Chris Turner

Phone Number: 813-732-8242 **Email:** christurner813@gmail.com

PROFILE

Former professional baseball player turned cybersecurity and Splunk expert with 15+ years of experience delivering advanced Splunk-based analytics, AI-enhanced SIEM solutions, and enterprise-scale cybersecurity architectures. Proven Solutions Architect specializing in Splunk Enterprise deployments, Splunk-to-Enterprise SIEM migrations, AI-driven threat detection, User Behavior Analytics (UBA), and advanced analytics automation. Recognized AWS-backed Splunk SME, skilled at integrating AI and machine learning techniques into cybersecurity workflows, real-time analytics, and threat intelligence platforms. Experienced technical content creator, Splunk Conf speaker, and mentor, passionate about driving strategic innovation through Splunk engineering, advanced detection logic, and scalable analytics platforms.

SOCIAL MEDIA

Linkedin

AWS Github Public Profile

Medium Professional Tech Content

Personal Github Public Profile

WORK EXPERIENCE

AI/ML & Data Analytics Solution Architect
Amazon Web Services (AWS)

02/2022 – present **REMOTE, USA**

AI-Augmented Splunk Engineering, Cybersecurity Analytics, and SIEM Innovation

- Led the integration of AI and machine learning pipelines within Splunk Enterprise, leveraging Python, Amazon SageMaker, vector search, and large language models (LLMs) to deliver context-rich threat detection, predictive analytics, and behavioral insights.
- Developed and deployed advanced User Behavior Analytics (UBA) models in Splunk using badge logs, Slack, endpoint telemetry, and identity-management data (SailPoint) to proactively detect lateral movement, insider threats, and anomalous behaviors.
- Architected AI-driven cybersecurity solutions for enterprises including **Western Union, Citibank, Adobe, Yahoo, and Capital One**, improving threat detection accuracy, search performance, and operational response times.
- Engineered and automated Splunk analytics pipelines, integrating CrowdStrike, Tenable, and identity telemetry for real-time threat correlation and detection, driving alignment with MITRE ATT&CK, NIST, and CIS frameworks.

Technical Leadership, Detection Engineering, and Public Enablement

- Presented cutting-edge approaches at industry conferences including Splunk Conf, AWS re:Invent, and PartnerCast, demonstrating practical integration of Generative AI, LLMs, and advanced analytics directly into Splunk workflows.
- Created comprehensive, hands-on workshops and technical training sessions focused on Splunk and AI integrations, teaching enterprise teams how to operationalize LLM-enhanced detection and investigation capabilities.
- Led AWS PartnerCast sessions dedicated to Splunk technologists, with topics covering:
- "Generative AI-Enhanced Detection in Splunk: Accelerating Threat Intelligence"
- "Building Automated UBA with Python and Splunk: From Raw Telemetry to Insightful Context"
- "Scaling Splunk Deployments with Python-Based CI/CD Automation"

AI Engineering, CI/CD Automation, and Advanced Splunk Deployment

- Deep technical expertise in Splunk Core/Enterprise architectures, Python scripting, REST API automation, and detection engineering.

WORK EXPERIENCE

- Skilled in building custom, Python-based Splunk add-ons, alerting logic, ingest parsers, and data normalization frameworks (HEC, Kinesis, Logstash, S3).
- Expert in defining and automating CI/CD pipelines for Splunk asset management and detection-as-code, utilizing GitHub Actions, Terraform, and Python scripting for vrsion-controlled knowledge objects.
- Experienced integrating AI/ML models and LLM inference endpoints within Splunk dashboards, enabling real-time analytics, enhanced threat scoring, and predictive insights.

PREVIOUS EXPERIENCE

Mgr. Cyber Analytics & Solutions Development @ Yahoo | Toyota | Dept. Homeland Security
Booz Allen Hamilton
01/2019 – 02/2022

- **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

Global Cyber Investigative Intelligence/Cyber Analytics Sr. Program Lead
Citibank
03/2018 – 01/2019 **TAMPA, UNITED STATES**

- 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.

Senior Security Engineer/Analyst
Centene
11/2015 – 03/2018 **TAMPA, UNITED STATES**
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.

Infrastructure IT Support
Raymond James Financial
01/2013 – 11/2015

Minor League Professional baseball player
Houston Astros Minor League
06/2007 – 06/2009

STRENGTH & SKILLS

AI/ML, GENERATIVE AI & DATA ENGINEERING

Amazon Nova, SageMaker Studio, Generative AI, Agentic AI, Predictive Modeling

Amazon Bedrock, Semantic Search, Neural Search, LLM Integration, Streaming, LangChain

Elasticsearch/OpenSearch, Glue, Athena, Data Lake, Kinesis, MSK, ETL Pipelines, Amzazon AI Services

SECURITY, INVESTIGATIVE & LOG ANALYTICS

Graylog, CrowdStrike, SailPoint, Tenable, Proofpoint, Splunk

Kali Linux, Metasploit, Maltego, OSINT, Cyber Investigations, Hadoop, AWS Security Services

NLP, Text Extraction, Fraud Detection, OpenSearch Ingestion Pipelines

CYBERSECURITY & INTELLIGENCE

Cyber Fusion Development, Security Analytics (SIEM), Cyber Investigations

Threat Intelligence, Threat Hunting, Fraud Detection

Open Source Intelligence (OSINT), All-Source Intelligence

DEVOPS, PROGRAMMING

Terraform, AWS CDK, CloudFormation, Ruby CodeBuild

Python, SQL, PowerShell, Pandas, NumPy, CodePipeline

CI/CD Automation, TensorFlow, PyTorch, Hugging Face

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

EDUCATION

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