MEHUL SEN

Rochester, New York • +1-585-298-7647 • mehulsen@mail.rit.edu • mehulsen.com • linkedIn.com/in/mehulsen

CompTIA Security+ and Network+ certified M.S. student in cybersecurity specializing in network security, vulnerability assessments, machine learning applications in cybersecurity and development of security tools.

EDUCATION

Rochester Institute of Technology, Rochester, NY

- **Master of Science in Cybersecurity -** GPA 3.9/4.0, *May 2024*
- **Bachelor of Science in Cybersecurity -** Summa cum laude, *December 2022*

SKILLS & CERTIFICATIONS

Technical Skills: Cybersecurity Fundamentals, Network Security, Vulnerability Assessments, Risk Analysis, Penetration Testing, Incident Response, Threat Intelligence, Python/Bash Scripting, SIEM and SOAR Management, OSINT, Metadata Analysis, Reverse Engineering, PCI/SOX, HIPAA and GDPR Compliance, Cryptography, System Administration, AI and Machine Learning, Offensive Security

Certifications: CompTIA Security+ (January 2024), Network+ (July 2022), Machine Learning Specialization (Coursera, January 2023)), Summer Learning Academy Externship (AT&T, July 2021)

Competitions: BSidesROC CTF 2024, Red Team (RIT's IRSec 2020), Blue Team (ISTS 17 and UB's Lockdown v5), Hackathons (Brickhack V and Brickhack VI)

PROFESSIONAL EXPERIENCE

Wegmans Food Markets, Rochester, NY *January 2022 – August 2022*

Network Support Technician Co-op

- **Collaborated with network engineers to configure and troubleshoot various network devices,** including Cisco and Arista routers, POLRE Phybridges, Raritan switches, wireless bridges, Palo Alto firewalls, Digi modems, and Cisco Jabber, ensuring robust organization-wide connectivity and direct support for employee network issues using Solarwinds Orion and BMC SmartIT, boosting operational efficiency.
- **Configured and deployed network infrastructure for new locations**, essential for expansion by establishing solid network foundations.
- **Developed and optimized tools for automating network configuration and troubleshooting processes**, reducing device configuration and deployment time across new and existing locations and significantly reducing configuration and troubleshooting time for connectivity issues.

Value Point Systems, Bengaluru, India *July 2019 – August 2019*

Security Operations Center Intern

- **Designed and deployed a brute-force detection playbook on the SOAR platform** (Demisto), integrating with IBM QRadar and Active Directory for enhanced threat detection. This playbook analyzes user login history and actions, streamlining the identification of brute-force attacks for faster response and remediation.
- **Developed custom scripts in Python to handle and analyze large datasets.** These scripts enabled the SOAR platform to process login attempts and flag suspicious activities efficiently, significantly improving the threat-hunting process by reducing manual data analysis and accelerating threat detection.
- **Executed comprehensive OSINT and vulnerability assessments,** pinpointing potential security vulnerabilities and information leaks. Generated detailed reports with actionable mitigation, strengthening security measures and enhancing the organization's security posture.

PROJECTS

- **Machine Learning applications in Cybersecurity** August 2023 – *December 2023*

Developed advanced machine learning models to improve cybersecurity measures. Some of my notable projects include deep neural networks to detect deepfakes, analyze anomalous traffic, spam and malicious traffic. I have also designed adversarial machine learning models that focus on generating and defending against malicious attacks. Additionally, I have expertise in designing website fingerprinting models using deep neural networks.

- **Triangulation Approach for Imminent Threat Detection** *January 2023 – May 2023*

Partnered with the U.S. Department of State Diplomatic Security Service through the Hacking for Diplomacy (H4D) program to enhance embassy security. Coordinated stakeholder interviews (over 50 participants), designed and implemented a triangulation-based solution for rapid threat detection, and improved emergency response protocols.

- **Vulnerability Assessment of Trillium Health** *August 2022 – December 2022*

Directed a thorough cybersecurity audit for Trillium Health, incorporating OSINT, metadata analysis, threat modeling, and social engineering tests. Delivered comprehensive reports with actionable insights, significantly enhancing the organization's cybersecurity posture.