Mandiant

COLLECTIONS TIPS AND TRICKS

Collections within Mandiant Advantage Attack Surface Management (MA-ASM) define the scope, type of data, and discovery task workflows perform.

Access control can be configured at the Collection, Project, and Organization level in MA-ASM. If you have requirements around controlling access, make sure to take this into consideration when building out your Collection plan.

Collections, when set up strategically, can serve as a way to segment based on business unit, team, subsidiary, and so on.

We suggest that you familiarize yourself with these two documents before establishing Collections:

- **Creating & Seeding Collections** **(https://docs.mandiant.com/home/creating-seeding-collections)**
- **Understanding Attack Surface Management Seeds** **(https://docs.mandiant.com/home/asm-seeds)**

Here are some best practices to help you get the most out of MA-ASM Collections.

A sample build-out

- Organization: **Acme Corporation**
  - Project: **Acme Widgets**
    - Collection: **Acme Widgets - External Surface**
    - Collection: **Acme Widgets - Cloud Surface - AWS Accounts**
    - Collection: **Acme Widgets - Cloud Surface - GCP Accounts**
    - Collection: **Acme Widgets - Cloud Surface - Github Account**
  - Project: **Acme Offices**
    - Collection: **Acme Offices - External Surface**

General guidelines

- Only one organization per Collection
- Add Seeds for specific asset types or unique parts of your organization: IPs, top-level domains, netblocks
- 50 Collections or less per Project for maximum performance

Business Unit and Subsidiary Considerations

It's key to configure Collections in a way that makes this easy going forward. Think of Collections as a way to configure groupings of assets and findings together.

Building your first Collection

The key to setting a Collection up for success is accounting for the time and resources available for managing the attack surface. We recommend slowly and strategically building Collections within the module to ensure that your security team can manage the flow of data.

Seed and Scope Selection

MA-ASM uses Seeds to define the scope of asset discovery.

The following are the recommended Seed types to use when building your first Collection:

Seed Type	Quantity per Collection
Netblocks (IPv4 or IPv6)	500 IP Addresses per
Primary Domains	1-5
IP Addresses	500

Avoid using RFC 1918 addresses.

Using one or more of these recommended Seeds will produce a baseline view of external assets and security issues. Then you can have your security team assess the external asset, Entity, and inventory, and prioritize critical and high severity Issues.

Using Integrations

Inbound integrations (https://docs.mandiant.com/home/asm-inbound-integrations) reduce manual tasks to upload Seeds to Collections. As you onboard, start with a single integration to make data management easier on your security team.

Account Permissions
Where applicable, identify the cloud or DNS administrators before configuring the integration.

Creating an individual Collection per integration will enable cleaner data segmentation later on.

The following inbound integrations are available for integration with MA-ASM:

- **Akamai** (https://docs.mandiant.com/home/asm-akamai-integration): Retrieve DNS zones
- **AWS** (https://docs.mandiant.com/home/asm-aws-integration): Retrieve EC2 instances, S3 buckets, route 53 zones, and RDS
- **Azure** (https://docs.mandiant.com/home/asm-azure-integration): Retrieve virtual machine instances, storage accounts (blobs), and public DNS zones
- **Cloudflare** (https://docs.mandiant.com/home/asm-cloudflare-integration): Retrieve DNS zones
- **GitHub** (https://docs.mandiant.com/home/asm-github-integration): Retrieve Organization and Account information
- **GoDaddy** (https://docs.mandiant.com/home/asm-godaddy-integration): Retrieve DNS zones
- **Google Cloud** (https://docs.mandiant.com/home/asm-gcp-integration): Retrieve APIs via API Gateway, applications, cloud functions, cloud SQL instances, compute, storage, and DNS

Once integrations have been established in MA-ASM, they must be linked to a relevant Collection.