IBRAHIM K

Splunk Architect | Splunk Developer | SOC | Cyber Security

Address Bangalore, India 560008

Phone +91 961 190 0310

E-mail kibrahimhassan@gmail.com

LinkedIn https://www.linkedin.com/in/ibrahim-k-splunk/

Dynamic and results-oriented Splunk Admin and Architect with over 10 years of IT experience, including 8+ years specializing in Splunk Monitoring and administration. Expertise in designing, deploying, and maintaining multi-site Splunk environments, onboarding critical applications, and developing use cases to enhance security operations. Certified Splunk Architect and Ethical Hacker with a proven track record of mentoring teams, driving incident response, and delivering robust security solutions.

Work History

2023-12 - 2024-04

Associate Consultant

TCS Pioneer, ITPL, Bengaluru, India

- Primary role involves managing and optimizing the SIEM Splunk platform to ensure seamless collection, analysis, and storage of security logs, empowering SOC analysts
  to effectively detect and investigate threats.
- Optimized Splunk use cases by enhancing searches, leveraging data models, and implementing summary indexing, cutting query times by 30% and improving resource efficiency.
- Applied Splunk best practices in data onboarding and indexing to enhance platform scalability and handle billions of events daily.
- Trained Security Analysts on Splunk navigation, custom alerts, and threat analysis, boosting productivity by 30%.
- Provided end-to-end Splunk support for the Incident Response Team, ensuring timely resolution of critical security incidents with custom dashboards and troubleshooting.
- Created advanced correlation searches and alerts, reducing false positives and enhancing threat detection accuracy.

2021-05 - 2023-08

Security Delivery Associate Manager

Accenture India Private Limited, Bangalore

- Designed and architected Splunk solutions to support large-scale data ingestion, analysis, and visualization, ensuring scalability, reliability, and performance.
- Installed, configured, and maintained multi-site Splunk Enterprise environments, enabling SOC monitoring and operational efficiency.
- Led the onboarding of 100+ critical applications into Splunk within six months, significantly enhancing visibility, security, and data correlation.

- Managed a 10-member team of Splunk developers and administrators, ensuring efficient deployment, configuration, and administration of a complex Splunk environment.
- Authored 20+ architectural designs, runbooks, and deployment guides, defining best practices for Splunk deployment, troubleshooting, and data collection.
- Developed custom dashboards, alerts, and reports using advanced SPL (Search Processing Language) to meet diverse business and operational requirements.
- Monitored and optimized Splunk infrastructure for high availability and performance, performing regular health checks and audits.
- Troubleshot and resolved complex production issues related to Splunk performance, indexing, and data ingestion in collaboration with the Splunk Support team.
- Provided guidance and mentorship to junior Splunk administrators and developers, fostering a culture of continuous learning and improvement.

2015-08 - 2021-03

Senior SOC Analyst

Schweickert India Pvt Limited, Bangalore

- Primary role involves managing and optimizing the SIEM Splunk platform to ensure seamless collection, analysis, and storage of security logs, empowering SOC analysts to effectively detect and investigate threats
- Responsible for overseeing the operations of the entire Splunk and SOC team, ensuring robust threat detection, efficient incident response, and compliance with regulatory standards
- Designed, implemented, and managed a Splunk environment comprising 78+ components
- Configured and maintained high-availability syslog servers to ensure robust logging
- Monitored Splunk functionality using custom scripts and tools (e.g., Nagios, DMC)
- Integrated Splunk with external ticketing tools and implemented secure communications
- Assisted in developing SAP monitoring tools for IT operations and threat detection

2013-04 - 2015-07

Security Consultant

IBM India Pvt Limited, Bangalore

- Designed and deployed managed file transfer (MFT) solutions for 200+ clients using Axway Secure Transport
- Automated 50+ file transfers through Perl and Shell scripting
- Implemented secure file transfer protocols (FTP, SFTP, HTTP, HTTPS) and PGP encryption
- Migrated Oracle Identity Manager to IBM Security Identity Manager
- Implemented multiple scripts for automating the migration of different Identity and access manager solutions to IBM Security identity Manager

Education

2008-08 - 2012-09 **Bachelor of Engineering: Computer Science**
CSI College of Engineering - Ooty

Skills & Technologies

- Splunk Enterprise
- Splunk ES
- Microsoft Defender
- Active Directory
- Perl
- Python

Certifications

2018-02 Splunk Certified Architect

2018-01 Implementing Splunk ITSI, Splunk Inc

2014-08 Certified Ethical Hacker, EC-Council

Personal Information

- Passport Number: Z5176306
- Date of Birth: 08/05/88
- Gender: Male
- Nationality: Indian

Declarations

I, Ibrahim K, hereby declare that the information contained herein is true and correct to the best of my knowledge and belief.