Mandiant

ASM AWS INTEGRATION CONSIDERATIONS

AWS information collected by MA-ASM

When you integrate Mandiant Advantage Attack Surface Management (MA-ASM) with your Amazon Web Services (AWS) account, the following information is accessed and collected:

- **Public EC2 instances:** Details about your publicly accessible EC2 instances.
- **S3 buckets:** MA-ASM checks if your S3 buckets are publicly accessible and creates Issues for any that are.
- **Route 53 zones:** Information about your Route 53 hosted zones and their associated resource record sets (such as DNS records).
- **RDS DB instances:** MA-ASM uses Mandiant Security Integrations-as-a-Service (MSI) to collect data about your Amazon Relational Database Service (RDS) instances.

These are the current MA-ASM AWS integrations, but any asset that is accessible through boto3, the AWS SDK for Python, can be acquired.

MA-ASM asset identification

MA-ASM identifies assets in your AWS account using boto3, the AWS SDK for Python. This SDK allows MA-ASM to interact with various AWS services and retrieve information about your resources.

For example, in the provided source code for the AWS RDS integration:

- `boto3.client("rds", ...)` establishes a connection to the AWS RDS service using your provided credentials.
- `self.aws_client.describe_db_instances(...)` makes API calls to retrieve detailed information about your RDS instances.

The response from these API calls contains data such as instance identifiers, names, endpoints, statuses, tags, and more. MA-ASM then maps this raw data into a standardized format using a `field_map` dictionary, making it easier to understand and analyze within the MA-ASM platform.

Additional entity types

While four asset types are explicitly referenced, note that the JSON policy you create in AWS during integration also includes permissions for:

- `s3:ListAllMyBuckets` : This allows MA-ASM to list all of your S3 buckets, not just the public ones.
- `ec2:DescribeInstances` : This allows MA-ASM to collect information about all of your EC2 instances, regardless of their public accessibility.

Therefore, MA-ASM is capable of collecting data on other AWS resources, beyond the ones explicitly referenced, depending on the specific configuration and permissions granted during integration. However, the primary focus of this integration is to collect only the four asset types listed.

The scope of data collection can vary based on your AWS account configuration and the permissions you grant to MA-ASM during the integration process. It's essential to review the policy and permissions carefully to ensure they align with your security and compliance requirements.

Additional considerations

- MA-ASM uses cross-account access and temporary tokens for secure authentication with your AWS account, minimizing the need for long-term access keys.
- Mandiant recommends using the AWS (Roles) integration method for enhanced security.

- Regularly review and update your integration settings to ensure they remain aligned with your evolving needs.