

Christopher (Chris) Turner

Profile

Former professional baseball player turned **AI/ML and cybersecurity leader** (ex-AWS, ex-Yahoo, Booz Allen) with 15+ years across the full cyber stack: **IAM (SailPoint)** at Centene, **nation-state APT and OSINT investigations** at Citibank, **Splunk-powered Cyber Fusion Centers** for DHS, Yahoo, and Toyota at Booz Allen, then **AWS Splunk and OpenSearch SME** leading Fortune 500 migrations and speaking at **re:Invent and Splunk .conf**.

Now applies that foundation to **agentic SecOps**: multi-agent systems (**MCP, RAG, LLMs, AgentCore**) that turn fusion investigations into AI-assisted reasoning with **autonomous triage, enrichment, and human-on-the-loop oversight**. Use cases span **insider threat** (DLP fused with badge and physical signals), **OSINT and dark-web intelligence, fraud and financial crime** (synthetic identity, mule detection), **GenAI incident response, ATT&CK-mapped threat hunting**, and **cloud control-plane analytics** (CloudTrail, GuardDuty, Security Lake) across Splunk, Palantir, and OpenSearch. Focused on moving regulated and defense environments from SIEM analytics to **secure, auditable autonomous investigation**, from Bedrock and Nova to open source models on **EKS and air-gapped on-prem**

Social Media

 LinkedIn

 Medium Tech Blog (Pending)

 Public Github

 Portfolio Site (Card)

Work Experience

10/2025 – 08/2026
Remote, Global

Senior Manager - Generative AI Engineering - Automation and Cognitive Solutions
PwC

Enterprise Generative AI & Cyber Engineering: Led enterprise Generative AI, cyber analytics, Splunk, and data engineering initiatives for regulated finance, healthcare, and government clients, architecting agentic AI systems, SIEM/cloud-native modernization, and AI governance, owning the relationship between the AI platforms and the business and mission teams using them from first training session through ongoing use; partnered with business owners and end users to map current-state processes, understand where teams struggled to apply AI, quantify inefficiencies, and prioritize high-impact use cases; embedded ML, LLMs, and agentic reasoning into Splunk Cloud and cloud-native ecosystems; designed secure, auditable architectures uniting LLMs, RAG pipelines, custom agents, real-time cyber/risk analytics, OpenSearch, Redis, and Amazon Bedrock; unified Palantir, Splunk, and OpenSearch threat data into shared analytics layers and built custom ontology models powering OSINT search and investigative/threat intelligence workflows.

Agentic Threat Operations: Applied AI anomaly detection, threat modeling, and policy-aware reasoning to autonomous alert triage, enrichment, and investigation with human-on-the-loop oversight; integrated LLM enrichment and model-based alerting into Splunk/Palantir SOC streams with vector retrieval for continuous monitoring; built multi-agent systems using CrewAI, LangGraph, LangChain, and MCP for contextual retrieval, tool calling, and policy enforcement; exposed Splunk searches and triage actions through custom MCP servers and Bedrock AgentCore Gateway for AWS threat detection, enrichment, response, and human-readable incident narratives; worked alongside SOC analysts and investigators to understand where alert fatigue and manual triage slowed them down, designed agent workflows around how they actually worked, and built a reusable library of prompt patterns, agent templates, and playbooks teams could pick up directly.

Splunk Detection & Data Architecture: Integrated LLMs with Splunk using LangChain and Bedrock for natural-language-to-SPL, so analysts without SPL expertise could search and investigate in plain English, automated correlation, and insight summarization; implemented CIM-normalized data models, correlation searches, risk-based alerting, and embedded ML anomaly detection in Enterprise Security for higher-fidelity alerts; engineered Cribl Stream and Fluent Bit pipelines to route, reduce, and enrich telemetry pre-index to lower license costs; implemented S3/Apache Iceberg tiering with Federated Search reach-back and tiered Splunk/OpenSearch architectures supporting zero-loss cutovers, schema evolution, replay/backfill, and offloading vector/warm-tier workloads

Work Experience

while retaining Splunk as the detection core.

AWS Data, MLOps & Cloud Engineering: Architected AWS-native data pipelines using Glue and modern cloud data services, including scalable data lake/warehouse platforms optimized for lineage, security, and regulatory compliance; implemented Terraform, AWS CDK, CloudFormation, CodeBuild, and CI/CD for reproducible containerized Splunk and AI workloads; built FastAPI and Kubernetes/EKS GenAI microservices with telemetry, evaluation, and model observability using Langfuse and Portkey, using usage and evaluation data to track adoption and see where outputs fell short for users, and serving as the primary channel bringing user feedback back to product, engineering, and design.

AI Governance, Security & Compliance: Implemented Bedrock Guardrails, AgentCore policy controls, IAM role segregation, encryption at rest/in transit, and cloud-native identity controls supporting HIPAA and FedRAMP environments; hardened AI agents against prompt injection and tool misuse using OWASP LLM Top 10 and MITRE ATLAS; aligned AI architectures with enterprise risk, security, governance, and compliance frameworks; helped teams understand AI capabilities and limits within privacy, security, and responsible-use constraints so they could adopt AI with confidence.

Technical Leadership & Delivery: Hired and led data scientists, AI engineers, cloud engineers, and cybersecurity architects applying ML and GenAI to detection logic, performance tuning, decision automation, threat intelligence, and Splunk observability; served as hands-on technical leader architecting systems, writing production code, and leading end-to-end delivery of AI-driven cyber, threat intelligence, data, and observability platforms for government, finance, and healthcare clients; ran onboarding sessions, office hours, hands-on demos, and team-specific training tailored to how each group worked; coached delivery teams and stakeholders on AI adoption, translated technical capabilities into business value for leadership, and measured adoption after go-live.

Previous Experience

02/2022 – 10/2025

Global

AI/ML & Data Analytics Solution Architect

Amazon Web Services (AWS)

OpenSearch & Splunk SME, Customer Discovery: Recognized Amazon OpenSearch and Splunk SME, advancing neural, multimodal, and hybrid (BM25 + neural reranking) search and contextual ranking with platform engineering; directed global OpenSearch initiatives delivering AWS-native analytics and AI/ML to Fortune 500 clients; served as trusted technical advisor running discovery sessions with business, security, and analytics stakeholders to understand how their teams worked, where they struggled to apply AI/ML, and which use cases would deliver the most value, and channeled customer and partner feedback back to OpenSearch and Bedrock service teams to shape product roadmap.

Enterprise Migrations & GenAI Delivery: Led Splunk-to-OpenSearch migrations and AI-driven security solutions for Western Union, Citibank, Adobe, Yahoo, and Capital One; delivered search and GenAI solutions for Zscaler, American Express, McKinsey, Cisco, and Redpanda, starting each engagement by mapping existing analyst and business processes with the teams who would use the systems and staying engaged from first session through production rollout and ongoing use.

Insider Threat & Detection Engineering: Built Splunk UBA and detection pipelines, modeling badge, Slack, endpoint, and SailPoint identity telemetry to detect lateral movement and insider threats; correlated CrowdStrike, Tenable, and identity data against MITRE ATT&CK, NIST, and CIS; embedded SageMaker models and LLM endpoints in dashboards for threat scoring; designed detections around how SOC analysts and insider-threat investigators actually triaged cases.

Splunk Tooling & Detection-as-Code: Engineered Splunk tooling and detection-as-code, building Python add-ons, alerting, ingest parsers, and normalization frameworks (HEC, Kinesis, Logstash, S3) with GitHub Actions, Terraform, and Python for version-controlled knowledge objects.

MLOps & Data Platforms: Designed MLOps and data platforms on MLflow, Apache Spark, Airflow, Kubeflow on EKS, and SageMaker Pipelines for batch training, real-time inference, automated retraining, and lineage; containerized ML with Docker, GitHub Actions, and ECR; petabyte-scale event pipelines on AWS Glue, Apache Iceberg, and Delta-style data lakes feeding Spark feature engineering across AWS and on-prem.

Previous Experience

Enterprise RAG & LLM Systems: Developed enterprise RAG and LLM systems with LangChain, Amazon OpenSearch, GPT-4, and Claude for semantic search, summarization, and document intelligence; Redis-backed vector memory and conversational cache; AWS CDK stacks for one-click Bedrock + OpenSearch RAG environments; fine-tuning and inference at scale with Hugging Face Transformers, SageMaker Hugging Face containers, and SageMaker Studio; Python NLP pre/post-processing (chunking, embeddings, entity extraction) with tool-calling hooks; optimized prompt libraries, caching, streaming, async retrieval, and index tuning; paired with customer teams on prompt design and evaluation so they could extend and operate the systems themselves.

GenAI Reliability & Evaluation: Established GenAI reliability and evaluation practices, defining SLOs (latency budgets, throughput, cost controls); bias, drift, and regression detection via SageMaker with Grafana/Prometheus dashboards; A/B evaluation harnesses for retrieval quality, policy adherence, and hallucination reduction; Guardrails.ai safe-completion policies on GPT-4 outputs, cutting manual review cycles 60% after studying how reviewers used and corrected model outputs.

Enablement, Training & Adoption: Mentored teams and led public enablement on prompt engineering, RAG architecture, NLP, and evaluation frameworks, codifying reference designs and playbooks; presented at AWS re:Invent, Splunk .conf, and PartnerCast; built hands-on workshops teaching enterprise teams to operationalize LLM-enhanced detection and investigation; led proof-of-concepts, immersion days, office hours, and follow-up sessions tailored to each team, built reusable prompt libraries and agent templates teams could pick up directly, and tracked adoption after rollout.

01/2019 – 02/2022

Mgr. Cyber Analytics & Solutions Development @ Yahoo | Toyota | Dept. Homeland Security

Booz Allen Hamilton

- **Managed and matured cybersecurity architecture and data engineering** for Booz Allen's Commercial Cyber Fusion Center (CFC), leading enterprise-scale Splunk deployments (AWS/on-prem), integrating CrowdStrike, and developing advanced analytics, dashboards, security essentials, and automated workflows for threat detection, rapid response, incident management, and vulnerability assessments
- **Engineered AWS-based AI/ML-driven cyber intelligence capabilities**, creating data-driven analytics and machine-learning models to proactively detect sophisticated cyber threats, anomalies, and TTPs from diverse threat actors (nation-state, criminal, hacktivist); collaborated with cross-functional teams (cybercrime, e-crime, government, intelligence)
- **Provided senior leadership, strategic oversight, and technical mentorship**, leading cybersecurity engagements, proposal development, client presentations, risk identification and mitigation, attack surface management, and utilization of collaboration platforms (Jira, ServiceNow, Confluence), enabling cybersecurity program maturity, threat intelligence, and enhanced decision-making for commercial and government clients

03/2018 – 01/2019

Tampa, United States

Global Cyber Investigative Intelligence/Cyber Analytics Sr. Program Lead Citibank

- Led data science and machine learning initiatives for a Global Cyber Investigative Intelligence program; developed cyber intelligence, OSINT, investigative analytics, and threat intelligence using data lake architectures for efficient analysis.
- Tracked nation-state actors/APTs by analyzing SOC reports to identify tactics, techniques, and procedures (TTPs); conducted cyber threat research, including dark web analysis, forensic data evaluation, and penetration test reviews to detect security gaps.
- Enhanced cybersecurity analytics by quantifying cyber intelligence into mathematical models; applied GDPR knowledge to implement security controls for EU data compliance, and recommended actionable controls for security improvements.

11/2015 – 03/2018

Tampa, United States

Senior Security Engineer/Analyst Centene

Identity and Access Management (IAM) with SailPoint

- Delivered comprehensive IAM solutions integrating critical infrastructure with SailPoint IdentityIQ, automating role assignments and policy enforcement.
- Drove best practices in Role-Based Access Control (RBAC), creating custom IAM attributes and security policies within SailPoint to effectively manage access risk and compliance.

 Previous Experience

01/2013 – 11/2015	Infrastructure IT Support Raymond James Financial
06/2007 – 06/2009	Minor League Professional baseball player Houston Astros Minor League

 Strength & Skills

– CYBERSECURITY, INTELLIGENCE & COMPLIANCE		
Splunk, CrowdStrike, SailPoint IdentityIQ, Tenable, Proofpoint, Palantir, Cribl, Kali Linux, AWS Security Services (GuardDuty, Security Hub, Security Lake)	Cyber Fusion Development, Security Analytics (SIEM), Threat Intelligence, Threat Hunting, Insider Threat, Fraud Detection, Metasploit, Maltego	Cyber Investigations, OSINT, All-Source Intelligence, MITRE ATT&CK, MITRE ATLAS, NIST, CIS, OWASP LLM Top 10, IAM/RBAC, HIPAA, HITRUST, FedRAMP, GDPR
– AI/ML, DATA & CLOUD ENGINEERING		
Generative AI, Agentic AI, AI Adoption & Enablement, RAG, LLM, NLP, Text Extraction, LangChain, LangGraph, MCP, Hugging Face, TensorFlow, PyTorch, Predictive Modeling Professional	Amazon Bedrock, Bedrock AgentCore, Amazon Nova, SageMaker Studio, OpenSearch, Glue, AWS HealthLake, Amazon Comprehend Medical, FHIR, PHI De-identification Professional	Python, SQL, Pandas, NumPy, Kinesis, MSK, ETL Pipelines, Streaming, Terraform, AWS CDK, CloudFormation, CodeBuild, CodePipeline, CI/CD Automation Professional

 Achievements

- AI/ML, Analytics & Enablement Leadership** - Led 150+ strategic partner and client engagements across AI/ML, data analytics, and cybersecurity, including IBM’s EMEA cybersecurity restructuring and PwC’s Cyberfusion Center; mentored 50+ mentees, onboarded hundreds of AWS partners, and trained ~1,000 AWS employees. Built an internal Generative AI Salesforce analytics tool, transforming opportunity management and strategic forecasting with LLM-powered insights.
- AWS Technical Content Creation & Public Enablement** - Featured presenter and technical content builder at AWS re:Invent (2023–2024), Splunk Conference 2024, and AWS Summit, focused on generative AI, cybersecurity, and data platforms. Developed hands-on labs and technical enablement content across AWS Workshop Studio, Solutions Library, and GitHub Samples.
- AWS Skill Builder - PartnerCast Series (2023–2024)** - Delivered global technical PartnerCast sessions on advanced fraud detection, real-time threat analytics, and LLM-enhanced search with OpenSearch, SageMaker, and Bedrock. Sessions include:
- **Advanced Fraud Detection with Amazon Kinesis, MSK, OpenSearch & Fraud Detector**
 - **Enabling Semantic Search with OpenSearch & Amazon SageMaker**
 - **Advanced Search with LLMs in OpenSearch & Bedrock**
 - **Generative AI for Splunk: Cyber Insights with OpenSearch**
 - **Real-Time Threat Detection with OpenSearch Security Analytics**
-  Education
- University of South Florida, Tampa, FL
Master of Science (M.S.), Cybersecurity (Cyber Intelligence)
Bachelor of Arts (B.A.), Criminology
- Hillsborough Community College, Tampa, FL
Associate of Science (A.S.), Network Security & Digital Forensics
-  Certificates
- AWS Certified: AWS Data Analytics, AWS Solutions Architect, AWS Associate, Developer Associate, Cloud Practitioner • Splunk Power User