RELIAQUEST

Securonix Unified Defense SIEM Integration Guide

Securonix Unified Defense SIEM is a cloud-native security platform that combines log management, user and entity behavior analytics (UEBA), and security incident response into a single, cohesive solution. It collects and analyzes massive volumes of data in real-time, using patented machine learning algorithms to detect advanced threats and automate response actions.

Deployment Type

This integration supports **on-premises**, **private cloud**, and **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please check your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Securonix, collect the following details:

- URL
- Username
- Password

See instructions below to gather the required information.

Create a User

1. In Securonix, click **Access Control**.
2. Select **Manage Users**.
3. Click **Add New User**.
4. Enter the **User Authentication Type as Service API** with the following permissions:
    - ROLE_RBAC_API_ACCESS
    - ROLE_SERVICE_ACCOUNT

See Securonix Documentation.

Configure Intel Push Templates

1. Within the Securonix Menu, click **Add Data**.
2. Select **Lookup Data**.
3. Click **New Connection**.
4. For Connection Type, choose Database, File Import, Splunk, AWS S3 using SQS, or another.
5. Create a new lookup table (add unique name if desired).
6. Select **User** or **System** for Lookup Table Type, depending on your needs. (See Configuration Connection documentation)
7. Follow the Securonix documentation based on the Connection Type:
    - Database
    - File Import
    - Splunk
    - AWS S3 using SQS

8. Complete the following information in the Connection Details section:
    - **Restrict Access to this lookup table to your user group**: Disable to allow all users to access this lookup table if desired.
    - **Parsing Technique**: Technique to parse the data.
    - **(Optional)** Delete Old Lookup Data: Select one of the settings
        - **YES:** Allows you to remove previous data from the lookup table.
        - **NO**: Does not allow previous data removal.
    - **Delimiter:** Used in file. Example, comma and pipe.
    - **Exclude Header:** Ignore the header row.
    - **Number of Lines to ignore:** Number of header lines to ignore.
9. Complete the following information in the Connection Properties section:
    - **Select Access Type**: Access type for AWS S3.
    - **SQS Queue URL**: URL to access the SQS Queue.
    - **SQS Access Key**
    - **SQS Secret Key**: Secret key associated with the SQS access key.
    - **S3 Region**: Region where SQS is located.
    - **S3 Access Key**
    - **S3 Secret Key**
    - **S3 Region**
10. Click **Save And Next**

Third party intel is not available through the APIs and required manual setup, which can be done through webhooks, file upload, threat systems, etc. See Securonix documentation.

Permissions and Functionality

Permissions

GreyMatter Capability	Required Permission
Investigate / Hunt	ROLE_RBAC_API_ACCESS ROLE_SERVICE_ACCOUNT
Asset Inventory	ROLE_RBAC_API_ACCESS ROLE_SERVICE_ACCOUNT
Detect	ROLE_RBAC_API_ACCESS ROLE_SERVICE_ACCOUNT

Investigate/Hunt

Activity within Investigate, also known as "event data", are security logs collected from a variety of structured and unstructured data sources.

Spotter search used for this functionality can support other sources for querying, which require enabling additional sources in the GreyMatter settings:

- Name of the table needs to match the name of the index which will be used in the API.
- Example: index = archive
- Corresponding field mappings will have to be added for each additional source.

Detect

Securonix supports **Detection at Source.**

Note Syncing and **State Syncing** are supported for **Vendor-Authored detections.**
Vendor-Authored detections retrieve incident records generated from out of the box detection rules/policies and any custom rules/policies.
ReliaQuest-Authored detections query activity index (or any other custom index) to apply GreyMatter Query Language rule logic to identify detection events. Data lookups used in ReliaQuest rule logic have to be manually configured to be imported into Securonix.

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.