Megha Nettem

Plano, TX | mnettem21@gmail.com | (219)-576-4962 | linkedin.com/in/megha-nettem/

Security+ certified Computer Science student with hands-on GRC and SOC experience. Skilled in SIEM, phishing simulations, and secure system design, with proven results driving audit readiness and reducing risk.

EDUCATION

• **The University of Texas at Dallas, Richardson TX:** B.S. in Computer Science   December 2025

TECHNICAL SKILLS

Certifications:	CompTIA Security+, Microsoft AZ-900, Microsoft AI-900, Google Cloud Digital Leader, PCEP – Python
Security Tools:	Rapid7 InsightIDR/VM, Microsoft Defender, Cisco Umbrella, SendGrid, Grafana, Wireshark, Kali
Frameworks:	NIST CSF, MITRE ATT&CK, ISO 27001, SOC 2, GLBA, PCI-DSS, GDPR/CCPA
Processes:	Incident Response, Risk Assessment, Policy & Compliance Review, Vulnerability Management, Phishing Sim.
Other:	Azure, GCP, Power BI, Agile/Scrum, API Development, Python, C++, C#, Java, JavaScript, HTML/CSS

WORK EXPERIENCE

Cybersecurity & Policy Intern, Upbound Group | *Plano, TX*   June 2025 - August 2025
• Triaged **100+** weekly security alerts in **Rapid7 InsightIDR, Microsoft Defender, and Cisco Umbrella**, reducing false positives by **~20%** and enabling faster SOC response.
•Designed and executed phishing simulations for **3,000+** employees, cutting click-through rates by **45%** in 2 months and improving security awareness scores.
• Reviewed and updated **15+** internal security policies to align with **NIST CSF and ISO 27001**, increasing audit readiness by **30%** for the next compliance cycle.
• Contributed to incident response playbooks, expanding coverage by **25%** and improving cross-team escalation workflows during tabletop exercises.

eCommerce Developer Intern, Upbound Group | *Plano, TX*   June 2024 - August 2024
• Migrated **25+** corporate pages to **SAP Commerce Cloud,** improving page load speed by **18%** and ensuring secure content integration.
• Built executive **Power BI** dashboards tracking key performance metrics, improving leadership reporting turnaround time by **20%.**

IT Integration Intern, Ryder Inc. | *Remote*   June 2023 – Present
• Developed a secure onboarding API (**C# + RBAC**) for telematics data, reducing unauthorized access incidents by **15%** and improving partner onboarding efficiency.
• Cleaned **1,200+** geofences from telematics systems, improving asset location compliance by **35%** and reducing false location alerts.
• Tested & documented AI-powered tools leveraging **OpenAI APIs** with secure authentication, ensuring **100%** compliance with data handling policies.
• Led summer intern Agile program, managing sprint boards in **Azure DevOps** and integrating secure coding reviews, which improved code quality by **20%.**

PROJECTS

Underight, AI-Driven Underwriting Platform   **Feb 2025 - Present**
• Designed secure system architecture for an AI-powered DSCR loan underwriting platform, embedding **RBAC, data encryption, and audit logging** to meet financial services security standards.
• Integrated compliance-by-design practices, mapping workflows to **SOC 2, GLBA, and CFPB** guidance, reducing future regulatory risk and simplifying investor due diligence.
• Conducted risk assessments for data handling, vendor integrations, and third-party APIs, creating a **mitigation plan** to address **confidentiality, integrity, and availability** risks.
• Implemented **AWS Textract OCR + RAG** pipeline with **LangChain + Pinecone**, enabling automated document ingestion and instant investor eligibility checks with **~60%** reduction in manual data entry errors.
• Collaborated with **6+** lenders and brokers to validate **risk, compliance, and operational requirements**, ensuring the platform aligns with investor expectations and industry regulations.

Secure Customer Document Portal   **June 2024 - August 2024**
• Designed and developed a secure document portal that supports **file upload, malware scanning, RBAC-based permissions, and encrypted storage** to simulate enterprise-grade document workflows.
• Implemented **secure authentication and session management**, protecting sensitive data from unauthorized access.
• Focused on privacy-by-design principles, improving system resilience to **OWASP Top 10 threats**.

LEADERSHIP & INVOLVEMENT

Toyota Hackfesta CTF - Hardware Security Challenge: Performed CAN bus packet sniffing and ECU reverse engineering, exploiting vulnerabilities to demonstrate potential attack vectors.
Capture the Comet (CTC) - UTD Club : Founded and led UTD's first CTF club; grew participation by **40%**, and built a pipeline preparing students for national contests like **picoCTF and Hack the Box**.