

JIGAR HIRANI

hirani.jigar117@gmail.com | [Linkedin](#) | [Github](#)

SUMMARY

Hands-on Splunk Administrator with strong 2+ years of experience in data onboarding, parsing, indexing, and day-to-day platform administration. Proven expertise in managing large-scale Splunk environments, ensuring reliable data flow, troubleshooting ingestion and performance issues, configuring roles and access, and maintaining stable, secure, and highly available Splunk platforms

PROFESSIONAL EXPERIENCE

Rojo Integrations (Full Time)

May 2026 - Present

Splunk Engineer & Observability Engineer

Tools and Technology: Splunk, Datadog, Python

Responsibilities:

- Building end-to-end P2P (Procure-to-Pay) visibility by designing observability pipelines that collect and monitor data flowing through enterprise integration adapters.
- Built Splunk and Datadog dashboards with monitors and alerts for real-time visibility into P2P pipeline health, adapter performance, and integration flow status.
- Developing custom Splunk Add-ons and automation scripts to extend observability coverage across hybrid environments.
- Implemented alerting and automation workflows to proactively detect and surface issues across business-critical P2P integration flows.

Data Elicit Solutions Pvt. Ltd. (Full Time)

Aug 2024 - April 2026

Splunk Admin

Client: Regeneron Pharmaceuticals

Tools and Technology: Splunk, Ingest/Edge Processor, Cribl, Python

Responsibilities:

- Manage Splunk Environment and Ensure all the data is flowing without any issue.
- Daily Ingestion 10TB+
- Created 20+ dashboards that turn raw logs into useful insights.
- Created 50+ alerts for efficient monitoring and action.
- Onboard AWS Logs, XDR, EDR, etc in Splunk and work with the security Team to implement their use cases.
- Implemented Splunk Ingest Processor to reduce Splunk Ingestion by 3TB.

SPLUNK EXPERIENCE

- Assess Splunk on-prem environment and suggest/implement best practice
- Managed Splunk Env which includes standalone, distributed, clustered environment (10TB daily ingestion with around 10k forwarders & maintained around 99.9% SLA).
- Troubleshooting Splunk issues (indexer, search head, deployment server, etc.)
- Onboard data from various data sources like application logs, firewall logs, FortiGate logs to Splunk and created custom routing and filtering data using regex
- Creating Index and Search time field extractions and fixing parsing issues
- Configuring new roles based on the user requirement.
- Created complex dashboards and alerts to monitor and troubleshoot Splunk environments
- Implement use cases in ES like Host is not reporting, Brute force attack detection
- Upgrade Splunk Env including Heavy Forwarders
- Various Integration with Splunk to third party tools like Splunk to Slack Alert, ServiceNow Ticket, etc.

- Created customized Add-on to fetch logs from third party application (2 Add-ons published on SplunkBase)
- Develop Custom Splunk Commands
- Onboard logs from AWS to Splunk using Splunk Add-on for AWS, Created Lambda/SQS/Cloudwatch for any custom Source

Splunk Ingest/Edge Processor Experience

- Designed and implemented Splunk Ingest / Edge Processor pipelines to optimize data ingestion and reduce license cost and storage consumption in production environments.
- Transformed Trend Micro EDR logs into optimized CSV format, reducing daily ingestion by approximately 1TB and achieving 60–70% storage reduction without loss of data, fields, or analytical capability.
- Optimized high-volume Windows Event Log sourcetypes (EventCode 5157, 4627, 5156, and others), reducing ingestion from ~1TB/day to ~550GB/day (~50% reduction) while preserving all index-time and search-time field extractions.
- Implemented Edge Processor in an on-premises environment, including configuration of Edge nodes, pipelines, and data processing workflows for secure and reliable data flow.
- Worked with multiple data sources including firewall logs, AWS logs, Carbon Black, Nexthink, and Linux system logs to normalize, filter, and optimize data before indexing.
- Ensured zero data loss during ingestion optimization by maintaining full field fidelity and compatibility with existing searches, dashboards, alerts, and Splunk Enterprise Security use cases.
- Developed field extractions compatible with default Splunk add-ons and Technology Add-ons (TAs) to ensure seamless integration and continued supportability.

CRIBL EXPERIENCE

- Onboard data from various data sources using Collectors supporting push & pull methods
- Created Routes/Quick Connects for sending data to proper destinations like Splunk, AWS S3, Elastic Search
- Created Pipeline/Packs for data extractions, data transformation, Field extractions, etc

AWS and Other DevOps Experience

- Created EC2 instances, Load Balancers, Security Groups required for Splunk Env.
- Configure IAM role to provide required access to all other AWS services
- Created Lambda to implement various use cases such as sending logs of S3 to Splunk etc.
- Developed shell scripting-based automation to monitor critical services, automatically restart failed services, and trigger alerts to ensure system stability.
- Managed and administered Splunk deployments across both Linux and Windows environments, with strong hands-on experience in provisioning, configuring, and maintaining Linux and Windows systems.
- Created Python Scripts to implement use case in Lambda, Fetch data from 3rd Party API and create file, etc.

TOOLS

- DevOps/SIEM tools: Splunk, Edge/Ingest Processor, Cribl, Datadog
- Programming Language: Python
- Cloud Platform: AWS (Lambda, S3, EC2, VPC, IAM)
- Scripting: Shell-scripting

EDUCATION

Darshan University

Oct 2022 - Jun 2025

Bachelor of Engineering: Computer Science Engineering

GPA: **8.29**

Gujarat Technological University

July 2019 - JUN 2022

Diploma in Engineering: Computer Engineering

GPA: **8.24**

LANGUAGE

- English: Fluent (speaking, reading, writing)
- Hindi: Advanced proficiency (speaking, reading, writing)
- Gujarati: Native