Praj Sanjay Shete

380 John St, Rochester, NY | Phone: (585)-537-8489 | Email: ps7600@rit.edu | linkedin.com/in/praj-shete-32b452163/ | GitHub: @prajshete

OBJECTIVE

Actively looking for roles as Security Analyst in Blue team. Currently pursuing a Master's in Computing Security. My technical skills encompass incident response, malware analysis, threat hunting and security monitoring. Strong communicator adept at collaborating with cross-functional teams.

EDUCATION

Rochester Institute of Technology (RIT) – Rochester, NY

Master of Science Computing Security **GPA: 3.7/4.0** 2024 (expected)

- Cryptography & Authentication, Trusted Computing, Network Security, Malware Reverse Engineering, Adv. Malware Forensics, OSINT.

Pune University - Pune, India

Bachelor of Engineering – Information Technology **GPA: 7.55/10** 2020

WORK EXPERIENCE

Tata Consultancy Services Ltd.

Cybersecurity Analyst 2021-2022

- Analyze and respond to potential phishing email alerts generated by Agari Phishing Defense and Abnormal Security
- Monitor and Triage endpoint security alerts by Crowdstrike.
- Resolve any email gateway related issue by finetuning the email gateway configuration (Proofpoint).
- Triage any custom created alerts in Splunk SIEM.
- Actively hunt IOC's over threat intel sites and perform checks and blocks in the environment.
- Prepare and update SOP's related to alerts and tools.

PROJECTS

Ransom note detection using CNN.

Adv. Malware Forensics (Final Project) – Spring 2022

- Trained the CNN model to classify Ransom notes with clear explanation of the tools use case and produces accuracy of 70%

Quantum Key Distribution

Cryptography and Authentication (Research Paper) – Fall 2022

- Discuss QKD Network Architecture & challenges faced in QKD Networks. Derive solutions that might lead to maximizing this distance.

Architecture and Advancement in Virtualization of TPM

Trusted Computing (Research Survey)

- Discuss various hardware architectures & List out different methods for virtualizing the TPM. Understanding attacks and mitigations on TPM.

Reversing RedLine Stealer Malware

Malware Reverse Engineering – Summer 2023

- Performed Basic Static, Basic Dynamic, Advanced Static analysis on Redline Stealer malware.

PE File Signature Generator

Summer 2023 (Personal Project)

- Automate extraction of file signatures like file properties, hashes, API calls, loaded libraries, IP address/FQDN's/URL's in the form of C2.

Directory Integrity Checker

Summer 2023 (Personal Project)

- Developed an automated file hash checker which will execute at regular intervals to check for modifications made in any directory.
- Provides an alert if any modifications are found.

EXTRA CURRICULAR

RITSEC – RIT Cybersecurity club

- Active participation in interest groups like Incident Response and Reversing & participate in any competitions organized by the club.

Online Learning Platform

- **Cyber Defenders:** Complete CTF challenges related to Reverse Engineering, DFIR, Threat Hunting.
- **Blue Team Labs:** CTF challenges and tasks related to malware analysis, threat hunting and DFIR.

CERTIFICATIONS

- SOC 1 Learning Path (Try Hack Me)
- Cyber Defense (Try Hack Me)
- Practical Malware Analysis and Triage (TCM Security)
- Malware Analysis and Intro to Assembly Language (IBM)
- Splunk Fundamentals Part 1
- Splunk Enterprise Security

SKILLS

Tools: Crowdstrike | Splunk | Sysinternals Suite | IDAPro | x32Dbg | Wireshark | Autopsy | Velociraptor | Zeek

Domains: Incident Response | Malware Analysis | Threat Intelligence | Threat Hunting | Digital Forensics

Programming: Python | C | C++