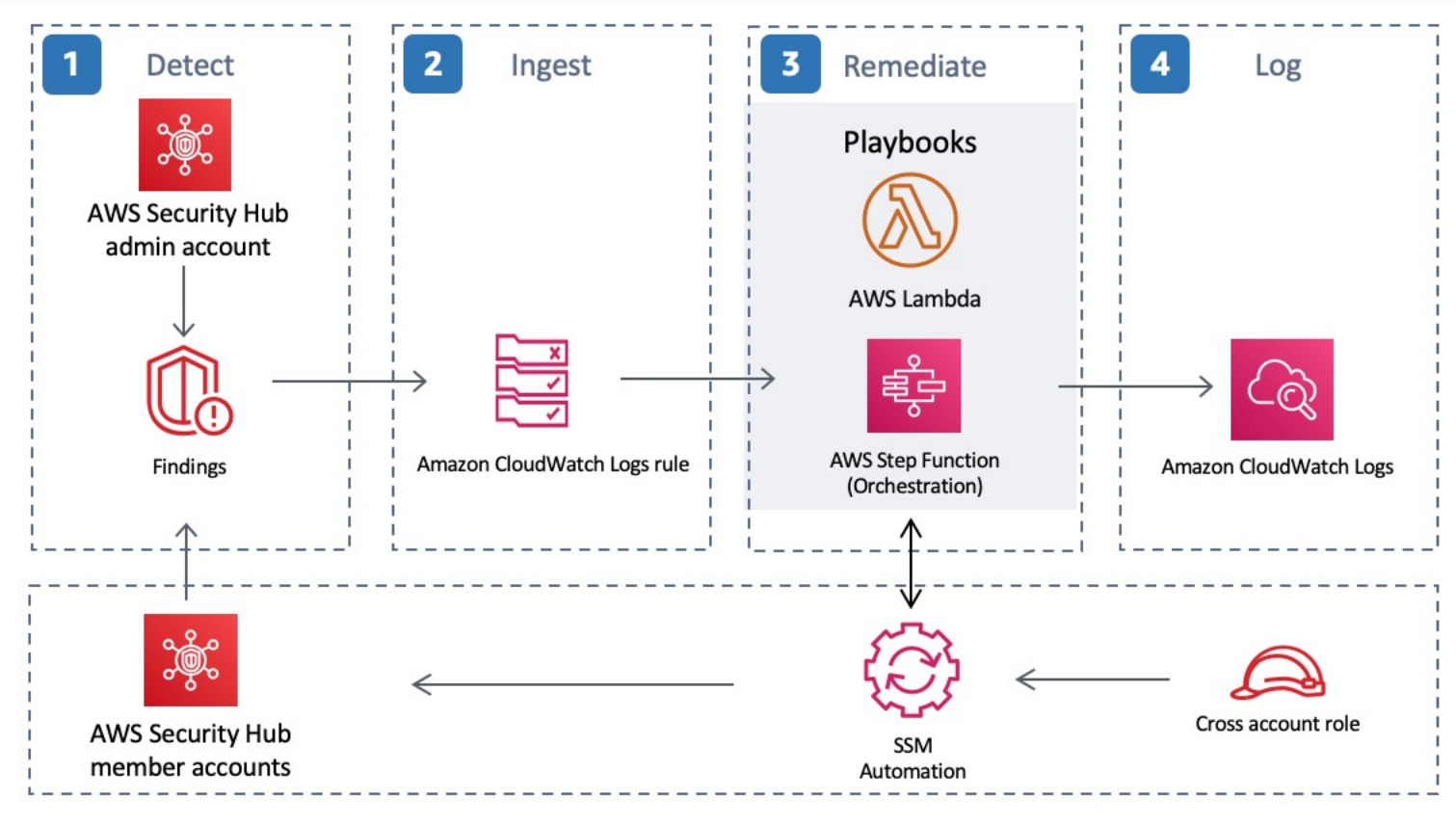
AWS Security Hub Automated Response and Remediation

This solution helps AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS. To deploy this solution using the available AWS CloudFormation template, select **Deploy with AWS**.



1. **Detect**: AWS Security Hub provides customers with a comprehensive view of their AWS security state. It helps them to measure their environment against security industry standards and best practices. It works by collecting events and data from other AWS services, such as AWS Config, Amazon Guard Duty, and AWS Firewall Manager. These events and data are analyzed against security standards, such as CIS AWS Foundations Benchmark. Exceptions are asserted as findings in the AWS Security Hub console. New findings are sent as Amazon CloudWatch Events.

2. **Ingest**: AWS Security Hub Custom Actions and Amazon CloudWatch Events rules initiate Security Hub Automated Response and Remediation playbooks to address findings. Two CloudWatch Event Rules are deployed for each supported control by the solution: one rule to match the custom action event (user-initiated remediation), and one rule (disabled by default) to match the real-time finding event. Customers can use the Security Hub Custom Action menu to initiate automated remediation, or after careful testing in a non-production environment, they can enable automatic triggering for automated remediation. This decision can be made per remediation—it is not necessary to enable automatic triggers on all remediations.

3. **Remediate**: Using cross-account AWS Identity and Access Management (IAM) roles, the automated remediation uses the AWS API to perform the tasks needed to remediate findings. All playbooks in this solution call AWS Lambda functions. Some Lambda functions perform remediation directly. Others use AWS Systems Manager automation documents.

4. **Log**: The playbook logs the results to the Amazon CloudWatch Logs group for the solution, sends a notification to an Amazon Simple Notification Service (Amazon SNS) topic, and updates the Security Hub finding. An audit trail of actions taken is maintained in the finding notes. On the Security Hub dashboard, the finding workflow status is changed from NEW to either NOTIFIED or RESOLVED on the Security Hub dashboard. The security finding notes are updated to reflect the remediation performed.

Deploy with AWS

aws **Deployable AWS Reference Implementation**