

VIKAS MAHESHWARAM

+1 414-807-3010 | vikas.splunk2@gmail.com | [Linkedin.vikasreddy6668](https://www.linkedin.com/in/vikasreddy6668)

SUMMARY

SOC Analyst with hands-on experience in SIEM platforms (Splunk, ELK), real-time log monitoring, and incident response workflows. Strong capability in identifying threats through malware analysis, IOC enrichment, MITRE ATT&CK mapping, and packet analysis using Wireshark. Proficient with Nessus, Qualys, Nmap, and various security tools to enhance visibility and improve detection accuracy across enterprise environments.

TECHNICAL SKILLS

- **Security Operations:** SIEM (Splunk, ELK/Kibana), Log Monitoring, Incident Response
- **Threat Detection:** Malware Analysis, IOC Collection, MITRE ATT&CK
- **EDR/XDR:** CrowdStrike, Carbon Black, Microsoft Defender ATP
- **Threat Intelligence:** VirusTotal, Abuse.ch, AlienVault OTX
- **Vulnerability Management:** Nessus, Qualys, Patch Management, OpenVAS (basic)
- **Cloud Security:** IAM, AWS/Azure Security Fundamentals, AWS CloudTrail, Azure Monitor
- **Log Sources:** Windows Event Logs, Syslogs, Firewall Logs, VPN Logs
- **Email Security:** Proofpoint, Microsoft Defender for Office 365 (EOP)
- **SOAR Platforms:** Splunk SOAR (Phantom), Playbook Automation
- **Networking & Security:** TCP/IP, Firewalls, IDS/IPS, VPNs, Wireshark, Snort, Suricata, Zeek
- **Endpoint Management:** Microsoft Intune, SCCM/MECM, Group Policy (GPO)
- **OS & Scripting:** Linux (Kali, Ubuntu), Windows Server, Python for Automation (log parsing, IOC extraction)
- **Tools:** Nmap, Burp Suite (basic), Kibana, Hybrid Analysis
- **Version Control:** Git, GitHub
- **Ticketing Tools:** ServiceNow, Jira

PROFESSIONAL EXPERIENCE

TATA CONSULTANCY SERVICES (TCS)

SOC ANALYST

INDIA · Mar 2021 - Sep 2023

- Monitored security events using Splunk, ELK, and performed log analysis to detect threats and escalate incidents.
- Conducted malware analysis (static/dynamic) and generated IOCs to enhance threat detection and SIEM rules.
- Performed incident triage, investigation, containment, and remediation for malware, phishing, and network intrusions.
- Analyzed network traffic with Wireshark, TCP/IP, IDS/IPS, and identified suspicious connections or lateral movement.
- Executed vulnerability scans using Nessus, Qualys and supported patch management activities.
- Used Python/Bash scripts to automate log parsing and indicator extraction.
- Collaborated with network/security teams to improve firewall, IPS, and endpoint protections.
- Documented incidents, prepared reports, and updated IR runbooks aligned with MITRE ATT&CK.
- Reviewed and analyzed Windows Event Logs, Syslogs, firewall logs, and VPN logs to identify authentication anomalies, unauthorized access attempts, and potential indicators of compromise.
- Monitored cloud environments leveraging AWS/Azure IAM concepts to evaluate access permissions, detect misconfigurations, and strengthen identity-based security controls.
- Investigated cloud-related security alerts by validating IAM roles, policy changes, login behaviors, and privileged access events to ensure compliance with security standards.

IT SECURITY SPECIALIST

INDIA · Mar 2020 - Feb 2021

- Performed vulnerability scanning using Nessus/Qualys and coordinated remediation with system and network teams to reduce high-risk exposures.
- Monitored Windows Event Logs, Syslogs, firewall logs, and VPN logs to identify suspicious activities, unauthorized access attempts, and policy violations.
- Managed IAM access controls by creating, modifying, and revoking user accounts, enforcing least privilege, and investigating login anomalies.

- Supported endpoint security by ensuring patch compliance, antivirus updates, and system hardening across organization-wide devices.
- Assisted in incident response by collecting logs, analyzing impacted endpoints, validating alerts, and escalating confirmed incidents to senior SOC analysts.

EDUCATION

Concordia University Wisconsin, USA
Master's, Computer Science (Software Engineering)

Oct 2023 - Oct 2025
USA

CERTIFICATIONS & TRAINING

- **Cisco:** Cisco IT Essentials, Introduction to Cybersecurity
- **IBM:** Cybersecurity Fundamentals
- **Palo Alto Networks:** Cloud Security Fundamentals, Certified Cybersecurity Practitioner, Network Security Fundamentals
- **ISC2:** CC Certified in Cybersecurity (CC)
- **Cybersecurity from beginner to Expert:** Udemy
- **Splunk:** Splunk Enterprise Security (eLearning), Splunk Fundamentals, Splunk Observability Cloud & SOAR, SOC Essentials, Detection Engineering
- **CompTIA Security + & CySA+:** In Progress