Mouli Dutta

AI Security Engineer | Detection Engineering | Security Automation

mouliduttawork@gmail.com — LinkedIn/mouli-dutta — GitHub/mouli-dutta — Portfolio

PROFESSIONAL SUMMARY

AI-driven Security Engineer with 2 years of experience in detection engineering, security automation, and threat analysis. Experienced in Google SecOps, YARA-L, Python, and LLM-powered security solutions, with a track record of reducing false positives, automating SOC workflows, and improving detection efficiency.

TECHNICAL SKILLS

Security Engineering: Google SecOps (Chronicle SIEM/SOAR), Detection Engineering, YARA-L, UDM, Threat Hunting, Log Analysis, Incident Response, MITRE ATT&CK

Security Automation: Python, REST APIs, SQL, Pandas, NumPy

AI Security: LLM Security, OWASP Top 10 for LLM Applications, Prompt Injection, RAG

Tools & Platforms: Git, GitHub, ServiceNow, Jira, Confluence, VS Code, Jupyter Notebook, Windsurf, Claude Code

WORK EXPERIENCE

Accenture **Oct 2024 – Present**

Security Transformation Analyst

- Optimized **30+ production YARA-L detection rules** in Google SecOps, reducing false positives by **80%** and improving MITRE ATT&CK coverage across endpoint telemetry.
- Developed **Python-based SOC automation workflows** using REST APIs, automating **70% of repetitive triage tasks**, saving **15+ analyst hours/week**, and reducing incident review time by **40%**.
- Built **Google SecOps dashboards and automated reporting pipelines** to track alert trends, detection KPIs, threat-hunting coverage, and SOC performance metrics for weekly and monthly leadership reviews.
- Collaborated with stakeholders to identify detection gaps and translate incident-response findings into **new and optimized detection logic**, strengthening coverage against emerging threats.

PROJECTS

SecOpsGPT - AI-Native Security Investigation Platform **April 2026**

Tech Stack: *Python, Claude API, Chronicle API, HTML/CSS/JavaScript*

- Built an AI-native security investigation platform integrating **Google SecOps and Claude API** to summarize security alerts and generate **YARA-L detection-tuning recommendations**, reducing investigation time by **50%**.

MailQuery - Security Data Automation Pipeline **August 2025**

Tech Stack: *Python, Pandas, Outlook API, Regex, OpenPyXL*

- Developed a Python-based automation pipeline to extract and structure data from Outlook emails and attachments into Excel, eliminating repetitive manual reporting and reducing data-processing time by **70%**.

CERTIFICATIONS

- **Claude Code in Action** — Anthropic — Apr 2026
- **Machine Learning Specialization** — DeepLearning.AI — Feb 2026
- **Finetuning Large Language Models** — DeepLearning.AI — Feb 2026
- **Fortinet Certified Associate Cybersecurity** — Fortinet — Dec 2025
- **Google Cloud Certified: Associate Data Practitioner** — Google — Jul 2025
- **Google Cloud Certified: Generative AI Leader** — Google — Jun 2025
- **Microsoft Certified: Security, Compliance, and Identity Fundamentals** — Microsoft — Mar 2025

EDUCATION

Master of Computer Applications, *85.58%* 2022 – 2024

University of Kalyani, Kalyani, WB

ACHIEVEMENTS

- Recognized by leadership as **Best Security Ops Engineer** for use-case optimization & security automation. Aug 2026
- Awarded **Google Cloud merchandise** for completing hands-on cloud architecture and security labs. Dec 2025
- Solved **500+** LeetCode problems to strengthen data structures and algorithmic problem-solving skills. 2024 – Present