Karanveer Singh

Cybersecurity · AI Engineering · Cloud Infrastructure · MLOps
Greater Sudbury, ON • karangill.1708@gmail.com • linkedin.com/in/ksingh1708 • GitHub

PROFESSIONAL SUMMARY

Cybersecurity and AI/ML graduate with a rare dual-domain background and a portfolio of production-grade systems spanning autonomous threat detection, full-stack AI SaaS deployment, LLM-driven security automation, and ML-powered vulnerability intelligence. Hands-on internship experience deploying enterprise SIEM, building virtualized security labs, and contributing to ISO 27001 certification. Equally fluent across defensive security engineering and modern AI infrastructure — including AWS (Lambda, Bedrock, SageMaker), Terraform IaC, GitHub Actions CI/CD, and multi-provider LLM orchestration. Brings a security-first design mindset, an AI-native workflow, and the rare ability to operate at the intersection of both disciplines.

PROJECTS

SentinelAI — Autonomous Threat Intelligence & Incident Response Platform · *Personal Project*

- Autonomous SOC Tier-1 platform: ingests network logs via ELK (Logstash → Elasticsearch → Kibana), runs two-stage ML inference — IsolationForest on BENIGN-only traffic for zero-day anomaly detection, followed by XGBoost multi-class classifier for known attack labelling (DDoS, PortScan, etc.) on CICIDS-2017 — and maps every finding to MITRE ATT&CK with SHAP-explainable incident reports generated as PDFs.
- Enterprise security posture: Argon2id password hashing, timing-attack-safe login (dummy hash on unknown emails), HS256 JWT with role hierarchy (viewer/analyst/admin), JWT stored in-memory (not localStorage) to prevent XSS token exfiltration, CSWSH defense on WebSocket, SHA-256 model artifact verification before every deserialization, nginx TLS 1.3 with strict CSP and HSTS, containers hardened with cap_drop: ALL and read_only: true.
- Full 9-service Docker stack: FastAPI backend, React 18/TypeScript real-time dashboard with WebSocket feed and zod runtime payload validation, PostgreSQL, MLflow experiment tracking, MinIO, Kibana. CI pipeline runs ruff, bandit, pip-audit, pytest (44 tests), and vitest on every push.

CodeGuard — AI-Powered Security Code Review SaaS · *AI/ML Project · Cambrian College*

- Full-stack AI SaaS delivering structured, severity-graded security code reviews mapped to OWASP Top 10 and CWE identifiers — powered by AWS Bedrock Nova Lite and OpenAI GPT-4o-mini backends. Three live deployments: Vercel, manual AWS, and Terraform-automated AWS.
- Complete AWS infrastructure provisioned with Terraform IaC: Lambda, API Gateway, S3, CloudFront, DynamoDB (conversation history, 30-day TTL), Secrets Manager, and scoped IAM. GitHub Actions CI/CD pipeline uses AWS OIDC for keyless authentication — no long-lived credentials stored anywhere.
- Server-side JWT verification via Clerk JWKS in FastAPI (enforced on every request, not just client-side), Pydantic v2 input validation, and AWS Secrets Manager for runtime secret injection. Next.js/TypeScript frontend with streaming SSE output and subscription gating.

AI Red-Team Agent — LLM-Driven OWASP Security Assessment Tool · *Personal Project*

- LLM-driven ReAct agent that performs scoped OWASP Top 10 assessments against intentionally vulnerable Docker targets (DVWA, Juice Shop, WebGoat, VAmPI) with MITRE ATT&CK mapping, CVSS enrichment, OWASP ZAP baseline comparison, Playwright-based recon, and multi-provider LLM support (OpenAI, Gemini, Claude, OpenRouter).
- Security-first design: strict scope validation, rate limiting, sensitive data redaction, CI-backed testing, and automated report generation with full assessment history.

VulnPredict — ML-Driven Vulnerability Prioritization & Patch Intelligence · *Personal Project*

- Ingests CVE and exploit data from NVD, CISA KEV, EPSS, and ExploitDB; trains LightGBM models to estimate 30/60/90-day exploitation risk — enabling security teams to prioritize remediation beyond raw CVSS scores.
- End-to-end MLOps pipeline: PostgreSQL ingestion, FastAPI endpoints, Plotly Dash dashboard, Apache Airflow scheduling, Slack alerting, fully containerized with Docker.

AI-Powered Interview Coaching System · *AI/ML Capstone · Cambrian College*

- Modular AI interview simulation platform with a smart-router inference engine supporting hot-swappable LLM backends (Ollama, GPT-4o, Gemini, Claude), adversarial stress-interviewer persona, and real-time acoustic analytics (WPM, filler words) tracked across sessions via Plotly.
- Docker-containerized; FastAPI backend with API key authentication, Streamlit frontend.

Local RAG System for Privacy-Preserving NLP · *AI/ML Project · Cambrian College*

- Fully local Retrieval-Augmented Generation system (PyMuPDF, ChromaDB, local embedding models) for confidential enterprise document Q&A with zero cloud exposure and perplexity-based evaluation.

Cloud-Native Movie Recommendation Engine · *AI/ML Project · Cambrian College*

- REST API recommendation engine (MovieLens) deployed on AWS SageMaker with MLflow experiment tracking; led system architecture, model training pipeline, and production deployment.

EXPERIENCE

Cybersecurity Capstone Intern — *Spectrum Telecom Group Ltd.* Jan 2025 – Apr 2025

Greater Sudbury, ON · 4-month placement

- Designed and deployed a full hypervisor-based virtual lab provisioning Windows Server, Windows Enterprise, Wazuh SIEM, and MikroTik router/firewall — scoped entirely to the company's ISO 27001 certification effort.
- Deployed and configured Wazuh SIEM end-to-end: detection rule authoring, log source integration, and alert tuning. Contributed to ISO 27001 certification readiness documentation and control alignment.
- Administered Active Directory: user/group/OU provisioning, GPO configuration, credential lifecycle management, Windows Server role management, and Windows Event Log analysis for anomaly triage.
- Configured MikroTik router/firewall within the virtual environment to enforce network segmentation and access control policies.

Independent AI & Security Practitioner — *Self-Directed* July 2017 – Present

AI Research · Agentic Development · PC Hardware · Network Configuration

- Designed and shipped multiple production-grade AI and security systems using AI-native development workflows (Cursor IDE, Claude Code) — directing architecture, security decisions, and system design throughout.
- Continuously researched and tested emerging LLM tooling, agentic frameworks, and security techniques across OpenAI, Anthropic, Google Gemini, Ollama, and OpenRouter ecosystems.
- Built and maintained high-performance custom PC systems — developing deep practical knowledge of hardware compatibility, BIOS/UEFI, OS installation, and Windows optimization at an advanced level.
- Configured home network environments including router/firewall dashboards, DNS, DHCP, port forwarding, and LAN/WLAN segmentation — hands-on grounding in practical network administration.

TECHNICAL SKILLS

Security & SIEM: Wazuh SIEM, ELK Stack (Elasticsearch, Logstash, Kibana), ISO 27001, OWASP Top 10, MITRE ATT&CK, CVSS, CWE, OWASP ZAP, Argon2id, JWT, adversarial testing

ML & AI: IsolationForest, XGBoost, LightGBM, SHAP explainability, Scikit-learn, PyTorch, MLflow, RAG (ChromaDB, PyMuPDF), LLM orchestration, ReAct agents, prompt engineering

LLM APIs & Tooling: OpenAI (GPT-4o/mini), Anthropic Claude, AWS Bedrock (Nova Lite), Google Gemini, Ollama, OpenRouter, HuggingFace, hybrid inference routing

Cloud & IaC: AWS (Lambda, API Gateway, S3, CloudFront, DynamoDB, Secrets Manager, Bedrock, SageMaker, IAM), Terraform, Vercel

CI/CD & DevOps: GitHub Actions (AWS OIDC, keyless auth), Docker (multi-service compose), FastAPI, Apache Airflow, PostgreSQL, MinIO

Frontend: React 18, Next.js, TypeScript, Vite, Tailwind, Streamlit, Plotly Dash, zod, WebSocket

Windows & Infra: Windows Server, Active Directory, GPO, MikroTik, hypervisor VM deployment, BIOS/UEFI, Windows 10/11 advanced optimization

Dev Tools: Git / GitHub, Cursor IDE, Claude Code, Jupyter Notebooks, VS Code

Operating Systems: Windows (advanced), Linux (working proficiency)

EDUCATION

Graduate Certificate — Artificial Intelligence & Machine Learning Sept 2025 – Apr 2026
Cambrian College · Sudbury, Ontario, Canada
President's Honor Roll

Graduate Certificate — Cybersecurity (CSEC) Sept 2024 – Apr 2025
Cambrian College · Sudbury, Ontario, Canada
President's Honor Roll

Bachelor of Computer Applications (BCA) Aug 2019 – May 2023
Punjabi University · Patiala, Punjab, India
First Division

CORE COMPETENCIES

Security-first system design · AI-native builder workflow · Dual-domain security & AI thinking · Infrastructure-as-code discipline · Self-directed research · Rapid tooling adoption