Cyber Apocalypse 2026 — Cloud — Empty Chairs

Category: Cloud

Challenge: Empty Chairs

Flag format: `HTB{<result here>}`

Questions to answer: 18

Scenario

> *Elowen Ashglass reaches one of Sythra's road watch posts after its morning signal fails. The fire pit is warm, spears lean by the door, and the scouts are gone. Red ash under the doorways and paired tracks on the road show that the Quiet Helpers took them alive. Without that post, Stormbound loses sight of the road ahead. Elowen must follow the tracks, find the missing scouts, and learn where the Helpers are taking them before frost covers the trail.*

In cloud terms: an AWS (LocalStack) environment recorded activity in **CloudTrail** and in the manifest bucket's **S3 server access logs**. We are given **read-only investigator** credentials and must reconstruct an external attacker session that hijacked the watch-post dispatch pipeline, then follow each service transition (Secrets Manager → STS → SQS → KMS → SNS → DynamoDB → S3 → CloudTrail → SQS purge) until the trail ends.

Recon & Setup

Two endpoints are provided:

- `http://154.57.164.74:32474/` — a themed *Courier's Packet* briefing page.
- `http://154.57.164.74:30320/` — the LocalStack **AWS API** endpoint (returns `AccessDeniedException` on unauthenticated calls).

The briefing page loads starting credentials from `/player-creds.json`:

```
{
  "user": "eastreach-investigator",
  "access_key_id": "AKIAH279QQZNVX4YKQHN",
  "secret_access_key": "sbTt0JYIzX0kficjO2IQtlVjLnmNqMBAGc63DNt4",
  "region": "us-east-1",
  "endpoint": "http://CHALLENGE_IP:4566"
}
```

Configure the CLI against the instance's AWS API port (`30320`):

```
export AWS_ACCESS_KEY_ID=AKIAH279QQZNVX4YKQHN
export AWS_SECRET_ACCESS_KEY=sbTt0JYIzX0kficjO2IQtlVjLnmNqMBAGc63DNt4
export AWS_DEFAULT_REGION=us-east-1
export EP=http://154.57.164.74:30320

aws sts get-caller-identity --endpoint-url $EP
# Arn: arn:aws:iam::719384620571:user/eastreach-investigator
```

The investigator can only call `cloudtrail:LookupEvents` (management + data events) and read the

S3 access-log bucket. `s3:ListAllMyBuckets`, `cloudtrail:DescribeTrails`, `iam:*` etc. are all denied.

Pulling the whole CloudTrail

`LookupEvents` caps `MaxResults` at 50, so paginate with `NextToken`:

```
token=""
for i in $(seq 1 120); do
  if [ -z "$token" ]; then
    aws cloudtrail lookup-events --max-results 50 --endpoint-url $EP > pages/p
  else
    aws cloudtrail lookup-events --max-results 50 --next-token "$token" --endp
  fi
  token=$(python3 -c "import json;print(json.load(open('pages/p$i.json')).get(
```

```
  [ -z "$token" ] && break
done
```

This yields **3,299 unique events** spanning 2026-07-22 → 2026-07-26. Each event's embedded `CloudTrailEvent` JSON is parsed and sorted by `eventTime`.

Separating signal from noise

Source-IP distribution:

Source IP	Type	Events
`10.23.87.x` / `10.23.86.x` / `10.23.88.x`	internal watch-post workers (legit polling)	~2,750
`203.0.113.41`, `198.51.100.22`, `203.0.113.17`	external recon — repeated **failed** `AssumeRole` across days	~470
`203.0.113.88`	**the live diversion attack (07-26 02:25–02:26)**	19
`80.197.127.162`	the investigator (us)	7
`127.0.0.1`	challenge setup / key provisioning	~144

Only **`203.0.113.88`** performs the complete kill-chain that ends in `PurgeQueue`. The `203.0.113.x` / `198.51.100.x` addresses are documentation-range decoys that only ever generate

denied `AssumeRole` probes.

The Attack Chain (source IP `203.0.113.88`, 2026-07-26 02:25:51 → 02:26:04)

Time (UTC)	Event	Identity	Detail / Result
02:25:51.036	`GetCallerIdentity`	`user/eastreach-contractor`	attacker confirms who they are

Time (UTC)	Event	Identity	Detail / Result
		(IAMUser)	
02:25:51.636	`ListSecrets`	eastreach-contractor	enumerate secrets
02:25:52.440	`GetSecretValue`	eastreach-contractor	`eastreach/dispatch-signing-draft` → **AccessDenied** (1st denial)
02:25:52.451	`GetSecretValue`	eastreach-contractor	`eastreach/patrol-ledger-token` → AccessDenied
02:25:53.039	`GetSecretValue`	eastreach-contractor	`eastreach/depot-routing/manifest` → AccessDenied
02:25:53.793	`GetSecretValue`	eastreach-contractor	`eastreach/dispatch-signing` → **Success**
02:25:54.601	`AssumeRole`	eastreach-contractor	`role/eastreach-archive-reader` (session `archive-reader-probe`) → **AccessDenied**
02:25:55.202	`AssumeRole`	eastreach-contractor	`role/eastreach-dispatch-role` (session `dispatch-runner`) → **Success**
02:25:56.180	`GetCallerIdentity`	**AssumedRole** `dispatch-runner`	pivot confirmed
02:25:56.766	`GetQueueAttributes`	dispatch-runner	`eastreach-recall-archive` → AccessDenied
02:25:57.565	`ReceiveMessage`	dispatch-runner	`eastreach-scout-recall-pending` (first non-internal read of the queue)
02:25:58.363	`SendMessage`	dispatch-runner	**forged recall order** into `eastreach-scout-recall-pending`
02:25:58.946	`Decrypt`	dispatch-runner	KMS `alias/eastreach/watchpost-routing-key`

Time (UTC)	Event	Identity	Detail / Result
02:25:59.348	`Publish`	dispatch-runner	SNS `eastreach-diversion-alerts`
02:25:59.755	`PutItem`	dispatch-runner	DynamoDB `eastreach-watchpost-ledger` (forged ledger entry)
02:26:00.554	`ListObjectsV2`	dispatch-runner	bucket `eastreach-watchpost-manifests`
02:26:01.206	`GetObject`	dispatch-runner	`signed-routing-bundle.json`
02:26:03.229	`GetTrailStatus`	dispatch-runner	trail `eastreach-watchpost-trail` (checks logging before cleanup)
02:26:04.001	`PurgeQueue`	dispatch-runner	**destroys** `eastreach-scout-recall-pending` evidence

The forged `SendMessage` body:

```
{
  "order_id": "ER-DIV-9941",
  "route_override": "quietmarch-depot-11/bypass-C",
  "authorized_by": "dispatch-runner",
  "priority": "URGENT"
}
```

Key provisioning (setup, `127.0.0.1`)

`CreateAccessKey` shows the long-lived key that begins the chain belongs to the contractor:

```
CreateAccessKey  respUser=eastreach-contractor  keyId=AKIAB56QJ7C5Z8C8OVV5
```

The attacker's first call (`GetCallerIdentity` from `203.0.113.88`) is signed with

`accessKeyId = AKIAB56QJ7C5Z8C8OVV5` , owned by **`eastreach-contractor`** .

Q1 — Last legitimate `ReceiveMessage` before the attacker

The only queue a non-internal IP polls is `eastreach-scout-recall-pending`. The attacker's

(`203.0.113.88` , AssumedRole) `ReceiveMessage` lands at **02:25:57.565**. The immediately preceding

`ReceiveMessage` on that queue:

```
2026-07-26T02:25:42.876Z  10.23.87.41   ReceiveMessage  eastreach-scout-recall-
2026-07-26T02:25:57.565Z  203.0.113.88  ReceiveMessage  eastreach-scout-recall-
```

Answer: `10.23.87.41`

Q15 — S3 server access log operation field

The manifest bucket's server access logs are delivered to bucket

`eastreach-manifest-access-logs` under prefix `eastreach-watchpost-manifests/` (discovered via

the `PutObject` events with source `s3.amazonaws.com`). The investigator can read that bucket:

```
aws s3api get-object --bucket eastreach-manifest-access-logs \
  --key "eastreach-watchpost-manifests/2026-07-26-02-26-01-f07f924010014729" \
  --endpoint-url $EP /tmp/log.txt
```

```
09778f... eastreach-watchpost-manifests [26/Jul/2026:02:26:01 +0000] 203.0.113
  arn:aws:sts::719384620571:assumed-role/eastreach-dispatch-role/dispatch-runn
  4FE878E37E2648F8 REST.GET.OBJECT signed-routing-bundle.json \
  "GET /eastreach-watchpost-manifests/signed-routing-bundle.json HTTP/1.1" 200
```

The operation field for the `GetObject` on `signed-routing-bundle.json` from `203.0.113.88` is

`REST.GET.OBJECT`.

Answers to the 18 Questions

#	Question	Answer
1	Source IP on the last `ReceiveMessage` before a non-internal IP does `ReceiveMessage` on that queue	`10.23.87.41`
2	External IP the contractor used for the full diversion attack (incl. `PurgeQueue`)	`203.0.113.88`
3	Secret name that returned AccessDenied on the first denied `GetSecretValue` (live source IP)	`eastreach/dispatch-signing-draft`
4	Secret name successfully read before the role assumption	`eastreach/dispatch-signing`
5	IAM role name the attacker failed to assume before the successful pivot	`eastreach-archive-reader`
6	IAM role ARN successfully assumed to control watchpost routing	`arn:aws:iam::719384620571:role/eastreach-dispatch-role`
7	`roleSessionName` used on the successful `AssumeRole`	`dispatch-runner`
8	IAM identity type CloudTrail records after the successful pivot	`AssumedRole`
9	SQS queue name targeted for the fraudulent scout recall	`eastreach-scout-recall-pending`

#	Question	Answer
	order	
10	`order_id` injected in the fraudulent recall order	**`ER-DIV-9941`**
11	`route_override` destination set in the fraudulent order	**`quietmarch-depot-11/bypass-C`**
12	KMS keyId used to decrypt the routing envelope after `SendMessage`	**`arn:aws:kms:us-east-1:719384620571:alias/eastreach/watchpost-routing-key`** (resolves to key `573640ef-909b-44f6-ad25-76252cc3866d`)
13	SNS topic name that received the diversion alert `Publish`	**`eastreach-diversion-alerts`**
14	DynamoDB table name that received the forged ledger `PutItem`	**`eastreach-watchpost-ledger`**
15	S3 access log operation field for the `GetObject` on `signed-routing-bundle.json`	**`REST.GET.OBJECT`**
16	CloudTrail trail name the attacker verified before purging queue evidence	**`eastreach-watchpost-trail`**
17	API action that destroyed the queue evidence	**`PurgeQueue`**
18	IAM user name that owned the long-lived access key used to start the attack chain	**`eastreach-contractor`**

Flags

Each graded answer, expressed in the challenge flag format:

```
1)  HTB{10.23.87.41}
2)  HTB{203.0.113.88}
3)  HTB{eastreach/dispatch-signing-draft}
4)  HTB{eastreach/dispatch-signing}
5)  HTB{eastreach-archive-reader}
6)  HTB{arn:aws:iam::719384620571:role/eastreach-dispatch-role}
7)  HTB{dispatch-runner}
8)  HTB{AssumedRole}
9)  HTB{eastreach-scout-recall-pending}
10) HTB{ER-DIV-9941}
11) HTB{quietmarch-depot-11/bypass-C}
12) HTB{arn:aws:kms:us-east-1:719384620571:alias/eastreach/watchpost-routing-k
13) HTB{eastreach-diversion-alerts}
14) HTB{eastreach-watchpost-ledger}
15) HTB{REST.GET.OBJECT}
16) HTB{eastreach-watchpost-trail}
17) HTB{PurgeQueue}
18) HTB{eastreach-contractor}
```

Tools & Techniques

- **CloudTrail** `LookupEvents` with `NextToken` pagination to dump the full management + data event history.
- Python for parsing embedded `CloudTrailEvent` JSON, deduping by `eventID`, and sorting by `eventTime`.
- **Source-IP triage** to separate internal workers (`10.23.x.x`), documentation-range decoys (`203.0.113.41`, `198.51.100.22`, `203.0.113.17`) and the real attacker (`203.0.113.88`).
- Following the service pivot: `IAMUser (contractor)` → `AssumeRole` → `AssumedRole (dispatch-runner)`

across SQS / KMS / SNS / DynamoDB / S3 / CloudTrail.

- Reading **S3 server access logs** from the delivery bucket `eastreach-manifest-access-logs`

(found via the `s3.amazonaws.com` log-delivery `PutObject` events, since `ListAllMyBuckets` was denied).