ASM GOOGLE SECOPS SIEM INTEGRATION

Google Security Operations (SecOps) SIEM (Security Information and Event Management) **(https://cloud.google.com/security-information-event-management)** provides threat detection and investigation with integrated threat intelligence. This integration allows Google SecOps to ingest data from Mandiant Advantage Attack Surface Management (MA-ASM). Specifically:

- **Entities** **(https://docs.mandiant.com/home/asm-entities)** discovered by MA-ASM are ingested as entity objects.
- **Issues** **(https://docs.mandiant.com/home/asm-issues)** detected by MA-ASM are ingested as events.

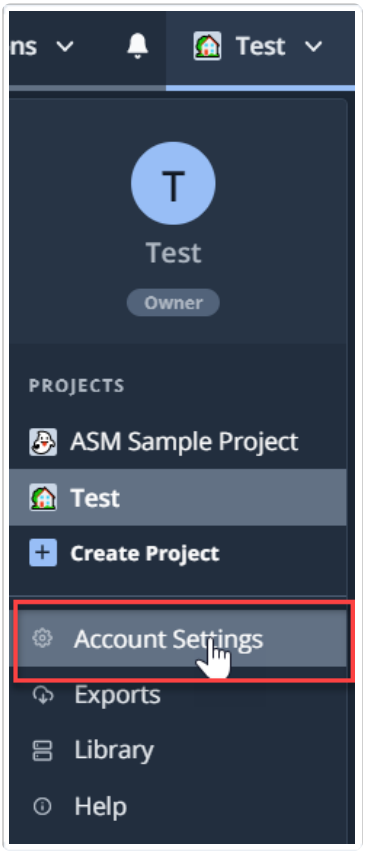
An MA-ASM Issue represents a detected vulnerability or potential cyber security weakness in a customer's infrastructure. Surfacing this information in Google SecOps SIEM provides greater visibility and awareness to the customer.

Configure the Google SecOps SIEM integration

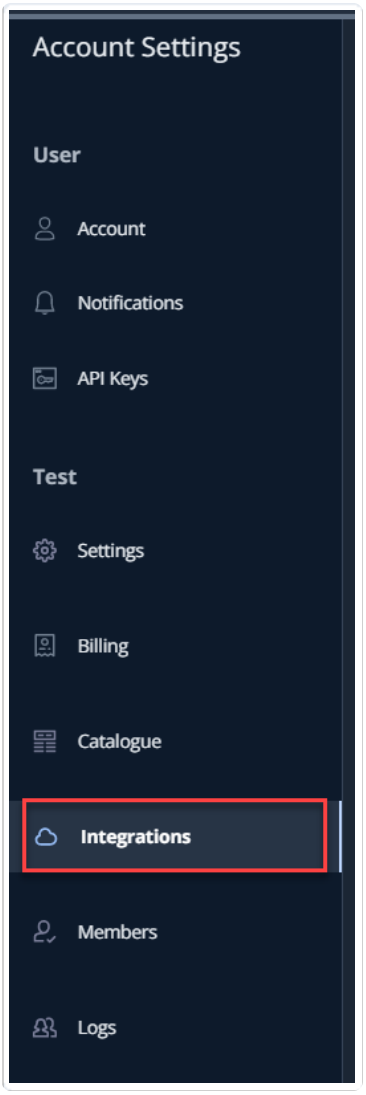
> This integration only runs when a Collection Scan finishes. For example, if this integration is added on Monday, but the next applicable Collection Scan is scheduled for Tuesday, the integration runs on Tuesday when the Scan finishes.

1. From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click **Account Settings**.

   > This integration is applied to the selected Project and all Collections that Project contains.

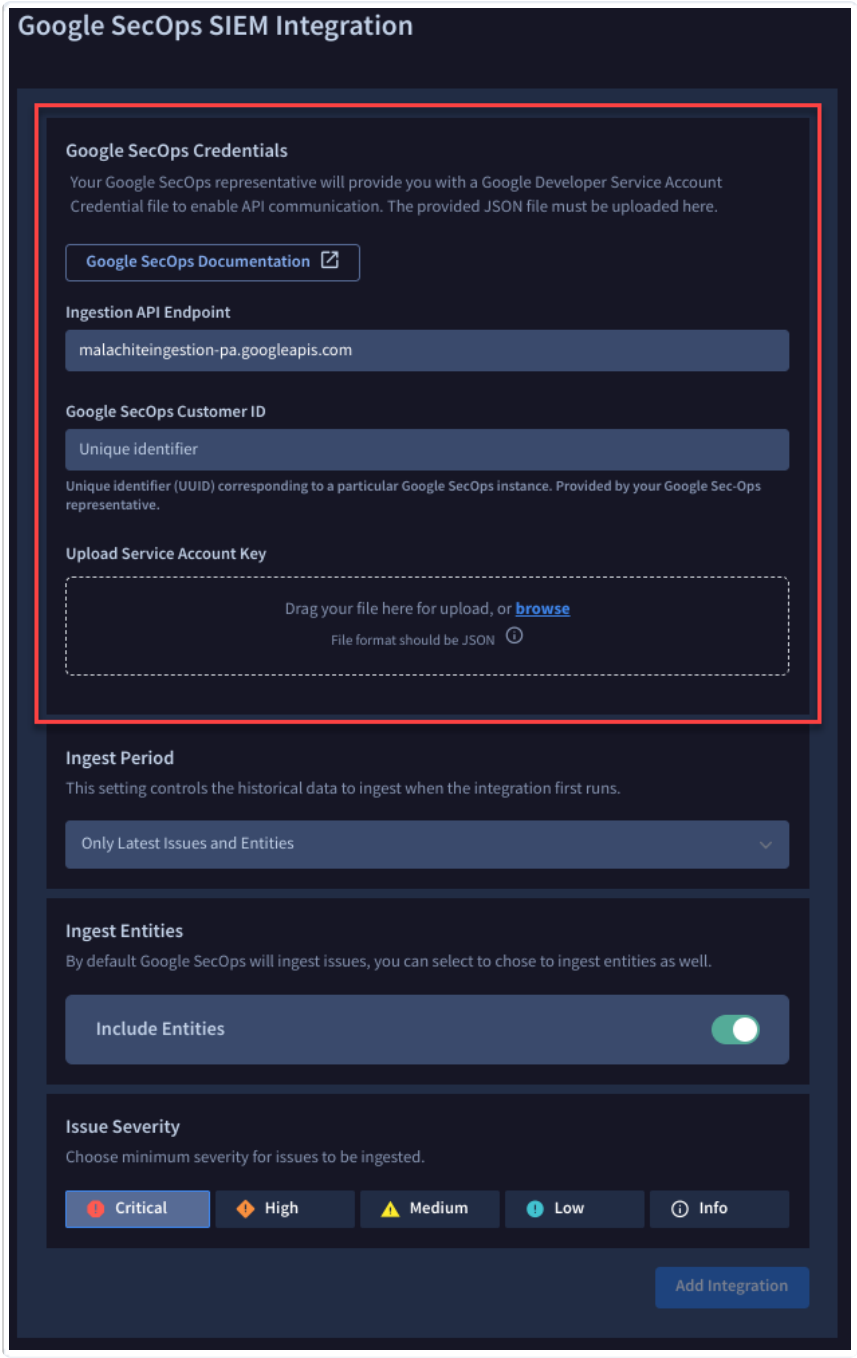


2. Click the **Integrations** tab.

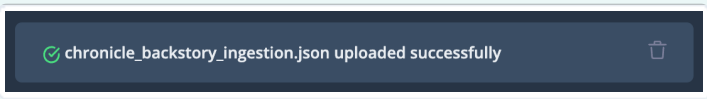


3. Go to **Outbound Integrations** and click **Add New** next to **Google SecOps SIEM**.

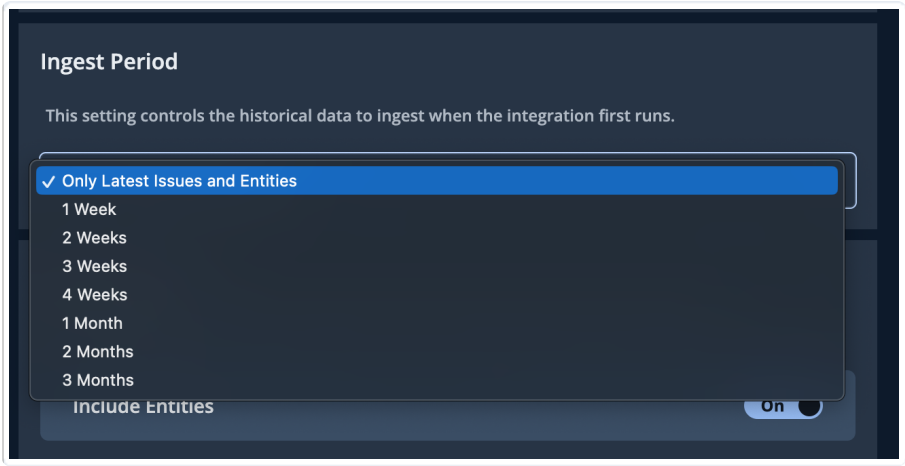
4. In the **Google SecOps Credentials** section:
    a. Update your **Ingestion API Endpoint**, if necessary. This defaults to `malachiteingestion-pa.googleapis.com`.
    b. Enter your **Google SecOps Customer ID**.
    c. **Upload Service Account Key**. This is a JSON file that has been provided to you by your Google SecOps representative.



Once the JSON file uploads successfully, you are notified.

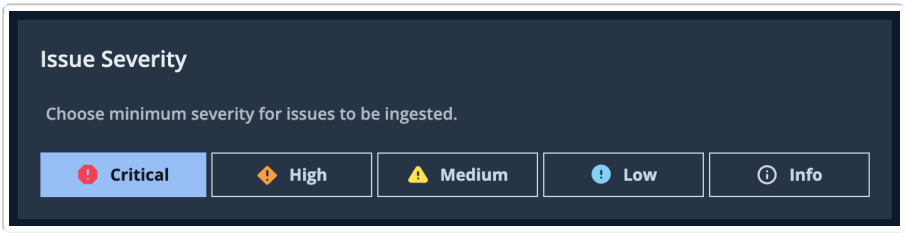


5. Select an **Ingest Period** from the drop-down.



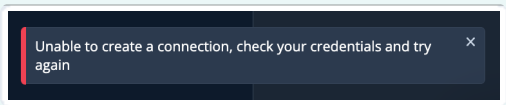
6. Select the minimum **Issue Severity** for Issues to be ingested into Google SecOps.

   - For example, if you select **Info**, all Issue Severities are selected meaning that issues of any severity are ingested.
   - If no **Issue Severity** is selected, only Critical Issues are ingested as this is the default.



7. Click **Add Integration** to create the integration.

   When the wrong credentials are entered, the integration fails to connect.



Find MA-ASM Issues using UDM search

Once MA-ASM Issues are ingested into Google SecOps, you can find them using the following UDM query in the Google SecOps UDM Search console: `metadata.product_name = "Mandiant Attack Surface Management"`