Splunk SIEM Report

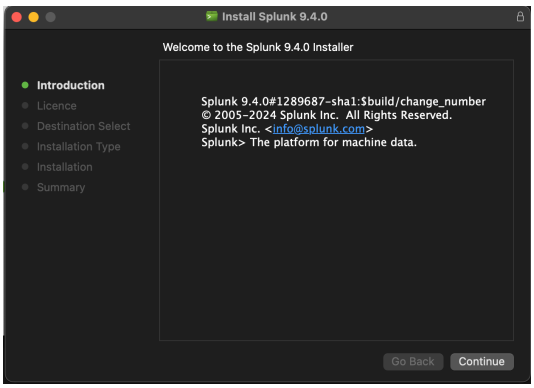
Installation

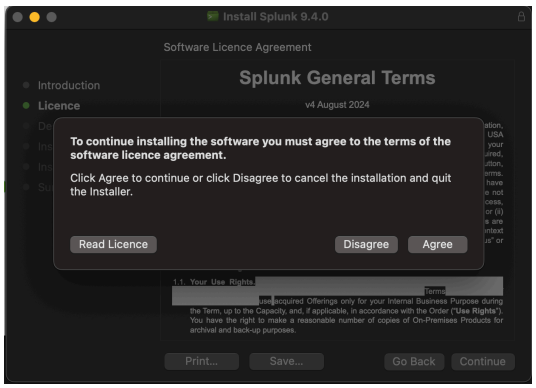
After downloading the splunk's dmg file from their official website, I ran a hash check on the file to make ensure its integrity.

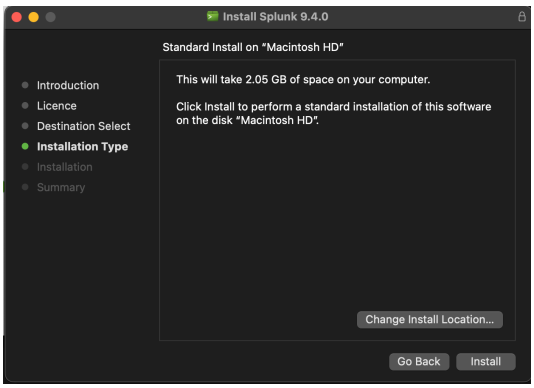
```
kusoterababalola@Maccy-Mac Splunk_SIEM % shasum -a 512 splunk-9.4.0-6b4ebe426ca6-darwin-intel.dmg
87d0679b538246cce9f09fc7101c6a3700d5e0c2702191d5140fa07bcc19e5f7cfbc4c102ec72a075d34f702a81633758a3d3cde4f18144361fdf42e807a80d7  splunk-9.4.0-6b4ebe426ca6-darwin-intel.dmg
kusoterababalola@Maccy-Mac Splunk_SIEM %
```

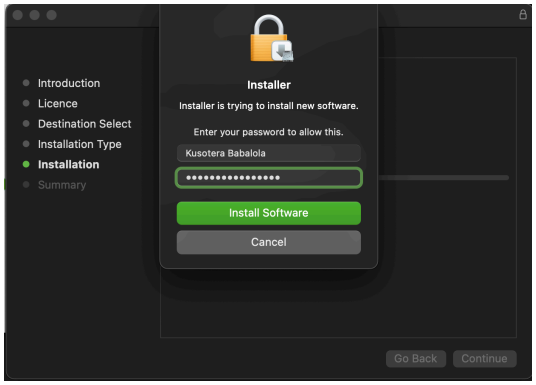
```
SHA512(splunk-9.4.0-6b4ebe426ca6-darwin-intel.dmg)=
87d0679b538246cce9f09fc7101c6a3700d5e0c2702191d5140fa07bcc19e5f7cfbc4c102ec72a075d34f702a81633758a3d3cde4f
18144361fdf42e807a80d7
```

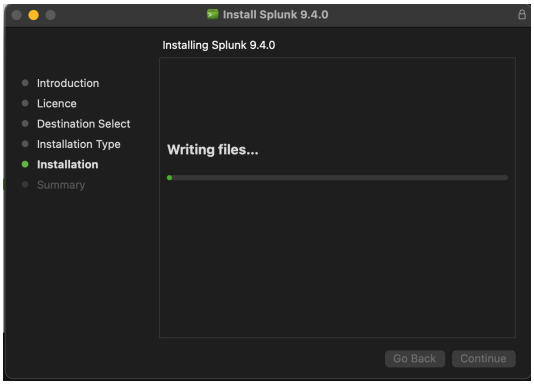
I double-clicked the installer and followed the instructions. I've provided screenshots below to highlight every time I was prompted.

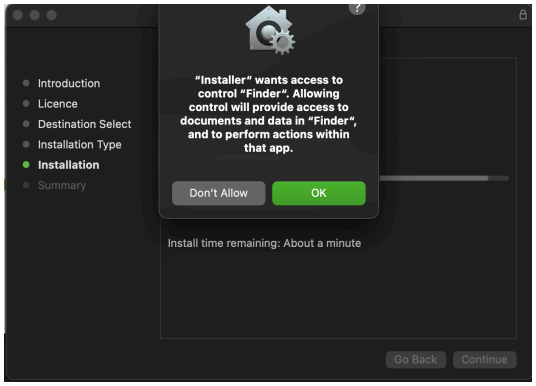


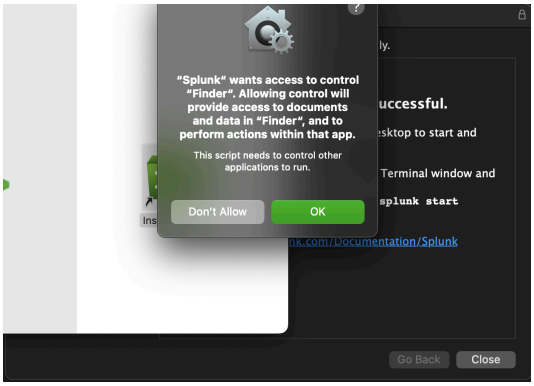

Install Splunk 9.4.0
Software Licence Agreement
Introduction
Licence
Splunk General Terms
v4 August 2024
To continue installing the software you must agree to the terms of the software licence agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.
Read Licence
Disagree
Agree
Print...
Save...
Go Back
Continue

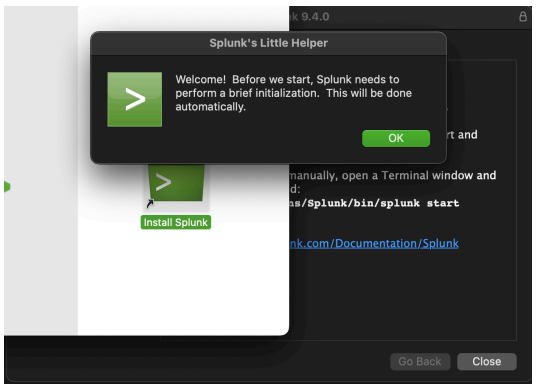

Install Splunk 9.4.0
Standard Install on "Macintosh HD"
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
This will take 2.05 GB of space on your computer.
Click Install to perform a standard installation of this software on the disk "Macintosh HD".
Change Install Location...
Go Back
Install

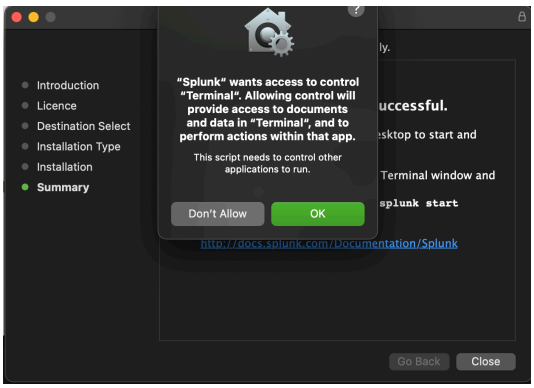

Introduction
Licence
Destination Select
Installation Type
Installation
Summary
Installer
Installer is trying to install new software.
Enter your password to allow this.
Kusotera Babalola
Install Software
Cancel
Go Back
Continue


Install Splunk 9.4.0
Installing Splunk 9.4.0
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
Writing files...
Go Back
Continue

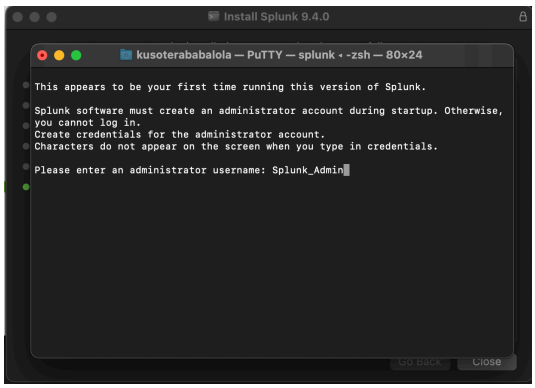

Introduction
Licence
Destination Select
Installation Type
Installation
Summary
"Installer" wants access to control "Finder". Allowing control will provide access to documents and data in "Finder", and to perform actions within that app.
Don't Allow
OK
Install time remaining: About a minute
Go Back
Continue

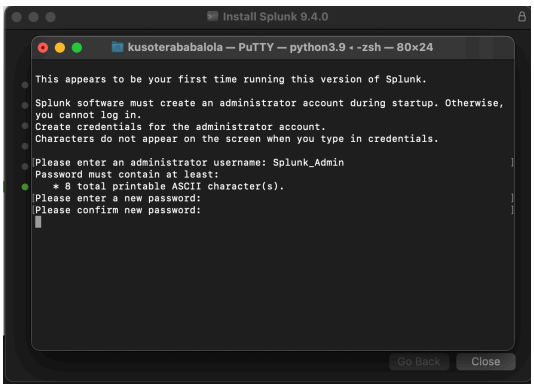

"Splunk" wants access to control "Finder". Allowing control will provide access to documents and data in "Finder", and to perform actions within that app.
This script needs to control other applications to run.
Don't Allow
OK
Terminal window and
splunk start
Go Back
Close

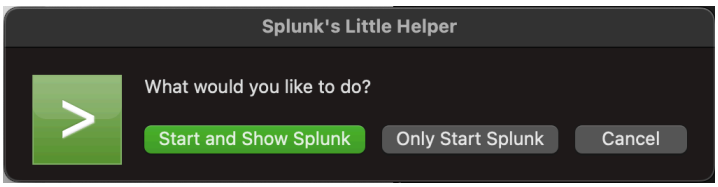

Splunk's Little Helper
Welcome! Before we start, Splunk needs to perform a brief initialization. This will be done automatically.
OK
Install Splunk
Go Back
Close


Introduction
Licence
Destination Select
Installation Type
Installation
Summary
"Splunk" wants access to control "Terminal". Allowing control will provide access to documents and data in "Terminal", and to perform actions within that app.
This script needs to control other applications to run.
Don't Allow
OK
Terminal window and
splunk start
Go Back
Close

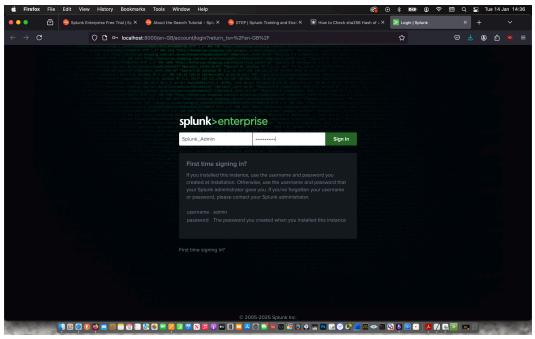
Created a username and password for my admin splunk account and started the web application.

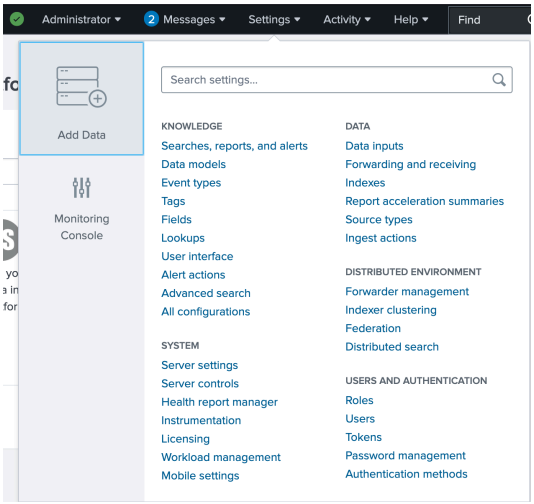


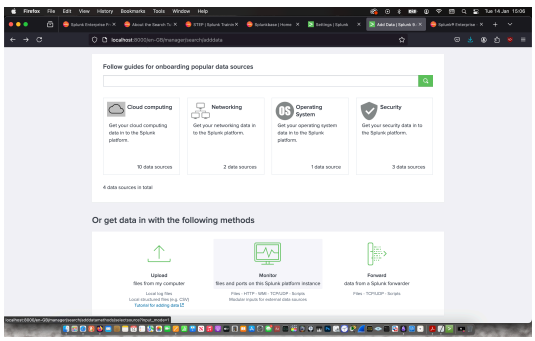


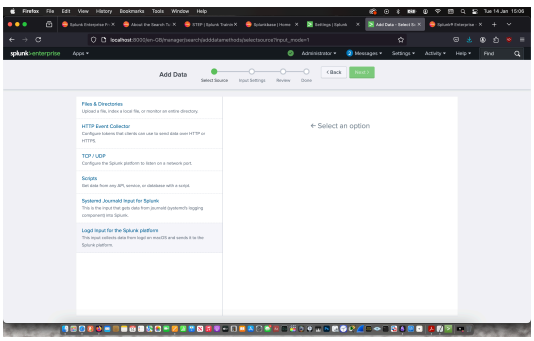


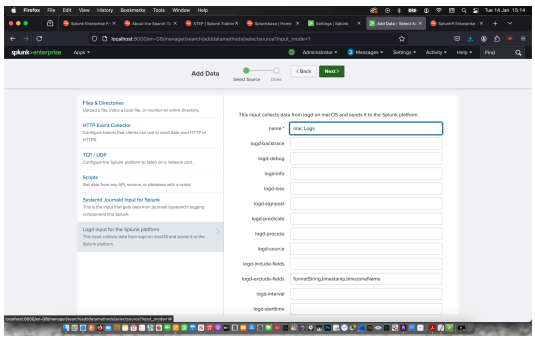
Then I signed it and immediately ingested the log data from my laptop

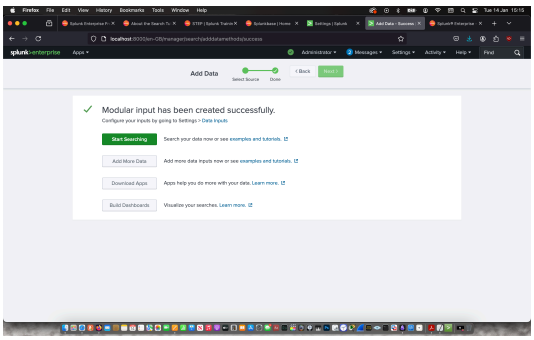




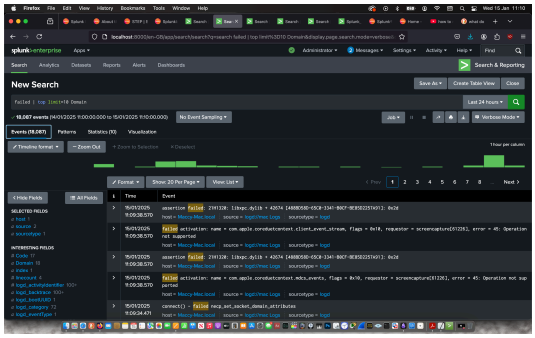


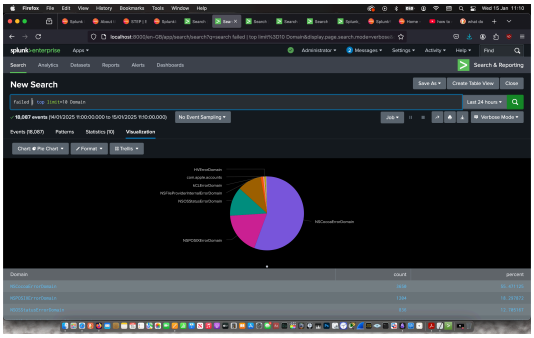


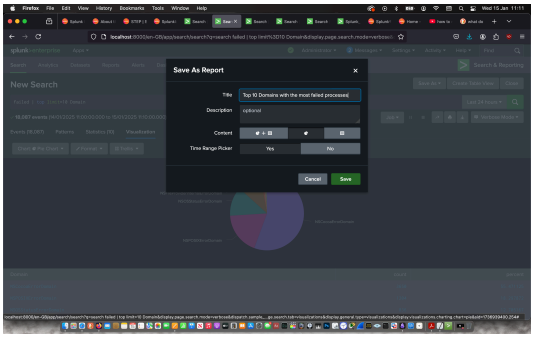




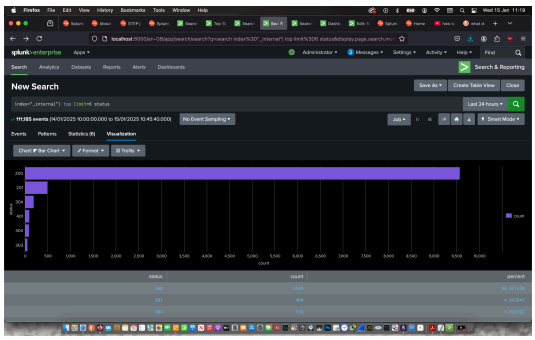
Then I used the "Search & Reporting" app to search for the top domains with the most failed processes with the command "failed | top limit=10 Domain". Then I used the visualisation feature create a pie chart to represent the information and saved it as a report to later add it to a Dashboard. From this visualisation, I can determine that NSCocoa Domain had the most failed processes which willed a further investigation.

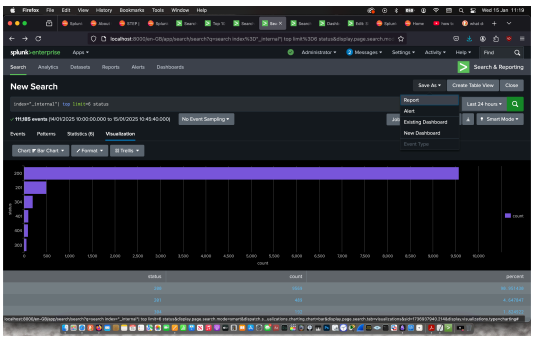


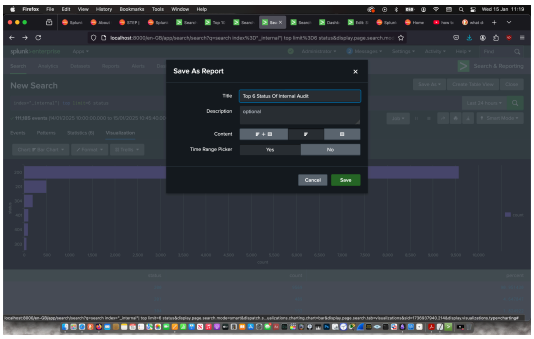




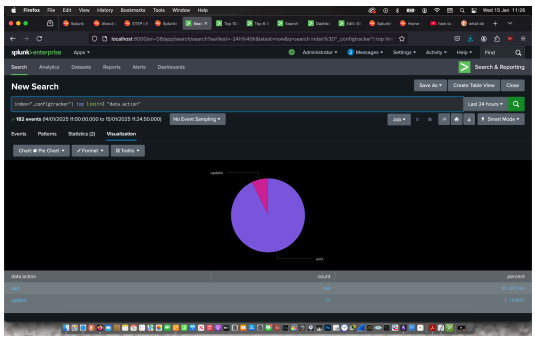
Then I used the "Search & Reporting" app to search for the status of processes on the internal system with the command "index="_internal" | top limit=6 status". Then I used the visualisation feature create a bar chart to represent the information and saved it as a report to later add it to a Dashboard. From this visualisation, over 90% of the processes have a status of 200 which signifies a smooth running system.

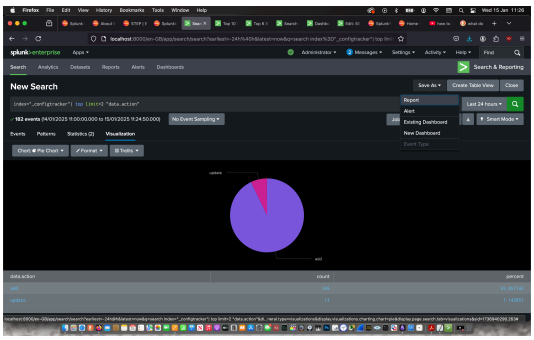


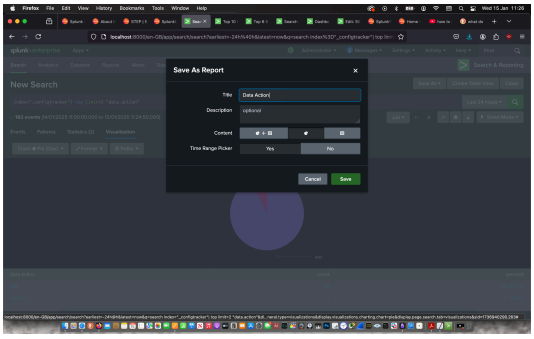




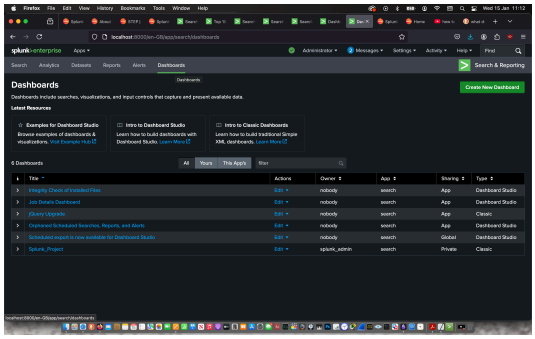
Then I used the "Search & Reporting" app to search for the actions taken on the config data with the command "index="_configtracker" | top limit=2 "data.action"". Then I used the visualisation feature create a pie chart to represent the information and saved it as a report to later add it to a Dashboard. From the pie chart, I can determine that only 7% of the config data was updated.

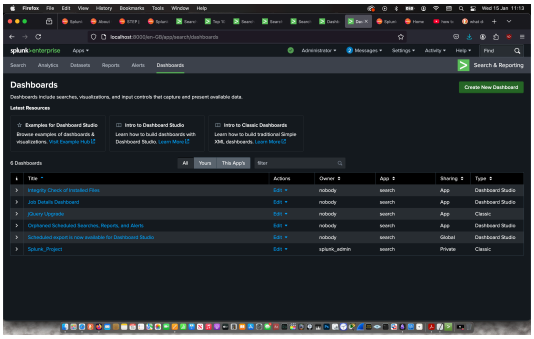


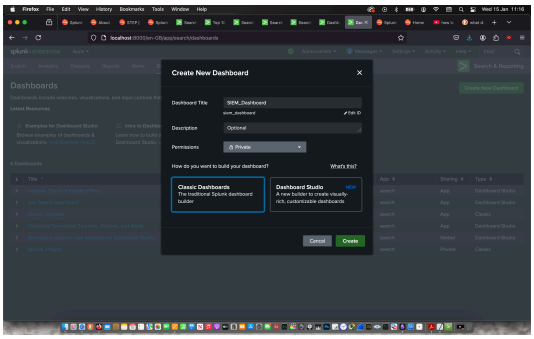




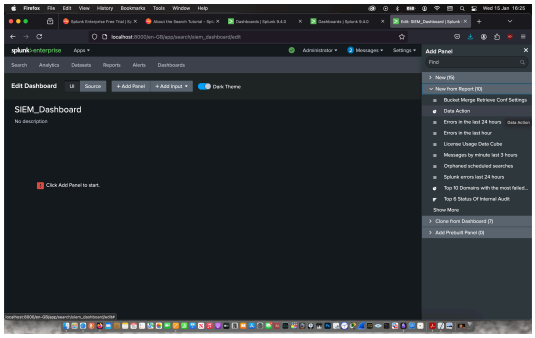
I Created a new dashboard in classic mode.

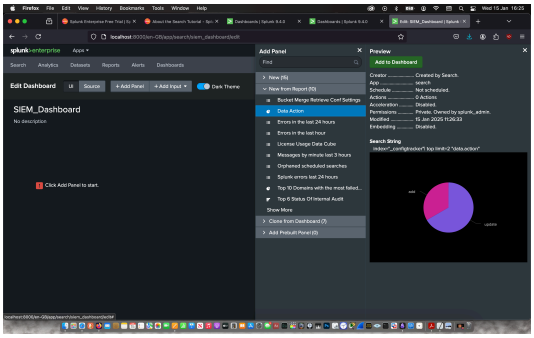


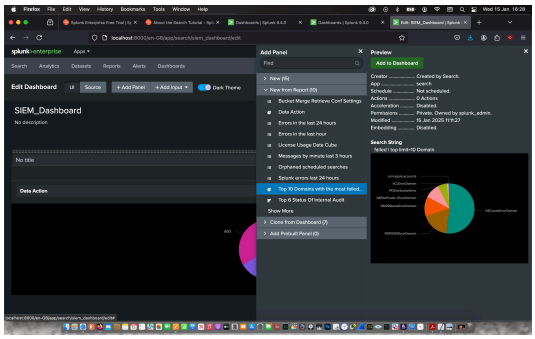


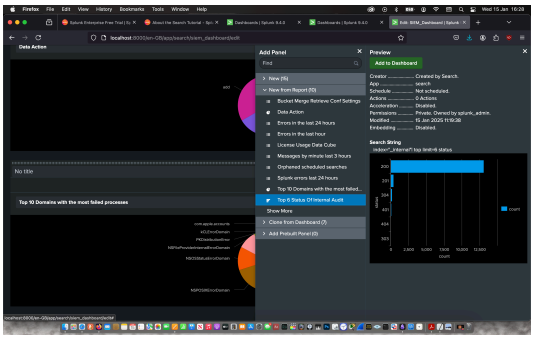


Then I imported all three reports into the dashboard.









Finally, I cloned my dashboard in dashboard studio in grid mode for a better presentation.