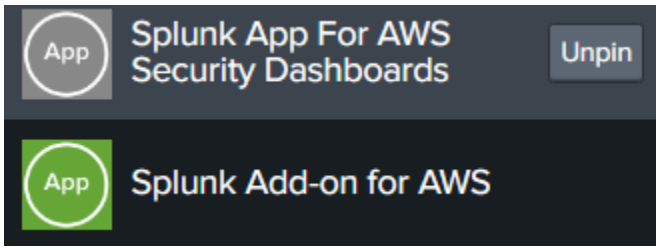
Make sure to add these apps on Splunk Cloud



Create a policy using this

https://docs.splunk.com/Documentation/SplunkCloud/9.2.2403/Admin/AWSGDI#:~:text=You%20need%20a%20valid%20AWS%20account%20with,ability%20to%20collect%20data%20from%20your%20AWS

Then create a new user, and skip the AWS management console access. Attach that new policy to it. After creation, create a security access token, and make sure to choose “service from outside AWS” for it since Splunk cloud is running outside of it.

Download the CSV file and note down the access key token and most importantly note down the SECREY KEY.

This will be used within the Splunk Cloud webui for the AWS add-on app when we create a new account. I followed this video for cloud trail integration. He used an older piece of documentation but the new version is here for reference, NOTE I did not refer to this document when following the video, I used the previous linked file above.

https://splunk.github.io/splunk-add-on-for-amazon-web-services/

Splunk AWS Add-on : Ingestion of AWS Cloudtrail data in Splunk

Right now everything is being sent to the default index, and the index as I understand it is responsible for parsing and normalizing the logs so Splunk Cloud can read from. Maybe for best results it's better to send the data to more than one index. Create specific indexes to better organize and separate where to find the data needed.

The Splunk Add for AWS is what is responsible for shipping all the logs over to Splunk Cloud.

TIP: Write the service you want on the search query and pick and choose the details you want. Then go to visualization -- Pivot Table -- and make your customizations there. But the AI chat is helping a lot in visualizing data right now.

index=* | stats count by source type

TO ADD THREAT INTELLIGENCE

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": "guardduty.amazonaws.com"
         },
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::YOUR-BUCKET-NAME/*",
         "Condition": {
            "StringEquals": {
               "aws:SourceAccount": "AWS-ACCOUNT-ID"
            },
            "ArnLike": {
               "aws:SourceArn": "arn:aws:guardduty:*:AWS-ACCOUNT-ID:detector/*"
            }
         }
      }
   ]
}
```

Make sure to add the for every bucket you want to act as a threat intelligence feed. This allows Guard Duty to grab these items from the bucket.

Use the S3 URL ONLY

Some threat lists to look at https://www.misp-project.org/feeds/