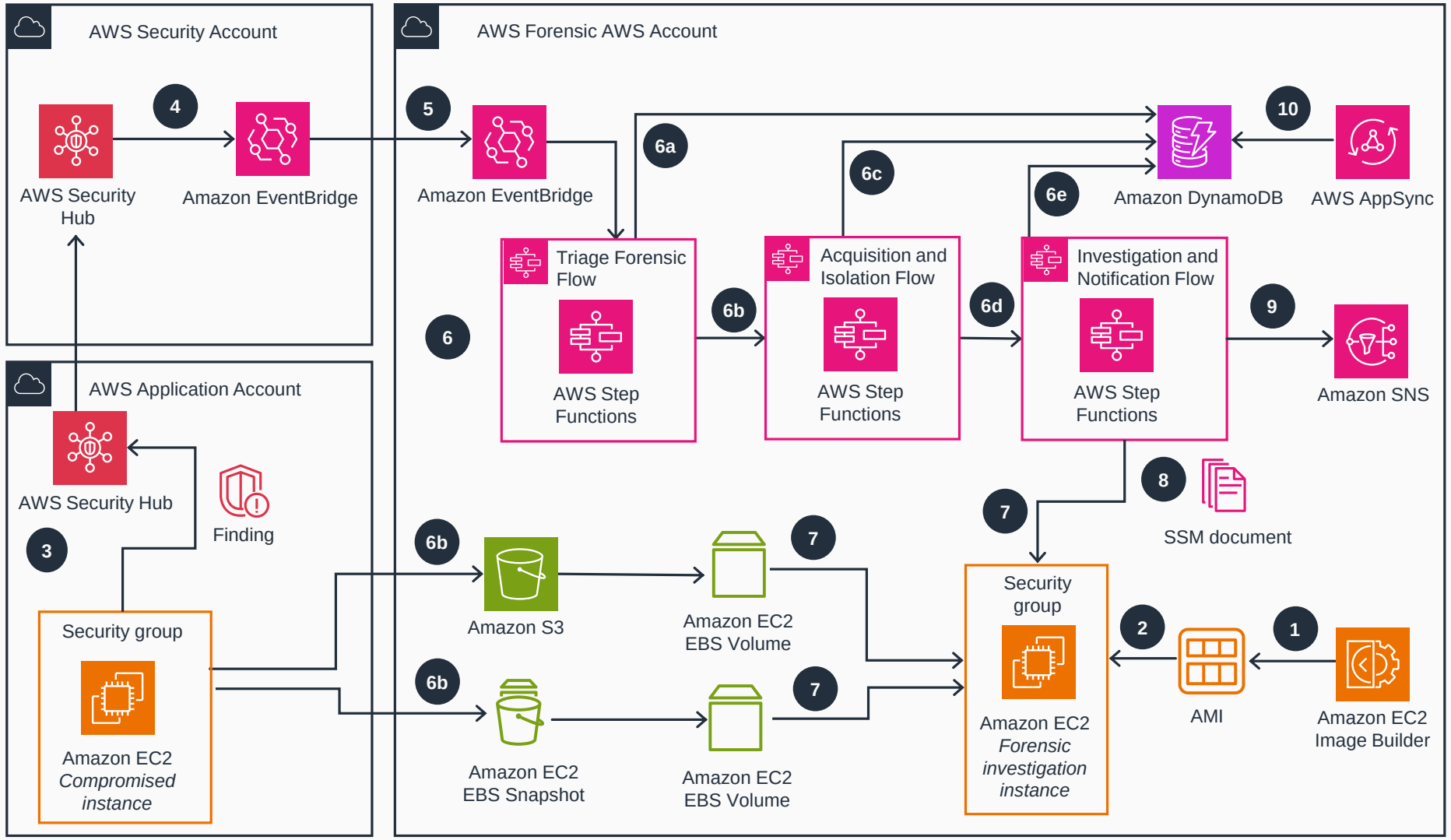
Guidance for Automated Forensics Orchestrator for Amazon EC2

This architecture diagram deploys a mechanism that orchestrates and automates key digital forensics processes and activities for Amazon EC2 instances in the event of a potential security issue being detected. This slide shows steps 1-6a.



1. Prior to running the workflow, you will need a forensic Amazon Machine Image (AMI). You can use **Amazon EC2 Image Builder** to build a new forensic AMI or an existing forensic AMI.
2. **AWS Step Functions** leverages the forensic AMI to perform memory and disk investigation.
3. In the AWS application account, **AWS Config managed rules**, **Amazon GuardDuty**, and third-party tools detect malicious activities that are specific to **Amazon Elastic Compute Cloud (Amazon EC2)** resources. For example, an **EC2** instance queries a low reputation domain name that is associated with known abused domains. The findings are sent to **AWS Security Hub** in the security account through their native or existing integration.
4. By default, all **Security Hub** findings are then sent to **Amazon EventBridge** to invoke automated downstream workflows.
5. For a specified event, **EventBridge** provides an instance ID for the forensics process to target, and initiates the **Step Functions** workflow.
6. **Step Functions** triages the request through the following approach: It first gets the instance information. It then determines if isolation is required based on the **Security Hub** action and if acquisition is required based on tags associated with the instance. Finally, it initiates the acquisition flow based on triaging output.

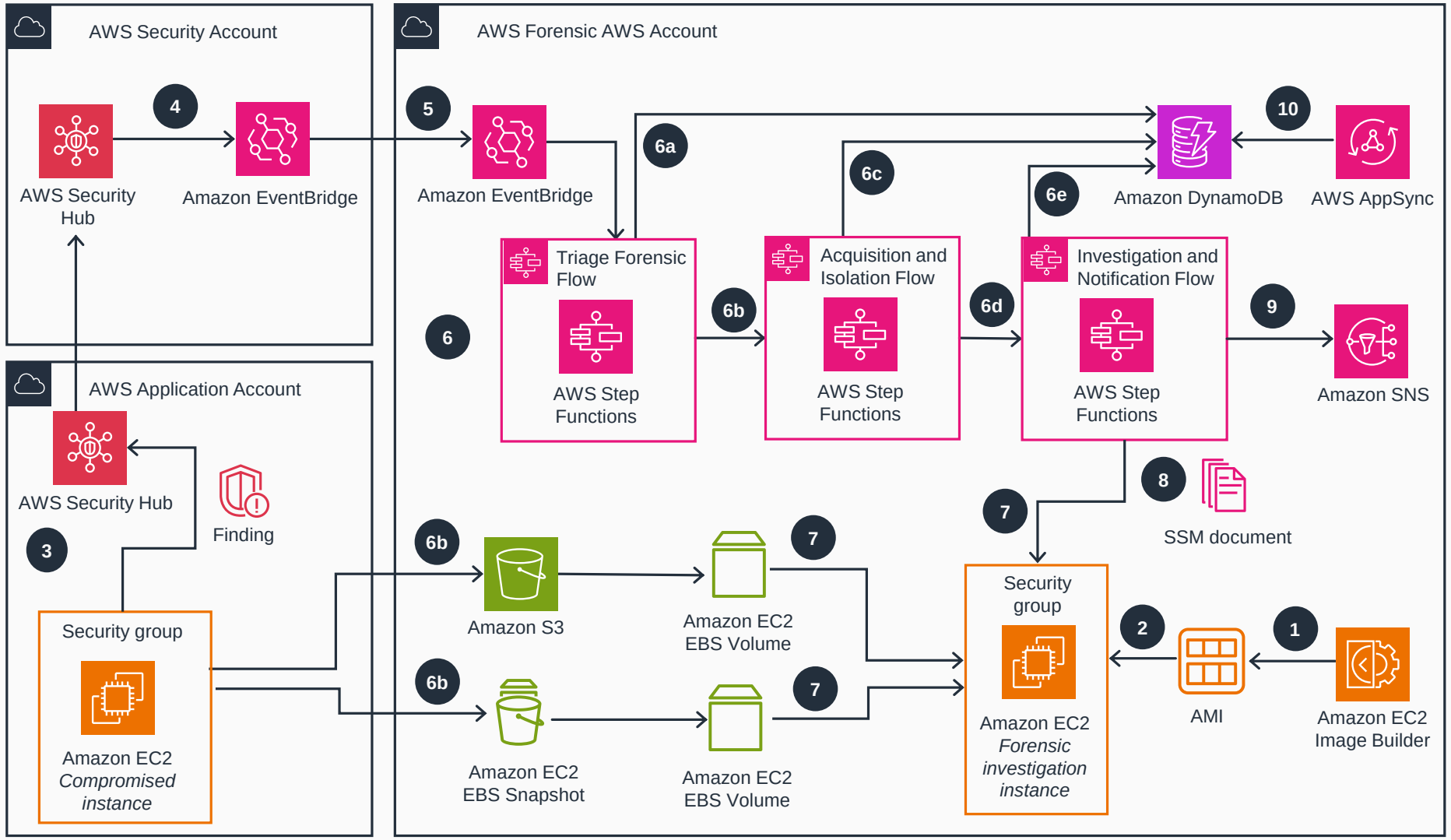
6a. **Amazon DynamoDB** stores triaging details.

Reviewed for technical accuracy April 25, 2025

AWS Reference Architecture

Guidance for Automated Forensics Orchestrator for Amazon EC2

This architecture diagram deploys a mechanism that orchestrates and automates key digital forensics processes and activities for Amazon EC2 instances in the event of a potential security issue being detected. This slide shows steps 6b-10.



6b Two acquisition flows are initiated in parallel: The *Memory Forensics Flow* is a **Step Functions** workflow that captures the memory data and stores it in **Amazon Simple Storage Service (Amazon S3)**. Post memory acquisition, the instance is isolated using security groups. To help ensure the chain of custody, a new security group gets attached to the targeted instance and removes any access for users, admins, or developers. Isolation is initiated based on the selected **Security Hub** action. The *Disk Forensics Flow* is a **Step Functions** workflow that takes a snapshot of an **Amazon Elastic Block Store (Amazon EBS)** volume and shares it with the forensic account.

6c **DynamoDB** stores acquisition details.

6d Once the disk or memory acquisition process is complete, a notification is sent to an investigation **Step Functions** state machine to begin the automated investigation of the captured data.

6e When the **Step Functions** jobs are complete, **DynamoDB** stores the state of forensic tasks and their results.

7 Investigation **Step Functions** starts a forensic instance from an existing forensic AMI loaded with customer forensic tools. **Step Functions** loads the memory data from **Amazon S3** for investigation, creates an **EBS** volume from the snapshot, and attaches the **EBS** volume for disk analysis.

8 **AWS Systems Manager** documents (SSM documents) run forensic investigation.

9 **Amazon Simple Notification Service (Amazon SNS)** shares investigation details with customers.

10 **AWS AppSync** can query the forensic timeline. For more details, refer to Sample AppSync API to query forensic details.

AWS Reference Architecture