

Chris Turner

Tech Blogs: <https://cat-ai.io/blog>

Linkedin Page: [linkedin.com/in/christopher-turner-61b3894b](https://www.linkedin.com/in/christopher-turner-61b3894b)

Portfolio Site: <https://cat-ai.io/>

Github Repos: <https://github.com/jitter-ai>



Splunk Engineering & Generative AI Integration

Splunk Enterprise • Splunk Enterprise Security (ES)

- **Designing AI/ML and Generative AI-enhanced SIEM architectures** that merge detection, observability, and automation.
- Integrating **Retrieval-Augmented Generation (RAG)**, large language models (LLMs), and agentic Splunk bots for real-time incident analysis, narrative generation, and context-aware search.



PROJECTS & CODE REPOSITORIES

Featured Projects & Platforms

PwC AI/ML & Generative AI-Augmented Splunk

- Unified Splunk, AWS Bedrock, and OpenSearch for LLM-driven correlation, automation, and real-time summarization

Real-Time Sentiment Insights

- AWS pipeline using **Comprehend** and **OpenSearch** for streaming sentiment analytics with Terraform automation.
- github.com/jitter-ai/aiml-realtime-opensearch-comprehend-sentiment-insights

Real-Time AI Fraud Detection Pipeline

- Serverless **AI/ML fraud scoring** with **Kinesis**, **Fraud Detector**, **OpenSearch**, and **Splunk** for multi-sink analytics
- github.com/jitter-ai/aws-realtime-ai-fraud-pipeline



AWS Skill Builder & PartnerCast Sessions

AI-Driven Cyber Insights: Generative AI for Splunk Powered by OpenSearch

- **Demonstrated how to apply Generative AI and machine learning** for Splunk security analytics using **OpenSearch** and **SageMaker**, enabling AI-driven threat detection and conversational security insights

Presentation: <https://vimeo.com/1104611723>

Demo: <https://vimeo.com/1104611963>

Real-Time Threat Detection with Amazon



AWS Skill Builder & PartnerCast Sessions

OpenSearch Security Analytics

- **Built a unified SIEM solution** integrating **Splunk** and **OpenSearch** with **OCSF** normalization for real-time threat detection and automated incident response.

Presentation: <https://vimeo.com/1104592171>

Demo: <https://vimeo.com/1104592118>

Advanced Fraud Detection with AWS

- **Architected a real-time fraud detection system** using **MSK**, **Kinesis**, **OpenSearch**, and **Fraud Detector** for streaming analytics and AI-driven risk scoring.

Presentation: <https://vimeo.com/1104604778>

Demo: <https://vimeo.com/1104604690>



AI/ML Engineering, Automation & Skills

Splunk Architecture & Engineering

- Architecting **enterprise-scale Splunk environments** for security, observability, and data analytics- covering **indexer clustering**, **search head architecture**, and **forwarder management**.
- Developing **advanced detections, correlation searches, dashboards, and SPL logic** that transform data into actionable security insights.
- Implementing **data onboarding, CIM normalization, and ingestion pipelines** integrating cloud, endpoint, and identity telemetry.
- Automating **Splunk deployment and configuration** using **Terraform**, Git-based workflows, and modularized app packaging for repeatable, version-controlled delivery.

AI/ML & AWS Integration

- Extending Splunk with **AI/ML pipelines and Generative AI** for anomaly detection, enrichment, and natural-language search.
- Integrating **AWS services** such as **SageMaker**, **Bedrock**, **Glue**, and **Kinesis** to enable streaming analytics, predictive modeling, and scalable data pipelines

Explore full skill set: <https://cat-ai.io/skills/>