James Clair

Distributed Software and Enterprise Infrastructure Engineer

With 18 years of experience in software engineering, operations, and security, I specialize in microservice development, devops, finops, gitops, secops, observability, data intensive applications, distributed architecture and scalable cloud infrastructures. My extensive background in all aspects of modern enterprise software allows me to drive successful projects and mentor teams to achieve excellence. Let me shape your next-gen architecture to unlock its full potential.

Skills

Development: Data Modeling/Ingestion/Processing, Data Storage/Retrieval/Reporting/Analytics, REST APIs, Relational/Non-Relational Datastores, Enterprise Integration Patterns, Test-Driven Dev, Domain-Driven Design, Event-Driven Architectures, Data Mesh Architecture, Kubernetes Operator Dev, CI/CD, Typed Object-Oriented Languages, Self-Service Infra, AuthN & AuthZ Svc(s), 12-Factor App, Bug Mgmt, Refactoring, Mono-Repo Design, Trunk-based Dev, System Design, Infra & Policy As Code, SLA/SLO/SLI Definition, Config Mgmt, Data Structures & Algorithms
Operations: Relational/Non-Relational Datastores, Customer Support, Alarm/Log/Event/Metric Mgmt, Container Orchestration, Technical Docs, Domain & Layer 1-7 Network Design, Risk Mgmt, Business Intelligence, Object & Block Distributed Storage, Cost Optimization, VPN/Proxy Admin, HA/DR Planning, Scaled Agile Framework, Capacity Planning, Team & Technical Leadership
Security: Threat Intelligence, Vulnerability Mgmt, Domain & Network Security, Security Analytics, Dark-Site Mgmt, Federated AuthN & AuthZ, PKI Mgmt, Zero Trust Architecture, Compliance Mgmt (HIPAA,SOC2,FIPS,PCI,NIST CSF/800-53,ISO 27001), Secrets Mgmt, Static & Run-time Analysis

Tools

Languages & Frameworks: Python, SQL, JavaScript, Bash, Django, Celery, Java, React, Golang, KubeBuilder, Yeoman, FastAPI, Maven, Quarkus, RegEx, Lucene, PromQL, EJS, Jinja, Kustomize, YAML, XML, HTML, CSS, JSON, CSV, C++, Powershell
Data & Secrets Management: PostgreSQL, Elasticsearch, Opensearch, AWS S3, Kafka, Flink, Vault, External Secrets, Etcd, SQL Server, AWS Redshift, Snowflake, Github Secrets, Raft, Consul, LogRhythm AIE, GoPass, Oracle, Excel
Infrastructure & Orchestration: Kubernetes, AWS (EKS, EC2, Lambda, ECR, ControlTower), Terraform, ArgoCD, Kops, Docker, GitHub Actions, Linux, Git, Veracode, Sonarqube, Ansible, Salt, Rundeck, GCP, Windows, SAMBA, VMWare
Networking & Security: Istio, AWS (ELB, VPC, Route53, IAM, Security Groups, SSO), Keycloak, Okta, Pomerium, Certificates Manager, HAProxy, Apache HTTP, Palo Alto, BlueCoat, Checkpoint, F5, Cisco, Wireshark
Monitoring & Logging: Grafana, Prometheus, AWS Cloudwatch, Sentry, StatsD, LogRhythm, Loki, Jaeger, Kiali, AWS Cloudtrail, Sysdig, Status Page, InfluxDB, Telegraf, pager duty, slack

Education & 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

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

Administration School

Professional Experience

Senior Platform Software Engineer - Select Star (Remote)

Jul 2023 - Jan 2024

Designing, refactoring, building, securing, and supporting enterprise pipeline and platform with a focus on collection, ingestion, processing, and analysis of data warehouse and business intelligence data.
Achievements: Enabled asynchronous and parallel data collection and ingestion. Improved pipeline testability by adding an ingested batch persistence layer. Introduced the 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.

Staff Integration Engineer - Solv (Remote)

Feb 2023 - Jun 2023

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.

Tech Lead, Platform Engineering - LogRhythm (Remote/Boulder, CO)

October 2014 - Sep 2022

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: Led 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 CI/CD. 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 CI/CD 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.

Cloud DevOps Engineer III

Served as LogRhythm product expert on the 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 offerings. Automated deployment of LogRhythm core services to Google Cloud Compute environment. Earned certifications in DevOps foundations, ITIL service management, Oracle SQL, and web development.

Global Technical Release Manager

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 releases. 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 the tiger team in the creation of a comprehensive Advanced Intelligence Engine best practice guide. Earned certifications in Project+.

Enterprise Consulting Lead, Professional Services

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 led LogRhythm's largest enterprise deployment consisting of more than 30 Data Indexers, 28 Data processors, 4 Platform Managers, 4 Event Managers, 4 Advance Intelligence Engines(AIE), 4 Metadata, 4 Archival, and 4 Network Monitor servers over the course of a year, reaching record-breaking 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 a framework for routing events to the 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.

Enterprise SIEM Engineer - Fishnet Security Inc (Overland Park, KS)

July 2012 - October 2014

Administration, onboarding, 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 certifications in LogRhythm.

Enterprise Escalations Engineer

Supported enterprise customers with a multitude of perimeter security products including high performance firewalls, proxies, VPNs, and endpoint security.

Achievements: Became the sole crossbeam expert and well-known for firewall kernel debugging expertise. Earned 11 industry leading certifications: CISSP, MCSA, MCSE, CCNA, CNSA, CNSE, BCCPA, BCCPP, CCSA, CCSE, and CCMSE.

Network Security Administrator - Pro Air Inc (Olathe, KS)

Jan 2011 - Mar 2012

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

Achievements:Graduated New Horizon's Cyber Defender Specialty Bootcamp and earned a large number of prestigious industry certifications.

Operations Manager, Systems Administration - USMC (Miramar, CA)

Mar 2007 - Aug 2010

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

Achievements: Earned two Colonel's coins for leading the successful deployment of Service Pack 26 across the west coast. First cross-regional HA over SIPRnet VPNs in over four years. Awarded Honor Graduate, Top of Class, Iron Man, and Meritorious MAST.

Authored Works	Projects
EventProcessingServiceArchitecure.md	My Website
OLAP_OLEP_OLTP_And_DataMeshes.md	ML Game Sales Prediction
Splunk Integration Guide (authored original version)	Dijkstra's Delivery Path Finder
LRCloud Original Reference Architectures	TerraformNginxHADemo
Alarm Best Practices Database and Guide	PokemonsterClientAndAPI
Federal Information Processing Standards (FIPS)	AI Career Advice Chatbot
Custom STIX/TAXII Threat Provider feeds	Team Scheduler
LogRhythm Diagnostic Module User Guide	Inventory System
Install a LogRhythm HA + DR Combined Solution	Student Roster
184 posts and 24 solutions LR Community (requires login)	