Jermaine D. Hunter

Atlanta, GA | jermaine.hunter.resume@gmail.com | Portfolio | LinkedIn | GitHub

Professional Summary

Cloud Security / Application Security engineer with hands-on experience designing identity-first security systems, building deterministic detection logic, and deploying cloud-hosted portfolio environments on Google Cloud. Strong foundation in IAM, logging/telemetry, threat modeling, and incident response workflows; combines UX design background with security engineering to build secure, explainable systems and clear documentation for stakeholders.

Selected Projects (HunterCloudSec)

Identity-First Signup Threat Detection — *Application Security • Detection Engineering*

- Designed a pre-authentication inspection layer that evaluates signup attempts in real time and returns deterministic outcomes (Allow / Challenge / Block).
- Implemented explainable, rule-based detection signals: disposable email domains, bot-style user agents (e.g., curl/sqlmap), weak password indicators, and injection patterns.
- Defined a canonical JSON security event schema and captured all signup attempts for analyst triage and downstream SIEM compatibility.
- Documented detection gaps intentionally (SQLi variant missed without an explicit rule), reinforcing "systems only detect what engineers encode."

Identity Is the Control Plane — *Secure UX • Application Security*

- Modeled multi-role trust boundaries (Veteran, Mentor, Employer) and designed post-login routing driven by identity claims rather than a single shared dashboard.
- Applied least-privilege and data-minimization principles to role visibility, permissions, and exposure contexts.
- Produced artifacts that connect UX decisions to security primitives: RBAC/claims model, role matrix, and canonical login event example.

Cloud Threat Detection & MITRE Mapping — *Chronicle SIEM • Splunk*

- Built detection workflows for simulated phishing/malware activity; analyzed logs and alerts in Chronicle SIEM and Splunk.
- Mapped detections to MITRE ATT&CK; techniques and documented escalation playbook steps for SOC triage.

Experience

Federal Highway Administration — *HR Assistant Atlanta, GA • Feb 2023 – Present*

- Reported and escalated phishing attempts; supported awareness and response processes for end-user threats.
- Partnered with IT/HR security stakeholders to reinforce IAM controls within onboarding workflows and protect sensitive employee data.

National Park Service — *Web Design & Data Analysis Intern Atlanta, GA • Feb 2019 – Feb 2020*

- Led CMS migration (Google → Microsoft) with minimal downtime.
- Improved website accessibility and reduced maintenance effort through redesign and staff enablement.

Technical Skills

Cloud & AppSec:

- Google Cloud (Cloud Storage, Cloud Run, Logging/Monitoring)
- IAM
- security design for public web entry point

Detection & Telemetry:

- Chronicle SIEM, Splunk
- Event Threat Detection
- canonical event modeling(JSON/JSONL)

Networking & Systems:

- VPC concepts
- firewall rules
- Linux (Ubuntu, Kali)

Frameworks:

- MITRE ATT&CK
- least privilege
- Defense-in-depth
- threat modeling
- PCI DSS (foundational)

Education & Certifications

B.A., Visual Communication — *Savannah College of Art & Design*

Google Cybersecurity Professional Certificate

Google Cloud Security Professional Certificate

CompTIA Security+ (in progress)