NETAPP CLOUD INSIGHTS CLOUD SECURE

& Splunk API Integration Guide, v1.4

January 2021

Abstract

This document provides the information needed to perform a REST API integration between NetApp Cloud Insights - Cloud Secure and Splunk

Steve Chesney, PhD(c), Cloud Sales Representative
Amit Schwartz, MBA, Sr. Product Manager

chesney@neapp.com, amit.schwartz@netapp.com

Table of Contents

Table of Figures

Introduction

Hybrid-cloud Infrastructures are the most common cloud deployment model used by organizations, today [1]. In fact, many organizations utilize the hybrid-multicloud deployment model, as reported by Gartner in 2018 [2]. Although these infrastructures offer the best innovations of cloud technologies, they also introduce increased complexity into Information Technology (IT) environments. Much of this innovation has been enabled by RESTful API's (application programming interface), which are the cornerstone of software-defined data centers. RESTful API's reach beyond the barriers of physical devices and software platforms and enable the sharing of data. When data is shared in this manner, information silos are eliminated, and automation increases. Data sharing is essential to hybrid-infrastructure management and monitoring, as there are many tools available to users to provide visibility and operational control to their environments. NetApp Cloud Insights and Splunk are two leading tools, although they are from different genres – hybrid-infrastructure monitoring and SIEM (security information and event management), respectively.

NetApp's Cloud Insights helps users mitigate the complexities of hybrid-cloud deployments, as single-vendor, device-level tools have become obsolete. Cloud Insights provides centralized hybrid IT infrastructure monitoring, IT cost control and infrastructure optimization, and the means to reduce exposure to insider threats, malware and ransomware attacks through its Cloud Secure module. When security alerts from Cloud Secure are shared with Splunk, users are able to leverage the capabilities of both solutions to protect their environments.

NetApp Cloud Insights & Secure

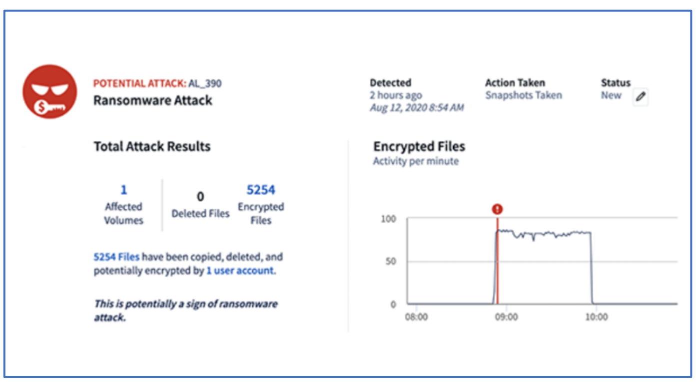

Figure 1 Cloud Secure Ransomeware Detection

Cloud Insights is a SaaS infrastructure and service monitoring solution that works for on-premises, private cloud and public cloud environments including AWS, Azure and Google Cloud. Cloud Secure, a feature of NetApp Cloud Insights, analyzes data access patterns to identify risks from ransomware attacks [3]. Cloud Secure helps users to detect and stop ransomware attacks, protect intellectual property from theft by malicious users, and ensure compliance of digital assets by auditing access patterns to critical data [3]. Cloud Secure automatically learns user behavior patterns and alerts when anomalies occur, without the need to configure thresholds or to define complex patterns [3]. Moreover, with Cloud Secure, users can automatically detect and classify different attack and threat patterns, and trigger alerts and automated response policies [3]. These alerts can be shared with Splunk through the Cloud Secure REST API.

The Cloud Secure REST API

The Cloud Secure API enables NetApp customers and independent software vendors (ISVs) to integrate Cloud Secure with other applications, such as ticketing systems and SIEM tools (Splunk). The Cloud Secure API, is documented via Swagger and can be found by clicking Cloud Secure

The requirements for Cloud Secure's API Access are below:

- An API Access Token model is used to grant access.
- API Token management is performed by Cloud Secure users with the Administrator role.

This REST API Token management and documentation can be accessed from the Cloud Insights by taking the following steps:

1. Click the Cloud Secure link from the Cloud Insights navigation panel (on the left side of the web browser window).
2. Click Admin in the Cloud Secure window navigate panel.
3. Click API Access to Cloud Secure. From this page you can generate and manage the API Access Tokens.
4. To access the REST API documentation, Click the API Documentation link on the top-right corner of the page.

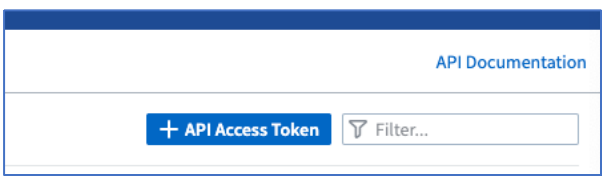

Figure 2 Cloud Secure API Documentation Link

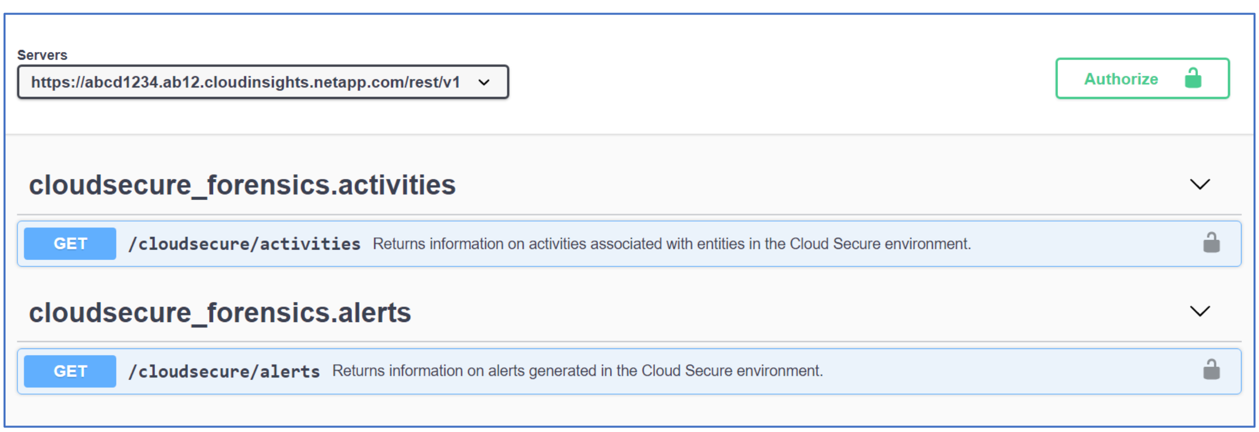

Figure 3 Cloud Secure REST API (Swagger)

Splunk

Splunk, a NetApp partner [4] helps users solve the machine data challenge and collects, indexes and harnesses an organization's unstructured, time-series machine data - physical, virtual and cloud. Splunk can read data from any source, such as network traffic, web servers, custom applications, application servers, hypervisors, GPS systems, stock market feeds, social media, and preexisting structured databases.

Splunk delivers a real-time understanding of what's happening and deep analysis of what's happened across a user's IT systems and infrastructure, turning machine data into insights for informed decision-making [4]. These capabilities help organizations to manage, secure and gain operational intelligence from IT infrastructures, by enabling organizations to search and analyze their machine data from a single location in real time, troubleshoot application outages, investigate security incidents, and gain new levels of insight [4]. When the capabilities of Cloud Secure and Splunk are combined, users have enhanced and holistic IT security protection.

The Splunk Add-on Builder - REST API Modular Input

The Splunk REST API Modular Input captures polling data from disparate REST APIs and indexing the responses. This feature is enabled through the Splunk Add-on Builder. The module can be obtained from Splunkbase (https://splunkbase.splunk.com), once a user has a registered account [5]. This module provides several input parameters for communicating with third-party API's, such as the REST API target URL, REST Request Headers, Event Extraction Settings, Checkpoint Settings and other parameters. Details for configuring the Splunk REST API Modular Input with Cloud Secure have been provided later in this document. Once the Splunk REST API Modular Input has been installed within Splunk, a desired logo can be imported for ease recognition. Figure 5 shows how the Cloud Secure logo has been imported into this module.

Features [6]:

- Perform HTTP(s) GET/POST/PUT/HEAD requests to REST endpoints and output the responses to Splunk
- Multiple authentication mechanisms
- Add custom HTTP(s) Header properties
- Add custom URL arguments
- HTTP(s) Streaming Requests
- HTTP(s) Proxy support, supports HTTP CONNECT Verb
- Response regex patterns to filter out responses
- Configurable polling interval
- Configurable timeouts

- Configurable indexing of error codes
- Persist and retrieve cookies

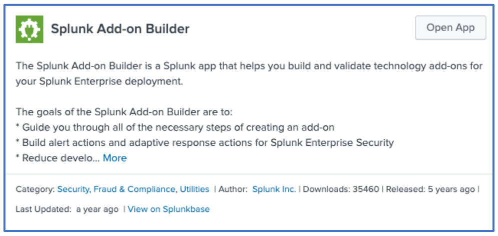

Figure 4 The Splunk Add-on Builder - REST API Module

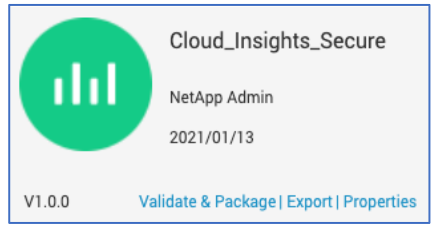

Figure 5 Cloud Secure Logo Example in the Splunk REST API Module

Cloud Secure and Splunk REST Integration Steps

The steps below detail what is required to integrate Splunk with Cloud Secure via the Cloud Secure REST API. These integration steps are based the latest SaaS-based release of Cloud Secure, as of January 2021 and Splunk, version Splunk Version 8.1.0, build f57c09e87251.

Cloud Secure Setup Prerequisites

1. **Create a Cloud Secure REST API token**
   1.1. From the Cloud Insights Navigation pane, click Cloud Secure -> Admin -> API Access to Cloud Secure
   1.2. Click the "+ API Access Token" button at the top-right areas of the window
   1.3. Provide a name for the token
   1.4. Select the desired expiration length of the token
   1.5. Once the token is created copy the token and store in a secure location for future use. Note: Your token will only be available for copying to the clipboard and saving during the creation process. Tokens cannot be retrieved after they are created.
   1.6. Click the Save button

Note: Refer to the Cloud Secure API online documentation for details: https://docs.netapp.com/us-en/cloudinsights/concept_cs_api.html#api-documentation-swagger

Splunk Setup Prerequisites

2. **Install the Splunk Add-on Builder** [5]
   2.1. Within Splunk, click the "+ Find More Apps" link in the navigation pane, on the right side of the main Splunk window.
   2.2. Search for "Splunk Add-on Builder
   2.3. Click Install.

2.4. Login to Splunk with your Splunk account credentials.
2.5. Click the “Restart Now” button, once the download and installation are completed. This will restart the Splunk server.
2.6. Once the Splunk server has restarted, log back into the Splunk instance and click the “splunk>enterprise” logo in the top left corner of the window.
2.7. Verify that the “Splunk Add-on Builder” icon is visible under that Apps section of the navigation pane.

Create the Integration

Note: See the Splunk Add-on Builder User Guide: Configure data collection using a REST API call in the Reference section of this document [6].

3. Click the “Splunk Add-on Builder” icon

3.1. Click the “New Add-on” button
3.2. Enter a name for the App
3.3. Fill out the other fields as desired and upload an icon/logo if desired.
3.4. Click Configure Data Collection, then New Input
3.5. Click the REST API icon
3.6. Enter a Source Type Name, i.e. “netapp:cloud_secure:alerts”
3.7. Enter the Input Display Name (“cloud_secure_alerts”), the Input Name (“cloud_secure_alerts”) and a Description
3.8. Enter the “Collection Interval”, i.e. 60 seconds. Collection interval should be greater than 30 seconds and less than 2 hours (7,200 seconds).
3.9. Click Next and continue to Step 4.

4. Create Data Input (See Figures 6 and 7 below)

4.1. Enter the REST URL in the Splunk REST Settings form.
4.1.1. To obtain this URL from Cloud Secure, click Admin, API Documentation
4.1.2. Under the “cloudsecure_forensics.alerts” section, click “Get”
4.1.3. Click “Try it out”, then click the blue “Execute” bar.
4.1.4. Copy the URL output from the “Request URL” section and place it in the Splunk REST URL section, e.g., https://accd1234.ab12.cloudinsights.netapp.com/rest/v1/cloudsecure/alerts (See Figure 6 below; copy everything up to the “?”)
4.2. Enter the URL Parameters in Splunk
4.2.1. Click “New Parameter”, and enter Name: “limit”, Value: “10”
4.2.2. Click “New Parameter”, and enter Name: “timeRange”, Value: “THREE_HOURS”
4.2.3. Click “New Parameter”, and enter Name: “sort”, Value: “alertTimestamp”
4.3. Enter the Cloud Secure REST API Header and Token into Splunk’s REST Request Headers section.
4.3.1. The header is “X-CloudInsights-ApiKey”
4.3.2. The token is the string of characters that was copied in the Cloud Secure Setup Prerequisites Section, Step 1.

5. **Event Extraction Settings** – Enter “$.results[*]” in the JSON Path field

6. **Checkpoint Settings** (See Figure 8)
   6.1. Enable checkpointing: Click the checkbox
   6.2. Checkpoint parameter name: “alerttimestamp”
   6.3. Checkpoint field path: “$.results..alertTimestamp”
   6.4. Checkpoint initial value: Enter the value from the “alertTimestamp” field from the Cloud Secure Response Body output (See Figure 9).
   6.5. Response timestamp format: “%s”
   6.6. Request timestamp format: “%s”

7. **Click Test** (in Splunk)

   Note, if Cloud Secure did not generate any alerts in the past three hours, an error log would appear in the Splunk output panel. For testing, you can change the 'timeRange' parameter value to "ONE_WEEK". Don't forget to change it back to "THREE_HOURS".

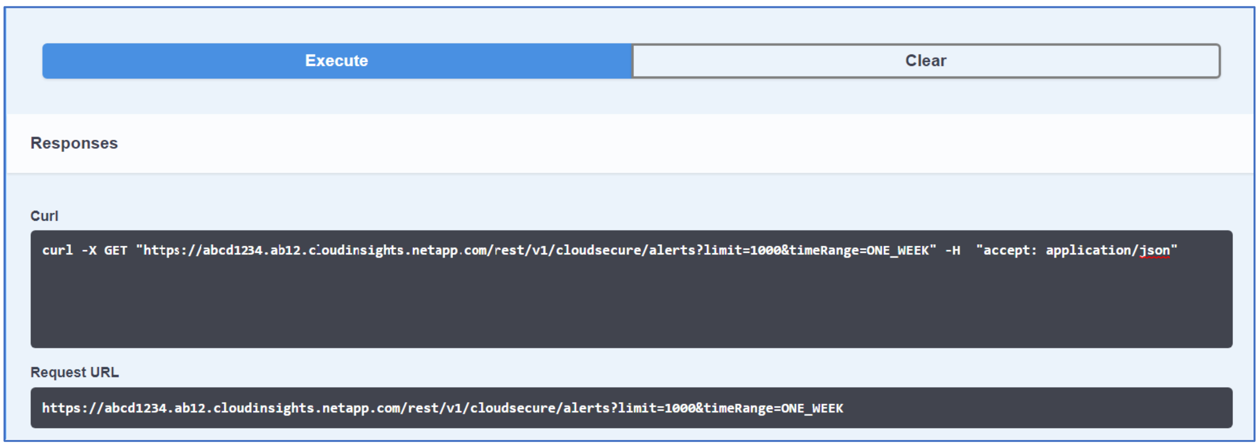

Figure 6 Cloud Secure Request URL

Figure 7 Splunk Define the Data Input Section

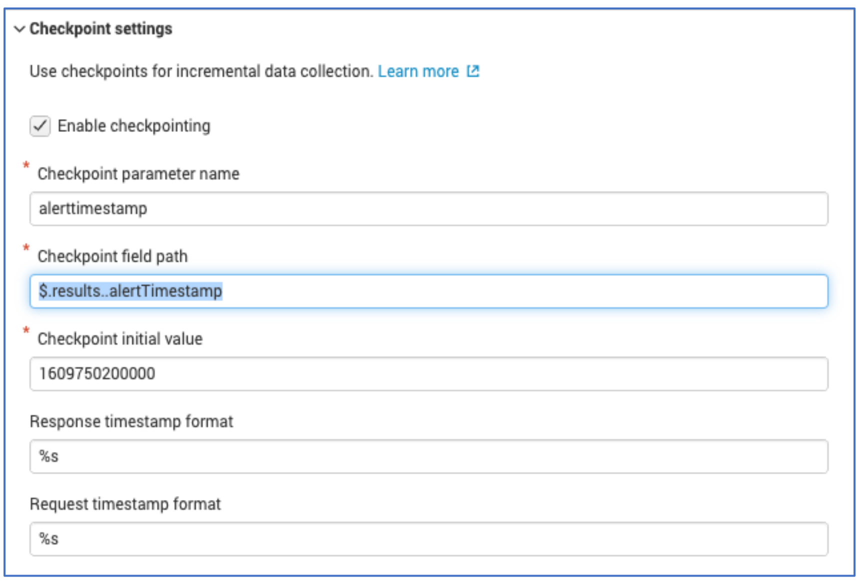

Figure 8 Splunk Checkpoint Settings

Response body


```
{
  "count": 9,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "actions": [],
      "alertTimestamp": 1610558340000,
      "alertType": "User Activity Rate",
      "attributes": {
        "changePercentage": "690.68"
      },
      "id": "eb2a7524-1715-4106-9216-93d5fb1d7cc6",
      "note": "",
      "severity": "warning",
      "status": "New",
      "userDisplayName": "Cade Cervantes",
      "userId": "BD98761637E3A3CD35A8ABA11E06C5C68B075A99BD3E2AB913CB5F50442BD043"
    },
    {
      "actions": [
        {
          "actionType": "create_snapshot",
          "lastActionDetails": {
            "mode": "Automatic",
            "status": "Success",
            "timestamp": 1610526702368
          }
```


Figure 9 Cloud Secure Response Body

Examine Cloud Secure Data in Splunk

Once the Splunk REST API Modular Input has been configured, and has captured alert data from Cloud Secure, take the following steps to examine the data in the Splunk Search engine:

1. Click the “splunk>enterprise” logo in the top-left corner of the window.
2. In the Search window, enter index=“main”
3. Click the Search icon (the magnifying glass) and verify the output (See Figure 10)
4. Click the “+” signs after the actions and attributes fields to see additional Cloud Secure alter details

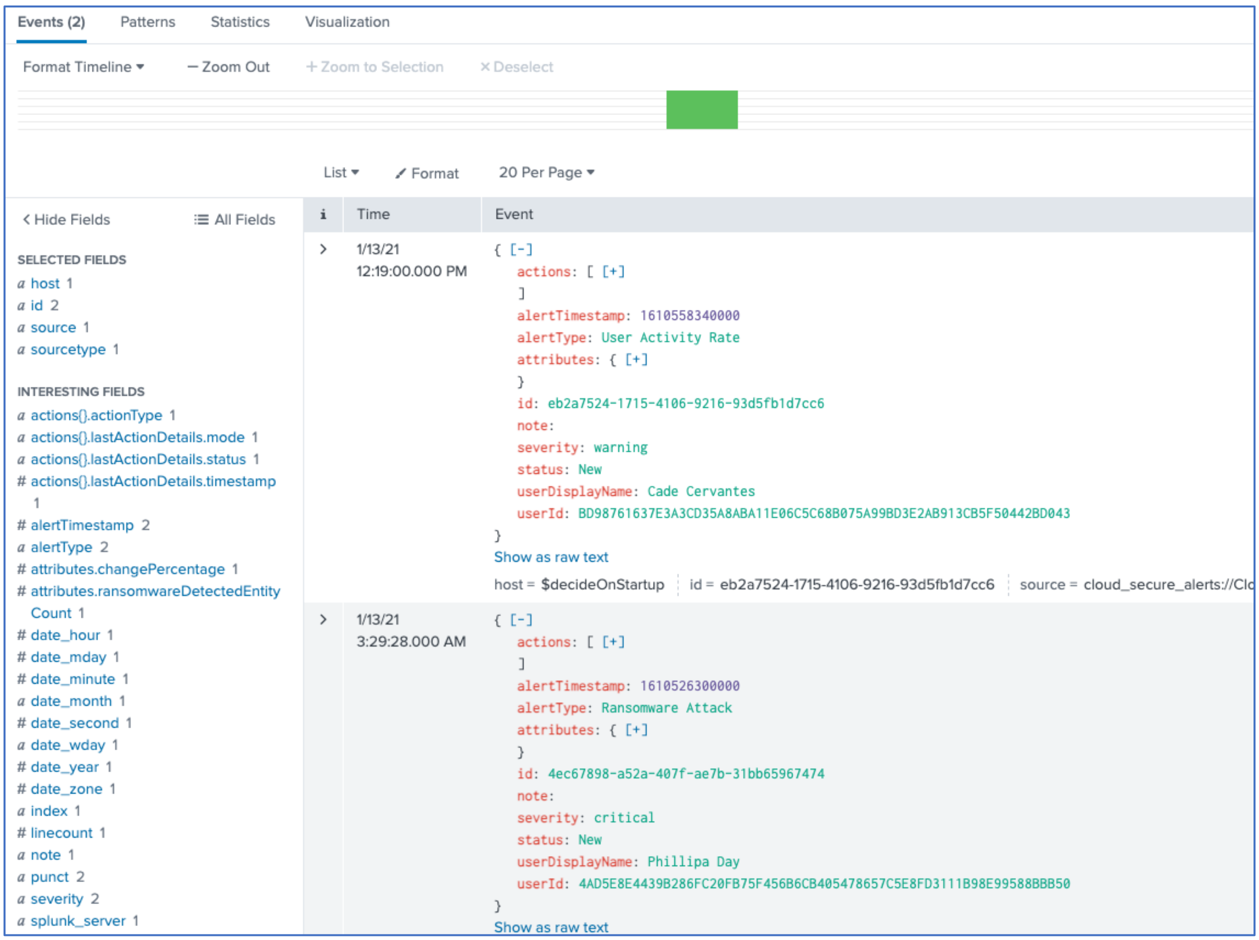

Figure 10 Splunk Search Output of Cloud Secure Alert Data

Conclusion

This document has provided a brief overview of the integration between NetApp Cloud Insights and the Cloud Secure feature, and the Splunk REST API Modular Input. Through this RESTful API integration, alert data from Cloud Secure can be made visible within Splunk for further data processing. This document has also provided the basic steps to create this integration; however, for full details the official documentation of each solution should be referenced.

References

[1] P. Raj and A. Raman, Software-Defined Cloud Centers: Operational and Management Technologies and Tools, Cham: Springer International Publishing, 2018.

[2] M. J. Turner, "Automation, Analytics and Governance Power Enterprise Multicloud Management Strategies," IDC, 2019.

[3] NetApp, Inc., "Cloud Insights," NetApp, Inc., January 2021. [Online]. Available: https://cloud.netapp.com/cloud-insights. [Accessed 12 January 2021].

[4] Splunk, Inc., "NetApp Partner Directory - Splunk," NetApp, Inc., 2021. [Online]. Available: https://partner-connect.netapp.com/de/partner-directory/splunk-inc. [Accessed 12 January 2021].

[5] "Splunk Add-on Builder," 18 December 2019. [Online]. Available: https://splunkbase.splunk.com/app/2962/#/overview. [Accessed 12 January 2021].

[6] Splunk, "Splunk Add-on Builder User Guide: Configure Data Collection Using a REST API Call," Splunk, [Online]. Available: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/ConfigureDataCollection?ref=hk. [Accessed 12 January 2021].