Jagadeesh Varma Kakarlapudi

+1(832)9082143 | jagadeeshvarmasce@gmail.com | LinkedIn | GitHub | Portfolio

Objective

Cybersecurity professional with a Master's degree and hands-on experience in intrusion detection, threat analysis, and vulnerability assessments. Skilled in Snort, ELK Stack, Nessus, and Python, with a strong foundation in SIEM, incident response, and security frameworks. Committed to continuous improvement, clear communication, and delivering effective security solutions.

Education

University of Houston, Houston, TX. *May 2025*

Masters in Cybersecurity *GPA - 3.96*

Data & network security, Data science for Cybersecurity, Design data analytic solutions, cryptography, SOC, and advanced SOC Analysis, Risk management.

GVP College of Engineering, India. *July 2023*

Bachelor of Technology Electronics and Communication Engineering *GPA – 3.20*

Projects

SOC Analyst Project - Threat Correlation, Alerting, and Detection Engineering

- Deployed and configured ELK Stack (Elasticsearch, Logstash, Kibana) for centralized log management, improving threat detection and security monitoring. Ingested and analyzed logs from firewalls, servers, endpoints, and cloud environments, detecting and responding to security incidents.
- Developed custom SIEM correlation rules to identify brute-force attacks, privilege escalation, and anomalous logins, enhancing SOC threat detection accuracy and designing real-time Kibana dashboards
- Configured ElastAlert for automated alerting, enabling real-time notifications for unauthorized access, lateral movement, and high-risk security events. Reduced false positives by 35% through log enrichment, threshold tuning and integrated external threat intelligence feeds to detect and block malicious IPs, domains, and threat actors.

Security Analyst Project - Network Threat Detection using Snort & Logstash

- Centralized system, application, network, and security logs with Logstash and Event Viewer for intrusion detection, using SIEM to improve incident response
- Built Kibana dashboard, visualizations, and alerts in Kibana to monitor suspicious activities, document findings, to streamline threat response efficiency.
- Implemented and deployed Snort for network intrusion detection, achieving a 95% detection rate for known threats, and developed custom rules to reduce security incidents by 30%.

Cyber Threat Analyst Project - ML-Based Intrusion Detection using UNSW-NB15 Dataset (Coursework Project)

- Developed a network intrusion detection system using the UNSW-NB15 dataset and machine learning models (Random Forest, SVM, Logistic Regression).
- Implemented optimized feature selection and IQR-based outlier detection, improving threat detection accuracy by 15%.
- Built a Python-based command-line tool for anomaly detection with CSV export, and generated HTML reports featuring visualizations and statistical summaries for streamlined threat analysis.

Skills

Languages & Operating Systems: Python, C, HTML, Bash, Windows, MacOS, Kali, Ubuntu, CentOS, BlackArch Linux, Verilog,
Vulnerability Assessment: Nessus, Nikto, Wireshark, Burp Suite, Metasploit, TCP dump, Nmap, OpenVAS.

Threat Intelligence & Technologies: Security Onion**,** Azure Sentinel, Event Viewer, Threat Hunting, OSINT, SIEM (Splunk), Intelligence Report writing.

Cloud Security & Network tools: Azure, Docker, Kubernetes**,** IPsec, VLAN, TCP/IP, DNS, VPN, Zeek, Ettercap, PuTTY.

Security Architecture & Frameworks: ISO27001, NIST 800-53, NIST 800-61, NIST Risk Management(RMF), HIPAA, FISMA, Palo Alto Networks, Snort/Suricata.

Office Productivity: Microsoft 365(Share Point), Google Workspace(Sheets, Docs), WinRAR, 7Zip.

Soft Skills: Attention to detail, Analytical Thinking, Team Coordination, Communication, Adaptability, Technical documentation.

Certifications

- **EC-Council Certified Ethical Hacker (CEH)**
- **IBM Cybersecurity Analyst Professional**
- **Google Cybersecurity Professional**
- **SIEM Splunk Hands-On Guide Specialization**
- **Palo Alto Networks Cybersecurity Professional**
- **Practical Ethical Hacking by TCM Security**
- **Microsoft's MTA: Security Fundamentals**