Ghost Vector

PILLAR GUIDE

AWS INCIDENT RESPONSE

AWS Incident Response in APAC: A Regulatory and Technical Playbook

How AWS incident response works across Australia, Singapore, India, and the wider ASEAN region — the reporting clocks, the detection toolchain, and the operational gotchas that change as you cross borders.

AUSTRALIA SINGAPORE INDIA MALAYSIA THAILAND INDONESIA PHILIPPINES VIETNAM

By Matt Gurr
12 May 2026

ghostvector.ai/guides

GHOST VECTOR — PILLAR GUIDE

AWS Incident Response in APAC: A Regulatory and Technical Playbook

TL;DR

This is the pillar guide for AWS incident response across Asia-Pacific. APAC has the world's most fragmented incident reporting landscape — every country runs its own regulator, its own clock, and its own definition of what counts as a reportable incident. The right strategy is not one runbook per country but a single AWS-native detection and response capability that can fan out into multiple reports in parallel. This guide covers what AWS does and does not do for you, the country-by-country clock table, the AWS services that make up an effective IR stack in this region, and a 30-day plan for getting ready.

Contents

What AWS incident response actually means

AWS operates on a **shared responsibility model**: AWS is responsible for security *of* the cloud (data centres, hypervisor, hardware, managed-service control planes), and you are responsible for security *in* the cloud (IAM, network configuration, application code, customer data, and everything you build on top of AWS services).

In incident response terms, this maps to two non-negotiable points:

- **AWS will not file regulatory reports for you.** If your S3 bucket leaks because of a misconfigured policy, that is your incident, your investigation, and your CERT-In or OAIC report.
- **AWS will notify you of incidents on their side.** If AWS detects a compromise of infrastructure that affects your account, they will tell you — and they sometimes detect things in your account before you do, via abuse signals from peers. The AWS Trust & Safety team is real and reachable.

Most APAC regulatory obligations sit cleanly on your side of the line. This guide assumes that and focuses on what you can and should do with AWS-native tools.

The APAC regulatory reporting clock

This is the highest-value reference on this page. APAC incident reporting deadlines vary by an order of magnitude — from 1 hour to 72 hours — and the same incident can trigger several in parallel. Snapshot as of mid-2026:

Country	Regulator	Trigger	Clock	Sector
Australia	OAIC (Privacy Act NDB)	Eligible data breach	As soon as practicable after assessment (assessment due within 30 days)	All
Australia	APRA (CPS 234)	Material information security incident	72 hours	Regulated FSI
Australia	ACSC / Home Affairs (SOCI Act)	Critical / significant cyber incident	12 hours (critical) / 72 hours (relevant)	Critical infrastructure
Singapore	PDPC (PDPA)	Notifiable data breach (≥500 individuals or significant harm)	3 calendar days	All
Singapore	MAS (TRM Guidelines)	Relevant incident	**1 hour**	FSI
Singapore	CSA (Cybersecurity Act)	Cybersecurity incident on CII	2 hours	Critical information infrastructure
India	CERT-In (2022 Directions)	Any of 20 listed incident types	**6 hours from noticing**	All
India	Data Protection Board (DPDP Act 2023)	Personal data breach	Without delay	All
India	RBI (Master Directions)	Cyber incident	2–6 hours	Banks, NBFCs
Malaysia	PDP Commissioner	Personal data breach	72 hours	All

Country	Regulator	Trigger	Clock	Sector
	(PDPA 2024 amendments)			
Malaysia	NACSA (Cyber Security Act 2024)	Cyber incident affecting NCII	6 hours	National critical info infrastructure
Thailand	PDPC (PDPA 2019)	Personal data breach	72 hours	All
Thailand	NCSA (Cybersecurity Act 2019)	Cyber threat to CII	Per regulator direction	Critical infrastructure
Indonesia	Personal Data Protection Agency (PDP Law 2022)	Personal data breach	3×24 hours	All
Indonesia	BSSN (GR 71/2019)	Electronic system incident	Immediate	ESPs
Philippines	NPC (Data Privacy Act)	Personal data breach (real risk of serious harm)	72 hours	All
Philippines	BSP	Major cyber incident	2 hours	Banks
Vietnam	MPS / A05 (Cybersecurity Law)	Cyber incident	Immediate	All
Vietnam	(PDP Decree 13/2023)	Personal data breach	72 hours	All

Caveat: these are snapshot summaries and many of these regimes are evolving — India's DPDP rules and Malaysia's NACSA framework in particular are still being operationalised. Confirm the current rule for your sector before relying on this table during a live incident.

Deep dives per jurisdiction:

- Meeting CERT-In's 6-hour incident reporting rule on AWS
- APRA CPS 234 notification obligations on AWS
- MAS TRM and AWS incident response — Singapore FSI 1-hour clock
- OAIC Notifiable Data Breach scheme on AWS — Australian privacy regulator

The AWS-native IR toolchain

The most economical IR stack on AWS for APAC regulatory expectations is built from six services. None of them are exotic and most of them are cheap to run.

- **CloudTrail** — the audit log of every API call. Non-negotiable. Configure as an organisation trail with the S3 destination in your primary regulated region.
- **GuardDuty** — managed threat detection. Turn it on in every region you use, including ones you do not actively operate in (attackers will spin resources up in unused regions).
- **Security Hub** — aggregates findings from GuardDuty, IAM Access Analyzer, Macie, Inspector, and partner tools. Your single pane of glass for triage.
- **Detective** — investigative graph view that lets you trace an alert across accounts, users, and resources. Optional but valuable in fast triage.
- **CloudWatch Logs + VPC Flow Logs** — your evidence baseline for network and application activity.
- **Macie** — for any account holding personal data; flags S3 buckets with unusual access patterns or exposed sensitive data.

The mapping of these services to the incident categories that regulators care about is covered scenario-by-scenario in dedicated guides for each major APAC jurisdiction.

The first 60 minutes on AWS

A generic AWS incident response runbook, jurisdiction-agnostic. The first hour is the same regardless of which regulator you eventually report to.

1. **Minute 0 — Detect and confirm.** An alert fires (GuardDuty, custom CloudWatch alarm, customer report, AWS abuse notification). An analyst confirms it is a real incident. Record this timestamp — *most regulatory clocks start here.*
2. **Minutes 0–10 — Mobilise.** Page the incident commander. Open a war-room channel. Identify the affected accounts, regions, and services.

3. **Minutes 10-25 — Contain.** Quarantine compromised resources without destroying evidence. For compromised IAM keys: deactivate the key, not the user. For compromised EC2: isolate via security group swap, do not terminate. For S3 exfiltration: block public access at the account level, tighten bucket policies.
4. **Minutes 25-40 — Preserve evidence.** Snapshot EBS volumes, copy CloudTrail and VPC flow logs for the relevant time window into a forensics S3 bucket, capture memory if your EDR supports it.
5. **Minutes 40-55 — Assess scope.** What was accessed, by whom, from where, when. This is where Detective and CloudTrail Athena queries earn their cost.
6. **Minute 55-60 — Decide on notifications.** Apply the regulatory clock table above to determine who needs to know and within what timeframe. If you have users in multiple APAC countries, you may be filing several reports.

A 60-minute window is the right design target — it leaves headroom under every clock in the table except MAS TRM's 1-hour rule, which requires its own dedicated runbook.

Region selection and data residency

APAC has more AWS regions than any other continent. The current map (mid-2026):

- **Australia** — ap-southeast-2 (Sydney), ap-southeast-4 (Melbourne)
- **Singapore** — ap-southeast-1
- **Malaysia** — ap-southeast-5 (Kuala Lumpur)
- **Thailand** — ap-southeast-7
- **Indonesia** — ap-southeast-3 (Jakarta)
- **India** — ap-south-1 (Mumbai), ap-south-2 (Hyderabad)
- **Japan** — ap-northeast-1 (Tokyo), ap-northeast-3 (Osaka)
- **Korea** — ap-northeast-2 (Seoul)
- **Hong Kong** — ap-east-1

Three IR-relevant patterns:

- **Data residency rules narrow your options.** India and Indonesia have explicit in-country storage rules for certain data classes. Singapore and Australia do not, but sector regulators (MAS, APRA) impose effective in-country preferences.

- **Service availability is uneven across regions.** SES, Bedrock, and several newer services are not available in every APAC region. Plan IR notification and analytical tooling around the regions where they actually exist.
- **Cross-region log replication is your friend.** Replicate CloudTrail and security logs to a secondary region within the same jurisdiction for resilience. Do not replicate across jurisdictions if residency rules apply.

When to call an external IR partner

Three triggers usually justify external help:

- **Capacity.** Your team can handle one incident; a serious incident often runs three or four parallel workstreams (containment, forensics, communications, recovery). External hands fill the gap.
- **Specialist skills.** Cloud-native forensics, malware reverse engineering, regulatory drafting in non-English jurisdictions — most internal teams do not maintain these year-round.
- **Independence.** Some regulators and most insurers expect an external party's signoff on the post-incident report.

Establish a retainer *before* you need one. Time-to-engage matters more than hourly rate. Ghost Vector's managed detection service covers AWS incident response with APAC regulatory awareness baked in.

Building an APAC-ready IR plan in 30 days

A realistic 30-day work programme to move from "we have GuardDuty turned on" to "we can hit every APAC reporting clock that applies to us." A four-week sprint:

Week 1 — Inventory and obligations. Map your AWS accounts, regions, and the countries you serve. Cross-reference to the regulatory clock table. Identify the tightest deadline that applies to you and design the rest of the plan around it.

Week 2 — Detection and logging baseline. Confirm CloudTrail organisation trail is live, GuardDuty is on everywhere, Security Hub is aggregating, log retention meets the strictest applicable rule (180 days in-India for CERT-In if you have Indian exposure, longer for regulated sectors elsewhere).

Week 3 — Runbooks and notification readiness. Draft scenario runbooks for the five most likely incident types: compromised IAM keys, S3 exfiltration, ransomware on EC2, account takeover, GuardDuty critical finding. Pre-stage

reporting templates for each regulator that applies to you. Register or refresh your point-of-contact details with CERT-In if applicable.

Week 4 — Tabletop. Run a timed exercise against a realistic scenario. Measure time from "alert fires" to "report submitted." Find the bottlenecks. Iterate.

This skeleton is the starting point. Every section above has a deeper guide either live or in development — start with the CERT-In playbook if India is in scope, or get in touch if you would like to short-cut the 30-day plan with a structured review.

Frequently asked questions

Common questions about AWS incident response in APAC are answered in the FAQ schema attached to this page — scroll back to the top of the rendered article for the structured-data version, or search the page for the question you have in mind.