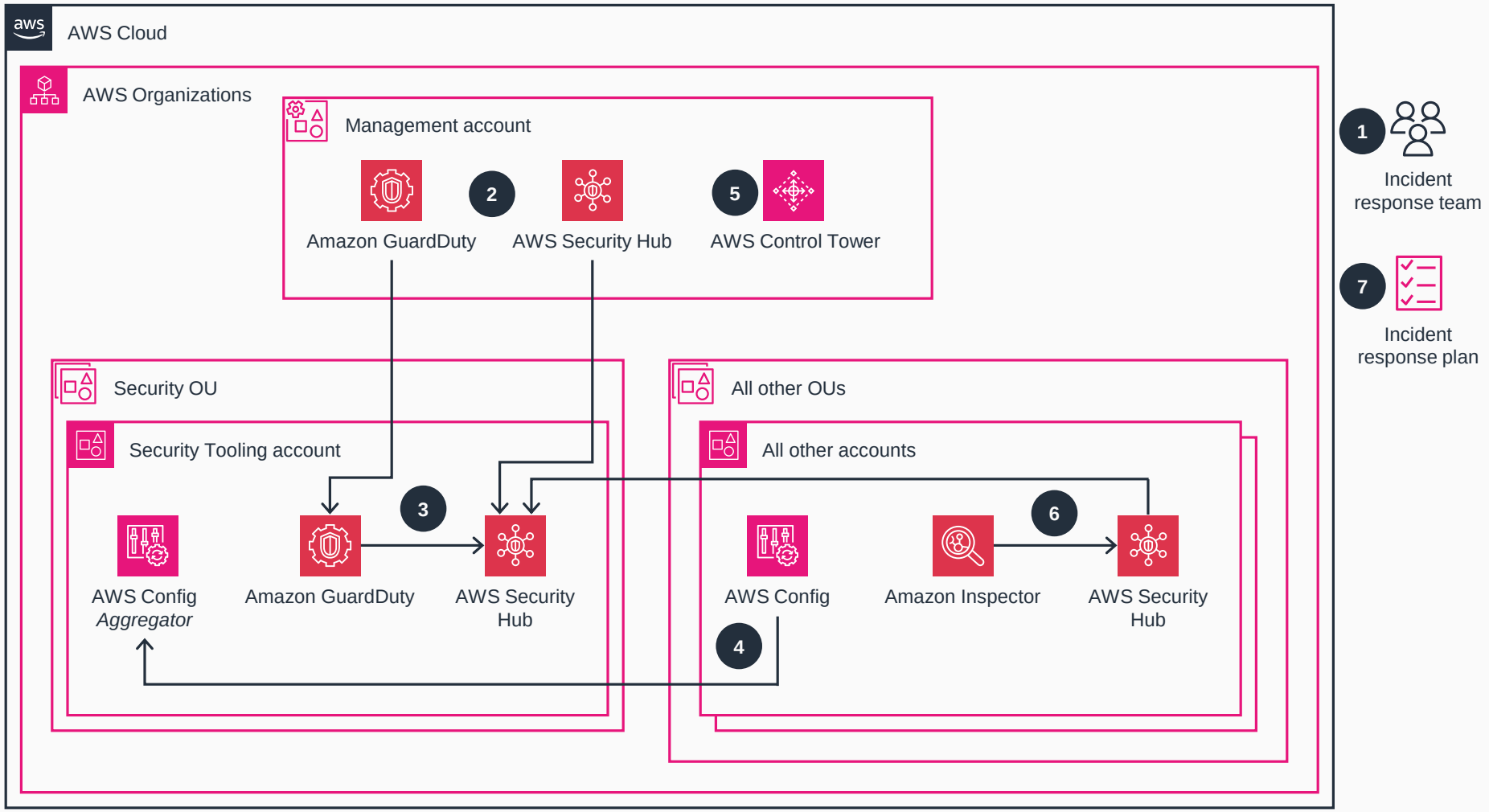
Guidance for Threat & Vulnerability Management on AWS

This architecture diagram shows you how to scan for, centralize, and respond to threats and vulnerabilities in your environment.



1 Incident response team

7 Incident response plan

1. Establish an incident response team and an incident response plan.
2. Enable and delegate the administration of **Amazon GuardDuty** and **AWS Security Hub** (using the **AWS Organizations** integration documentation for **GuardDuty** and **Security Hub**) to the Security Tooling account in the security organizational unit (OU). This moves the administration of these tools outside the management account.
3. **GuardDuty** findings will be sent to **Security Hub**. Use **Security Hub** in the aggregation AWS Region of your Security Tooling account for a comprehensive view of the security state in your **Organizations** and to respond to security incidents.
4. Use **AWS Config** to deploy a **configuration recorder** and **delivery channel** to all operating Regions (that are not prohibited by **your service control policies**) in all member accounts to identify and track assets. Deploy an **AWS Config aggregator** in the Security Tooling account to centrally view or query the resource configuration and compliance of **AWS Config** resources.
5. Create **AWS Config rules** using **detective controls** in **AWS Control Tower** or using **AWS Config managed rules** to evaluate your resource configurations and confirm alignment to best practices.
6. Enable **Amazon Inspector** in your **Organizations accounts** to identify vulnerabilities in **Amazon Elastic Compute Cloud (Amazon EC2)**, your **Amazon Elastic Container Registry (Amazon ECR)** container images, and **AWS Lambda** functions. The findings will be sent to **Security Hub** and are centralized to **Security Hub** in the Security Tooling account.
7. Respond to the incident based on your incident response plan. This can include recovering systems, remediating findings, or isolating affected systems. **Automated Security Response on AWS** creates predefined response and remediation actions based on industry compliance standards.

Reviewed for technical accuracy February 28, 2024

AWS Reference Architecture