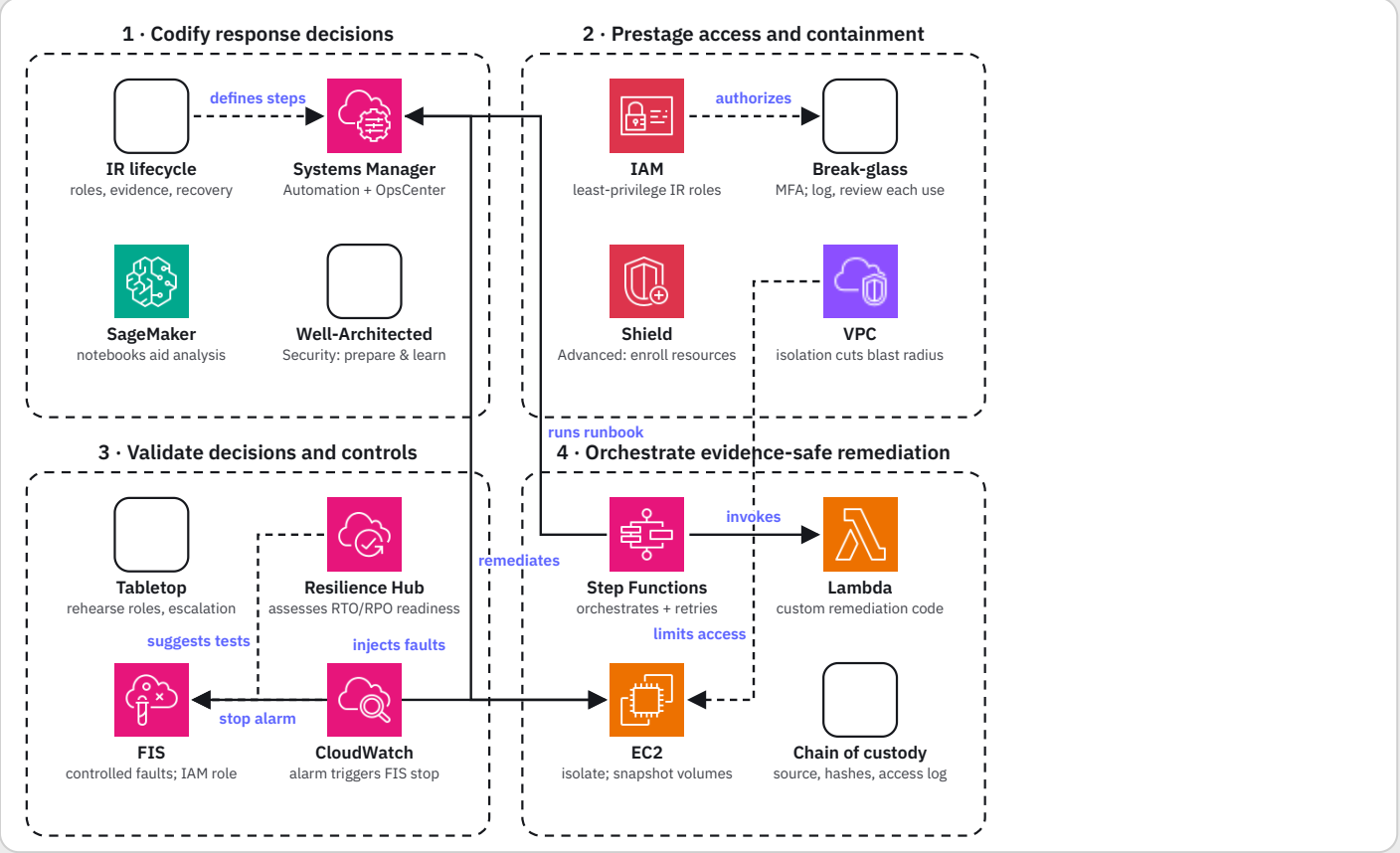
DOMAIN 2 · INCIDENT RESPONSE · 14% OF THE EXAM · TASK STATEMENT 2.1

Design and test an incident response plan

Plan, prepare, test, remediate



1 Codify response decisions

Use **runbooks** for repeatable response: OpsCenter tracks OpsItems; Systems Manager Automation executes procedures. Notebooks support investigation. Define authority, communications, and recovery criteria.

2 Prestage access and containment

Preprovision and test **break-glass access** before incidents; restrict and audit use. Predeploy response tools. Shield Advanced requires protection enrollment; DDoS protection is not host remediation.

3 Validate decisions and controls

Tabletop exercises validate decisions and communications, not live controls. Chaos engineering uses hypotheses and measurable outcomes; FIS injects bounded faults. Resilience Hub assesses resilience against RTO/RPO goals.

4 Orchestrate evidence-safe remediation

Chain of custody requires artifact IDs, timestamps, hashes, and an access trail. Preserve evidence before destructive remediation; make runbooks idempotent so retries do not repeat harmful actions.

Exam traps

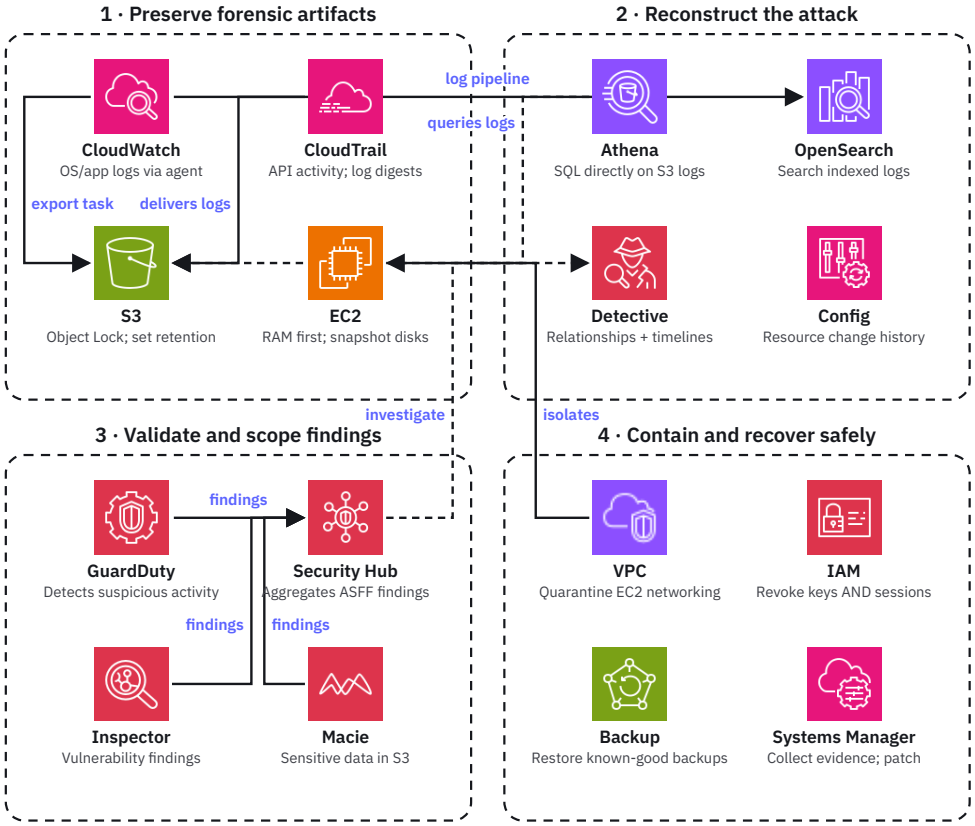
- **FIS stop conditions** stop experiment actions, not a guaranteed rollback of every effect; recovery and cleanup still need tested procedures.
- Step Functions retries do not guarantee **idempotency**; incident/resource keys and state checks prevent duplicate or destructive remediation.
- **Volume snapshots are not memory captures**. Preserve required volatile evidence before stopping or terminating a compromised instance.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 2 · INCIDENT RESPONSE · TASK STATEMENT 2.2

Respond to security events

Preserve, correlate, validate, recover



1 Preserve forensic artifacts

For **evidence integrity**, capture RAM before stopping EC2 and snapshot disks. Hash artifacts, record chain of custody, retain originals with S3 Object Lock, and enable CloudTrail log validation to detect tampering.

2 Reconstruct the attack

For **root cause**, normalize fields and correlate event times, accounting for clock skew and delivery delays. Combine Detective relationships, CloudTrail events and Config history to reconstruct timelines and attack paths.

3 Validate and scope findings

Assess **blast radius** across identities, resources, accounts and exposed data. Corroborate findings with logs to distinguish false positives and authorized activity; severity alone neither proves compromise nor establishes scope.

4 Contain and recover safely

Use **immutable infrastructure** to replace compromised hosts with trusted images after preserving evidence. Isolate networks, revoke compromised access, remove persistence, restore clean data and validate recovery before reconnecting.

Exam traps

- **CloudTrail Event history** covers 90 days of regional management events, not application logs or data events. Configure a trail and required event selectors for retained forensic coverage.
- **Security group isolation** does not reliably terminate tracked connections. Network ACL deny rules can interrupt traffic immediately but are stateless and can affect other resources in the subnet.
- **Deleting an access key** does not invalidate temporary credentials already issued from it. Revoke affected role sessions and address downstream credentials; stopping EC2 alone does not revoke access.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 2 · INCIDENT RESPONSE · WHAT TO REMEMBER

Concepts and services of Incident Response

Concepts to know

Incident Response Lifecycle

Preparation, detection and analysis, containment, eradication, recovery, and lessons learned organize response. The deciding factor is **the incident phase**: containment limits damage; eradication removes the cause; recovery restores trusted operations.

Evidence Integrity

Evidence integrity preserves authentic, unchanged artifacts. **Preserve before destructive remediation** distinguishes forensic collection from recovery; hashes, protected storage, and documented handling support defensible analysis.

Network Isolation

Network isolation restricts compromised resources' communications while retaining investigative access. **Contain without destroying evidence** favors quarantine over termination; security group changes alone may not interrupt established connections.

Core services



AWS Systems Manager

Automation runbooks execute repeatable containment and recovery; Run Command executes commands on managed nodes. **Automation** fits coordinated remediation with approvals and controlled execution.



AWS CloudTrail

Records AWS API activity for identity attribution and incident timelines. **Who called which API, and when** points here; S3 object-level activity requires relevant data events to be enabled.



Amazon Detective

Correlates supported identity, network, and finding data for investigation. **Scope and root cause** point here; initial threat detection belongs to Amazon GuardDuty.

Get practice exams and lessons for AWS Certified Security - Specialty