CHRIS McMILLON

Security Engineer | AI-Augmented Security Systems | Cloud Security Operations

Seattle, WA | 702-530-6401 | stealinglight@gmail.com | linkedin.com/in/cmcmillon | cm-sec.ai

SUMMARY

Security Engineer with hands-on experience building AI-augmented security systems at enterprise scale. Currently developing automation and agentic AI solutions on AWS Security's Operational Research & Development team, integrating large language models into incident response, threat detection, and security validation workflows. Background spans cloud security operations, incident response, SOC analysis, and security tooling development. Strong engineering fundamentals with a track record of shipping production systems that reduce response times, improve detection capabilities, and scale across distributed infrastructure.

TECHNICAL SKILLS

Security Operations: Incident Response, Threat Detection, Security Automation, Alert Triage, Playbook Development, Anomaly Detection, Log Analysis, Splunk, SIEM, Cloud Security Posture

AI/ML & LLM: LLM Integration & Orchestration, Agentic AI Systems, MCP Server Development (FastMCP), Amazon Bedrock, Claude, Prompt Engineering, RAG Architectures, AI-Augmented Security Workflows

Languages & Tools: Python, TypeScript, Golang, SQL, AWS CDK, Step Functions, Lambda, REST APIs

Cloud & Infrastructure: AWS (IAM, Lambda, DynamoDB, S3, Step Functions, SNS, API Gateway, Bedrock, EKS/Kubernetes), Distributed Systems, Event-Driven Architecture, Infrastructure as Code

PROFESSIONAL EXPERIENCE

Amazon Web Services (AWS) | Seattle, WA

Security Engineer – Operational Research & Development | June 2025 – Present

- Build security tooling and APIs for AWS Security Operations organizations, connecting large-scale data pools and enabling cross-team data enrichment for tier 2 escalations and investigation workflows
- Design and deploy multi-agent AI workflows using Amazon Bedrock, including self-evaluating and self-learning agent architectures that improve detection accuracy and response quality over time
- Architect production-ready data collection, enrichment, and security tooling pipelines, ensuring secure handling of sensitive datasets across distributed infrastructure
- Conduct Tier 2 security response escalations while developing AI-augmented tooling to streamline responder workflows and detection capabilities
- Build MCP servers using FastMCP to expose security operations tooling to AI agents, enabling seamless integration between LLMs and internal security platforms
- Collaborate across security operations, platform, and data teams to deliver tooling that integrates with existing security workflows, providing regular updates to senior security leadership on tool adoption and operational impact

Security Engineer – Cloud Security Response Platform & Tooling | Dec 2024 – June 2025

- Integrated large language models into security validation processes, automating effectiveness assessment of proposed security solutions and detection rules
- Expanded advanced search and analysis features for security platforms, enabling faster threat hunting and investigation capabilities across distributed systems
- Developed API-driven decision services and event-driven automation patterns for cross-functional security teams, improving response coordination
- Collaborated with platform, data, and security teams to demonstrate LLM integration capabilities and incorporate stakeholder feedback into production tooling

Security Engineer – Data Enrichment & Automation | Apr 2024 – Dec 2024

- Operated within the Cloud Security Response organization, building automation and analysis tooling to support frontline incident responders and coordinating with cross-functional teams on high-priority investigations

- Developed Splunk queries and Python-based analysis pipelines to extract actionable intelligence from large-scale security datasets, identifying anomalies and recurring threat artifacts
- Built and executed broad-scope security scans across AWS infrastructure to surface anomalies and potential indicators of compromise at scale
- Designed repeatable automation workflows and playbooks using Lambda, Step Functions, and DynamoDB, enabling responders to consistently triage and investigate recurring incident patterns
- Supported leadership escalations by preparing data-driven findings and analysis summaries for senior security leadership review and decision-making

Cloud Security Responder | Nov 2023 – Apr 2024

- Served as first-line incident responder for AWS Security, triaging and driving remediation of security incidents across the full breadth of AWS services and cloud infrastructure
- Coordinated directly with service teams across AWS to contain threats, perform root cause analysis, and drive mitigation through to resolution across a wide scope of security issues
- Processed and actioned bug bounty reports, red team findings, CVEs, and security embargoes, ensuring timely response and appropriate escalation
- Drove cross-organizational coordination on high-severity incidents, escalating to and briefing senior security leadership on active threats, impact assessments, and remediation status
- Developed response playbooks for recurring incident patterns, improving consistency and speed of future response efforts

CloudOps Security Engineer (Team Lead) | May 2022 – Nov 2023

- Led security operations team managing real-time incidents for AWS CloudOps, mitigating threats across enterprise infrastructure
- Developed automation scripts and tooling to optimize security alert triage, reducing operational workload by automating repetitive detection and response tasks
- Created and maintained incident response procedures and runbooks, driving continuous improvement in response metrics

Olezka Global | Las Vegas, NV

Security Operations Center Analyst | Dec 2021 – May 2022

- Monitored and responded to security events across enterprise environments using CrowdStrike EDR, Tenable, and Fortinet SIEM
- Conducted security assessments, performed root cause analysis, and coordinated incident response with internal and external stakeholders

Caesars Entertainment | Las Vegas, NV

IT Support Specialist II | July 2021 – Apr 2022

- Delivered technical support across casino and hospitality properties spanning POS systems, banking and compliance software, gaming technologies, networking infrastructure, and office systems
- Supported diverse operational environments including restaurants, retail, call centers, and large-scale special events such as the World Series of Poker, managing everything from backup tapes and peripherals to event-specific technology deployments

EDUCATION

Bachelor of Science, Cybersecurity & Networking (Minor: Data Science)
University of Maryland Global Campus

Associate of Arts and Sciences, Cybersecurity
Northern Virginia Community College