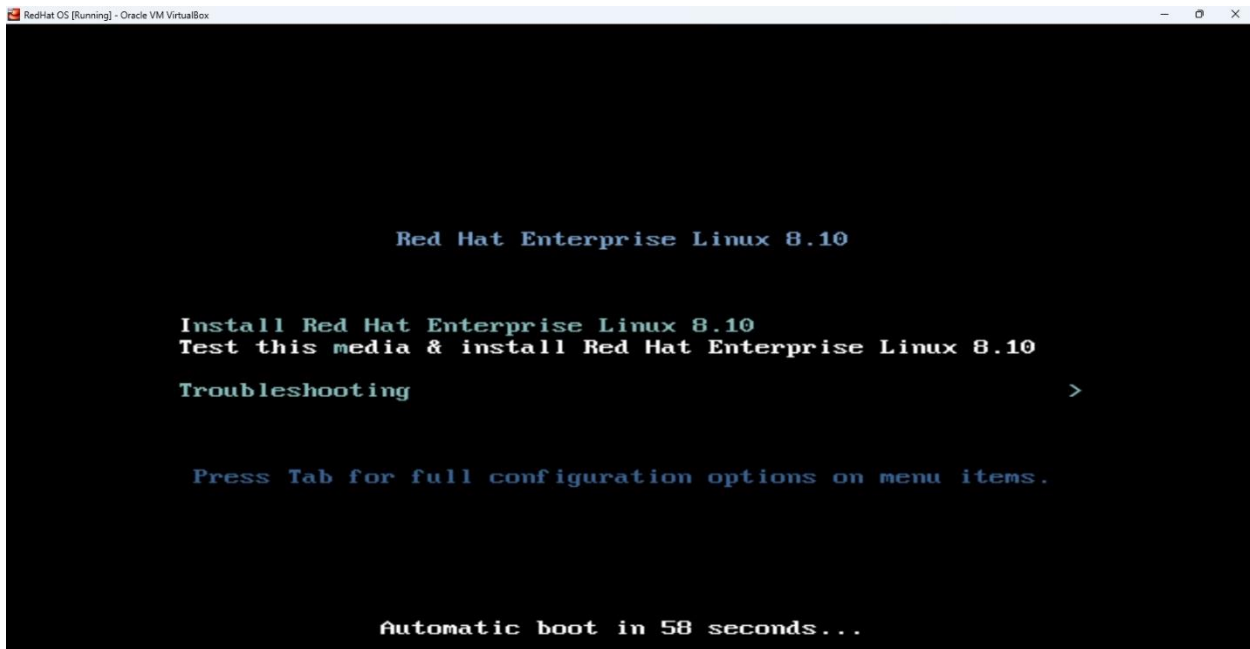


Building on my previous blog, I'll demonstrate how to:

- Generate reports and alerts for senior management
- Create an index from log events for security insights
- Create interactive dashboards
- Automate incident response with Splunk SOAR custom playbooks



Running Splunk SOAR on Red Hat Enterprise Linux 8.x will be covered in an upcoming article.

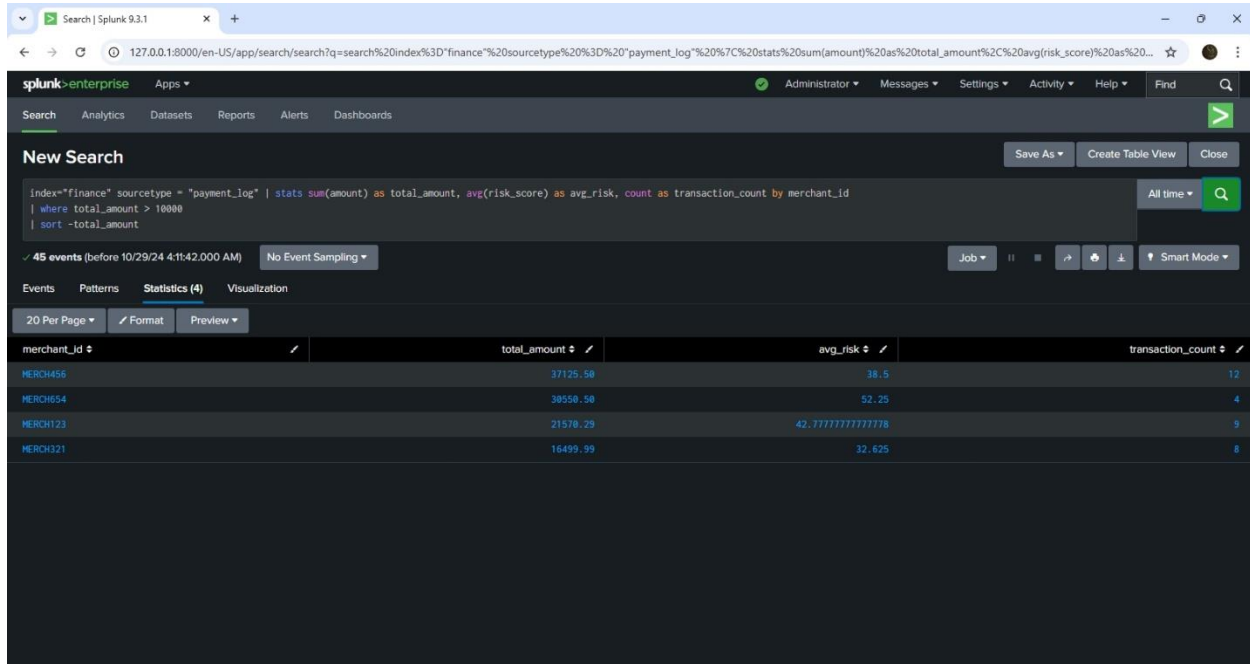
REPORTING GENERATION IN Splunk

Why create a report?

Report provides visual representation of data, enabling quick identification of trends, patterns and anomalies. Report can be easily shared amongst stakeholders to ensure speed collaboration and awareness.

Scenario: The Product Manager wants to see a detailed report of merchants with high value transaction on a daily basis by 9:00AM (WAT).

Approach: We start by running a splunk query on our log data.



The screenshot shows the Splunk Enterprise interface. The search bar contains the following query: `index="finance" sourcetype="payment_log" | stats sum(amount) as total_amount, avg(risk_score) as avg_risk, count as transaction_count by merchant_id | where total_amount > 10000 | sort -total_amount`. The search results show 45 events. The table displays the following data:

merchant_id	total_amount	avg_risk	transaction_count
MERCH456	37125.50	38.5	12
MERCH654	30550.50	52.25	4
MERCH123	21570.29	42.77777777777778	5
MERCH321	16499.99	32.625	8

Once done, we then set up the permission for the report. Our preference in this case is to ensure that report is shared in app so that other members of the security team can view the report as well, and a mail is sent to the product manager once a report has been generated.

High Value Transaction Report

127.0.0.1:8000/en-US/app/search/report?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FHigh%2520Value%2520Transaction%2520Report%2520By%2520Merchant&dispatch.sample_ratio...

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

High Value Transaction Report By Merchant

Last 30 days

45 events (9/29/24 12:00:00.000 AM to 10/29/24 4:16:30.000 AM)

4 results20 per page

merchant_id

MERCH456

MERCH654

MERCH123

MERCH321

EditPermissions

ReportHigh Value Transaction Report By Merchant

Owneradministrator

Appsearch

Display ForOwnerAppAll apps

Run AsOwnerUser

Learn More ID

Everyone

admin

can_delete

power

splunk-system-role

user

Read

Write

CancelSave

g_risk

transaction_count

38.5

52.25

21578.29

32.625

12

4

9

8

High Value Transaction Report

127.0.0.1:8000/en-US/app/search/report?s=%2FservicesNS%2Fadministrator%2Fsearch%2Fsaved%2Fsearches%2FHigh%2520Value%2520Transaction%2520Report%2520By%2520Merchant&dispatch.sample_ratio...

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

High Value Transaction Report By Merchant

Last 30 days

45 events (9/29/24 12:00:00.000 AM to 10/29/24 4:16:30.000 AM)

4 results20 per page

merchant_id

total_amount

avg_risk

transaction_count

MERCH456

37125.50

38.5

12

MERCH654

38550.50

52.25

4

MERCH123

21578.29

42.77777777777778

9

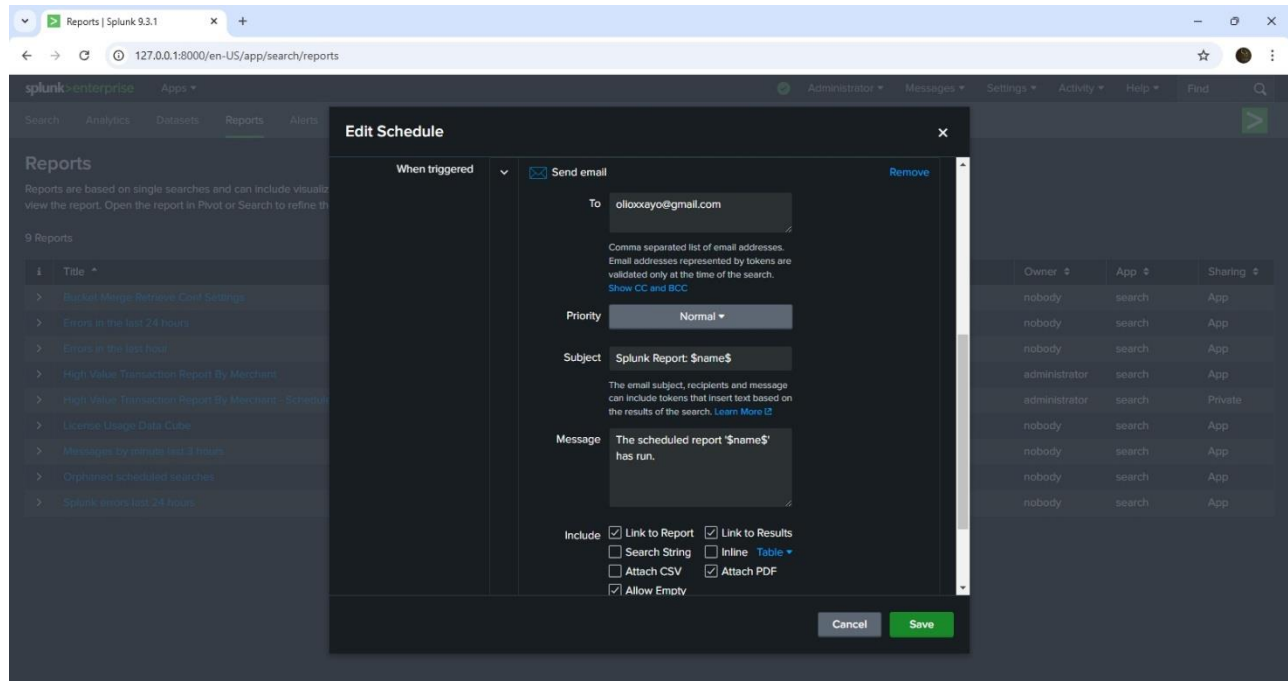
MERCH321

16499.99

32.625

8

For the report to be scheduled, we will need to clone our initial report, as I added a time picker in the initial report. Cloning the report and scheduling it will make it possible for the product manager to get the scheduled report everyday at 9:00AM.



After this whole setup is done, every day at 9:00AM, the product manager gets a report of the merchants who collected the most money.

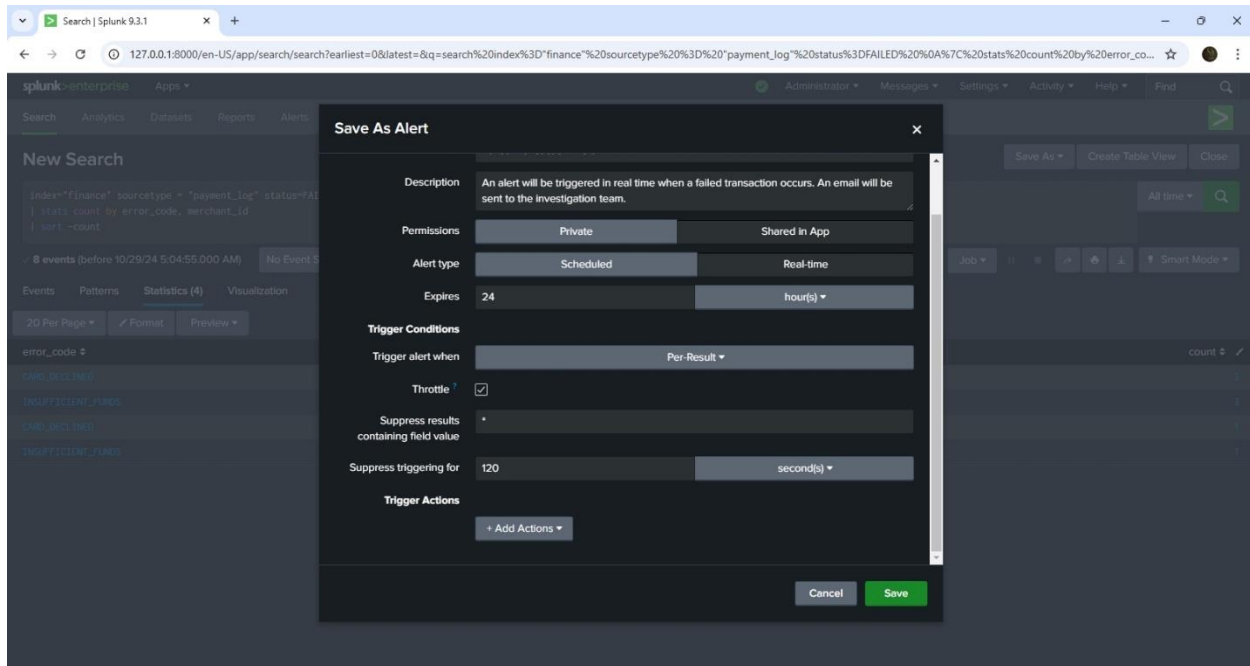
ALERT TRIGGERING IN Splunk

Why alerts triggering is important?

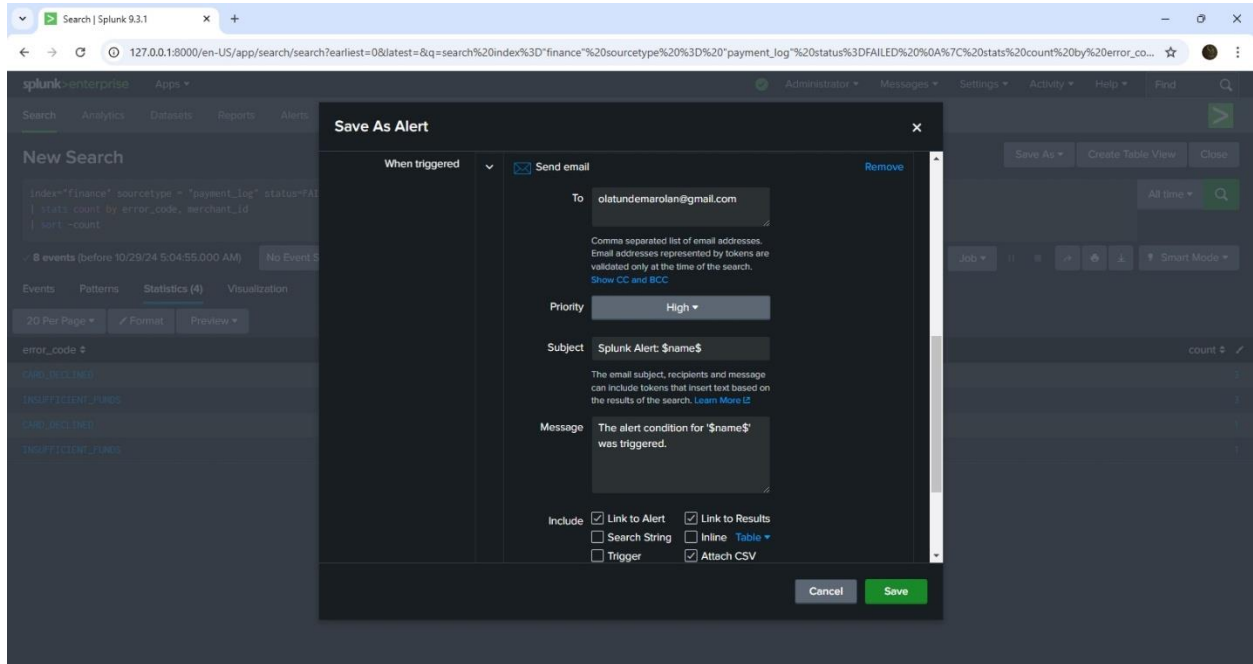
Alert triggering helps the security team to be notified and be able to quickly respond to a critical or high alert securities event.

Scenario: The CEO is particular about failed transaction, and wants an alert triggered for each failed transaction.

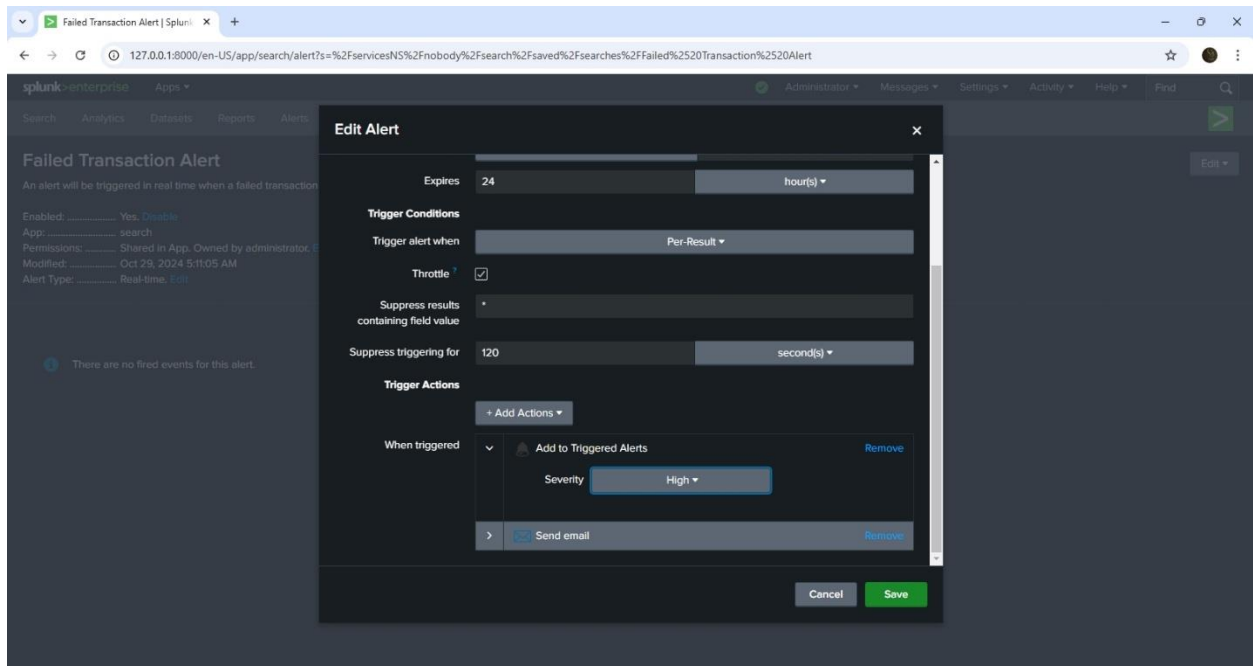
Approach: As always we start with a SPL query. Then move on to create an alert (this time it is scheduled), but depending on preference or use case, the alert can run real time.



The alert gets triggered when a failed transaction is detected, and in this case I have configured Splunk to send an email to the CEO. I also added it to triggered alerts, so that the other security team members can see the list of triggered alerts as well. In a professional setting, the triggered alerts list is what security teams monitor regularly to be able to quickly investigate an incident.



Send email to CEO



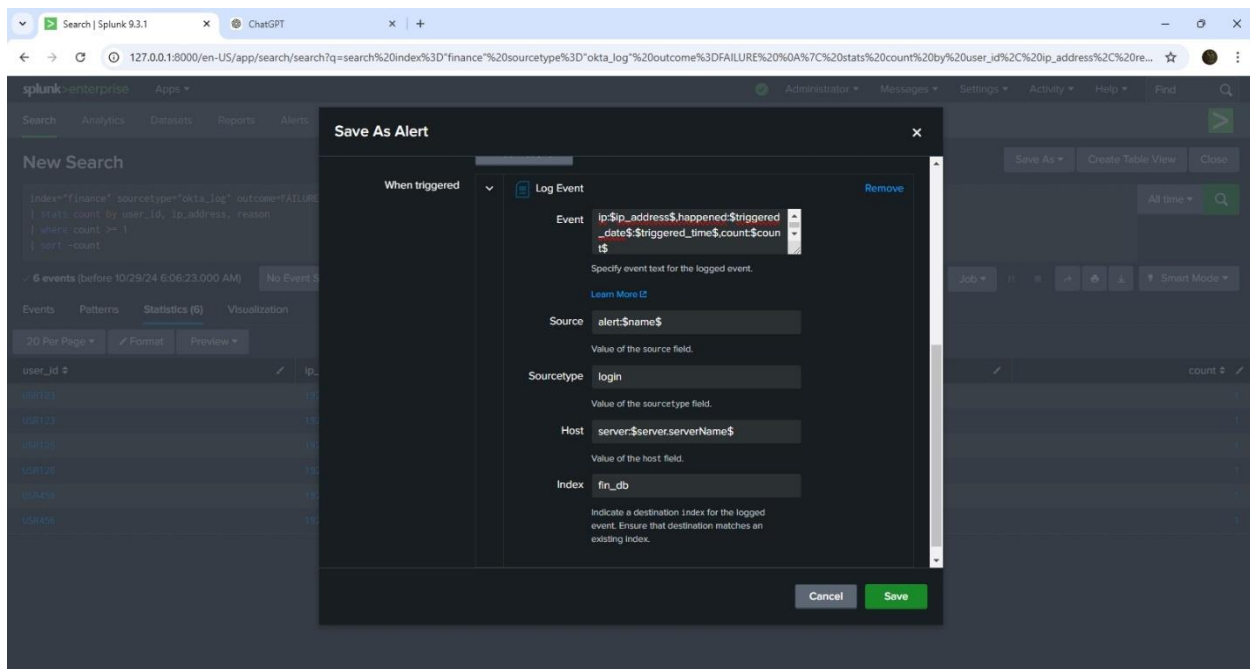
Triggered Alert

LOGGING EVENTS IN Splunk

Scenario: The CEO wants to see the users who failed authentication. He has asked if it is possible to see just the required fields in the events.

Approach: We start with a SPL query to find out users with failed authentication login. We schedule the alert to run daily. Then in the **Trigger Alert > Add Actions**, we choose Log Event. Then we continue by specifying the Event Text, Source type, Host Name, and Index.

Note that the index must exist before it can be used.



You can only log events when you have the admin permission or enable_tcp permission.

From the above image. When the CEO searches the fin_db index, he gets the IP address of the device with failed authentication login, when it happened, and how many times the failure occurs.

DASHBOARD CREATION IN Splunk

Why is dashboard important?

One of the many reasons why I love dashboard is that it organizes complex data into intuitive visualizations. Another is that dashboards enables the sharing of key performance metrics across teams and organizations.

Scenario: The Engineering Manager has requested that we prepare a dashboard showing the errors by each API endpoint. This dashboard will then be shared to Company A, so that their development team can work on improving the functionality of these endpoints.

Company A is our payment gateway partner.

Approach: We start with a SPL search, then proceed to creating a new dashboard.

After the dashboard is created, it appears to be static. But then we want a situation where the both the Engineering Manager and the development team at Company A, can view results dynamically. What I mean is they can tell Splunk to customized the dashboard and display results in the last 7 days, last 30 days, All time, or even in the last hour.

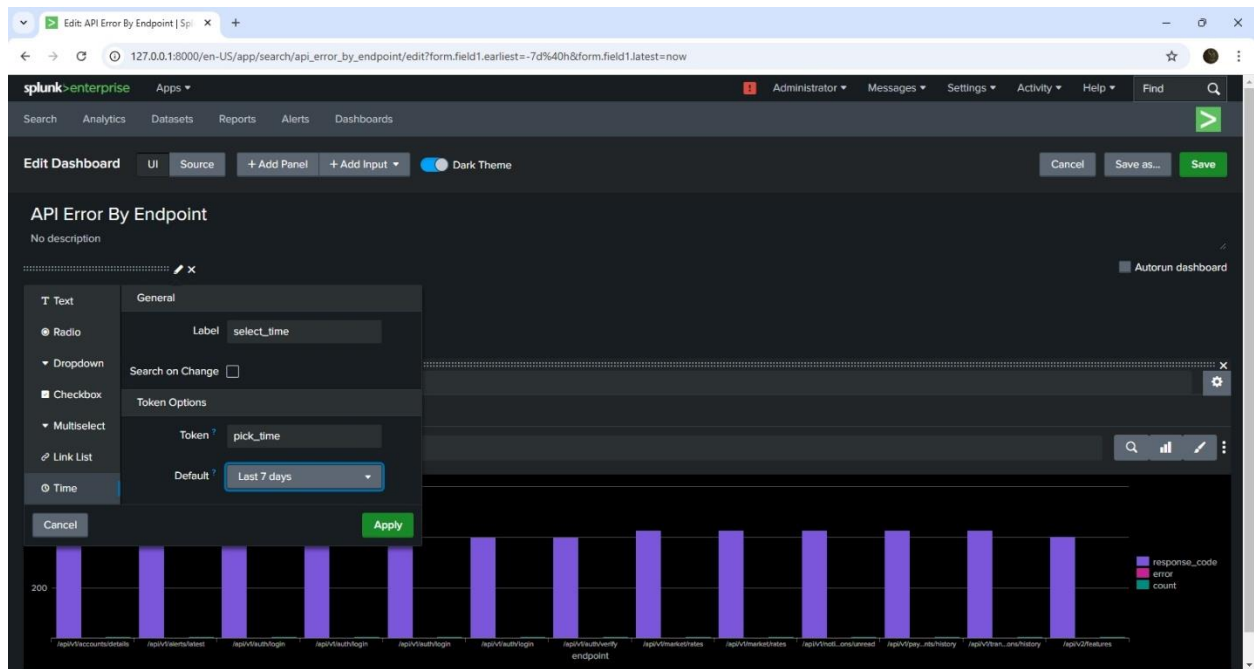
To achieve this we use a Time Input and enable the Time Input in our dashboard.

With the time input added, these stockholders can ask splunk to generate results based on time.

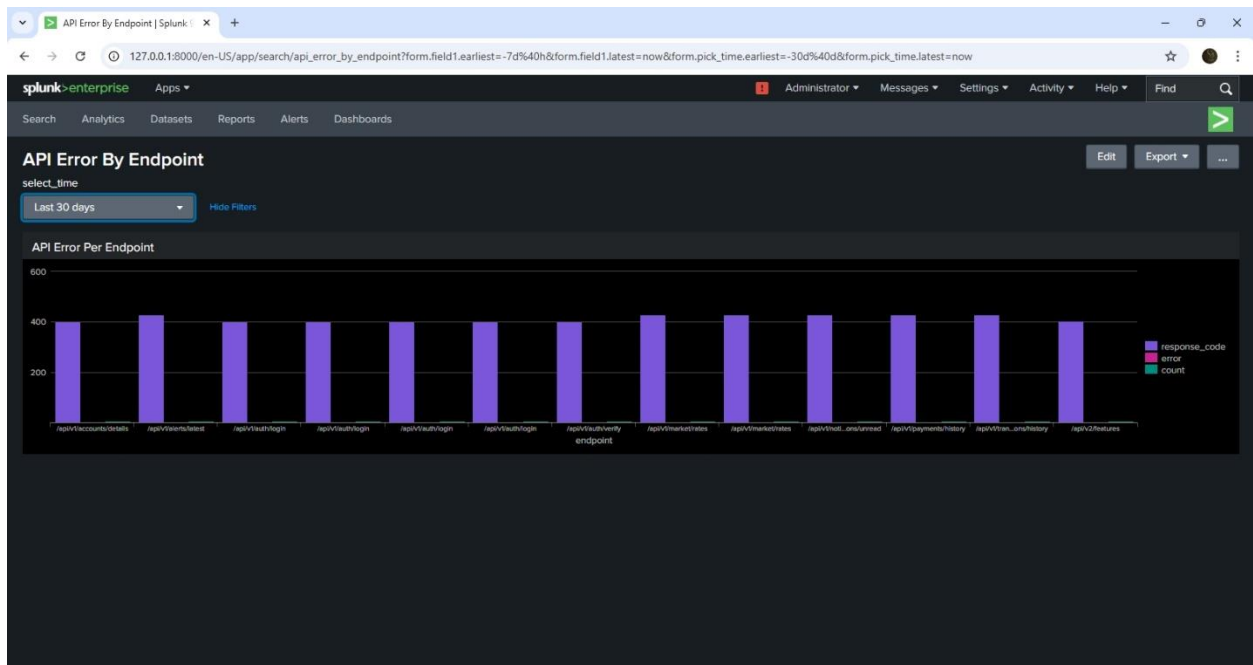
We went a little further by generating a pdf of the dashboard.

As a best case scenario, when creating a dashboard ensure that it is simple to understand, strive to keep at most 4 different visualizations in a single dashboard, if you need to add more visualizations consider creating a new dashboard. Also sparingly use pie-chart. It is to complex to understand most times.

Keeping things simple and clean is the way to go...



Adding Time Input



Time Range Added

A simple playbook with Splunk SOAR.

Up till this point, we have detected events and anomalies in our mock Fintech environment. We can even go a step further by orchestrating our operations and responding to security events or anomalies.

Our response could range from blocking a suspicious transaction, or locking out a users after a number of failed transaction.

In Splunk SOAR, we have the liberty to create playbooks. A playbook is simple a rule that runs when an event or anomaly is detected. To use Splunk SOAR, you'll need Red Hat Enterprise Linux 8.x

To view the playbook click this link :

<https://gist.github.com/praiseolotu/d44820e996e1de7fe1511f3c08815e00>

If you are very familiar with the Python programing language, it will be easy to understand the workings of this playbook.

You can choose to use the playbook studio, or write a custom playbook. But most times it starts with the playbook studio to test simple playbooks, and then you can proceed to writing your custom playbook for added flexibility.

Note that the first line of code is very important, if it's not written, the playbook won't run.

Once an event or anomaly is detected and sent over to SOAR, this playbook will run thereby giving us an extra layer of security.

To send data from our splunk Enterprise to splunk SOAR, we need to install the Splunk App for SOAR Export.

Happy Splunking !!!