Khushi Mitesh Shah

khushims@andrew.cmu.edu | Pittsburgh, PA | www.linkedin.com/in/shahkhushimitesh/ | https://shahkhushimitesh.blogspot.com/

SUMMARY

Motivated graduate student in Information Security Policy & Management with hands-on experience in **intrusion detection**, **incident handling**, & **cyber forensics**. Experienced in leveraging **threat intelligence** & **generative AI** to enhance detection capabilities and streamline incident handling. Seeking full-time opportunities starting May 2025 as a **SOC Analyst** to apply my skills in protecting **critical assets** & **mitigating cyber threats** in dynamic, fast-paced environments

EDUCATION

Carnegie Mellon University, H. John Heinz III College, Pittsburgh — May 2025
Master of Science, Information Security Policy and Management — **CGPA**: 3.78
Affiliated with Women in Privacy & Security at DEFCON 2024, Organized Privacy + Security Spring Academy 2024

Ahmedabad University, School of Arts and Sciences, India — July 2023
Bachelor of Science, Computer Science, Minor: Psychology — **CGPA**: 3.34
Teaching Assistant for Human-Computer Interaction, Peer Tutor for Mandarin

SKILLS & COURSEWORK

Tools: Argus, Amazon Cloud Services (AWS), Azure, Burp Suite, Cellebrite, GCP, Git, Graylog, Kibana, MISP, Microsoft Intune, Microsoft Sentinel, Microsoft Office Suite, Nmap, OllyDbg, Splunk, Security Onion, Wireshark, Wazuh, XRY | **Frameworks/ Compliance:** ISO27001, PCI-DSS, GDPR, NIST SP 800-60, FIPS 199, FIPS 200

Databases & Programming Languages: Bash, MySQL, C, C++, Java, KQL, Linux/ Unix, MATLAB, Python, R

CERTIFICATIONS

- CompTIA Security+ [Credential ID: FPDJN71QZ14Q1JG5] — **January 2025**
- ISC2 Certified in Cybersecurity [Certificate No.: 2065997] — **June 2024**
- Security Analyst Fundamentals (IBM) [Credential ID: DMC33NTNPA2M] — **January 2021**

ACADEMIC PROJECTS

Enhancing Insider Threat Detection with Moral Foundations Theory and NLP
- Developed an innovative insider threat detection model integrating Moral Foundations Theory with NLP, achieving 88% accuracy on the CMU Insider Threat Dataset and 80% on the Enron Email Dataset
- Implemented a novel NLP framework using the extended Moral Foundations Dictionary to extract moral features from textual data, enhancing behavioral analysis for threat detection

Intrusion Detection & Prevention using Snorby and Suricata
- Analyzed 1,000+ alerts from Snorby (IDS) for web application exploits and SQL injection attempts, identifying 3 attack vectors and a 200% increase in malicious traffic from 5 IP addresses at the firewall
- Developed 15 custom Suricata (IPS) rules using bash scripting, automating updates to reduce manual effort by 75% and blocking 95% of unauthorized communication attempts, enhancing network security

Implementing Security Operations Centre using Open-Source Software
- Orchestrated the establishment of a cutting-edge SOC center leveraging Docker technology, integrating Wazuh and Graylog as SIEM tools for robust log ingestion and building a data pipeline for processing, while employing Kibana and Grafana for dynamic visualization
- Currently trouble-shooting implementation of OpenCTI and MISP for seamless threat intelligence communication, complemented by the integration of Wazuh for advanced Endpoint Detection and Response (EDR) capabilities

WORK EXPERIENCE

Concepta Innovation Solutions, Maryland | *GEN AI Security Intern* — **May 2024 - August 2024**

Policy Management:
- Spearheaded the development and implementation of a BYOD policy and Role-Based Access Control (RBAC) using Microsoft Intune, improving organizational security, and access management
- Conducted in-depth testing, training, and optimization of Copilot for Security, enabling the tool to autonomously handle policy-based security operations, boosting operational efficiency by 65% and reducing workload by 70%

Incident Monitoring:
- Designed and configured analytical rules and conditions within Sentinel using Kusto Query Language (KQL), facilitating real-time TTP-based threat detection, scheduled queries, and incident logging to enhance overall Intrusion Detection and Prevention Systems (IDS/IPS) and Security Incident and Event Management (SIEM)

Directorate of Forensic Science, India | *Summer Intern* — **June 2022 – July 2022**
- Demonstrated analytical skills in collaboration with cross-functional teams to provide pivotal insights on 15 cybercrime cases, along with conducting technical examinations and delivering concise, court-ready reports
- Employed advanced forensic tools, including Cellebrite and XRY, to recover and analyze digital evidence crucial for court proceedings by extracting and assessing electronic data of over 35 devices, ensuring its integrity