



DRUMIN GAJJAR

 [linkedin.com/in/drumin](https://www.linkedin.com/in/drumin) |  gajjar.drumin@gmail.com

PROFESSIONAL SUMMARY

AI Security Engineer owning MasterControl's AI security program from strategy to execution. Leading LiteLLM gateway and Onyx guardrails deployment, enforcing organizational wide AI governance through Netskope and Acceptable Use Policy and building detection coverage for prompt injection, data leakage and shadow AI across internal and customer facing environments.

TECHNICAL SKILLS

Languages: Python, Bash, SQL, YAML, Java, C

Platforms: AWS, Kubernetes, Claude Code

Tools: Wiz, Tenable, Jira, Terraform, Domo, GitHub, LiteLLM

Domains: Cloud Security, FedRAMP, AI Security

EXPERIENCE

MasterControl, Inc.

AI Security Engineer

Jun 2026 – Present

Salt Lake City, UT

- Owning MasterControl's AI security program end-to-end, formalizing the AUP and developer security training.
- Deploying LiteLLM Enterprise and Onyx guardrails to secure LLM traffic, enforcing policy-compliant AI usage.
- Enforcing AI governance by blocking unauthorized AI tools org-wide via Netskope, eliminating shadow AI and data exposure.

MasterControl, Inc.

Cloud Security Engineer

Feb 2025 – Jun 2026

Salt Lake City, UT

- Driving adoption of an AI guardrails platform to enforce policy-compliant AI usage and prevent prompt injection and data leakage.
- Deployed Wiz Admission Controller to validate signed container images and enforce workload integrity in Kubernetes.
- Built multi-agent security workflows in Claude Code to automate RRAs, code reviews, and vulnerability assessments.

MasterControl, Inc.

Security Engineer Intern – Cloud Security & Vulnerability Management (FedRAMP)

May 2024 – Dec 2024

Boston, MA

- Conducted vulnerability assessments with Tenable and Wiz on AWS infrastructure to maintain FedRAMP compliance.
- Authored custom Wiz detection rules for malicious activity, improving asset visibility and accelerating incident response.
- Led scanning coverage initiatives and coordinated vulnerability detection for AWS assets during STIG audits.

MasterControl, Inc.

Security Engineer Intern – Security Operations

July 2023 – Dec 2023

Boston, MA

- Deployed NIDS and Honeypots within a FedRAMP environment to strengthen threat visibility and early detection capabilities.
- Validated SIEM and CrowdStrike detection rules via adversary simulation, identifying coverage gaps and improving accuracy.
- Built real-time Domo dashboards for executive security visibility, enabling data-driven decision-making for stakeholders.

Larsen & Toubro Infotech Limited

Summer Intern

May 2021 – Jul 2021

Mumbai, India

- Designed real-time traffic analytics solutions for India's Smart City Mission, enabling data-driven decisions for city authorities.
- Built Python automation scripts to process social media data streams, updating traffic congestion metrics hourly in SQLite.

PROJECTS

CI/CD Pipeline Security Automation with Semgrep

Sept 2024 – Nov 2024

- Programmed a GitHub Action to automate static code analysis with Semgrep, integrating custom rules into CI/CD pipelines.
- Implemented a gating mechanism to block merges on detected vulnerabilities, enforcing security compliance pre-production.

Secrets Detection Tool

Aug 2024 – Sept 2024

- Built a Python secrets detection tool to identify exposed credentials, simulating attacker reconnaissance across large codebases.
- Integrated live API validation to filter expired tokens, improving detection precision across large codebases.

EDUCATION

Northeastern University

Master of Science in Cybersecurity

Sep 2022 – Dec 2024

GPA: 4.0 / 4.0

NMIMS University

B.Tech in Information Technology with Honors in AI/ML (in partnership with IBM)

Jul 2018 – May 2022

GPA: 3.48 / 4.0

CERTIFICATIONS

Associate of ISC2

October 2025

CompTIA Security+

October 2025