Bhargav Ram Puli

bhargavrampuli@gmail.com https://www.linkedin.com/in/bhargavrampuli

Professional Summary:

5+ years of experience across security research, secure code review, incident response, SIEM & SOAR integrations, security engineering, risk investigations, change management, Java, Python, and ITIL CMDB. Within my experience I have developed personal and leadership qualities and practiced them at various levels.

Education:

- Pursuing Master of Science in Cybersecurity & Trusted Systems at Purdue University - May 2022.
- Post Graduate Programme in Cyber Security from Gujarat Forensic Science University.
- Bachelor of Science in Computer Science from Osmania University.

Experience:

Incident Response Intern

IUPUI *(Indiana University Purdue University) / Indianapolis, Indiana* ***October 2021 – May 2022***

Responsibilities: Tier 1 technical analysis and response for incidents in IUPUI network.

- Perform triage, analysis, and response of routine security incidents, threats, and vulnerabilities.
- Provide security consulting to IT staff, university account holders, and external vendors for collaborations.
- Communicate and educate users regarding incidents, blocks, violations, or abuse via emails and calls.
- Identify and escalate high-impact issues to specific tier-2 investigators, team leads, and security engineers.
- Add or improve technical content in the SOP documents to stay up to date with current attack vectors.

Software Engineer - Security Research

LoginSoft */ Hyderabad, India* ***August 2019 – July 2021***

Responsibilities: Secure code review and research of vulnerabilities in open-source applications, build SOC efficient SIEM Apps, threat research & integrations to security products.

- Researched vulnerability-specific insecure code in open-source libraries and suggested patch with version information that was used by industry leading SAST tools.
- Created alerts to guide developers for using fixed versions or implement suggested fixes at the code/infrastructure level.
- Researched and generated threat feed and attributed it to actors and IOCs that are active over the web using honeypots and filtered noise before feed publication.
- Deployed and configured security tools in the network and maintained accurate logging into SIEM tools like Splunk and QRadar for faster alerting and incident management.
- Designed and developed SIEM Apps/Integrations to help SOC analysts fetch data from threat feed providers and made actionable interfaces in the SIEM environment for faster incident response.
- Gained expertise on SIEM Integrations that involve log data ingestion, developing dashboards, on-demand enrichments, and actions on IOCs based on vendor's API capabilities. Developed 3 Splunk apps and 2 QRadar apps that are live in respective marketplaces.
- Consulted as security integrations specialist to derive optimal use-cases for vendors on security platforms like SIEM/SOAR/TIP's.

Transaction Risk Investigator

Amazon */ Hyderabad, India* ***August 2016 - July 2018***

Responsibilities: To determine the possible fraud on Amazon transactions using digital fingerprinting of profiles.

- Dived deep into anomalies in transactions and took ownership of tasks to protect systems from any attacks and abuse.

- Continuously derived patterns from anomalies and created signatures to eliminate risks in the future automatically.
- Analyzed and determined the digital profile's fingerprint match and eradicated abuse of the system with the findings.
- Actively participated in strengthening the risk framework at Amazon with SOP improvements.
- Worked on operational queues, created and followed up on tickets and collaborated with related teams to drive changes by feedback.
- Performed quality audits on randomly selected transactions to determine success percentage of risk detection rules.

Environment: Risk Framework, SQL, Amazon In-House analysis tools.

Java Engineer
Atos */ Mumbai, India* ***May 2015 - May 2016***
Responsibilities: ITIL CMDB (Configuration Management Database) discovery and Java dashboard developer.
Project: Reliance JIO (India's largest telecom Industry)

- Developed UNIX scripts to discover and tag all available servers at the infrastructure level for server health monitoring. Maintained 2000+ servers information using HP UCMDB.
- Used Java JDBC to develop dashboards for instant monitoring of near expiry tickets and statuses for war room and CMDB teams.
- Developed JavaScript to make Ajax calls to APIs to retrieve datasets for dashboards.
- Collaborated with incident management, change management, configuration management database teams to review and maintain asset information and identification.
- Supported CAB (Change Advisory Board) to work on change requests in the ITIL Framework.
- Participated in high-priority incident calls and initiated war-room communication to gather system-critical information to facilitate faster resolution.

Environment: JDBC, Java, JavaScript, Unix, CMDB, ITIL Framework.

Academic Project:

Traceroute Analyzer
Networking system designed to host traceroute analysis as a web server
IUPUI (Indiana University Purdue University) */ Indianapolis, Indiana* ***Nov 2021 – Dec 2021***
Responsibilities:

- Designed a robust networking system design for continual traceroute analysis on fixed hosts.
- Developed Python scripts, Flask Rest API, and NPM web server for hosting this web service on AWS.
- Maintain and support this tool as a networking learning exercise.
- GitHub link: https://github.com/bhargavrampuli/Traceroute-Analyzer

GIRA (GUI for Important Registry Artifacts)
Windows standalone application for extraction of prominent forensics data
Gujarat Forensic Science University */ Gujarat, India* ***Jan 2019 – Feb 2019***
Responsibilities:

- Researched and collated the most used registry values from top forensic investigators in the industry through connections.
- Developed python code to create a standalone windows application that shows all important registry artifacts for forensic investigations.
- Maintain and support this tool as a community contribution.
- GitHub link: https://github.com/bhargavrampuli/GIRA

Technical Skills:

SIEM & SOAR Tools	Splunk, QRadar, XSOAR, ThreatConnect, Sentinel, ThreatQuotient.
Security tools	Burp Suite, Wireshark, Metasploit, Nikto, Nmap, Nessus, SQLmap, Dirbuster, John the ripper, Hashcat, Drozer, Mobsf, Volatility, Dex2Jar, Autopsy, Encase toolkit, FTK.
Threat intelligence tools	Intel 471, FireEye, FarSight, Bandura ThreatBlockr, Avalon, Crowdstrike, CipherTrace.
Programming languages	C, Java, JavaScript, jQuery Python, SQL, Bash.
DevOps tools	GitHub, AWS, GCP, Jira, Trello, Slack bots.
Operating Systems	Windows, macOS, Linux (Ubuntu, CentOS, RedHat, Kali, Parrot Security).

Certifications:

1. Oracle Certified Associate Java SE 7 Programmer I
2. Oracle Certified Associate Database 11g SQL Fundamentals I