GOKUL SATHIYAMURTHY

Union City, NJ-07087| gokul.sathiyamurthy@pace.edu | 551-358-1893 | LinkedIn | GitHub |Portfolio

OBJECTIVE

Dedicated cybersecurity professional with hands-on experience in threat analysis and incident response, seeking part-time roles for Fall 2024 and Spring 2025, as well as a full-time position for Summer 2025. I aim to leverage my skills and contribute to cybersecurity initiatives through my expertise in vulnerability management and SIEM within a dynamic organization

EXPERIENCE

Cantonica Inc. New York, US

Security Analyst Intern June 2024- September 2024

- Conducted vulnerability and open port scans, prioritized risks with MITRE ATT&CK, and collaborated on remediation, reducing security risks by 40% and improving threat detection by 30%.
- Assisted in incident response by developing plans, investigating incidents, and implementing mitigation strategies, reducing resolution time by 25% and enhancing security monitoring by 20% through SIEM setup.
- Stayed updated with cybersecurity trends and engaged in continuous training, ensuring team adherence to best practices.
- Authored blogs on LinkedIn about Ensuring Robust Security in Progressive Web Apps (PWAs), contributing to industry knowledge and enhancing the Cantonica LinkedIn page.

LTIMindtree LTD Chennai, India

Dex Hunter (SOC analyst) November 2022 - August 2023

- Investigated 100+ malware samples embedded in MS Office files, utilizing Reverse Engineering techniques for identifying risk, vulnerability assessment and threat intelligence enhancement
- Cataloged behavior of 50+ malware instances using Security software tools like Procmon, Nmap, and Regshot, leading to improved threat detection, mitigation, Endpoint Information security and incident response capabilities
- Analyzed 200+ Carbon Black alerts, refining security policy, protocols and enhancing system resilience, resulting in a 25% reduction in incident response time

Mindtree LTD Chennai, India

MTE Threat Researcher April 2021 – November 2022

- Improved incident response capabilities by implementing EDR solutions, risk management and using MITRE attack tactics, techniques, resulting in a 30% reduction in IT Security incident resolution time
- Deployed automated threat hunting and advanced malware analysis techniques, integrating with Threat Intelligence Platforms (TIPs) to increase threat detection efficiency by 50% and enhance overall cybersecurity posture
- Executed over 1000 targeted threat hunts utilizing NIST and CIS controls, enhancing GRC (Governance, Risk, and Compliance) posture and cyber defense infrastructure

ACADEMIC WORKS

Implemented Network Defense for Luna Bags April 2024

- Installed and configured Apache web server in Luna Bags' DMZ to host a generic website accessible via port 80
- Enhanced security by implementing HTTPS and TLS protocols through the creation and installation of a web certificate
- Developed and enforced firewall policies on the router based on access control policies to regulate traffic between the DMZ and internal network
- Strengthened threat detection capabilities by deploying Snort for intrusion detection and Splunk as a SIEM tool to monitor network traffic

ICMP Redirect Attack Case Study March 2024

- Conducted comprehensive analysis on ICMP Redirect Attack in a virtualized lab environment, demonstrating successful execution using Scapy Python library
- Investigated mitigation strategies, including disabling ICMP redirects, network filtering, monitoring, and traffic integrity measures
- Performed additional experiments to analyze attack behavior under different scenarios, such as remote IP redirection and router configuration changes
- Documented findings, insights, and recommendations in a detailed report, emphasizing potential risks and importance of robust network security

Foolish Firewall Configurations Challenge (pfSense) November 2023

- Configured network firewall using NAT and Iptables to allow essential traffic (HTTP, HTTPS, SSH), enforced an implicit deny rule, and aligned TCP/IP routers and switches to enhance network administration security
- Established precise inbound rules on server host firewalls (Ubuntu, Windows, Linux) via iptables and Windows Firewall, limiting access to required ports (MySQL, SSH, Samba), enhancing overall system defense technology

EDUCATION

Pace University, Seidenberg School of Computer Science and Information Systems — New York, NY
Master of Science (MS) in Cybersecurity | GPA: 3.77/4 — May 2025

Anna University, Panimalar Engineering College — Chennai, India
Bachelor of Engineering (BE) in Computer Science and Engineering | CGPA: 7.22/10 — April 2020

TECHNICAL SKILLS & CERTIFICATIONS

Programming Languages: Python, C, HTML, CSS, SQL Database, and KQL
Operating Systems: MAC OS, Windows, Unix, Kali-Linux, Ubuntu
Tools: Wireshark, Metasploit, Nmap, Burp suite, Splunk, Tcpdump, Regshot, firewall (Pfsense), Shell scripting and PowerShell
Productivity Suites & Frameworks: office 365 (Excel, Power BI, Azure AD, MFA, Defender ATP) and MITRE ATT&CK
Certifications: Security Operations Analyst Associate (Microsoft, 2023) | Cyber Security Essentials (Cisco, 2023) | Python (Hacker Rank, 2023) | Security Fundamentals (AWS, 2023) | Security+ (CompTIA, 2024)

VIRTUAL WORK EXPERIENCE

Telstra - Cybersecurity Job Simulation, The Forage — November 2023
- Detected and responded to a malware attack using statistic and behavior analysis techniques, utilizing cybersecurity tools to swiftly mitigate the threat, and conducting a detailed incident postmortem to future incident response strategies

AIG - Shields Up - Cybersecurity Job Simulation, The Forage — October 2023
- Addressed a zero-day vulnerability through strategic utilization of industry-standard tools, including intrusion detection systems, threat intelligence platforms, and network traffic analyzers, applying ransomware bypass techniques to fortify cybersecurity defenses and safeguard vital data assets

JP Morgan Chase and Co - Cybersecurity Job Simulation, The Forage — October 2023
- Analyzed large fraud datasets, applied application security concepts to secure websites, built email classifiers for spam filtering, and designed access control systems for sensitive information through practical tasks spanning fraud detection, web application security, machine learning, and data protection strategies

VOLUNTEER EXPERIENCE

BHUMI NGO — Chennai, India
Volunteer — May 2019 – April 2020
- Facilitated impactful societal change through education, volunteerism, and environmental conservation initiatives
- Conducted 20+ introductory talk sessions & self-development programs across all age groups during COVID-19

Study Monk Pvt Ltd — Chennai, India
Student Management Lead — September 2018 – October 2018
- Implemented guidance to over 30 students, coordinated in assisting coursework navigation
- Teamed up closely with the Educational Consultant to ensure 100% accuracy in coursework review
- Planned events and increased attendance by 20% and orientation turnout by 30% through engaging initiatives

ADDITIONAL ACTIVITIES

TECH DUELS debate at Pace University on Data Privacy versus National Security — April 2024
- Advocated for individual data privacy over national security, showcasing strong rebuttals, leading the team, consisting of three members, by answering 5 questions from the judges, and handled 4 audience inquiries, resulting in the growth of public speaking skill