Praj Shete

Rochester, NY (OPEN FOR RELOCATION)
✉ prajshete17@gmail.com in linkedin.com/in/prajshete github.com/prajshete

Summary

Passionate cybersecurity enthusiast with a Bachelor's in IT and experience as a Security Analyst. Currently pursuing MS in Cybersecurity. Looking for Fall 2024 Co-op/Fulltime Roles in Cyber Defense domains.

Education

Rochester Institute of Technology (RIT) - Rochester, NY **August 2022 – August 2024**
Masters of Science in Cybersecurity *GPA - 3.70*

Pune University - Pune, India **June 2016 – May 2020**
Bachelor of Engineering in Information technology *GPA - 3.30*

Experience

Algosmic Cybersecurity **June 2024 – Present**
Information Security Intern *Pune, India*

- Contribute towards in-house SOC in investigating and remediating security incidents
- Create and fine-tune threat detection rules in ELK SIEM thereby expanding MITRE coverage by 30%
- Develop an automated Incident Response tool that will pull logs from ELK SIEM perform analysis and respond by taking necessary actions

Cyber Defense and Intelligence Centre **April 2024 – July 2024**
Cyber Threat Intelligence Analyst – Volunteer *Romney, VA, USA, Remote*

- Perform Surface Web OSINT to gather evidence associated with ongoing threat campaigns.
- Research security threat intel sites/blogs to evaluate current attack campaigns and develop reports to present to the management

Tata Consultancy Services Ltd. – *Fulltime* **August 2020 – August 2021**
Assistant Systems Engineer-Cybersecurity Analyst(Project Role) *Pune, India*

- Co-ordinated in a 24x7 Security Operation Centre (SOC) to proactively detect and respond to threats
- Performed email analysis for more than 20 phishing emails per day
- Analyzed and triaged endpoint security alerts, using Proofpoint TAP, Crowdstrike EDR, and Splunk SIEM from around 20,000 endpoints present globally.
- Performed threat hunting operations by developing and executing proactive search queries across the network
- Monitored and remediated suspicious sign-in attempts through Azure Active Directory

Projects

Automate Incident Response | *Python, ELK SIEM, GitHub Link*

- Developed an automated incident response tool that will pull logs from ELK SIEM, perform threat intel analysis on IOCs like network connections and take responsive actions like blocks, host isolation and email reporting.

SOCker: A robust Incident Management and tracking application (Capstone Project. In Progress)| *GitHub Link*

- Developed an open-source web application ticketing system for SOC Analysts, streamlining incident response workflows and documentation for enhanced tracking, auditing, and analysis.

Ransom Note Detection using Convolutional Neural Network | *Neural Networks, CNN, Ransomware, GitHub Link*

- Crafted a CNN model utilizing TensorFlow and Keras to classify ransom notes through image analysis, significantly bolstering ransomware detection capabilities.

Reversing Redline Stealer Malware | *Malware Reverse Engineering, GitHub Link*

- Conducted comprehensive analyses (Basic Static, Dynamic, and Advanced Static) of Redline Stealer malware, utilizing tools like strings, TCPView, and IDAPro, and detailed the malware's mechanisms in a thorough report

Attack and Defend Windows Active Directory | *Windows AD, Splunk SIEM*

- Emulated successful attacks on Active Directory, provided means of detection in the form of event logs and Splunk queries, mitigation, and best practices to avoid such attacks.

Cybersecurity Evaluation of Real-World Enterprise | *Vulnerability & Risk Assessment, Controls & Budget*

- Evaluated the cybersecurity posture of the real-world company by researching open source vulnerabilities, suggesting controls and mitigations, and estimating the budget for the suggested controls.

Certifications

- CompTIA CySA+(COMP001022374766)
- EC-Council Certified Incident Handler(ECC2013974856)
- ISC2 Certified in Cybersecurity(1229888)
- Hack The Box CDSA(In Progress)
- Chronicle Certified SOAR Analyst
- SOC Level 1 (Try Hack Me)
- SOC Level 2 (Try Hack Me)

Volunteer Experience & Competitions

RITSEC – RIT Cybersecurity club

- Active participation in interest groups like Incident Response, CTFs, Reversing.

IRSec - RITSEC Red vs Blue Team Competition

- Participated as a blue team member to maintain the service up-time of the provided services.
- Monitor logs for applications/services to determine breach
- Craft an incident response report documenting attacks on our infrastructure

CORA - Cyber Operations and Remediation Assessment | *Mini Attack vs Defend Competition*

- Competed in a 4-member team as a blue team member to scan vulnerable services and patch them to secure the boxes
- Monitor attacks on our infrastructure and provide Incident Response report

Student Volunteer - Rochester Security Summit, BSides Rochester| *G Drive Link*

- Volunteered for administrative activities and attended sessions in Rochester Security Summit and BSides Rochester

Alumni Guest Lecture for Junior undergraduate students| *G Drive Link*

- Conducted a session on “Introduction to Cybersecurity” for Junior undergraduate students by providing them with insightful knowledge regarding CIA Triad, Network Security, Cyber Defense, and Career Opportunities

Technical Skills

Domains: Incident Response, Malware Analysis, Threat Hunting, Email Security, Endpoint Security, Vulnerability Management

Tools: Crowdstrike EDR, Splunk SIEM, ELK SIEM, Abnormal Security, Proofpoint, Active Directory, Sysinternals Suite, IDAPro, x32Dbg, Wireshark, nmap, GitHub, IDS/IPS, Firewalls, Microsoft Office, Office 365

Scripting: Python, C, C++, Powershell, HTML, CSS, Javascript

Soft Skills: Communication Skills, Teamwork, Adaptive, Time Management, Critical Thinking, Problem Solving