securiCAD for AWS supported services and threat library

This document describes supported AWS services and the types of threats and attacks that are simulated during the analysis.

Supported services

Below is a summary of supported AWS services and concepts.

IAM and KMS
Groups, Users, Roles, Policies, Permissions, Actions, Console Passwords, Access Keys, AWS Managed Keys, Customer Managed Keys

EC2 and VPC
EC2 Instances, Security Groups, Elastic IPs, Key Pairs, Network Interfaces and Load Balancers, VPCs, Subnets, Route Tables, Internet Gateways, NAT Gateways, Network ACLs, and Virtual Private Gateways

RDS, S3 and DynamoDB
DB Instances and Subnet Groups, S3 Buckets, S3 Objects, DynamoDB Tables

Lambda
Lambda Functions and Execution Roles

ECS and ECR
Clusters, Container Instances, Services, Tasks, Containers, Fargate, Network Interfaces and Listeners

Amazon Inspector

Threat library

Below is a summary of potential threats and attacks that an attacker can use to reach high value assets in the securiCAD for AWS simulations.

Initial access

The attacker will attempt to gain initial access to the AWS environment by:

- Attempting to find reachable applications, services, databases, instances and containers by analyzing routing, network access control lists, security groups and gateways
- Exploiting public facing applications, services, databases, instances and containers that are reachable from the internet
- Finding reachable applications, services and instances for request forgery attacks against the AWS meta data service
- Finding reachable applications, services and instances for client side attacks and forged responses
- Spearphishing attempts against access keys, console passwords and SSH keys
- Attempting to access public facing databases, tables and buckets

Privilege escalation

The attacker will attempt to elevate its privileges in the AWS environment by:

- Credential exfiltration via successful request forgery attacks on instances to gain access to instance profiles and attached IAM roles

- Credential exfiltration of ECR registry passwords via ECS container instances
- Cracking encrypted ECR registry passwords
- Credential exfiltration of compromised docker images and containers
- Using spearphished credentials to gain access to high privileged IAM users, roles and groups
- Tampering with the IAM configuration to give itself additional permissions or access to high privileged roles and groups
- Credential exfiltration by creating instances or invoking AWS services such as Lambda, EC2, ECS, CloudFormation, CodeStar and Glue and passing IAM roles to them
- Credential exfiltration by passing IAM roles to compromised instances and containers
- Creating new console passwords, access keys and login profiles

Lateral movement

The attacker will attempt to move in the AWS environment and gain additional access by:

- Attempting to find internally reachable applications, services, databases, instances and containers by analyzing routing, network access control lists, security groups and gateways
- Finding internally reachable applications, services and instances for request forgery attacks against the AWS meta data service
- Finding internally reachable applications, services and instances for client side attacks and forged responses
- Attempting to access internally accessible databases, tables and buckets

Vulnerabilities and code execution

The attacker will attempt to gain persisted access or code execution by:

- Updating code of existing, or creating new lambda functions to inject arbitrary malicious code
- Poisoning ECR repositories to push docker images with arbitrary malicious code
- Finding and exploiting known vulnerabilities in instances, containers, applications and services
- Finding and exploiting unknown vulnerabilities in instances, containers, applications, unknown applications and services

Denial of service and information disclosure

The attacker will attempt to disrupt normal operation or read sensitive data in the AWS environment by:

- Using access to IAM users, roles and groups to perform actions that stops, terminates or deletes running instances, lambda functions, containers, container services and tasks
- Using access to IAM users, roles and groups to perform actions that deletes or writes to buckets, databases and tables
- Using access to IAM users, roles and groups to perform actions that exfiltrates or reads data in buckets, databases and tables

- Pulling docker images from ECR that might contain sensitive data or credentials
- Using access to KMS to encrypt buckets and databases for denial of service or extortion
- Using access to KMS to decrypt and read data in encrypted buckets and databases