Last updated in Feb 2026

Don Reece

DevOps Engineer | Python & Data Pipeline Development | Cloud Infrastructure & Automation

Detroit, MI   don@reece.cc   (231) 758-2183   donreecejr

Competencies

- ETL Pipeline Development & API Integration (Prefect, Python, REST APIs, data transformation)
- Python Development & Scripting (5+ years)
- Enterprise Platform Integration (SOAR, SIEM, SSO, Identity Management)
- Cloud Infrastructure & Container Orchestration (AWS, Docker, Kubernetes)
- AI/ML Integration & LLM Application Development (RAG, OpenAI, Claude)

Education

Lawrence Technological University, BS in IT — Sept 2010 – Sept 2014

Experience

Principal DevOps Engineer, Surefire Cyber – Remote — July 2023 – Jan 2026

- Architected and built end-to-end Incident Response Platform using AppSmith on AWS infrastructure with Docker and Kubernetes, supporting 20+ concurrent cases across DFIR operations, including resource allocation dashboards for PM team
- Built ETL pipelines using Prefect and NodeRED to extract data from enterprise APIs (SentinelOne, Hubspot, QuickBooks Online, Oracle NetSuite), transform metrics, and load into centralized dashboards, automating data collection across security, finance, and marketing systems
- Developed data transformation pipelines in Python that extracted raw threat actor file listings, transformed unstructured data into formatted reports for client deliverables, and reduced incident analysis time from 2-3 hours to 15 minutes
- Led platform modernization initiative with senior engineering team to migrate IRP to scalable architecture with proper APIs and databases, reducing page load times by 50%+
- Developed AI/LLM-powered automation systems including RAG-based threat intelligence analysis tools and report generation that automated data extraction from investigations and matched company writing standards, reducing incident response preparation time by multiple hours per week
- Evaluated and integrated multiple LLM providers (OpenAI, Anthropic Claude, open-source models) to assess capabilities for workflow automation and data processing use cases

Team Lead, Incident Response DevOps, Tetra Defense – Remote — Nov 2019 – July 2023

- Led dev team building Python applications and integrations in IBM QRadar SOAR (SentinelOne, malware sandboxes, threat intel feeds)
- Implemented SumoLogic log aggregation with real-time Slack alerts and automated incident creation in SOAR
- Built centralized DFIR evidence system in IBM QRadar SOAR as single source of truth for investigations
- Developed custom Ubuntu ISO for DFIR evidence gathering and PowerShell scripts for remote forensic triage
- Deployed and managed SentinelOne EDR for IR clients and conducted on-site incident triage at client locations

Information Security Consultant, eSentire – Remote Feb 2019 – Nov 2019

- Deployed and configured SumoLogic SIEM platform for enterprise clients, managing technical onboarding from planning through production
- Built custom SumoLogic content (parsers, alerts, dashboards) and automated log source onboarding for client SIEM deployments
- Developed PowerShell and Python scripts to automate log retrieval, reporting, and configuration management

Senior Security Operations Lead, Molina Healthcare – Troy, MI July 2015 – Feb 2019

- Deployed and configured Co3 Systems Resilient incident response platform (later renamed to IBM QRadar SOAR) with automated incident creation from SIEM alerts and custom parsers for evidence collection
- Managed enterprise security stack (BlueCoat proxy, FireEye appliances, RSA SIEM) supporting 20,000+ users across multiple locations

Skills

Languages: Python, PowerShell, Bash, Batch, JavaScript

Security & APIs: SentinelOne (EDR & API), IBM QRadar SOAR, SumoLogic, REST APIs, Hubspot, Oracle NetSuite, QuickBooks Online

AI & Machine Learning: LLM integration (OpenAI API, Anthropic Claude), RAG systems, vector stores, prompt engineering, AI-powered automation

Infrastructure & Automation: AWS, Docker, Kubernetes, Terraform, Prefect, n8n, NodeRED, PostgreSQL, AppSmith, JumpCloud, Git, Linux administration