Ahmet Furkan Koç

2701 Vista Oaks Dr., McKinney, TX 75072
954-859-9502 | ahmetffkoc@gmail.com | linkedin.com/in/ahmetfkoc | github.com/ahmetfkoc | Portfolio

Green Card holder - authorized to work for any employer in the United States without sponsorship.

Objective

I am a Computer Science graduate from UT Dallas and Toshiba's Intern of the Cohort, with hands-on experience across product security, cloud security, SOC alert triage, endpoint monitoring, vulnerability management, application security testing, and AI-assisted security automation. I am seeking security analyst, cybersecurity analyst, cloud security, SOC analyst, or security engineering opportunities where I can investigate risk, document findings clearly, and help teams improve security posture through practical technical work.

Education

University of Texas at Dallas December 2025
Bachelor of Science in Computer Science *Richardson, Texas*

Technical Skills

Security Operations: Microsoft Sentinel, Microsoft Defender, SIEM/EDR alert triage, incident documentation, threat intelligence, OSINT, MITRE ATT&CK
Cloud & Endpoint Security: Azure, Defender for Cloud, CSPM workflows, attack path analysis, endpoint monitoring, malware prevention signals, Entra ID concepts
Application & Vulnerability Security: SAST, DAST, SCA, OWASP Top 10, BlackDuck, OWASP ZAP, Burp Suite, vulnerability management, CVE review
Automation & Tools: KQL, PowerShell, Python, Azure Resource Graph, Jira, Confluence, GitHub, GitLab, Jenkins, Logic Apps, Power BI
Frameworks & AI: CIS Benchmarks, NIST, PCI DSS, SOC 2, ISO 27001, Claude Code, Codex, ChatGPT, OpenAI API, LangGraph, RAG

Professional Experience

TOSHIBA **May 2025 - Present**
Product Security Engineer Intern / Cloud Security Analyst *Frisco, Texas*

- Improved cloud security posture by 35% within six months by supporting remediation of 100+ misconfigurations identified through Defender for Cloud and benchmarked against CIS guidance.
- Performed initial triage and investigation of SIEM and EDR alerts in Microsoft Sentinel and Defender, identifying anomalies, validating risk, and escalating high-priority findings for remediation.
- Monitored endpoint security for 11,000+ assets, supporting proactive threat protection, malware prevention, device health visibility, and operational security control effectiveness.
- Automated vulnerability management checks with PowerShell and KQL to identify critical CVEs, query Azure Resource Graph, and accelerate repeatable security review workflows.
- Conducted application security testing using SAST, DAST, and SCA against enterprise SaaS solutions, reviewing findings against OWASP Top 10 risk areas.
- Prepared remediation guidance and Jira-ready ticket details for development, infrastructure, and resource owner teams, translating technical findings into clear actions, owners, severity, and follow-up steps.
- Built AI-assisted security workflows that summarized findings, classified alerts, supported owner notification, and preserved human analyst validation before operational decisions.
- Collaborated with senior engineers to review cloud, endpoint, application security, and vulnerability findings and prioritize work based on severity, exploitability, business context, and remediation feasibility.

AI CONNEX **May 2024 - August 2024**
Cybersecurity Intern *Frisco, Texas*

- Supported cybersecurity initiatives at an AI-focused startup, contributing to research, event coordination, and knowledge-sharing sessions.

- Gained hands-on exposure to EDR software, network protocol analysis, and security monitoring concepts, applying them to threat detection and mitigation exercises.
- Conducted OSINT research using threat intelligence tools to identify potential vulnerabilities, suspicious indicators, and threat landscape trends.

Projects

Agentic AI Threat Assessment System | *Python, LangGraph, FastAPI, OpenAI, Azure Defender* | *Internal Project - Toshiba* | MDFC Triage

- Built an autonomous multi-agent security system that triages Microsoft Defender for Cloud Attack Path alerts using ContextAgent, NetworkAgent, and ThreatHunter workflows.
- Automated classification of 200+ daily security logs and attack vector analysis, achieving 90% accuracy in risk severity labeling compared to manual assessments.
- Implemented Human-in-the-Loop interrupt gates requiring analyst approval before Jira ticket creation or alert dismissal, supporting validated case handling and accountable security decisions.

AI Security Agent for Cloud Monitoring | *RAG, Azure AI Foundry, Python* | *Internal Project - Toshiba*

- Built a security agent using Azure AI Foundry to detect publicly exposed cloud resources and identify security vulnerabilities across Azure infrastructure.
- Decreased Mean Time to Respond by 45% by automating notification of resource owners for publicly exposed assets.

CyberTrack – AI Mentor & Goal Tracking App | Next.js, Claude API, TypeScript, Vercel | CyberTrack

- "I had a problem and found a solution" approach; developed an app where recent graduates or job hunters will track their weekly goals here to achieve a bigger goal of securing a full-time position or passing a certification exam.
- Built a full-stack goal-tracking web app for job seekers with AI-powered onboarding that calls the Claude API to generate personalized weekly goal categories and starter tasks from 4 user inputs.
- Implemented a 4-step conversational onboarding flow with animated transitions, weekly streak tracking, week rollover logic, and an AI mentor chat with full conversation history persistence.

Achievements / Certifications

- **Intern of the Cohort Award at Toshiba (Fall 2025):** Recognized for outstanding performance, dedication, and contribution as a Product Security Engineer Intern.
- **WayUp Top Intern (Summer 2025):** Elected for being a top intern for contribution to company as an intern.
- CompTIA Security+
- GenAI for SOC Analysts
- SOC 2 Compliance Essential

Leadership / Extracurricular

Cybersecurity Community Team August 2024 - Present

President *UTD*

- Leading a mentorship program, guiding peers in skill development and fostering a collaborative environment.
- Engaging in discussions on recent industry news, cyber threats, ransomware campaigns, and AI/ML security topics.
- Staying current with emerging cybersecurity trends, ransomware campaigns, AI/ML vulnerabilities to enhance awareness.