Jagadeesh Varma Kakarlapudi

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

EDUCATIONT

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

Masters in Cybersecurity *GPA - 3.96/4*

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 – 3.20/4*

RESEARCH EXPERIENCE

SIEM Implementation, Rule Customization, and Threat Detection Optimization

- 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 designed real-time Kibana dashboards, reducing incident detection time by 40% and improving SOC operational efficiency.
- 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.

PROJECTS

Log Analysis, Intrusion Detection & Prevention system with Snort

- Centralized system, application, network, and security logs with Logstash and Event Viewer for intrusion detection, using SIEM to improve incident response
- Created dashboards, 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%.
- Integrated Snort with machine learning techniques, boosting detection accuracy by 20% and cutting down security incidents by 50% through continuous monitoring and rule optimization.

Vulnerability Assessment on a Network

- Conducted vulnerability assessments using Nessus and OpenVAS, identifying and prioritizing 8+ critical issues. Applied risk management best practices and mitigated 75% of vulnerabilities. Used SIEM (for log analysis and threat intelligence to support incident response and improve network security.
- Created detailed vulnerability reports with actionable insights, improving security compliance by 30% and strengthening network security.

Implemented Security Framework for IoT Devices

- Formulated a comprehensive cybersecurity framework for IoT environments, including device inventory management, firmware updates, and secure configuration protocols to safeguard against unauthorized access, cyber threats, and data loss prevention (DLP).
- Implemented network segmentation, real-time traffic analysis, and centralized logging with a Security Information and Event Management (SIEM) system to detect suspicious activities, enhance cyber threat monitoring, and optimize security operations for faster incident response.

SKILLS

Languages & Operating Systems: Python, C, Windows, Kali, Ubuntu, CentOS, Back Arch Linux, Security Onion.

Vulnerability Assessment: Nessus, Nikto, Wireshark, Burp Suite, Metasploit, TCP dump, Nmap, OpenVAS.

SIEM and technologies: Security Onion**,** Splunk, Linux, Azure Sentinel, Event Viewer.

Threat Intelligence: Threat Hunting, OSINT, Event Viewer, Intelligence Report writing.

Network and System: IPsec, VLAN, TCP/IP, DNS, VPN, Zeek, Ettercap, Putty.

Security Architecture: Palo Alto Networks, Snort/Suricata.

Security Framework: ISO27001, NIST 800-53, NIST 800-61, NIST Risk Management(RMF), HIPAA, FISMA.

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

CEH(V11) by EC-Council

Google Cybersecurity Professional

Introduction to SIEM (Splunk)

Microsoft's MTA: Security Fundamentals

Practical Ethical Hacking by TCM Security

Palo Alto Cybersecurity Professional