**Khushi Mitesh Shah**

[khushims@andrew.cmu.edu](mailto:khushims@andrew.cmu.edu) | (412) 933-0028 | Pittsburgh, PA | [LinkedIn](file:///C:\Users\Lenovo\Desktop\Khushi%20CMU\Internship%20Applications\linkedin.com\in\shahkhushimitesh\) | [Blogspot](https://shahkhushimitesh.blogspot.com/)

**SUMMARY**

Results-driven **Information Security graduate** student with skills in implementing SOCs, conducting log analysis, and developing intrusion detection systems. Experienced in AI-powered cybersecurity tools like **Copilot for Security, Microsoft Azure**, and frameworks like **NIST, FIPS, PCI-DSS, & ISO 27001**. Actively contributes to the cybersecurity community through research and volunteer work. Eager to apply a strong foundation in **SIEM, EDR, & digital forensics** to enhance security solutions 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:** Burp Suite, Wireshark, Nmap, Splunk, Kibana, Argus, Security Onion, OllyDbg, Cellebrite, XRY, Microsoft Intune, Microsoft Sentinel, Git | **Databases & Programming Languages:** MySQL, PostgreSQL, C, C++, Java, MATLAB, Python, R, TAXII | **Frameworks**: ISO27001, PCI-DSS, GDPR, NIST SP 800-60, FIPS 199, FIPS 200

**Certifications**

* CompTIA Security+ [Credential ID: FPDJN71QZ14Q1JG5] **January 2025**
* ISC2 Certified in Cybersecurity [Certificate No.: 2065997] **June 2024**
* Certification in Cyber Security & Cyber Defense [Certificate No.: 2201800] **April 2022**
* Security Analyst Fundamentals (IBM) [Credential ID: DMC33NTNPA2M] **January 2021**

**Coursework:** Software & Security, Malware Analysis, Usable Privacy & Security, Economic Analysis, Privacy in Digital Age, Statistical Reasoning with R, IT Project Management, Cybersecurity Policy & Governance, Privacy Policy, Law & Technology, Lean Innovation Lab, Organizational Design, Network Defenses

**ACADEMIC PROJECTS**

**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 working on the implementation of OpenCTI and MISP for seamless threat intelligence sharing, complemented by the integration of Wazuh for advanced Endpoint Detection and Response (EDR) capabilities

**Web Server Log Analysis with Kibana and Splunk**

* Utilized Kibana’s dashboards to analyse more than 50,000 web server logs as the product of an incident, extract valuable technical insights using data visualization, and identify patterns for status monitoring of future problems & devising protection strategies.
* Examined communications for 2 syslog collections using Splunk queries, detected SQL injection targeting 2 internal executable files, and tracked 10 IP addresses compromised by a botnet

**Intrusion Detection & Prevention using Snorby and Suricata**

* Investigated web application, SQL injection, and port scan alerts using Snorby (IDS) for an attack from external sources perpetrated against a DMZ network to identify vulnerabilities
* Engineered alerts and rules using bash scripting in Suricata (IPS), proactively preventing unauthorized traffic to communicate among the network infrastructure and enhance networking security

**Fatigue Failure Analysis**

* Devised a probability model in Python to understand the time to component failure in machines using Lagrange theory, and other core concepts like CDF and PDF

**UIDAI Analysis**

* Executed analysis of data of more than 100,000 ‘Aadhar Card’ holders collected from official websites of the Indian government; Incorporated tools including Hadoop and MapReduce for large-scale data analysis.

**Cryptocurrency Forecasting**

* Collaborated to forecast short-term returns on fourteen cryptocurrencies' time-series dataset using various machine learning algorithms such as XGBoost, LGBM, KNN, Ridge, and Lasso

**Privacy Policy Research on Voice Cloning Models**

* Collaboratively conducted in-depth research, of written privacy policies and their applications for innovative voice cloning artificial intelligence/ machine learning models, like RVC & Eleven Labs; Reviewed their use cases, implications, and provided solutions to raise awareness about privacy concerns

**Firewall Rule Optimization in pfSense and Endian**

* Crafted and optimized 10 firewall rulesets to safeguard against unauthorized access and threats, demonstrating practical knowledge in the development of network security architecture

**Privacy for Shared Smart Assistants** *(*[*Published by USENIX at SOUPS’24*](https://www.usenix.org/conference/soups2024/presentation/carreira-listening-poster)*)*

* Conducted research on privacy preferences for smart personal assistants as part of a team project; Surveyed both voice assistant users and non-users to identify effective fine-grained privacy controls for shared devices

**NetFlow Analysis**

* Explored traffic flow over a network for a pre-captured file to analyse and uncover evidence on execution of malicious activities using Argus and SiLK which work on UNIX commands

**Windows Server Environment Management and Group Policy Implementation**

* Demonstrated proficiency in setting up and managing Windows servers on specified parameters, including installing roles such as Active Directory, DHCP, and DNS, and joining workstations to a domain; Successfully deployed and observed group policies in action, showcasing knowledge and application of security protocols in a networked environment

**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.

**RELEVANT EXPERIENCE**

**Concepta Innovation Solutions** May – August 2024

GEN AI Security Intern

* Developed and implemented a BYOD & RBAC policy using Microsoft Intune, established an automated system for generating incident alerts on Microsoft Sentinel, and provided comprehensive training to Copilot for Security tool to autonomously carry out these processes
* Configured analytical rules and conditions in Sentinel dashboard using KQL for threat identification to process scheduled queries, real-time detection, and incident logging to enhance security monitoring and incident management (SIEM)

**Directorate of Forensic Science,** Gandhinagar, India June – July 2022

Intern

* Demonstrated analytical skills in collaboration with cross-functional teams to provide pivotal insights on 15 cybercrime cases, along with conducting in-depth 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