Introduction

As a recognized leader in both Identity Lifecycle Management and Identity Access Management Software and Services, Non-Employee Risk Management provides the most comprehensive solutions to addressing employee and non-employee identity lifecycle. With products like Lifecycle and Collaboration built to fill the gaps in Identity Governance & Administration (IGA) products' identity lifecycle capabilities, Non-Employee Risk Management provides software to gain full visibility of global identities and true management and control of non-employee lifecycle and risk.

You can find documentation for administrators of your non-employee system in our Admin Help section.

The SailPoint Non-Employee Risk Management AuditEvent Add-on is an open source Splunk add-on built using the Splunk Add-on builder. This add-on helps ingest, parse and normalize data from Non-Employee Risk Management API into Splunk allowing users to easily search and analyze their data. It leverages Splunk's data onboarding framework providing a seamless experience for integrating data into Splunk Enterprise and Splunk Cloud. The SailPoint Non-Employee Risk Management API is a RESTful API designed to manage and automate identity governance processes for non-employee identities within SailPoint platform. Non-Employee Risk Management is an add-on to Identity Security Cloud (ISC) that helps organizations track non-employees such as contractors, partners, and vendors, and their lifecycles within the organization.

For more information about the /search API used by the add-on, see https://developer.sailpoint.com/docs/api/nerm/v1/search/.

Key Features

1. Data Ingestion
   - Retrieves audit events data from SailPoint Non-Employee Risk Management API
   - Supports periodic polling with configurable intervals.

2. Data Normalization
   - Ensures consistent mapping for seamless integration with Splunk's Common Information Model (CIM).

3. Compatibility
   - Works with both Splunk Enterprise and Splunk Cloud.
   - Supports JSON, XML, and other structured formats returned by the SailPoint API.

4. Security and Compliance
   - Encrypts API credentials stored in Splunk's credential store.
   - Secures data transfer via HTTPS.

5. Customizability
   - Built-in flexibility for additional API endpoints or data sources.
   - Extensible field mappings and parsing logic using the Add-On Builder.

Lifecycle

Lifecycle is a powerful solution that allows an organization to easily manage business processes for third party identities, their relationships with your organizations and the risk associated with those relationships. With Lifecycle, users can:

- Quickly onboard third-party resources and other identity types
- Administer a single repository for all third-party identities and other identity types
- Create relationships across identities while making those relationships actionable through forms and workflows
- Easily configure the user interface and process workflows through an administrative UI
- Manage identity risk

Lifecycle is designed to provide your internal administrators, identity managers and owners the ability to manage third party identities.

Architecture Overview

1. Data Flow
   - The add-on fetches data from SailPoint's Non-Employee Risk Management API using RESTful calls.
   - Ingested data is indexed into Splunk, enabling its use in dashboards, searches, and alerts.

2. Components

- Inputs: Preconfigured REST API inputs to poll data from SailPoint.
- Modular Scripts: Python scripts created using Splunk Add-On Builder for data collection and parsing.
- Data Parsing: Transforms raw API responses into a structured format ready for indexing.
- Field Extraction: Uses knowledge objects for mapping fields to Splunk CIM for easy correlation with other datasets.

Splunk Enterprise/Splunk Cloud:

An event is a single piece of data in Splunk software, like a record in a log file or other data input. When data is indexed, it is divided into individual events. Each event is given a timestamp, host, source, and source type. Often, a single event corresponds to a single line in your inputs, but some inputs (for example, XML logs) have multi-line events, and some inputs have multiple events on a single line. When you run a successful search, you get back events. Similar events can be categorized together with event types.

Source Type

Source type is a default field that identifies the data structure of an event. A source type determines how Splunk Enterprise formats the data during the indexing process. Splunk Enterprise comes with a large set of predefined source types, and it assigns a source type to your data. You can override this assignment by assigning an existing source type or creating a custom source type. This add-on creates a custom source type 'sailpoint_non_employee_risk_management'. The Splunk indexer identifies and adds the source type field when it indexes the data. As a result, each indexed event has a source type field. A Splunk admin can use the source type field in searches to find all data of a certain type (as opposed to all data from a certain source).

Data Input

A Splunk deployment typically has three processing tiers: data input, indexing, and search management. A specific input consumes a raw data stream from its source and annotates each block with some additional metadata (host, source, and source type). Splunk does not look at the contents of the data stream at this point, so the metadata is consistent across all data in a single stream. After raw stream input, the next thing that occurs is the data is parsed into individual events. This add-on creates the events as part of the included scripts. Single data-input exists for the given sourcetype with the ability for the data input to specify execution interval. Recommended data input interval is 300 seconds (5 minutes).

Installation

Method 1: Install via Splunk Enterprise

- Log in to your Splunk instance
- Navigate to **Apps> Manage Apps**
- Click on **Install app from file**
- Upload the.tar.gz file from /build directory
- Click **Upload** and restart Splunk if prompted
- Find **SailPoint Non-Employee Risk Management AuditEvent Add-on** from the list and click Launch App

Method 2: Install on Splunk Cloud

- Navigate to **Splunk Cloud Admin Console > App > Browse More Apps**
- Search for the add-on and click **Install**
- Submit a request to Splunk support to get app cloud certified for installation

Configuration

Step 1: Configure Data Inputs

- Navigate to **Configuration** tab
- Go to **Add-on Settings**. Fill in the details and click **'Save'**

  - **Tenant URL**: Enter url of Non-Employee Risk Management tenant.
  - **API Key**: Enter SailPoint Non-Employee Risk Management API Key.

- Navigate to **Inputs** tab and click on **'Create New Input'**
- Fill in the required details and click **'Add'**

  Name: Enter unique name for the data input.
  Interval: Enter execution interval. Recommendation is 300 seconds (5 minutes).
  Index: Enter unique index.
  Tenant Name: Enter name of Non-Employee Risk Management tenant.

Compatibility

- Splunk Enterprise: Version 9.x and above
- Splunk Cloud: Supported (requires app-vetting)
- Add-on builder version: 4.x

Use Cases

1. Identity Governance Monitoring
   - Track identities and their roles across the organization.
   - Identify orphaned accounts, inactive users, or access policy violations.

2. Risk and Compliance
   - Monitor non-employee access to critical resources.
   - Ensure compliance with regulations by auditing entitlements and role assignments.

3. Access Insights and Reporting
   - Visualize identity and role-related data with Splunk dashboards.
   - Correlate SailPoint data with other security tools for comprehensive incident analysis.

Performance Considerations

- **Data Volume**: Adjust polling intervals to balance data ingestion rates and API limitations.
- **API Rate Limits**: Ensure API calls remain within the allowable limits to avoid throttling.
- **Indexing Efficiency:** Use filters to minimize unnecessary data collection and optimize storage.

Security Considerations

1. Authentication
   - Supports API Key and OAuth for secure access to SailPoint's API.

2. Encryption
   - Credentials are securely stored in Splunk's credential vault.
   - Communication between Splunk and SailPoint is encrypted using HTTPS.

3. Access Controls
   - Restrict access to sensitive dashboards and reports within Splunk.

Limitations

- Real-time streaming of data is not supported; only periodic polling is available.
- Requires additional customization for non-standard SailPoint API endpoints.
- Large-scale deployments may require performance tuning and optimized indexing strategies.

Conclusion

The SailPoint Non-Employee Risk Management AuditEvent Splunk Add-On simplifies the process of integrating identity governance data into Splunk. By leveraging Splunk's powerful analytics and visualization capabilities, organizations can gain actionable insights into their identity management processes, strengthen compliance efforts, and improve security posture.

This add-on is a valuable tool for organizations seeking to enhance their operational intelligence and streamline identity risk management.