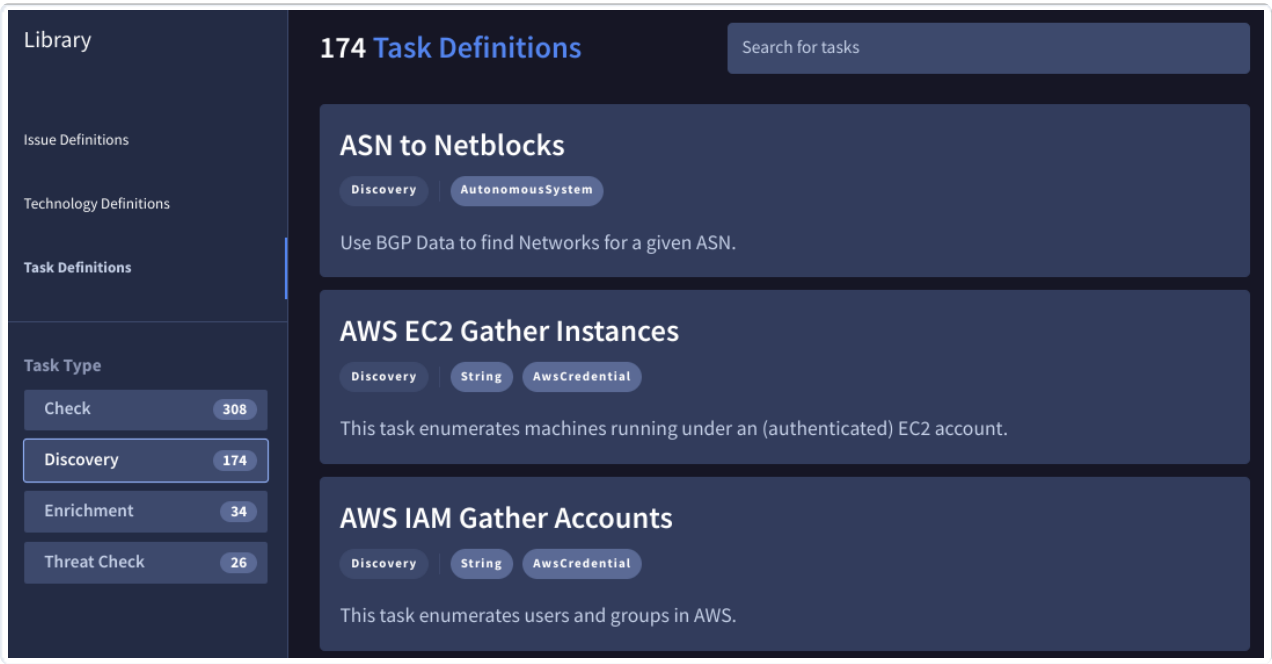
TASK LIBRARY

In Mandiant Advantage Attack Surface Management (MA-ASM), tasks are associated with Entities and vary depending on the Entity and what type of security issues MA-ASM is attempting to detect. When a task is run and results are found, MA-ASM will create an Issue that includes a calibrated priority and a corrective measure. In an MA-ASM workflow, tasks are associated with the Task Library.

Access Task Definitions in the MA-ASM Library

1. From the MA-ASM **Projects and Settings** menu, select **Library**.
2. Select **Task Definitions**.
3. Optional: To filter the list, select a **Task Type** and **Search**.



You see different task types along with definitions counts for each category. For each individual task, you see a title, task type, Entity types associated with the task, and a short description.

Task Types

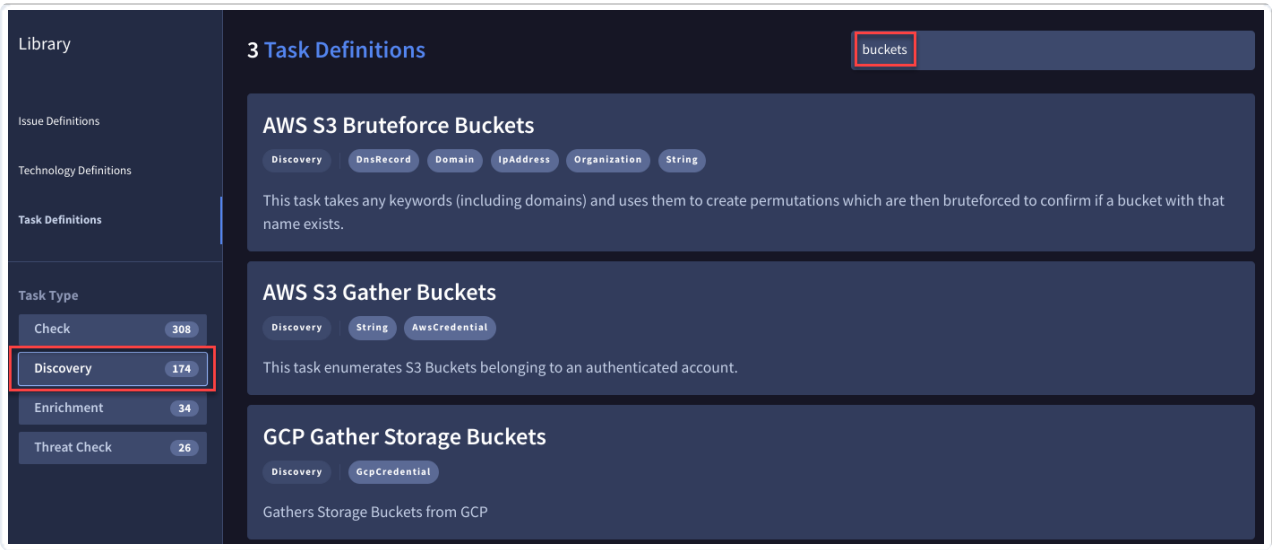
- **Check:** This task category provides additional checks for vulnerability detections, based on the Entity types in your environment.
  - Examples include:
    - **Accellion compromised secure file transfer appliance**
    - **Adminer - Server-Side Request Forgery (CVE-2021-21311)**
    - **Adobe Coldfusion Arbitrary Code Execution (CVE-2018-15961)**
- **Discovery:** This task category identifies Entities which are vulnerable or potential targets of compromise on your attack surface.
  - Examples include:
    - **ASN to Netblocks**
    - **AWS EC2 Gather Instances**
    - **AWS IAM Gather Accounts**

- **Enrichment:** This task category provides more contextual information for newly discovered Entities.
  - Examples include:
    - **AWS S3 Bruteforce Objects**
    - **Enrich ApiEndpoint**
    - **Enrich AwsEC2Instance**

- **Threat Check:** This task category reviews the known indicators of potential compromise associated with your organization.
  - Examples include:
    - **C2 Server Detection Through JARM hash**
    - **Search Alienvault OTX**
    - **Search Alienvault OTX (Hash)**

Task Definition Search

You can search for specific task definitions for each Task Type. For example, for the **Discovery** Task Type, when you search for ***buckets***, three task definitions are returned: **AWS S3 Bruteforce Buckets**, **AWS S3 Gather Buckets**, and **GCP Gather Storage Buckets**. For each of these tasks, you see a definition.



For additional details on MA-ASM tasks, use the API. See **Attack Surface Management API (https://docs.mandiant.com/home/asm-api)** for more information.