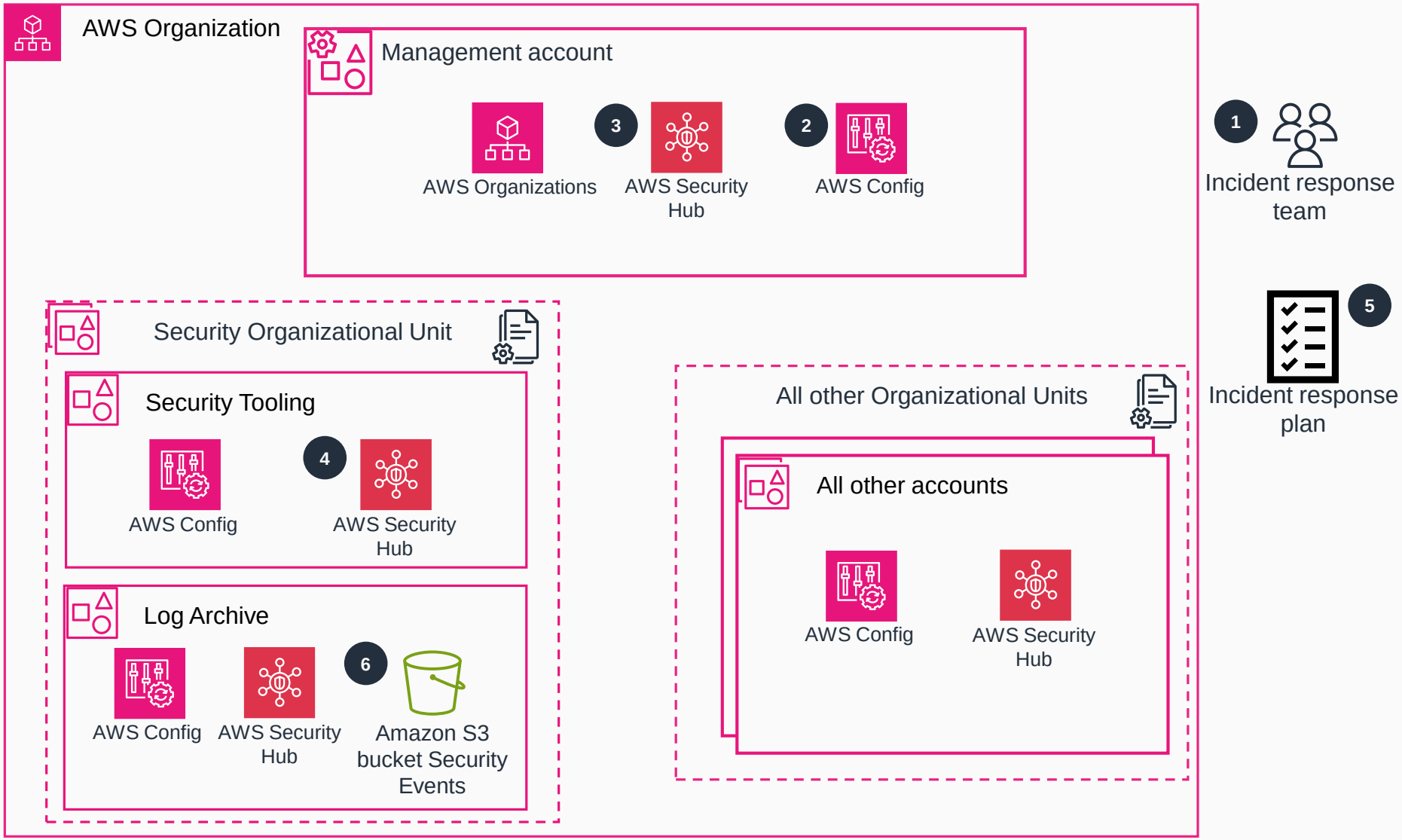
Guidance for Security Incident Response on AWS



1. Establish an incident response team and incident response plan.
2. Deploy an **AWS Config** configuration recorder and delivery channel to all operating Regions in all member accounts. Review service control policies (SCPs) for examples of deny list policy strategies. Configure the delivery channel to send to the **AWS Config Amazon Simple Storage Service (Amazon S3)** bucket in the Log Archive account.
3. Enable **AWS Security Hub** for your organization using the AWS Security Hub and AWS Organizations user guide to centralize security findings for a single account. Configure cross-Region aggregation to centralize Regional security findings to one Region.
4. Delegate the administration of AWS Security Hub to the Security Tooling Account to allow the security team to manage the **Security Hub** and any findings outside of the management account.
5. Respond to the incident based on the incident response plan. This can include recovery of systems, remediating findings, or isolating affected systems. The Automated Security Response on AWS solution creates predefined response and remediation actions based on industry compliance standards.
6. Send security event logs to a centralized **Amazon S3** bucket in the Log Archive account for retention as required.

Reviewed for technical accuracy January 4, 2024

AWS Reference Architecture