MADAN CHINTHAPALLY

Overland Park, KS - (913)-238-5530 – Chinthapallymadan@gmail.com - LinkedIn

OBJECTIVE

Entry-level cybersecurity professional with hands-on experience in Tier 1–2 incident response, SIEM operations, phishing investigations, malware analysis, and cloud-based security monitoring. Skilled in network protocols, log analysis, endpoint defense, and cybersecurity documentation. CompTIA Security+ and AWS Solutions Architect certified, with a strong foundation in NIST-based incident response and cloud security best practices. Proven ability to collaborate cross-functionally and work effectively under pressure.

SKILLS SUMMARY

• Programming: Python, Java, C, SQL, JavaScript

• Security Operations: Incident Response, Log Analysis, Malware & Phishing Analysis, Threat Detection

• Quality Assurance & Testing: Selenium, TestNG, Postman, REST APIs, Automation Testing, Manual Testing, Test Planning, Defect Management

• Tools: Splunk Cloud, Elastic SIEM, Wireshark, Nessus, Snort, GuardDuty, CloudTrail, CloudWatch

• Network & Systems: TCP/IP, DNS, DHCP, VPN, Subnetting, Windows, Linux (CLI), Active Directory

• Cloud & IAM: AWS, Azure, IAM, Azure AD, VPC Flow Logs, Security Groups

• Scripting & Automation: Basic Python, Bash, AWS Lambda

• Collaboration & Documentation: Jira, Confluence, Git, ServiceNow

SOFT SKILLS

• Analytical thinking, Communication, Teamwork, Adaptability, Attention to detail

EDUCATION

University of Central Missouri **Aug 2023 -May 2025**

Master of science in Cybersecurity and Information Assurance

- GPA: 3.6/4.0
- **Relevant Coursework:** Cybersecurity Essentials, Blockchain and Applications, Wireless Networks and Protocols, Cloud Computing, Incident Response, Network Security, Software Development, Cybersecurity Policy Development, Cryptography.

CERTIFICATIONS

• CompTIA Security+, Candidate ID: COMP001022619494, OCTOBER ,2024

• AWS Certified Solutions Architect – Associate, Credential ID AWS05062897, MARCH 2025

• Azure AZ-900 Certification (Microsoft Certified: Azure Fundamentals, Credential ID: F8102194B843DFC8, APRIL ,2023

• CompTIA IT Fundamentals+, Candidate ID: COMP001022619494, SEPTEMBER ,2024

• AWS Academy Cloud Security Foundations, AWS Academy.

• PCAP: Programming Essentials in Python (Python Institute).

• Cybersecurity Essentials (CISCO).

WORK EXPERIENCE

Cybersecurity Analyst

Cognizant Technology Solutions (Cognizant), **Aug 2022-July 2023**

Tech Stack: Java, Selenium, Postman, Jira, TestRail, Confluence, AWS, Agile Methodologies, TestNG, Git, Rest APIs

- Worked as part of a collaborative cybersecurity team to deliver efficient incident detection and response.
- Monitored and analyzed security events using Splunk Cloud and Elastic SIEM.
- Investigated phishing emails and performed email header analysis to detect threats.
- Conducted vulnerability scans using Nessus and assisted with remediation.
- Assisted in cloud security assessments using AWS GuardDuty and VPC Flow Logs.
- Improved detection rules and maintained documentation in Confluence.
- Authored incident response workflows and knowledge base articles.

Quality Assurance Tester

Cognizant Technology Solutions (Cognizant), **July 2021 – July 2022**

Client: London Stock Exchange Group (LSEG) | Jul 2021 – Jul 2022

Tools & Technologies: Jira, Selenium, Java, TestNG, XML, Security Monitoring, Git, Jenkins, IT Support

- Designed and implemented automation solutions for LSEG using Selenium, Java, and TestNG, streamlining testing processes and improving efficiency.
- Collaborated with cross-functional teams to streamline testing processes, reducing testing time by 40%.
- Utilized tools like JIRA, Confluence, and Git to manage tasks and collaborate across teams.
- Applied Agile methodologies for sprint planning, backlog grooming, and iterative delivery.
- Enhanced QA processes using CI/CD pipelines and Jenkins for automated testing and deployment.
- Led migration of testing processes to AWS, ensuring seamless integration and support.
- Communicated with developers, QA managers, and stakeholders for release management.

Programmer Analyst Trainee | Cognizant Technology Solutions (Cognizant) | Internship **Jan 2021- Jun 2021**

- Trained for Quality Assurance and Cybersecurity Analyst roles.
- Supported Tier 1 troubleshooting and IT support across software environments.
- Created and executed basic automated test cases using Selenium, Java, and TestNG.
- Assisted in basic security monitoring, log analysis, and access control management.

RELAVANT PROJECTS

AWS Security Monitoring & Incident Response

Skills Used: AWS (CloudTrail, CloudWatch, GuardDuty, Lambda, SNS), IAM, Incident Response, Python (basic)

- Built and deployed a real-time security monitoring system in AWS to detect unauthorized access and policy changes.
- Integrated CloudTrail to log API events and GuardDuty for threat intelligence.
- Created alert workflows using CloudWatch and SNS to simulate SOC incident handling.
- Automated incident response triggers using Lambda functions to align with Zero Trust principles.

Threat Hunting with Elastic SIEM (MITRE ATT&CK Simulation)

Skills Used: Elastic Stack (SIEM), Sysmon, Winlogbeat, MITRE ATT&CK, Log Analysis, Bash

- Configured Elastic Stack to ingest and analyze Windows Event Logs via Winlogbeat and Sysmon.
- Created and tuned custom detection rules to identify brute-force, DLL injection, and process tampering attacks.
- Mapped findings to the MITRE ATT&CK framework and documented response actions.
- Reduced false positives by optimizing data sources and filtering noise.

Network Traffic Analysis & Intrusion Detection

Skills Used: Wireshark, TCPdump, Snort, Custom Snort Rules, DNS, TCP/IP

- Captured and analyzed packet data using Wireshark and TCPdump to detect anomalies and exploits.
- Deployed Snort IDS and developed custom rules to identify DNS tunneling, port scans, and brute-force attempts.
- Tuned rule sets to optimize accuracy and reduce alert fatigue during testing.
- Demonstrated effective use of signature-based detection in simulated lab environments.

Vulnerability Assessment & Logging Hardening

Skills Used: Nessus, rsyslog, journald, Windows Event Viewer, Linux CLI

- Performed system-level vulnerability scanning on Linux and Windows using Nessus.
- Analyzed scan results to prioritize vulnerabilities based on CVSS and asset exposure.
- Hardened local system logging configurations on Linux (rsyslog, journald) and Windows (Event Viewer).
- Ensured logging integrity for security event traceability.

Secure Web App & OWASP Top 10 Testing

Skills Used: Web Security, OWASP Top 10, Burp Suite, Secure Coding Practices

- Simulated vulnerabilities such as SQL Injection, XSS, and CSRF in a test web application.
- Used Burp Suite and manual testing to demonstrate exploit paths.
- Implemented secure coding fixes such as input validation, output encoding, and token-based authentication.
- Presented findings as part of a secure development lifecycle (SDLC) demo.

Research Paper: AI in Cybersecurity

Skills Used: Machine Learning Concepts, SOC Automation, Threat Intelligence

- Researched and authored a technical paper on the application of machine learning in cybersecurity.
- Covered real-world use cases in malware classification, anomaly detection, and predictive threat modeling.
- Discussed how AI can enhance SOC efficiency by automating triage and prioritization of security incidents.

ADDITIONAL INFORMATION

• Leadership Experience |Chairperson |SAE Club, VBIT June 2021 to March 2022

Led a team in organizing technical events, fostering community engagement and professional development.

Additional Languages: Spanish (Introductory proficiency) , Telugu (Native Fluency) ,Hindi (Bilingual proficiency)