JASWANTH KARNAM SOMASEKHAR

Jersey City, NJ • ksjaswanth98@gmail.com • +1 (201) 726-0760
linkedin.com/in/jaswanthks • jaswanthks.com • github.com/jaswanthks

PROFESSIONAL SUMMARY

Cybersecurity professional with an M.S. in Cybersecurity and Privacy (NJIT, 2026) and 2.5 years of enterprise software and production-support experience on JPMorgan Chase banking systems. Hands-on experience building and operating a Microsoft Sentinel SOC environment - ingesting logs, writing KQL detection rules, simulating attacks, and triaging incidents. Strong foundation in network security, intrusion detection, and threat analysis. Seeking an entry-level SOC Analyst role to apply skills in SIEM monitoring, threat detection, and incident response.

TECHNICAL SKILLS

SIEM & Security Operations: Microsoft Sentinel, KQL, Log Analytics, Security Monitoring, Threat Detection, Incident Detection & Response, Alert Triage, Threat Analysis, MITRE ATT&CK

Security Tools: Nmap, Metasploit, Hydra, Suricata IDS, IPFire Firewall, Wireshark, Kali Linux, Slowloris

Cloud: Microsoft Azure, Log Analytics Workspace, Data Collection Rules, Microsoft Defender for Cloud, Azure Key Vault, Azure Firewall, AWS EC2

Networking: TCP/IP, DNS, HTTP/HTTPS, FTP, SSH, Firewalls, IDS/IPS, Vulnerability Assessment, Network Protocol Analysis

Programming & Scripting: Java, Python, JavaScript, SQL, ESQL, Bash, HTML/CSS

Operating Systems & Tools: Linux (Ubuntu, Kali), Windows, Git, GitHub, Jira, VS Code, Eclipse

SECURITY PROJECTS

Home SOC Lab — Microsoft Sentinel SIEM 2026
Azure | Microsoft Sentinel | KQL | Kali Linux | Windows 11 | Hydra

- Built an end-to-end SOC environment in Microsoft Azure, deploying a Log Analytics Workspace, Data Collection Rules, and the Windows Security Events connector to centralize log ingestion from a Windows 11 endpoint.
- Simulated brute-force authentication attacks using Hydra from a Kali Linux attacker VM to generate realistic failed-logon telemetry for detection engineering.
- Authored custom KQL analytics rules in Microsoft Sentinel to detect brute-force patterns, automatically generating incidents and alerts.
- Performed incident triage and investigation, correlating security events to identify attacker source IPs and targeted accounts; documented the full build and methodology in a public GitHub repository.

Defensive Network Security Lab — Suricata, IPFire & Kali Linux Nov 2025
NJIT | Kali Linux, Ubuntu, Suricata IDS, IPFire Firewall, Nmap, Metasploit, Slowloris

- Designed a multi-VM defensive network (Ubuntu victim, Kali attacker, Suricata IDS, IPFire firewall) simulating an enterprise security architecture with network segmentation and firewall policies.
- Performed reconnaissance and vulnerability assessment with Nmap (host discovery, TCP SYN scans, service enumeration, OS fingerprinting, stealth scanning).
- Conducted exploitation testing against a vulnerable ProFTPD service via Metasploit and simulated DoS attacks with Slowloris against an Apache server to evaluate detection and availability impact.
- Configured Suricata IDS rules to alert on reconnaissance, exploitation, and DoS traffic, and IPFire rules to block malicious connections; analyzed IDS and firewall logs to assess defense-in-depth.

PROFESSIONAL EXPERIENCE

Associate Software Engineer — Mphasis Dec 2021 – Jun 2024
Client: JPMorgan Chase — Core Deposit Platform (CDP) | Hyderabad, India

- Developed, enhanced, and maintained integration flows and banking application components on JPMorgan Chase's Core Deposit Platform using IBM Integration Bus (IIB) and ESQL.
- Provided production support by analyzing application logs, troubleshooting issues, and resolving incidents to ensure availability of critical financial systems.
- Performed certificate renewal, application testing, and deployment validation to maintain secure and reliable operations in a regulated banking environment.
- Conducted root cause analysis and collaborated with development, testing, and support teams to deliver fixes and production releases within an Agile workflow.

EDUCATION

M.S., Cybersecurity and Privacy 2024 – 2026
New Jersey Institute of Technology (NJIT) — Newark, NJ

B.E., Computer Science and Engineering 2016 – 2020
IFET College of Engineering — Villupuram, India

CERTIFICATIONS

Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900) Exam Scheduled
Cisco Introduction to Cybersecurity 2026
IBM zSystems Cybersecurity Insights 2026
IBM z/OS Security Essentials 2026
IBM Transitioning to Quantum-Safe Cryptography on IBM Z 2026

PUBLICATIONS

- Jaswanth K S, Dr. D. Stalin David, “A Novel Based 3D Facial Expression Detection Using Recurrent Neural Network,” IJSRCSEIT, ISSN: 2456-3307, Vol. 6, Issue 2, pp. 48–53, Mar–Apr 2020.