Vantalect



AWS FORENSICS · CLOUDTRAIL · RECOVERY

AWS Breach Forensics & Recovery

How they got in, what they touched, and whether they are still in, in two weeks. The door closed, and proven closed, in four.

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

November 6, 2026

The problem

You know you were breached. You do not yet know how, what the attacker touched, or whether they are still in. Your counsel cannot advise you on your legal exposure without those facts, and the facts have to come from logs and evidence that someone has to preserve and read.

This engagement finds out. The Investigation preserves the evidence, traces the attack through your logs, and gives your counsel the facts. The Recovery then closes the door, removes what was left behind, and proves it closed. It is for the work after containment, or after a breach found long after the fact; if the attack is still under way, start with AWS Incident Response at vantalect.com/incident-response.

The Investigation

Two weeks

$30,000

Up to 50 consultant hours

Your AWS organization, read from the inside after a breach. Evidence preserved first, then every attacker session traced across accounts, the compromise inventory, the causal analysis, a fix plan for your IT team, and the drafts counsel needs.

GUARANTEED

The Recovery

Four weeks

$50,000

Up to 110 consultant hours

The Investigation in the first two weeks. Then week three removes or isolates everything the attacker left and fixes the critical root causes as code. Week four runs the closure sweep the same way as week one and hands over.

The second half of the fee is invoiced only when the closure sweep finds every confirmed item in the compromise inventory removed, isolated, restored and verified, or covered by a named written acceptance (an item that cannot be confirmed has a documented disposition), no indicator of compromise active in the final seven days, and every critical root cause closed as code. A gap that remains in objects that already exist is disclosed as a residual risk with an owner and a date.

Who it is for

- A CISO, CIO, or general counsel whose production runs in one AWS organization of up to 50 accounts, with an organization trail or account trails that cover the period in question

- A control-plane attack (stolen keys, abused roles, ransomware by key or deletion, data copied out), or a compromise of EC2, containers, or Lambda inside AWS
- Outside counsel, or the willingness to engage counsel at the start, because counsel retains Vantalect

The scope is every enabled Region, the logs you hold for the period (by default the 90 days before discovery, longer by change order), and disk and memory analysis of up to ten compromised EC2 instances or container hosts, within the included hours: the instance count is a ceiling, and a host-heavy breach that uses the hours first moves to change order at $450 an hour, with an estimate of the hours each remaining host needs. Server logs means the logs your workloads write in AWS, where they exist: application logs, load balancer and CloudFront logs, VPC Flow Logs, S3 server access logs, and database audit logs. Their absence is itself a finding.

It is not the right engagement if most of the evidence is outside AWS (on-premises networks, laptops, mobile devices, email tenants, SaaS); we say so on the first call and analyze the AWS side only. It is not for a client who wants the attacker contacted, negotiated with, or paid, or who needs a testifying expert.

Week by week

The Investigation, two weeks.

Week	What happens
1. Preserve and map	The read-only role goes into every account on day one, with the same denies on reading stored data as in the security engagement. Evidence is preserved first, if a Response did not already. The estate is mapped (every account, principal, trust path, key, network path, and log source) and the log gaps recorded. Every known indicator is searched for across the whole period. Interviews with your platform lead and whoever found the breach.
2. Trace and report	Every attacker session reconstructed across accounts and role chains, from first access to containment. The compromise inventory, indicators of compromise, and the causal analysis of how the attack worked. Apart from it, the control gaps and fix plan for your IT team. The legal-considerations draft and the clocks worksheets for counsel, and a factual summary for counsel to release. The executive brief, read out to counsel and your sponsor.

The Recovery, four weeks.

Week	What happens
1 and 2. Preserve, map, trace	The Investigation's two weeks, with no changes to your workload accounts.
3. Eradicate and close	Every confirmed item in the compromise inventory removed, isolated, restored and verified, or covered by a named written acceptance, after it is preserved. An item that cannot be confirmed gets a documented disposition. Every critical root cause fixed as code through your repositories and review. The guardrails that would have stopped this attack attached at the organization (key origins other than AWS KMS, imported key material, customer-supplied encryption keys, external sharing of snapshots, lifecycle and versioning changes, trail changes), proven in a staging organizational unit first.
4. Closure sweep and hand over	The week-one map and every indicator search run again, the same way, plus seven days of watching with no indicator active. The factual summary, updated, the final custody log, the runbook for this attack, and the closing readout.

What you receive

Every report carries its distribution line: **Counsel only**, **Operational** (your incident team), or **Releasable** (counsel may share it). The Investigation alone delivers the first eleven.

The Investigation

1. **Estate Map and Evidence Preservation** (counsel only). The organization as it stood, every log source and its gaps, and what was preserved, so every later claim has a source.
2. **Attack Narrative and Timeline** (counsel only). What the attacker did, minute by minute, with each step's evidence, mapped to MITRE ATT&CK techniques, and the session tree across accounts.

3. **Indicators of Compromise** (releasable once counsel clears it). Every indicator in one table and in machine-readable form, with detection queries for your own monitoring.
4. **Executive Brief** (counsel only). The answer for the board: how they got in, what they touched, whether they are out, and what is still unknown.
5. **Compromise Inventory** (counsel only). Every principal, credential, resource, and data set the attacker used, created, changed, read, or copied, each with a confidence rating.
6. **Root Cause: How the Attack Worked** (counsel only). The causal analysis: why the attack worked at each step, with each step's evidence.
7. **Control Gaps and Fix Plan** (operational, an appendix to the root-cause report). The gaps in the estate, what closes each one, and which are critical. It states controls and fixes only, with no attack narrative, and it defines "critical" for the gate.
8. **Legal and Regulatory Considerations: Draft for Counsel** (counsel only). The facts counsel needs, organized by the regimes counsel may want to consider, with the questions only counsel can answer. A draft for counsel, not legal advice.
9. **Notification-Clock Worksheets** (counsel only). The deadlines that may run from your own determinations, computed from the times you enter.
10. **Factual Summary for Regulators, Insurers, and Auditors** (releasable through counsel). Facts only, with no analysis or opinion, at the Investigation's readout, for counsel to release.
11. **Chain-of-Custody Log** (counsel only). Every evidence item from collection to storage, hashed.

The Recovery

Everything in the Investigation, then two more, the factual summary updated at week four, and the custody log closed with the certificate for the working copies counsel authorized for destruction:

12. **Eradication and Root-Cause Closure** (operational). The disposition of every inventory item (removed, isolated, restored and verified, or accepted in writing) and every critical root cause fixed as code, each with its pull request.
13. **Closure Sweep** (operational). The gate: week one against week four, the same method, and seven days of watching.

How the result is measured

The closure sweep is the week-one map and every indicator search, run again the same way, with seven days of watching on top. Its results sit side by side with week one's, and the sweep proves that our roles are gone.

The gate

The second half of the Recovery fee is invoiced only when the closure sweep at week four finds every confirmed item in the compromise inventory removed, isolated, restored and verified, or covered by a named written acceptance (an item that cannot be confirmed has a documented disposition), no indicator of compromise active in the final seven days, and every critical root cause closed as code. A gap that remains in objects that already exist is disclosed as a residual risk with an owner and a date. The gate measures our work, not your choices. It is a gate on a second invoice, not a warranty that the attacker is out.

A critical root cause you accept in writing counts as closed, as does one whose fix you declined, or approved but had not applied before the sweep. If the attacker comes back in the last seven days, we rerun the sweep after the new activity is closed, the second invoice waits for the rerun, and the hours to chase the attacker and to rerun the sweep are inside the cap. If the gate is still not met after the rerun, the second invoice is not issued and you keep everything delivered. An indicator your own staff triggers, such as a scanner reusing an address, is closed by evidence in the sweep.

Beyond that gate, no particular result is guaranteed. We say what the evidence shows and how confident we are. We cannot promise that the evidence is complete, or that a regulator, insurer, or court will agree with a finding.

Terms at a glance

How an incident reaches us. The incident line is 877–HELM247 (877–435–6247). Vantalect publishes no incident mailbox. Anyone may call the line, and a call to it starts no response-time commitment: without a Retainer there is none, and only a Retainer holder has written commitments. The terms below are the standard terms, and the signed papers control.

Fees, hours, and scope. Invoices are due within fifteen days.

Term	The Investigation	The Recovery
Fee	$30,000, fixed	$50,000, fixed
Length	Two weeks	Four weeks
Consultant hours included	Up to 50	Up to 110
Beyond the cap	$450 per hour, by written change order agreed before the hour is spent	Same
Invoicing	In full at signature	Half at signature, half only if the gate is met

Term	The Investigation	The Recovery
After a Response	Preservation and tracing hours already worked are credited at $450 an hour, up to $10,000, against the signature invoice	Same
Scope	One AWS organization of up to 50 accounts, every enabled Region, the period's logs, and up to ten compromised instances	Same, plus fixes as code through your repositories
Bundle	Not a bundle member, with no bundle discount	Same

A longer period, more accounts or instances, evidence outside AWS, and support after the closing readout are outside scope, available only by written change order. We do not certify that data was "not accessed" in words that settle a notice duty, we do not opine on materiality, and we do not testify. Testimony is a separate engagement.

Counsel, evidence, and ransom

Nothing here is legal advice. The legal-considerations draft is a draft for counsel. It lists the regimes counsel may want to consider and the facts each one turns on, and it makes no determination that any applies. Reports never say that something is reportable, material, or lawful. Attribution is "consistent with" or "indicators overlap with," never "was."

Counsel retains Vantalect; you pay. Your outside counsel retains Vantalect for this incident, at counsel's direction, as a consulting expert, in papers written new for the incident. Counsel-track reports go to counsel only, and counsel decides who else sees them. A separate factual summary, with no analysis, is the one counsel releases to auditors, insurers, and regulators. If you have no counsel, we contract directly for operational work, say in writing that privilege may not attach to what we do before counsel signs, and re-paper through counsel when counsel arrives. Vantalect represents that it holds, or does not need, the licenses the law requires for this work in your state, and tells counsel in writing which it holds.

Vantalect plays no part in any ransom. We never contact the attacker, negotiate, advise on paying, or arrange, send, or hold a payment. We give counsel technical indicators, labeled as indicators, for sanctions screening.

Evidence is captured before any change, hashed at acquisition and after every transfer, analyzed on copies, and kept in an evidence account that is yours, owned and controlled by you from the day it is built and locked against deletion. Counsel decides the litigation hold at the start. We retain our working copies until counsel authorizes destruction in writing after confirming preservation obligations, then delete the authorized copies and provide a certificate on the agreed schedule.

Access, and what stays with you

Read-only roles in every account, from a template you read first, with explicit denies on reading stored data. Write access exists only in the evidence and vault accounts created for the engagement, which are yours. Disk and memory are acquired either by your engineer running our written runbook or under a scoped acquisition permission your approver grants for named instances, and the custody log records it. Every change in your workload accounts is made as code through your repositories and pipeline. The roles are deleted at the end, and the closure sweep proves it. Root credentials and payment methods stay with you.

What we need from you

- Outside counsel to sign the three-party Counsel Engagement Letter and the statement of work, both written new for this incident, or your written decision to proceed without counsel
- The read-only role in every account in scope on day one, and the evidence account
- A list of the logs you believe exist, and nothing deleted or rotated that you can keep
- Your platform lead, and whoever found the breach, for interviews in week one
- In the Recovery, each fix reviewed and approved or declined within two business days through your own change process
- Your sponsor and counsel at the readouts
- Your broker told, and the insurer's written consent requested if we are not listed on your policy

What comes with every engagement

- **Charles, personally.** Charles Sieg delivers every engagement inside your accounts, with your engineers and no hand-off to a junior team.
- **Evidence you can use.** A chain-of-custody log records who collected each item, when, from which resource, how it was hashed, and every transfer.
- **Counsel only.** Counsel-track reports go to counsel only, and counsel decides who else sees them.
- **How the agents and tools are used.** Charles directs software agents (AI tools) that read, analyze, and draft under his supervision; he reviews every deliverable and verifies every finding. By default they work inside your evidence account and your own accounts. Evidence goes to any other provider or region only with your and counsel's written consent for that incident, under terms that bar training on it and bar keeping it. Interceptor, Vantalect's tracker, reconstructs the attacker's sessions from the recorded API calls; it runs in an account you own, and its case database stays there.

- **Licensing and insurance.** Vantalect does not need a private-investigator license for this work. It carries errors-and-omissions insurance, carries no cyber insurance, and expects to need none.
- **Sample engagements.** The sample engagements on this site are fictional.
- **A readout to counsel and your sponsor** at the close of each shape.

Questions clients ask

How is this different from AWS Incident Response?

The Response is hourly work during the attack, to stop the damage and preserve evidence. This engagement is priced and scoped after containment, or for a breach found later with no attacker active, and it explains what happened.

Can you tell us whether we must notify regulators?

No. The worksheets compute deadlines from the times you record, and the legal draft lays out the facts. Whether any regime applies, and when your clock started, is a determination for you and your counsel.

What if our logs were not turned on?

Then the gap is a finding. The estate map states the limits of the evidence before any conclusion, and the control-gaps report says what to turn on so the next investigation has evidence.

Will you name the attacker?

We report indicators and say when activity is consistent with a known group, never that it was. Sanctions screening and law-enforcement contact belong to counsel.

Do we need the Recovery, or is the Investigation enough?

The Investigation answers what happened and, in the fix plan, what closes the door. The Recovery closes it, with the sweep to prove it. You choose at the Investigation's readout.

Start the conversation

If an attack is in progress right now, call the incident line on 877-HELM247 (877-435-6247), and call your own outside counsel and AWS Support. Without a Retainer there is no response-time commitment.

The full description is at **vantalect.com/breach-forensics**, and the standard terms are at **vantalect.com/terms**.

© 2026 Vantalect LLC. Prices and terms as of November 6, 2026; the terms at vantalect.com/terms govern.

AWS, Amazon Web Services, AWS Security Incident Response, 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. Vantalect is not affiliated with or endorsed by any of them.