DAY 1/100

CYBER SPACE

INTEGRATING

PEGA with SPLUNK

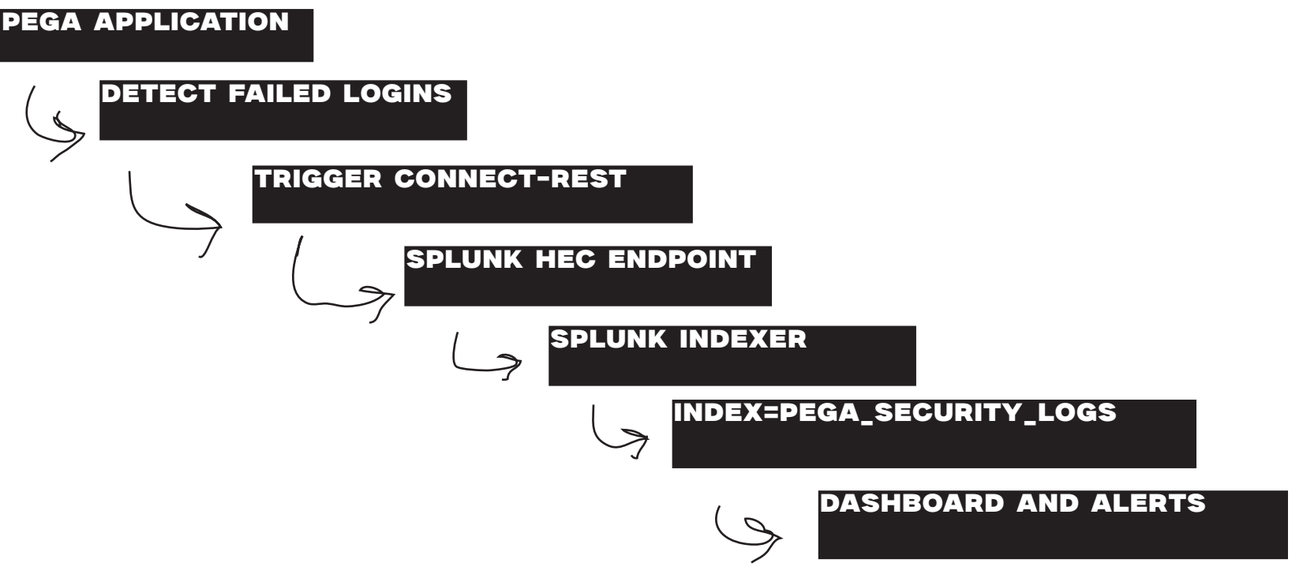
OBJECTIVE

Establish integration from Pega to Splunk using HTTP Event Collector (HEC) to monitor failed login attempts by Pega users for security operations, correlation with other data sources, and early detection of suspicious activity.

SCOPE

- Configure Splunk HEC to receive Pega failed login data.
- Configure Pega Connect-REST to push JSON events to Splunk HEC
- Validate ingestion and indexing in Splunk.
- Build basic dashboards for monitoring failed logins.

ARCHITECTURE OF THE MODEL



PRE- REQUISITE

- Splunk Enterprise/Cloud with admin access.
- Pega developer/admin access.
- Network connectivity from Pega to Splunk HEC (tcp/8088).
- HEC endpoint and token ready on Splunk.
- Identification of failed login attempts in Pega (fields like pyOperatorID, pyAuthenticationStatus, IP, timestamp).

HEC Configuration on Splunk

1. Navigate to Settings -> Data Inputs -> HTTP Event Collector.
2. Create a new token:

   Name: pega_failed_logins

   Sourcetype: pega:failed_login

   Index: pega_security_logs

   Enable acknowledgment if needed.
3. Note:

   Token: 08abcde9-xxxx-xxxx-xxxx-xxxxxxxxxxxx

   Endpoint: https://<splunk_fqdn>:8088/services/collector/event

IDENTIFY LOGIN FAILURES BY TRACKING:

pyAuthenticationStatus = “Fail”

pyOperatorID, pxRequestor, IP address, timestamp, failure reason, node ID.

CREATE CONNECT-REST

https://<splunk_fqdn>:8088/services/collector/event
Method: POST

HEADERS:

```
Authorization: Splunk <HEC_TOKEN>
Content-Type: application/json
```

PAYLOAD:

```
{
  “event”: {
    “OperatorID”: “<pyOperatorID>”,
    “RequestorID”: “<pxRequestor>”,
    “IPAddress”: “<RequestIPAddress>”,
    “FailureReason”: “<FailureReason>”,
    “AuthenticationStatus”: “Fail”,
    “Timestamp”: “<EventTimestamp>”,
    “NodeID”: “<NodeID>”,
    “Application”: “<ApplicationName>”
  },
  “sourcetype”: “pega:failed_login”
}
```

Attach this Connect-REST on the login failure handling activity or post-failure flow.

VERIFICATION

1. Log in to Splunk.

2. Run:

```
index=pega_security_logs sourcetype=pega:failed_login
```

Confirm events are received with correct timestamps and fields.

8. Dashboard and Alert Setup

Failed Logins Over Time:

```
index=pega_security_logs sourcetype=pega:failed_login
| timechart count by OperatorID
```

Top IP Addresses by Failed Logins:

```
index=pega_security_logs sourcetype=pega:failed_login
| stats count by IPAddress
| sort - count
```

Users with Most Failed Attempts:

```
index=pega_security_logs sourcetype=pega:failed_login
| stats count by OperatorID
| sort - count
```

Alert Example
Trigger on: 5 failed logins from the same IP in 10 minutes.

```
index=pega_security_logs sourcetype=pega:failed_login
| stats count by IPAddress
| where count > 5
```

Configure email/Slack notifications or integrate with SOAR workflows.