Jim Clair BSCS, CISSP
Cloud Software Engineer

Phone: 19136459996
email: clair.james88@gmail.com
GitHub: https://github.com/jimclair
LinkedIn: https://www.linkedin.com/in/jim-clair

With 18 years of experience in software engineering, operations, and security, I specialize in cloud-native platforms, microservice architectures, enterprise infrastructure, and scalable data pipelines. My background in all aspects of software engineering allows me to drive successful projects and mentor teams to achieve excellence.

Professional Experience

Senior Software Engineer - Data Platform & Pipeline

Jul 2023 - Jan 2024; Select Star Inc. (Remote)

Designing, refactoring, building, securing and supporting enterprise pipeline and platform with a focus on collection, ingestion, processing and analysis of datawarehouse and business ingelligence data.

Achievements: Enabled asyncronous and parallel data collection and ingestion. Improve pipeline testability by adding an ingested batch persistence layer. Introduced ability to combine multiple parsing engines. Designed foundations of next-gen scalable data pipeline architecture. Up to 700% load-time optimization of multiple web pages backed by SQL.

Skills: *Django, Celery, Python, Kubernetes, AWS, Docker, PostgreSQL, Prometheus, Grafana, Sentry, Snowflake, Github Actions, Git, Bash, Terraform, REST, Postman*

Staff Integration Engineer

Feb 2023 - Jun 2023; Solv. (Remote)

Led and mentored team in new greenfield development foundations to create a cost-effective and scalable integration platform.

Achievements: Created unified provisioning bootstrap to serve as the foundations of next generation platform. Partner refactor of Athena scheduling api integrations. Introduced Sentry Cron alerting for long running integration jobs.

Skills: *Python, Docker, Heroku, REACT, Grafana, Prometheus, Athena, Sentry, PostgreSQL, Confluence, Jira, Postman, REST, HIPAA, SOC2*

Tech Lead Cloud Platform Engineering

Aug 2018 - Sep 2022 - LogRhythm Inc. (Remote)

Created, led, and mentored a team of highly skilled engineers while researching, designing, and implementing industry best practice tools and frameworks. Building a cost-effective, highly-available and scalable, multi-tenant platform, pipeline, and infrastructure supporting up to a million messages per second.

Achievements: Lead the technical development of infrastructure for the new Axon cloud-native platform over 3.5 years with a public launch in early 2022. Developed comprehensive Kubernetes Operators for Opensearch, Flink, and LogRhythm Microservices/Microfrontends. Created a high performance multi-tenant data pipeline with enterprise service bus, self-serve domain-specific relational databases, central time-series and tiered storage nosql database, and tenant specific real-time analytics job clusters. Implemented fully secure and automated development golden paths for localdev and CICD. Automated creation, re-creation and configuration of templated GitOps infrastructure as code environments and platforms. Full migration and integration of newly acquired Mistnet software into gold standard CICD and platform. Providing best practice

secure and public access to APIs and WebUIs through identity federated role-based access. Founded and staffed "Colossus of Cloud", a team of highly successful and skilled engineers. Earned my Bachelor's in Computer Science and completed the complete data science bootcamp on Udemy.

Skills: *Kubernetes, AWS, Terraform, ArgoCD, Ansible, SQL, Docker, Python, Javascript, Yeoman, Golang, Bash, KubeBuilder, Elastic/Opensearch, Kafka, Strimzi, PostgreSQL, Zalando, Flink, Quarkus, Java, Maven, GitHub Actions, Git, Istio, Vault, Prometheus, Grafana, Loki, Keycloak, Okta, GoPass, External Secrets, Certificates Manager, HAProxy, Jaeger, Pomerium, LogRhythm, *Nix, Salt, Veracode, REST, Postman, Kiali, Sysdig, Powershell, Jinja, EJS, RegEx, Lets Encrypt, Wireshark, Yarn, Mistnet, Confluence, Jira, Rally, Zero Trust Architecture, SOC2, FedRAMP*

Cloud DevOps Engineer III

Jul 2017 - Aug 2018 - LogRhythm Inc. (Hybrid)

Served as LogRhythm product expert on DevOps team while migrating LogRhythm’s core services to a SAAS offering hosted on Google Cloud Platform.

Achievements: Developed de facto reference architecture and sizing guides for new cloud service offering. Automated deployment of LogRhythm core services to Google Cloud Compute environment. Earned certifications in DevOps foundations, ITIL service management, Oracle SQL, and web development.

Skills: *Google Cloud, Rundeck, LogRhythm, Ansible, Python, Consul, Telegraph, InfluxDB, Grafana, SQL Server, Elasticsearch, Apache HTTP Server, Salt, Linux, Windows Server, RegEx, Lets Encrypt, Wireshark, Confluence, Jira, REST*

Global Technical Release Manager

April 2016 - July 2017 - LogRhythm Inc. (Hybrid)

Delivered software to customers and internal teams through the development of release consulting, documentation, feedback, User Acceptance Testing, and bug management. Served part-time as TierIV escalations engineer contributing improvements and fixes directly to the core product.

Achievements: Successfully revived and managed the Global Early Access Beta Program into a cross-organizational effort that incrementally introduced software releases while gaining early feedback and re-establishing customer trust. Developed FIPS, High Availability, and Disaster Recovery guides for new next generation deployment architectures. Created Splunk Integration Guide allowing bulk exportation of data from Splunk to LogRhythm and easing the process of migration from our competitor. Co-Rebuilt the Release Champion Program tripling internal content contributions, improving cross-organizational relationships, and chopping our release cycle down from 1 year to 6 months. Co-Managed over 4 new product launches, 5 major and 23 minor relases. Authored Threat Intelligence Provider Service and LogRhythm SIEM to CloudAI integration guides. Continuously provided consultation and optimizations helping to scale beyond the 200k and 300k Messages Per Second benchmarks. Co-Authored and led tiger team in the creation of a comprehensive Advanced Intelligence Engine best practice guide. Earned certifications in Project+.

Skills: *LogRhythm Advanced Intelligence Engine, Splunk, CloudAI, Windows Server, Elasticsearch, PowerShell, Bash, Python, REST, STIX/TAXII, Postman, FIPS, HIPAA, PCI, NIST CSF, Behavioral Analytics, Threat Intelligence Services, Crystal Reports, C2 Auditing, Alarm and Event Mangagement, Syslog, API collection, database collection, file collection, stream collection, data processing analytics and management*

Enterprise Team Lead & Senior Professional Services Consultant

October 2014 - March 2016 - LogRhythm Inc. (Boulder, CO)

Led team that designed, operated, and scaled Security Operations Centers for large enterprise customers. Overcame some of the company’s toughest projects through carefully crafted solution architectures. Provided team management, mentorship, training, and guidance.

Achievements: Successfully lead LogRhythm's largest enterprise deployment consisting of more than 30 Data Indexer, 28 Data processor, 4 Platform Manager, 4 Event Manager, 4 Advance Intelligence Engine(AIE), 4 Metadata, 4 Archival, and 4 Network Monitor servers over the course of a year, reaching 100k and 150k Messages Per Second(MPS) ingestion benchmarks. Significantly reduced correlation gaps in Advanced Intelligence Engine for customers exceeding 90k MPS limit by developing framework for routing events to proper Engine on a per use-case

basis. Invented the Data Dictionary to help customers categorize parsed metadata from hundreds of supported logging sources. Created the TTL Projection Tool to calculate storage usage and requirements based on logging rates and average log sizes. Developed and published the Alarm Best Practices Database and Guide to provide and maintain recommended steps for pre-defined alarms a customer may receive.

Skills: *LogRhythm, SQL Server, Elasticsearch, Powershell, Bash, Windows Server, Microsoft Access, Excel, FIPS, HIPAA, PCI, NIST CSF, NIST 800-53, ISO 27001, Behavioral Analytics, Crystal Reports, C2 Auditing, Alarm and Event Mangagement, Syslog, API collection, database collection, file collection, stream collection, data processing analytics and management*

SIEM Engineer II

April 2014 – October 2014 - Fishnet Security Inc. - Overland Park, KS

Administration, on-boarding, and security consulting for enterprise customers. Improved internal integration services and aided customers in implementing lasting change in their incident, security, and operational processes.

Achievements: Co-Designed comprehensive SIEM/tool agnostic threat defense framework categorizing customer assets into groups for utilization in threat detection rules, reports and filtering. Successfully On-boarded over 12 enterprise SIEM customers each with different architectures, compliances, and use-cases. Earned 2 certification in LogRhythm.

Skills: *LogRhythm, McAfee Nitro, Qradar, IBM Arcsight, SQL Server, compliance consulting, onboarding and integrations, cybersecurity framework creation and implementation, Alarm and Event Mangagement, Syslog, API collection, database collection, file collection, stream collection, data processing analytics and management*

SOC Escalations Engineer

July 2012 – April 2014 - FISHNET SECURITY INC. - Overland Park, KS

Supported enterprise customers with a multitude of perimeter security products.

Achievements: Became sole crossbeam expert and well-known for my firewall kernel debugging expertise. Earned 11 certifications including my CISSP in ISC2, Microsoft, Cisco, Palo Alto, Bluecoat, and Checkpoint.

Skills: *Checkpoint, Palo Alto, JunOS, F5, Semantec, Cisco, BlueCoat, Fortinet, Crossbeam, Bash, Linux*

Network Security Administrator

Jan 2011 – Mar 2012 - Pro Air Inc. – Olathe, KS

Small Business Network and Security Administration while attending night school for cyber security.

Achievements: Earned certifications in networking and hardware. Graduated New Horizon's Cyber Defender Specialty Bootcamp.

Skills: *Cisco, Windows Server, Checkpoint, Microsoft System Center Configuration Manager*

Operations Manager, Systems Administration

Mar 2007 – Aug 2010 - USMC (Marines) – Miramar, CA

Led a team of systems and network administrators deploying and managing military data systems.

Achievements: Earned Two Colonel's coins for the successful rapid deployment of Service Pack 26 across entire west coast fleet of Tactical Battle Management Core Systems. First successful cross-regional HA over SIPRnet VPNs in over three years during single month deployment. Earned Honor Graduate, Top of Class, Iron Man, and Meritorious MAST certifications upon graduating Tactical Data Systems Administrator School.

Skills: *SafeNET VPN, Window Server 2k, SSL Proxy, Cisco Routers, Oracle Database, SAMBA Server, Active Directory, Unix, RAID controllers, VMWare, Air Tracking Software*

Education and Training

Western Governor's University - Bachelor's Degree in Computer Science
Udemy - Data Science Bootcamp
Coursera - Architecting w/ GCP
New Horizons Kansas City - Cyber Defender Specialty Bootcamp
U.S. Marine Corps - Tactical Data Systems Administration School

Certifications

CISSP, ITIL Service Management, Microsoft MCSA & MCSE, Project+, Oracle SQL Assoc, CISCO CCNA. DevOps Foundations, CIW HTML5/CSS3, Net+, A+, Palo Alto CNSE & CNSA, Bluecoat BCCA & BCCP, Checkpoint CCMSE & CCSA & CCSE, LogRhythm LCDE & LCP, Marines Tactical Data Systems Administrator

Published Projects

ML Game Sales Prediction
Dijkstra's Delivery Path Finder
TerraformNginxHADemo
PokemonsterClientAndAPI
AI Career Advice Chatbot
Team Scheduler
Inventory System
Student Roster
EventProcessingArchitecture

Authored Works

EventProcessingServiceArchitecure.md
OLAP_OLEP_OLTP_And_DataMeshes.md
Splunk Integration Guide (authored original version)
LRCloud Original Reference Architectures (authored original version)
Alarm Best Practices Database and Guide
Federal Information Processing Standards (FIPS) (authored 7.x first version)
Custom STIX/TAXII Threat Provider feeds (requires community login)
LogRhythm Diagnostic Module User Guide (authored original version)
Install a LogRhythm HA + DR Combined Solution (authored 7.x first version)
184 posts and 24 solutions on LogRhythm Community (requires community login)