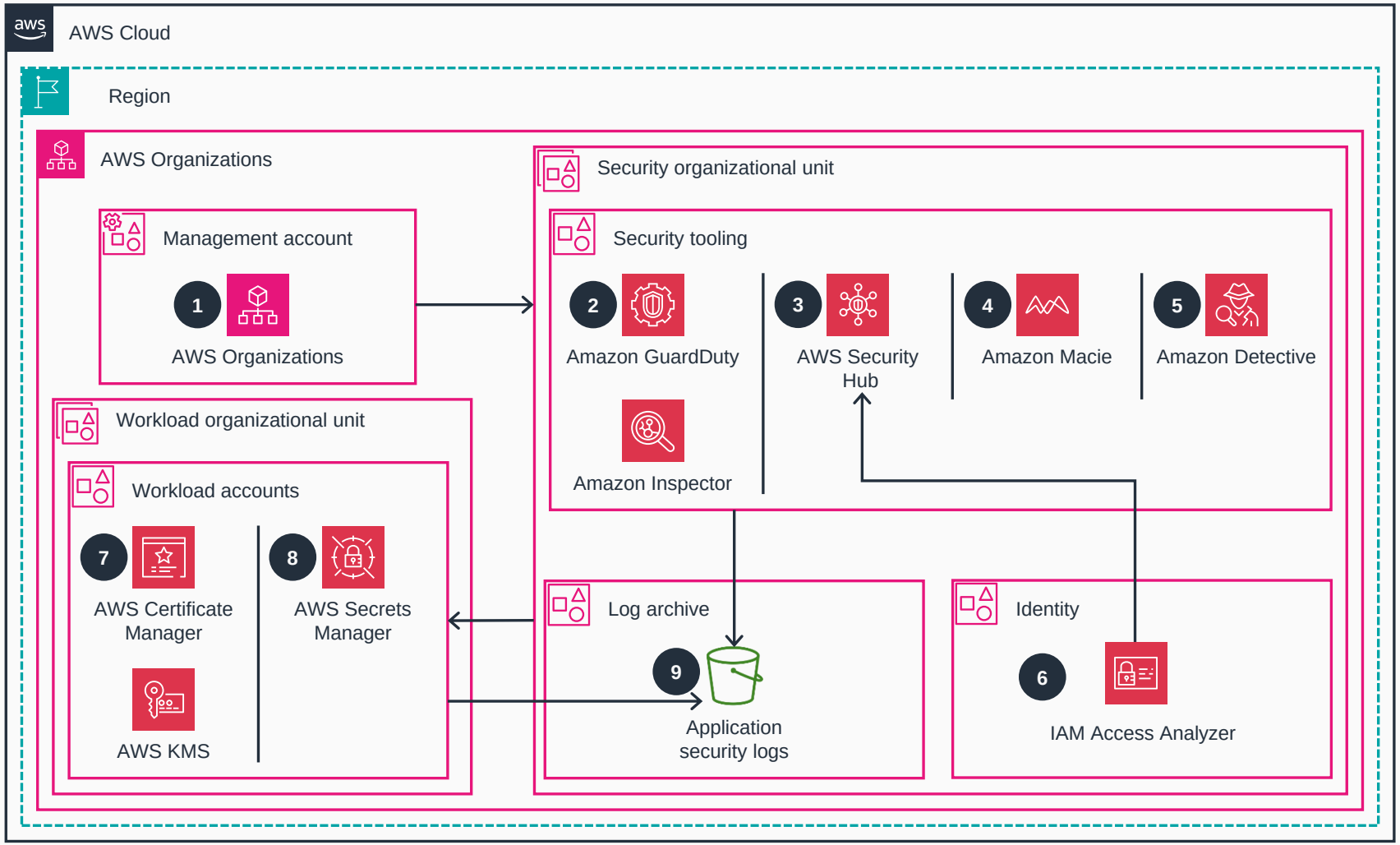
Guidance for Application Security on AWS

This architecture diagram shows how to integrate AWS security services to protect and manage your cloud resources and log application security as you build a reliable, secure, and scalable cloud environment.



1. Within **AWS Organizations**, enable **Amazon GuardDuty**, **Amazon Inspector**, **AWS Security Hub**, **Amazon Macie**, and **Amazon Detective** for your home and operational AWS Regions.
2. Set up **GuardDuty** for threat monitoring and **Amazon Inspector** for automated vulnerability scanning of **Amazon Elastic Compute Cloud (Amazon EC2)** instances, **Amazon Elastic Container Registry (Amazon ECR)** images, and **AWS Lambda** functions.
3. Configure **Security Hub** in your home and operational Regions to centralize security incidents within your AWS environment and maintain compliance with industry standards and best practices.
4. Enable and configure **Macie** in your home and operational Regions to identify sensitive data.
5. Enable and configure **Detective** in your home and operational Regions to streamline security analysis and conduct efficient security investigations.
6. Provide security teams with least privilege access to security services and the AWS environment using a federated solution. Review **AWS Identity and Access Management (IAM)** access using **IAM Access Analyzer**. Forward findings to **Security Hub.**
7. Use **AWS Certificate Manager** to provision and manage SSL or TLS certificates. Use **AWS Key Management Service (AWS KMS)** to manage keys associated with application resources.
8. Use **AWS Secrets Manager** to securely store and manage credentials such as database logins, API keys, and other secrets.
9. Send application security logs to a centralized log storage bucket for compliance retention and analysis.

Reviewed for technical accuracy July 10, 2024

AWS Reference Architecture