected with KMSInvalidStateException, because a key in PendingImport cannot be disabled; the key was kept as it is.
IOC-060	KMS alias	`alias/wf-backup-2026`	2026-07-04 01:06	2026-07-04 01:10	High	The same alias on all three attacker keys (wf-prod-lending, wf-prod-imaging, wf-prod-data); imitates a backup key. The bank has no key by this name.
IOC-061	Object name	`wf-imaging-archive-prod/RESTORE-INSTRUCTIONS.txt`	2026-07-04 03:30	2026-07-04 03:30	High	Ransom note written to wf-prod-imaging, encrypted under that account's attacker key; in the trail as a write data event.
IOC-062	Object name	`wf-datalake-prod/RESTORE-INSTRUCTIONS.txt`	2026-07-04 03:30	2026-07-04 03:30	High	Ransom note written to wf-prod-data, encrypted under that account's attacker key; in the trail as a write data event.
IOC-063	Object name	`wf-lending-docs-prod/RESTORE-INSTRUCTIONS.txt`	2026-07-04 03:30	2026-07-04 03:30	High	Third ransom note, in wf-prod-lending. Not in the trail (that bucket has no data events); known from the S3 object listing.
IOC-064	Snapshot name	`wf-los-prod-bk-20260703`	2026-07-04 01:58	2026-07-04 07:00	High	Copy of the loan database snapshot under the prod-lending attacker key, shared with account `777788889999` at 23:51 EDT on July 3 (EV-00520) and removed from the share at 02:08 EDT on July 4 after 137 minutes. The name is also the encryption context of the KMS Decrypt calls on the key, the last one on July 4.
IOC-065	Snapshot name	`wf-los-prod-manual-20260703-2122`	2026-07-04 01:22	2026-07-04 01:58	High	The attacker's own snapshot of wf-los-prod taken at 21:22 EDT (EV-00317), the source of the copy above.
IOC-066	S3 Batch job ID	`45eb31f1-d889-53b5-ac3d-236b4a64dea8`	2026-07-04 01:41	2026-07-04 05:28	High	Copy-in-place job on wf-imaging-archive-prod under the imaging attacker key; description "sync"; canceled July 4 at 01:28 EDT after 61.3 million objects.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-067	Tooling pattern	`sessionName matches ^jenkins-sync-[0-9]{4}$ on wf-deploy-pipeline`	2026-07-01 14:21	2026-07-04 05:24	High	The bank's own build sessions are named jenkins-build- and artifact-sync-; the attacker's name sits between them. 36 of 37 sessions fall in July 3 to 4.
IOC-068	Tooling pattern	`CreateKey with origin EXTERNAL, followed by GetParametersForImport and ImportKeyMaterial`	2026-07-04 01:06	2026-07-04 01:10	High	Three times in 4 minutes across three production accounts, then alias/wf-backup-2026 and a key policy naming account `777788889999`.
IOC-069	Tooling pattern	`ImportKeyMaterial with expirationModel KEY_MATERIAL_EXPIRES and validTo 2026-07-07T22:00:00Z`	2026-07-04 01:07	2026-07-04 01:10	High	The expiry equals the ransom deadline (Tuesday July 7, 18:00 EDT): the keys lock themselves. The bank's own keys are origin AWS_KMS.
IOC-070	Tooling pattern	`CopyObject with x-amz-server-side-encryption-customer-algorithm, 214 in 40 seconds, all AccessDenied`	2026-07-04 01:12	2026-07-04 01:12	High	The SSE-C attempt on wf-datalake-prod; the bucket blocks SSE-C, so no object was changed. A burst of this size from one session is the signature.
IOC-071	Tooling pattern	`PutBucketLifecycleConfiguration with noncurrentVersionExpiration of 1 day (rule id expire-old-versions)`	2026-07-04 01:14	2026-07-04 01:14	High	On wf-imaging-archive-prod at 21:14 EDT; removed at 01:35 EDT on July 4 (EV-00568) before any version was eligible.
IOC-072	Tooling pattern	`S3 Batch CreateJob with s3PutObjectCopy and kmsKeyArn of an external-origin key`	2026-07-04 01:41	2026-07-04 01:41	High	Role s3-batch-replication passed to the job; 61.3 million objects (21.4%) re-encrypted in 227 minutes.
IOC-073	Tooling pattern	`KMS CreateGrant, DescribeKey, ReEncrypt, Decrypt, RetireGrant by userIdentity.accountId 777788889999 on a bank key`	2026-07-04 04:06	2026-07-04 04:51	High	7 calls in 45 minutes, three of them (the ReEncrypt and two Decrypt) with sourceIPAddress rds.amazonaws.com: a grant for the attacker's role, a grant for the database service with that role as retiring principal, and a ReEncrypt to a key in the attacker's account. The calls are the shape of a database snapshot copy made in the attacker's account; the copy itself is not in the bank's trail.

ID	Type	Indicator	First seen (UTC)	Last seen (UTC)	Confidence	Context
IOC-074	Tooling pattern	`DeleteTrail of an account trail, then StopLogging on the organization trail`	2026-07-04 02:14	2026-07-04 02:15	High	DeleteTrail of wf-lending-legacy-trail succeeded (EV-00501); StopLogging on the organization trail was denied (EV-00502).
IOC-075	Tooling pattern	`organizations:ListAccounts denied for an IAM user, several times`	2026-06-29 07:20	2026-07-02 10:32	Medium	Four denials from svc-artifact-sync, one a day from June 29 to July 2. Early warning only: other tools make the same call.
IOC-076	Time window	`Discovery hours: 06:00 to 15:00 UTC each day, June 29 to July 2`	2026-06-29 07:14	2026-07-02 14:17	Medium	The window in which the discovery calls fell on each of the four days. Working hours are easy to copy, so match it only with another indicator.
IOC-077	Time window	`Destructive operation: July 3 21:04 EDT to July 4 03:00 EDT`	2026-07-04 01:04	2026-07-04 07:00	High	From the first write-capable session to the last call by the second key.

Machine-readable exports

This sample includes format excerpts only; complete machine-readable exports are not provided. The excerpts below show the CSV and STIX 2.1 shape for a few of the indicators in the table above, which is the full list. A real engagement delivers one CSV row and one STIX indicator object for each row of the table.

CSV

The CSV has one header row and one row per indicator: `indicator_id`, `type`, `value`, `first_seen_utc`, `last_seen_utc`, `confidence`, `tlp`, and `context`. Values are quoted where they hold commas. The `tlp` column holds the sharing marking. This public synthetic sample is marked `TLP:CLEAR`. In a real engagement, counsel controls distribution and sets the marking when it clears the report.

```text
indicator_id,type,value,first_seen_utc,last_seen_utc,confidence,tlp,context
IOC-001,"Access key
ID","AKIAWRFNEXAMPLE00001",2026-06-29T07:14:02Z,2026-07-04T05:24:05Z,High,TLP:CLEAR,"Long-lived
key of IAM user svc-artifact-sync in wf-tools (created March 14, 2023, never rotated)"
IOC-002,"Access key
ID","AKIAWRFNEXAMPLE00002",2026-07-04T02:31:58Z,2026-07-04T07:00:20Z,High,TLP:CLEAR,"Created by
the attacker for IAM user aws-support-sync in wf-prod-data at 22:31 EDT on July 3 (EV-00512)"
IOC-004,"Session name","jenkins-
sync-4471",2026-07-04T01:04:11Z,2026-07-04T01:22:17Z,High,TLP:CLEAR,"AssumeRole of wf-deploy-
pipeline in wf-prod-lending by svc-artifact-sync from 203.0.113.47 (EV-00083); 5 calls made in
the session"
IOC-050,"Account
ID","777788889999",2026-07-04T01:06:08Z,2026-07-04T07:00:20Z,High,TLP:CLEAR,"The attacker's AWS
account (outside the organization)"
IOC-051,"IP
address","198.51.100.23",2026-06-29T07:14:02Z,2026-06-30T13:51:06Z,High,TLP:CLEAR,"Residential-
proxy exit; the first use of the stolen key (June 29 to 30), discovery only"
IOC-053,"IP
address","203.0.113.47",2026-07-04T01:04:11Z,2026-07-04T07:00:20Z,High,TLP:CLEAR,"The operation
host: 463 events on July 3 and 4, 220 of them denied (214 SSE-C), including the second key's
calls after containment"
IOC-060,"KMS alias","alias/wf-
backup-2026",2026-07-04T01:06:15Z,2026-07-04T01:10:02Z,High,TLP:CLEAR,"The same alias on all
three attacker keys (wf-prod-lending, wf-prod-imaging, wf-prod-data); imitates a backup key"
IOC-061,"Object name","wf-imaging-archive-prod/RESTORE-
INSTRUCTIONS.txt",2026-07-04T03:30:11Z,2026-07-04T03:30:11Z,High,TLP:CLEAR,"Ransom note written
to wf-prod-imaging, encrypted under that account's attacker key; in the trail as a write data
event"
```

STIX 2.1

The STIX bundle holds one `indicator` object per row, with a `stix` pattern, a `confidence` (85 for High, 60 for Medium), and the first-seen time as `valid_from`; one `intrusion-set` named `VTL-C1`, which is Vantalect's invented tracking label and not a named group; and an `indicates` relationship from each indicator to the intrusion set. The excerpt has three indicators. It carries no TLP marking object, because this public synthetic sample is `TLP:CLEAR` and the marking is optional; in a real engagement, counsel controls distribution and adds the marking it chooses. We checked its structure with a script (identifiers, required properties, timestamps, and references); we did not run it through an OASIS validator.

```json
{
  "type": "bundle",
  "id": "bundle--e814da07-c470-5fb4-92d2-0443c2bc107e",
  "objects": [
    {
      "type": "intrusion-set",
      "spec_version": "2.1",
      "id": "intrusion-set--3273d65b-0322-5bfb-aca2-f1989dd59f29",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "name": "VTL-C1",
      "description": "Vantalect tracking label (invented for the sample). Not a named group.",
      "first_seen": "2026-06-29T07:14:02.000Z",
      "last_seen": "2026-07-04T07:00:20.000Z"
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--748e4c78-da40-52ee-9da6-7e7671e6179e",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "name": "Operation host, July 3 to 4 (IOC-053)",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[ipv4-addr:value = '203.0.113.47']",
      "pattern_type": "stix",
      "valid_from": "2026-07-04T01:04:11.000Z",
      "confidence": 85
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--07371e15-a14a-56ee-bad7-fe684a016407",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "name": "Attacker-created access key (IOC-002)",
      "indicator_types": [
        "malicious-activity"
```

```
      ],
      "pattern": "[user-account:user_id = 'AKIAWRFNEXAMPLE00002']",
      "pattern_type": "stix",
      "valid_from": "2026-07-04T02:31:58.000Z",
      "confidence": 85
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--7b19865c-5b31-5d2b-b626-6f02e4ef8a48",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "name": "Ransom note file name (IOC-061)",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[file:name = 'RESTORE-INSTRUCTIONS.txt']",
      "pattern_type": "stix",
      "valid_from": "2026-07-04T03:30:11.000Z",
      "confidence": 85
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--cbcd0eef-904d-53ec-922e-3af02be42427",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--748e4c78-da40-52ee-9da6-7e7671e6179e",
      "target_ref": "intrusion-set--3273d65b-0322-5bfb-aca2-f1989dd59f29"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--313939bd-658a-509f-a55b-32c74b0db6d6",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--07371e15-a14a-56ee-bad7-fe684a016407",
      "target_ref": "intrusion-set--3273d65b-0322-5bfb-aca2-f1989dd59f29"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--dc3a2c6c-ff32-5fc8-be24-c4431c825a72",
      "created": "2026-07-24T14:00:00.000Z",
      "modified": "2026-07-24T14:00:00.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--7b19865c-5b31-5d2b-b626-6f02e4ef8a48",
      "target_ref": "intrusion-set--3273d65b-0322-5bfb-aca2-f1989dd59f29"
    }
  ]
}
```

The IP address, user account, and file indicators use the STIX cyber-observable patterns for those types. AWS access key IDs and account IDs have no standard object, so we carry them as `user-account` values (`user_id` for a key, `account_login` for an account ID). A consumer that keeps its own convention for AWS identities should map them.

Detection queries

These queries would have caught the technique while it ran, and most would have caught it before the data was affected. The CloudTrail Lake queries are written for an event data store that holds the organization's management events and the S3 write data events on the buckets that matter. The EventBridge patterns match events from CloudTrail on the default bus. Replace `EVENT_DATA_STORE_ID` with the identifier of the event data store, and the two bank egress placeholders with the bank's own addresses.

> **Not run against a live store**
>
> We wrote these queries against the schema of CloudTrail Lake and the records of this incident. We have not run them against a live event data store. Test each with a short time range before you rely on it, and check the field names against your store.

CloudTrail Lake (SQL)

Q1. External-origin keys and imported key material

Catches the three CreateKey and ImportKeyMaterial pairs on July 3 within minutes. The bank has no legitimate use of imported material.

```sql
SELECT eventTime, recipientAccountId, eventName, userIdentity.arn AS caller, sourceIPAddress,
       element_at(requestParameters, 'origin') AS key_origin
FROM EVENT_DATA_STORE_ID
WHERE eventSource = 'kms.amazonaws.com'
  AND (eventName = 'ImportKeyMaterial'
       OR (eventName = 'CreateKey' AND element_at(requestParameters, 'origin') = 'EXTERNAL'))
  AND eventTime > '2026-06-01 00:00:00'
ORDER BY eventTime
```

Q2. Policies naming the known attacker account

Catches the three key policies and the OrgAccessBackup trust, which name account `777788889999`. It finds that one account ID only. To detect any outside account, parse the account IDs in each principal and compare them against the organization's approved account list.

```sql
SELECT eventTime, recipientAccountId, eventName, userIdentity.arn AS caller
FROM EVENT_DATA_STORE_ID
WHERE eventName IN ('CreateKey', 'PutKeyPolicy', 'CreateRole', 'UpdateAssumeRolePolicy')
  AND CAST(requestParameters AS VARCHAR) LIKE '%777788889999%'
ORDER BY eventTime
```

Q3. Snapshot permission additions to review

Catches ModifyDBSnapshotAttribute at 23:51 EDT on July 3, 15 minutes before the first cross-account KMS call. In this incident the share stayed open 137 minutes, so a page at the share leaves time to remove it. The two branches use the two request shapes, RDS `valuesToAdd` and EC2 `createVolumePermission`. The query lists every addition; it does not check whether a recipient is outside the organization. Read the recipient account IDs or public group from the request and compare them with the approved account list as the next step.

```sql
SELECT eventTime, recipientAccountId, eventName, userIdentity.arn AS caller,
       CAST(requestParameters AS VARCHAR) AS request
FROM EVENT_DATA_STORE_ID
WHERE (eventName IN ('ModifyDBSnapshotAttribute', 'ModifyDBClusterSnapshotAttribute')
       AND CAST(requestParameters AS VARCHAR) LIKE '%valuesToAdd%')
   OR (eventName = 'ModifySnapshotAttribute'
       AND CAST(requestParameters AS VARCHAR) LIKE '%createVolumePermission%'
       AND CAST(requestParameters AS VARCHAR) LIKE '%add%')
ORDER BY eventTime
```

Q4. A burst of denied SSE-C copies

Catches 214 denials in 40 seconds on wf-datalake-prod. Needs S3 write data events, which the bank logged on that bucket.

```sql
SELECT date_trunc('minute', eventTime) AS minute, userIdentity.arn AS caller, count(*) AS
denied_copies
FROM EVENT_DATA_STORE_ID
WHERE eventName = 'CopyObject' AND errorCode = 'AccessDenied'
  AND element_at(requestParameters, 'x-amz-server-side-encryption-customer-algorithm') IS NOT
NULL
GROUP BY 1, 2
HAVING count(*) >= 20
ORDER BY minute
```

Q5. Key use by a principal from another account

Catches the 7 KMS calls of the copy-out burst, from account `777788889999` on the prod-lending key (7 calls in all). Calls the key owner denies are logged only in the caller's account, which the bank does not hold.

```sql
SELECT min(eventTime) AS first_call, max(eventTime) AS last_call, eventName, errorCode,
userIdentity.accountId AS caller_account,
       recipientAccountId AS key_account, count(*) AS calls
FROM EVENT_DATA_STORE_ID
WHERE eventSource = 'kms.amazonaws.com'
  AND eventName IN ('CreateGrant', 'DescribeKey', 'ReEncrypt', 'Decrypt', 'RetireGrant',
'GenerateDataKeyWithoutPlaintext')
  AND userIdentity.accountId <> recipientAccountId
GROUP BY eventName, errorCode, userIdentity.accountId, recipientAccountId
ORDER BY first_call
```

Q6. Read-only reconnaissance with a long-lived key

Would have shown the discovery from June 29: ListAccounts denied for an IAM user, and an IAM user assuming a role in a workload account from an address outside the bank. Needs read-only management events in the event data store.

```sql
SELECT eventTime, recipientAccountId, eventName, errorCode, sourceIPAddress, userAgent
FROM EVENT_DATA_STORE_ID
WHERE userIdentity.type = 'IAMUser'
  AND ((eventName = 'ListAccounts' AND errorCode IN ('AccessDenied', 'AccessDeniedException'))
       OR (eventName = 'AssumeRole' AND CAST(requestParameters AS VARCHAR) LIKE '%role/wf-
deploy-pipeline%'))
  AND sourceIPAddress NOT IN ('BANK_EGRESS_ADDRESS_1', 'BANK_EGRESS_ADDRESS_2')
ORDER BY eventTime
```

Q7. Identity, lifecycle and trail changes to investigate

Lists, in time order, the events that include aws-support-sync at 22:31 EDT and the one-day lifecycle rule at 21:14 EDT. It is a list and does not join events. Whether the same session also created keys is a next step, by grouping the rows by `session_principal` over a time window the analyst chooses.

```sql
SELECT eventTime, recipientAccountId, eventName, userIdentity.principalId AS session_principal,
       CAST(requestParameters AS VARCHAR) AS request
FROM EVENT_DATA_STORE_ID
WHERE eventName IN ('CreateUser', 'CreateAccessKey', 'AttachUserPolicy',
'PutBucketLifecycleConfiguration', 'DeleteTrail', 'StopLogging')
  AND eventTime > '2026-06-01 00:00:00'
ORDER BY eventTime
```

EventBridge patterns (JSON)

EventBridge on the default bus receives write management events from CloudTrail through a rule in the ordinary `ENABLED` state. To include read-only CloudTrail management events, such as the `ListAccounts` calls behind query Q6, create the rule in the `ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS` state and test delivery for the APIs you need; an ordinary `ENABLED` rule does not include them (AWS Compute Blog, "Introducing support for read-only management events in Amazon EventBridge"). The patterns below match write events, so they work in either state. Each pattern goes in a rule; the target should be something that pages a person.

E1. Imported key material changes

Matches ImportKeyMaterial, DeleteImportedKeyMaterial, and RotateKeyOnDemand. The bank has no legitimate use of imported material. Target an SNS topic that pages a person.

```json
{
  "source": [
    "aws.kms"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "kms.amazonaws.com"
    ],
    "eventName": [
      "ImportKeyMaterial",
      "DeleteImportedKeyMaterial",
      "RotateKeyOnDemand"
    ]
  }
}
```

E2. A key created with external origin

Matches CreateKey with origin EXTERNAL, the first of the three keys at 21:06 EDT on July 3.

JSON

```
{
  "source": [
    "aws.kms"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "kms.amazonaws.com"
    ],
    "eventName": [
      "CreateKey"
    ],
    "requestParameters": {
      "origin": [
        "EXTERNAL"
      ]
    }
  }
}
```

E3. A database snapshot shared with another account

Matches the RDS share that preceded the outside account's KMS calls on the key by 15 minutes. The logs do not show whether a copy was made. The pattern matches any addition, not only one to an outside account; the EBS snapshot version is E8, because EC2 uses a different request shape.

JSON

```
{
  "source": [
    "aws.rds"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventName": [
      "ModifyDBSnapshotAttribute",
      "ModifyDBClusterSnapshotAttribute"
    ],
    "requestParameters": {
      "valuesToAdd": [
        {
          "exists": true
        }
      ]
    }
  }
}
```

E4. Logging tampering

Matches DeleteTrail and StopLogging, including the denied StopLogging, which is the better warning.

```json
{
  "source": [
    "aws.cloudtrail"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventName": [
      "StopLogging",
      "DeleteTrail",
      "UpdateTrail",
      "PutEventSelectors"
    ]
  }
}
```

E5. New identities and a lifecycle rule that expires versions

Matches CreateUser, CreateAccessKey, CreateRole, and PutBucketLifecycleConfiguration in production accounts.

```json
{
  "source": [
    "aws.iam",
    "aws.s3"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventName": [
      "CreateUser",
      "CreateAccessKey",
      "CreateRole",
      "PutBucketLifecycleConfiguration",
      "PutBucketVersioning"
    ]
  }
}
```

E6. An S3 Batch Operations job

Matches CreateJob. The attacker's job copied 61.3 million objects in 227 minutes; a page at job creation leaves hours to cancel.

```json
{
  "source": [
    "aws.s3"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "s3.amazonaws.com"
    ],
    "eventName": [
      "CreateJob"
    ]
  }
}
```

E7. GuardDuty IAM findings

Matches the finding type raised at 22:44 EDT on July 3 (Persistence:IAMUser/AnomalousBehavior), 1 hour 40 minutes after the first write. Route it to a person, not only to a provider queue.

```json
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "type": [
      {
        "prefix": "Persistence:IAMUser"
      },
      {
        "prefix": "PrivilegeEscalation:IAMUser"
      },
      {
        "prefix": "Impact:S3"
      }
    ],
    "severity": [
      {
        "numeric": [
          ">=",
          7
        ]
      }
    ]
  }
}
```

E8. An EBS snapshot shared with another account or made public

Matches ModifySnapshotAttribute when it adds a create-volume permission for an account or a group. EC2 reports this in `createVolumePermission`, not in `valuesToAdd`, so E3 does not match it. The pattern matches any addition; compare the recipient with the approved account list. Test it against a sample ModifySnapshotAttribute event from your own account before you rely on it.

```json
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "AWS API Call via CloudTrail"
  ],
  "detail": {
    "eventName": [
      "ModifySnapshotAttribute"
    ],
    "requestParameters": {
      "createVolumePermission": {
        "add": {
          "items": {
            "userId": [
              {
                "exists": true
              }
            ]
          }
        }
      }
    }
  }
}
```

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.