Vantalect



AWS INCIDENT RESPONSE · CONTAINMENT · EVIDENCE

AWS Incident Response

A responder on the bridge in the middle of an attack, paid by the hour. Or the first hour of the next one, bought back in advance.

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

October 30, 2026

The problem

Something in your AWS organization is deleting snapshots and changing keys right now, and it is not your pipeline. Nobody can scope the work yet. You need someone on the bridge who stops the damage first and preserves the evidence while doing it.

The Response is that person, paid by the hour, from the first call until you declare containment. The Retainer is the other half. The first hour of a real incident usually goes to finding a lawyer, signing paper, and creating a role, and the Retainer spends that hour now.

The Response

From activation to containment declared

$675 an hour

$450 an hour for Retainer holders

A responder on the bridge who stops the damage first and preserves the evidence while doing it. Time and materials, any hour of any day, retained through your outside counsel, from the first call until you declare containment in writing.

The Retainer

One year

$36,000

40 prepaid readiness hours

The access role, the logs, the paper, and the rehearsal, done in the first 30 days, so the first hour of a real incident goes to the incident. A 30-minute call-back and a 2-hour hands-on commitment, around the clock, with service credits.

Who it is for

- A CISO, CIO, or general counsel whose production runs in an AWS organization of up to 50 accounts (more by change order), with an organization trail or account trails that cover the period
- 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

It is not the right engagement if most of the evidence sits outside AWS: on-premises networks, laptops, mobile devices, email tenants, or SaaS. We say so on the first call and name the gap, and we analyze the AWS side only. It is also not for anyone who wants the attacker contacted, negotiated with, or paid, or who wants to hack back. And it is not for a client who needs a testifying expert. The Response works beside AWS Security Incident Response when you have it. After containment, AWS Breach Forensics & Recovery at vantalect.com/breach-forensics scopes the investigation and the repair.

Stage by stage

The Response has no fixed weeks. It has stages, and each ends at a named decision that your incident lead and counsel make in writing. An email is enough.

The Response, by stage.

Stage	What happens
0. Activation	Counsel signs a Counsel Engagement Letter and an incident statement of work, both written new for this incident and billed to counsel's matter. You deploy our incident role from a template you read first, and the bridge opens. Insurer notice runs in parallel through your broker.
1. Stop the bleeding	Containment that captures each setting before changing it: before every action, the state it will change (credential reports, access-key last-used data, policies, key policies, lifecycle and deletion settings, active sessions, job manifests) is captured, hashed, and saved to a locked location, and every change is recorded in the trail and the custody log. Then a deny-list service control policy on the affected organizational unit, the attacker's credentials disabled and sessions revoked, destructive jobs canceled, destructive settings reversed. Each action is proposed, approved by a named approver of yours, and logged with its rollback. It ends when the attacker's credentials show no successful write for 60 minutes.
2. Preserve	The organization trail and every other log source copied to an evidence bucket under S3 Object Lock in a new forensic account; disk and memory acquired from any compromised instance before it is touched; every item hashed and entered in the chain-of-custody log.
3. Protect and recover	Where data is at risk, such as an expiring key or a deletion schedule, an isolated vault account behind a deny-all policy with keys you hold. Data is copied in, verified, and locked, and clean restores go into production as you approve each.
4. Eradicate	Every persistence mechanism removed after it is preserved, the initial access path closed, trust policies and keys reissued. It ends when following every attacker credential shows none alive.
5. Containment declared	Your incident lead declares containment in writing. The executive brief and the clocks worksheet go to counsel, with an interim factual statement for counsel to release.

The Retainer's readiness work, about 48 hours of it.

In the first 30 days	What you get
The activation role	VantalectIncidentResponse, deployed by you from our template into every member account, and by one separate stack in the management account, usable only after activation: the role can be assumed, but every call it makes is denied until your approver removes a deny policy you own, in one scripted call. Its trust policy admits only Charles's named principal with multifactor authentication. Tested in a drill, from activation to first read, in under 15 minutes.
The log-readiness check	The organization trail, data events where they matter, management events, VPC Flow Logs, S3 server access logs, retention, integrity validation, and an evidence bucket under Object Lock. Each gap comes with its fix and its monthly cost.
The watch	Forwarding rules and a central queue in your audit account, with destructive-action and persistence alerts routed to your on-call and copied to us for context. This is not a monitored service: nobody at Vantalect watches the alerts, and the commitments below run only from your page.
The guardrail pack	Containment policies prepared, validated, and stored detached in your policy repository, so stage 1 of a Response is attaching, not writing.
The tabletop	A half-day exercise for your incident team and counsel, with an after-action report.
The paper	Draft forms for your outside counsel to review in advance, which bind no one: at an incident counsel signs new papers. A request to your broker to list Vantalect as a named non-panel provider; the call sheet.

What you receive

Every report carries its distribution line: **Counsel only**, **Operational** (your incident team), or **Releasable** (counsel may share it).

The Response

1. **Situation Reports** (counsel only). One every 12 hours, more often in stage 1: confirmed facts, working hypotheses labeled as such, actions taken and proposed, decisions needed, the notification clocks running, and what is not yet known.
2. **Containment and Eradication Actions** (operational). Every action, who approved it, what it changed, what was preserved first, and how to undo it.
3. **Executive Brief at Containment** (counsel only). One page the CEO and board can read: what happened, what is protected, what is still unknown, and which decisions are theirs.
4. **Notification-Clock Worksheets, interim** (counsel only). The deadlines that may run from your own determinations, computed from the times you enter, with the facts each one needs. The first goes to counsel within six hours of activation, and Vantalect updates it whenever you record a trigger.

5. **Chain-of-Custody Log** (counsel only). Every evidence item from collection to storage, hashed, so counsel can authenticate it.
6. **Interim Factual Statement** (releasable through counsel). Facts only, no analysis or opinion, at containment declared, for counsel to release to your auditor, insurer, a regulator, or the board.

The Retainer

Five documents, in the first 30 days:

7. **Activation Role and Drill.** The role deployed, the drill run, and the measured minutes from activation to first read.
8. **Log-Readiness Check.** Whether the evidence the next investigation needs will exist, and what each gap costs to close.
9. **Readiness Readout.** What you are ready for now, what is still exposed, and the commitments in force.
10. **Tabletop Exercise After-Action Report.** What your team did with a realistic scenario, where it slowed down, and what changes.
11. **Activation Call Sheet.** Who calls whom, in what order, with which numbers and documents, at 1 AM on a holiday.

How the result is measured

The Response has no outcome guarantee. It is measured by its stages: each ends at a decision you make in writing, and the engagement ends when your incident lead declares containment. Containment is not cleanup. Rebuilding systems, rotating every secret in the estate, and root-cause fixes beyond the initial access path belong to the Recovery.

Without a Retainer there is no response-time commitment. Charles reads the incident mailbox and answers the incident telephone around the clock when he can, but one consultant cannot promise a response while he may be on a bridge for another client. Round-the-clock response with written commitments is a Retainer feature. With the Retainer, these commitments run 24 hours a day, every day of the year:

Retainer response commitments.

Commitment	Default	Service credit if missed
Call-back after a page to the incident line given in your call sheet	30 minutes	10% of the annual fee
Hands-on (role assumed, containment proposed) after counsel signs the activation	2 hours	10% of the annual fee
Written situation report	Every 12 hours until containment is declared	None

The honest limit: one responder

Credits are capped at 30% of the annual fee a year. There is one responder, and the Retainer is capped at six clients. When two retained incidents overlap, the second gets the 30-minute call-back and a 4-hour hands-on commitment until a named backup responder exists. Beyond these commitments, no result is guaranteed: we cannot promise that an attacker is out, that data was not accessed, or that a regulator will agree with a finding.

Terms at a glance

Not yet offered. Vantalect does not yet offer the Response or the Retainer, and publishes no incident phone number or mailbox. The terms below are the terms it intends to offer, under counsel review; they are not an offer.

Fees, hours, and scope. The rate covers Charles and the agents he directs; they are not billed separately.

Term	The Response	The Retainer
Fee	$675 an hour, any hour of any day; $450 an hour for Retainer holders	$36,000 for one year
Length	From activation to containment declared	One year, with readiness done in the first 30 days
Consultant hours	Time and materials, logged in six-minute increments, with no premium for nights, weekends, or holidays and no minimum blocks. You set a not-to-exceed figure at activation, default 80 hours, and work stops for a written extension.	40 prepaid readiness hours at $450 ($18,000 of the fee), plus the readiness work. They are not drawn for an incident.
Invoicing	A 24-hour activation authorization of $16,200 ($10,800 for Retainer holders), invoiced to counsel's matter at activation and due on receipt, then weekly invoices in arrears due in fifteen days	Annually in advance, or $9,000 a quarter
Unused portion	Credited to the next invoice or to an Investigation, or refunded within fifteen days of containment declared	In the last 60 days, converted to readiness work (a second tabletop, a compromise assessment, a re-run of the log-readiness check); up to 20 hours roll into a renewal; no cash refund except as the master agreement's early-termination clause provides

Term	The Response	The Retainer
Scope	One AWS organization; your other environments only as named sources of evidence	One AWS organization
Bundle	Not a bundle member, with no bundle discount	Same

The authorization is a deposit against hours, not a minimum. After a Response, the preservation and tracing hours already worked are credited at $450 an hour, up to $10,000, against a following Investigation or Recovery. More than 50 accounts, and anything outside the scope above, are available only by written change order.

Counsel, evidence, and ransom

Nothing here is legal advice. Reports say what the evidence shows and which regimes counsel may want to consider. They never say that something is reportable, material, or not a breach, or that data was not accessed in a way that settles a duty. The worksheets compute deadlines; your counsel decides whether any regime applies.

Counsel retains Vantalect; you pay. For each Response, your outside counsel retains Vantalect, at counsel's direction, to help counsel advise you, in papers written new for that incident. Counsel-track reports go to counsel only, and counsel decides who else sees them. If you have no counsel at 1 AM, we still start on operational work: we contract directly, say in writing that privilege may not attach to what we do before counsel signs, write down only operational facts, give analysis orally, urge you to retain counsel at once, 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 do not contact, negotiate with, or advise on paying the attacker, and we never arrange, send, or hold a payment. We give counsel technical indicators, labeled as indicators, for sanctions screening, and we remind you that reporting to law enforcement matters.

Evidence is captured before anything changes, and nothing is destroyed unless you approve a specific destructive step in writing. The evidence account is yours, owned and controlled by you from the day it is built, and we hold only the investigator role in it. Counsel can direct that a call be recorded; otherwise we record nothing about the counsel track. 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.

What we need from you

- Outside counsel to sign the engagement letter and statement of work, or your decision to proceed without counsel, in writing
- Our incident role deployed in every account in scope, from the template you read, as soon as counsel signs; Retainer holders have it in place already
- A named approver for every containment action, and an incident lead who declares containment in writing
- Your broker told at once, and a request for the insurer's written consent if we are not listed on your policy; costs without consent may not be reimbursed
- A litigation-hold decision from counsel at the start
- The Retainer: the role deployed in the first 30 days, a named approver for the deny policy, and counsel to review the draft forms

What comes with every engagement

- **Charles, personally.** Charles Sieg works your incident himself, with no hand-off to a junior team.
- **Nothing changes without your approver.** Every action is proposed, approved by a named person of yours, and logged with its rollback.
- **Evidence you can use.** Items are hashed when taken and after every transfer, analyzed on copies, and recorded in a chain-of-custody log.
- **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 forensic 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. Pursuit, 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. 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.
- **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.

Questions clients ask

Do we need the Retainer for a Response?

No. The Response is designed to run without it. The Retainer buys the commitments, the lower rate, and an hour you do not spend on paperwork.

Will you handle the ransom?

No, in any form. We never negotiate, advise on paying, or touch funds. A client that decides to pay does so through counsel and a negotiator counsel selects, whom we do not recommend. We do give counsel the technical facts it needs for that decision, such as what can be recovered, the state of the backups, and when key material expires, and we make no recommendation on whether to pay.

Does our cyber insurance cover this?

That is a question for your broker. Many policies expect a panel vendor or written consent for another, so ask your broker now to list Vantalect as a named non-panel provider. The Retainer does the request for you.

What happens after containment?

You choose. Many clients move to the Investigation, and then the Recovery, which close the root causes. Others stop at containment, or take the Retainer.

Do you name the attacker?

We say that activity is “consistent with” or that indicators “overlap with” a known group, never that it was. That is a question for counsel and law enforcement.

Not yet offered

Vantalect does not yet offer AWS Incident Response or the Retainer. It publishes no incident phone number or mailbox, and nothing in this brief is an offer. If an attack is in progress, call AWS Support and your own outside counsel.

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

© 2026 Vantalect LLC. Prices and terms as of October 30, 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. Vantalect is not affiliated with or endorsed by any of them.