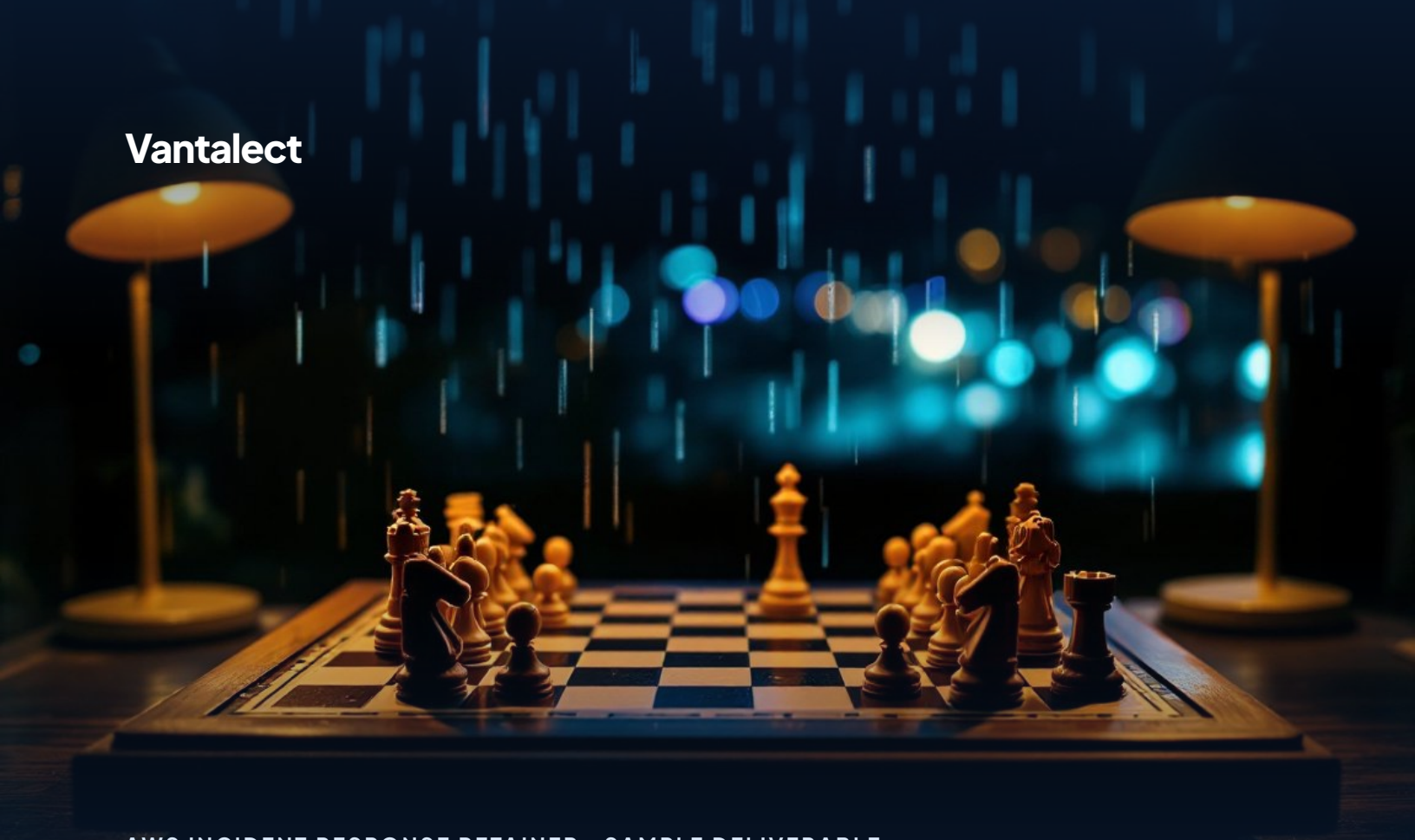
Vantalect



AWS INCIDENT RESPONSE RETAINER · SAMPLE DELIVERABLE

Tabletop Exercise After-Action Report

DISTRIBUTION: OPERATIONAL

Month 2 of the Retainer: Tabletop · prepared for Wrenfield Bancorp, Inc.

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

September 15, 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 scenario and the room 2

What the facilitator handed the team 4

Decisions and times 5

The measures 6

Where the team slowed down 7

What worked 8

Gaps, owners, and dates 9

Notice 11

What this report is

On Tuesday, September 15, 2026, the bank's incident team worked a scenario in which an IAM Identity Center administrator's session was hijacked. It took 77 scenario minutes from the first alert to containment, and the longest waits were in getting counsel's signed activation (21 minutes) and in finding the break-glass credential (17 minutes). Mireille Danvers: this is the after-action report. It names 8 gaps, each with an owner and a date. No one is blamed; every slowdown below is a missing line on a page, not a person.

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 one half-day exercise (09:00 to 12:30 EDT) held with 7 participants and the facilitator, Charles Sieg. It does not cover the July incident, and it does not test the activation role's mechanics, which the drill of August 12 did. The activation call was walked through in the room and not run. Every outside party (Vantalect, the provider, treasury operations, the administrator) was played by the facilitator. The decisions are the team's. The scenario is invented. Nothing here is a legal conclusion; where counsel was asked a question, the answer is recorded as hers.

The scenario and the room

In the scenario, an Identity Center administrator's session is hijacked. At 01:58 on a Sunday of a holiday weekend, someone using a stolen browser session of a platform administrator registers a second multi-factor device on the administrator's user, creates a permission set named `OpsAudit`

with administrator access, and assigns it to a new group in `wf-prod-treasury` and `wf-prod-lending`. The administrator is asleep. The session token was taken from a work laptop by malware; no one in the room knows that yet.

Who was in the room and what each person did.

Participant	Title	Role in the exercise
Mireille Danvers	Chief Information Security Officer	Incident lead once named; the activation approver
Imani Castell	Cloud Platform Lead	Technical lead; holds the break-glass role
Owen Tribble	Senior Cloud Engineer	First responder, paged by the watch
Harold Penwick	General Counsel	Calls counsel; owns questions to regulators and the broker
Anand Sethuraman	Chief Risk Officer	Asks what the board and the examiners will want to know
Colette Marsh	BSA/AML Officer	Asks whether any payment or account activity is affected
Diane Whitcombe	Partner, Tessaly & Brook LLP (outside counsel)	Signs the activation; decides what the bank asks of her
Charles Sieg	Vantalect	Facilitator; plays Vantalect, the provider, and the attacker's traces

Ground rules and assumptions:

- The watch is in place, including the Identity Center rule (G-9, added August 24).
- The activation role and its hold are as drilled on August 12. The script is walked through in the room, not run.
- The call sheet of August 14 is in the room, in paper form.
- The facilitator plays Vantalect, the attacker's traces, and any outside party the team calls.
- The scenario date is Sunday, October 11, 2026, a holiday weekend (Columbus Day falls on Monday, October 12). The scenario clock ran at room speed. Scenario 02:10 was 09:00 in the room.
- The hijacked user is `platform.admin2@wrenfield.example`; the sign-in comes from `192.0.2.201`, a documentation address.

What the facilitator handed the team

Eight injects, in scenario time. The facilitator gave the team only what the trail, the watch, or a phone call would have told them at that moment.

The eight injects. The first is the page from the watch.

ID	Scenario time (EDT)	What the team was told	Source
I-1	02:10 EDT	The watch pages the bank's on-call and Vantalect: `CreatePermissionSet` and `CreateAccountAssignment` in `wf-identity` from `192.0.2.201`, by `platform.admin2@wrenfield.example`, outside the change calendar.	Watch alert
I-2	02:15 EDT	The administrator does not answer her phone. Later, her partner says she has been asleep since 23:00 and no sign-in prompt appeared on her phone.	Phone, then a text
I-3	02:31 EDT	The trail shows a second multi-factor device registered for the administrator's user at 01:58, and sessions from the new permission set in `wf-prod-treasury` and `wf-prod-lending` that list buckets and database snapshots.	Trail extract
I-4	02:51 EDT	The bank's managed security service provider offers to disable the whole Identity Center instance. Every employee of the bank signs in through it.	Provider call
I-5	02:58 EDT	The only Identity Center administrators are the hijacked user and one colleague on leave. Removing the access needs the management account's break-glass role.	Facilitator card
I-6	03:24 EDT	The BSA officer asks whether any payment or account activity is affected. Treasury operations can check the wire console, which takes about 15 minutes.	Question from the room
I-7	03:40 EDT	The wire console shows no wire initiated from the treasury portal since Friday 17:00. The attacker's sessions in both accounts have made only read calls.	Treasury operations
I-8	03:45 EDT	The chief risk officer asks what the board, the broker, and the regulators must be told, and when.	Question from the room

Decisions and times

15 decisions, by the bank's team and Vantalect, in the order they happened. "Minutes" counts from the first alert at 02:10 EDT.

What the team decided and when, in scenario time. D-9 (03:15) happened after D-10 (03:05) because the activation was signed while the credential was still being found.

ID	Time (EDT)	Minutes	Who	Decision or action
D-1	02:12 EDT	2	Owen Tribble	Acknowledges the page and phones the administrator.
D-2	02:19 EDT	9	Owen Tribble	Stops phoning and calls Imani Castell, then Mireille Danvers (02:21).
D-3	02:22 EDT	12	Vantalect (facilitator)	Vantalect's call-back reaches the on-call engineer (played by the facilitator).
D-4	02:28 EDT	18	Mireille Danvers	Takes the incident lead after the room asks who leads an identity event.
D-5	02:33 EDT	23	Imani Castell	Reads the trail with Vantalect and confirms the new permission set and the two assignments.
D-6	02:38 EDT	28	Mireille Danvers	Decides it is an incident worth counsel's time and phones Harold Penwick.
D-7	02:41 EDT	31	Harold Penwick	Reaches Diane Whitcombe.
D-8	02:58 EDT	48	Mireille Danvers	Chooses targeted containment, not disabling the instance: one user, two assignments, the permission set, and the sessions already issued.
D-10	03:05 EDT	55	Diane Whitcombe	Signs the activation and emails it to Mireille Danvers and Vantalect.
D-11	03:12 EDT	62	Mireille Danvers	Runs the activation call (walked through, not run).
D-9	03:15 EDT	65	Owen Tribble	Finds the break-glass credential and hands it to Imani Castell.
D-13	03:25 EDT	75	Colette Marsh	Asks treasury operations to check wire initiation; accepts a 15-minute wait.

ID	Time (EDT)	Minutes	Who	Decision or action
D-12	03:27 EDT	77	Imani Castell	Completes containment with the break-glass role, in the supported order that starts at 03:16: deletes the user's Identity Center sessions, blocks the user, removes the attacker's second multi-factor device, the two assignments, and the `OpsAudit` permission set, and denies the already issued role sessions with a service control policy on the user's ID. The interval stops at 03:27, when a call with the attacker's existing credentials is denied in both accounts.
D-14	03:50 EDT	100	Harold Penwick	Parks the board, broker, and regulator questions with counsel and writes down the alert time and the confirmation time.
D-15	04:20 EDT	130	Mireille Danvers	Judges stage 1 complete: no successful attacker write since the verified containment at 03:27.

The measures

In the scenario the alert was acknowledged two minutes after it arrived, and the alert itself came 12 minutes after the 01:58 event; pager delivery was not tested. Most of the 77 minutes went between "someone knows" and "someone may act".

The exercise's measures, in scenario minutes.

Measure	Scenario minutes	Note
Event (01:58) to simulated alert	12	As played; pager delivery was not tested
Alert to page acknowledged	2	As played; the pager route itself was not tested
Alert to Vantalect's call-back	12	Commitment: 30 minutes after a page
Alert to incident lead named	18	S-1 and S-2
Alert to the decision to call counsel	28	S-3
Alert to counsel reached	31	
Alert to activation signed	55	S-5
Counsel signed to the activation call	7	Walked through. The drill measured the real call
Alert to verified containment of the hijacked user (existing credentials denied)	77	S-4 and S-6
Alert to the judgment that stage 1 is complete	130	No successful attacker write since containment

For comparison, and with care: in July the finding came at 22:44 EDT and the page at 23:18 EDT, 34 minutes later (a holiday on-call and a provider in the middle), and the containment policy was attached 2 hours 38 minutes after the finding. The two are not like for like: the exercise had a simulated alert, acknowledged two minutes after it arrived and 12 minutes after the event (pager delivery was not tested), a scenario that was smaller, and a team that had already lived the July night. We do not claim the bank is faster; we claim the bank knows where it is slow.

Where the team slowed down

Six places, none of them a person. Each row is a wait that a written line on the call sheet or in a runbook would shorten. The minutes are scenario minutes.

Where the team slowed down, and the gap each slowdown maps to. Some intervals overlap.

ID	Where	From	To	Minutes	Why	Gap
S-1	Reaching the administrator	02:12 EDT	02:19 EDT	7	On-call tried the person whose account it was before anyone else. It was a natural first move, and it spent seven minutes before escalation.	T-2
S-2	Who leads an identity event	02:21 EDT	02:28 EDT	7	The call sheet names a lead for an AWS data event, but this event touched sign-in. The room asked whether the platform lead or the CISO leads.	T-2
S-3	Deciding to call counsel	02:28 EDT	02:38 EDT	10	Ten minutes went to whether this was yet "an incident". Nobody was waiting for permission, but nobody had a written test.	T-3
S-4	Finding the break-glass credential	02:58 EDT	03:15 EDT	17	Two people knew the credential existed; one knew which safe; none had used it since it was sealed. It was the longest wait on the way to containment.	T-1
S-5	Counsel signing the activation	02:44 EDT	03:05 EDT	21	The signed pre-agreed statement of work was in counsel's office system, and she could not reach the pre-agreed documents from her phone. The August 14 call sheet in the room already printed the activation reference and the activation instructions.	T-4
S-6	Choosing how much to contain	02:51 EDT	02:58 EDT	7	The provider's offer to disable the whole instance was a sensible option. The room weighed every employee's sign-in against one user. The right call, taken with no written criteria.	T-5

The longest wait on the way to containment was S-4, the break-glass credential: 17 minutes from the decision to the credential in hand. Counsel's signature (S-5) took longer but ran alongside it. S-4 is gap T-1.

What worked

Four things the team did well, and should keep.

- The simulated alert arrived 12 minutes after the 01:58 event and was acknowledged two minutes later. The exercise did not test actual pager delivery.
- The team chose targeted containment, and every other employee's sign-in kept working.
- The risk and BSA questions were parked with counsel, with the alert time and the confirmation time written down, and not argued in the room.
- Counsel was reached three minutes after the decision to call her, and asked for the facts she needs on the first call.

The Identity Center rule (G-9, added August 24) is why the first line could be played as written. Before it, no watch rule covered Identity Center changes.

Gaps, owners, and dates

8 gaps, each with one owner and one date. Every date falls within the next seven weeks. Vantalect's own item is the first due.

After-action items, in order of due date.

ID	Gap	What we saw	Fix	Owner	Due
T-8	Vantalect's page text	The page said what happened, not what to do first.	Add the first three steps of the identity runbook to the Identity Center alert's page text.	Vantalect (facilitator)	Tuesday, September 22, 2026
T-2	Lead and first call for an identity event	On-call called the affected person first, and the room asked who leads when sign-in is the target.	Add a line to the call sheet: for an alert on an administrator's account, call the platform lead and the CISO first, then the person; the CISO leads.	Mireille Danvers	Friday, September 25, 2026
T-3	When to call counsel	No written test for the call; the room used ten minutes to discuss whether it was an incident.	Write a one-line test with counsel: a confirmed unfamiliar principal in the trail means the general counsel calls counsel, before scope is known. Counsel decides what follows.	Harold Penwick	Friday, September 25, 2026
T-4	Counsel's access to the pre-agreed documents	Counsel could not reach the pre-agreed documents from her phone; the signed statement of work was out of reach for about 20 minutes. The call sheet already printed the reference.	Provide an accessible authorized copy of the signed statement of work where counsel can open it from a phone, and rehearse retrieval. Keep the reference on the call sheet.	Diane Whitcombe	Friday, September 25, 2026

ID	Gap	What we saw	Fix	Owner	Due
T-1	The break-glass credential	Its location, its custodians, and its last test were not written down where the team would look.	Write the location (not the secret), the two custodians, and a test date on the call sheet; test the path in the management account once a quarter.	Imani Castell	Friday, October 2, 2026
T-5	Containment criteria for sign-in	Choosing between one user and the whole instance took seven minutes and no written criteria, and the room had no written order for ending the sessions already issued, which portal-session removal does not do.	Write the identity runbook in the order AWS supports: delete the user's Identity Center sessions, block the user, deny the already issued AWS role sessions (a service control policy deny on the user ID, kept at least 12 hours so the sessions expire), remove the attacker's multi-factor device, the assignments created in the last 24 hours, and the permission set, then verify denial from the attacker's existing credentials. Start the containment clock only when that check passes; disable the instance only if more than one administrator is affected. Include where each step is in the console and the API.	Imani Castell	Friday, October 2, 2026
T-7	The wire check	The BSA officer's question took 15 minutes to answer because the check was run by hand.	Write the query for payment initiation since a given time, and name who runs it and who reads it.	Colette Marsh	Friday, October 9, 2026
T-6	Administrator sessions	The hijacked session could register a second device and create administrator access without a new sign-in.	Shorten the administrators' session length, and require a fresh phishing-resistant sign-in before a device is registered or a permission set with administrator access is created.	Imani Castell	Friday, October 30, 2026

We will check the 7 items due by October 9 on that date and report what is done. The remaining item, the administrators' session settings, is a technical change with a test, and Imani Castell will report when it is tested. The Retainer's unused prepaid hours are not needed for any of this; if the bank wants a second tabletop, that is a use of unused hours in the last 60 days of the term.

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.