Vikas Maheshwaram

+1 414-807-3010 | LinkedIn | vikas.splunk2@gmail.com | Portfolio

SUMMARY

Cybersecurity professional with 4+ years of experience across SOC operations, incident response, vulnerability management, and cloud security within healthcare and enterprise environments. Proven expertise in SIEM/SOAR platforms (Splunk ES, QRadar, Sentinel), MITRE ATT&CK–driven threat detection, DFIR, and threat intelligence, with a strong focus on reducing MTTD/MTTR and false positives. Hands-on experience securing cloud and hybrid infrastructures (AWS, Azure, GCP), enforcing HIPAA, SOX, NIST, ISO 27001, PCI-DSS compliance, and leading enterprise vulnerability remediation programs. Strong background in automation and DevSecOps, leveraging Python, Bash, CI/CD security integration, SAST/DAST, IAM, and secrets management to strengthen secure SDLC practices. Adept at cross-functional collaboration, executive reporting, and mentoring, with a continuous-learning mindset and multiple industry certifications in progress.

EDUCATION

Masters of Science in Computer Science | **Concordia University Wisconsin, USA** Dec 2025

SKILLS & CERTIFICATION

Security Operations & Incident Response: Splunk ES, IBM QRadar, Microsoft Sentinel, Elastic SIEM, ArcSight, Cortex XSOAR, TheHive, Phantom (Splunk SOAR), ServiceNow SIR, Jira, Security Onion, NIST SP 800-61, MITRE ATT&CK, Cyber Kill Chain, Threat Hunting, Automated Playbooks, Incident Handling, Alert Triage, Log Analysis

Threat Intelligence & Analysis: MITRE ATT&CK, Diamond Model, Cisco Talos, VirusTotal, Phishtank, KnowBe4, MISP, Adversary TTP Mapping, Threat Enrichment Pipelines, OSINT (Any.run, Recon-ng, Maltego, Emailrep, ExifTool)

Vulnerability & Risk Management: Qualys, Nessus, OpenVAS, Tenable, Burp Suite, OWASP ZAP, CVSS Scoring, Secure SDLC, Risk Register, Software Risk Analysis, NIST Risk Framework

Digital Forensics & Malware Analysis (DFIR): Axiom Cyber, FTK, Autopsy, Volatility, Redline, Ghidra, Sysinternals, Memory & Disk Analysis, Reverse Engineering

Endpoint & Network Security: CrowdStrike, Carbon Black, Cortex XDR, MS Defender for Endpoint, Suricata, Zeek, Snort, Wireshark, Nmap, Deep Packet Inspection, Windows Event Logs, Osquery, Protocol Analysis (VPN, TCP/UDP, ARP, OSPF)

Governance, Risk & Compliance (GRC): SOX, HIPAA, PCI-DSS, ISO 27001, CIS Benchmarks, STRIDE, CAPEC, GLBA, FFIEC, SOC 2 Type II, Audit Support, Policy Adherence

Cloud & Hybrid Security: AWS (IAM, Security Hub, S3, VPC, WAF), Azure (Sentinel, Defender, AD, Key Vault), GCP (Chronicle), Microservices & Hybrid Infrastructure Monitoring

Scripting & Automation: Python, Bash, SQL, Log Parsing, CI/CD Security Integration, DevSecOps Workflows

Soft Skills: Analytical Thinking, Communication, Planning & Articulation, Collaboration, Resilience, Time & Stress Management, Continuous Learning, Ethical Mindset

CERTIFICATION: Cisco IT Essentials, Introduction to Cybersecurity | IBM Cybersecurity Fundamentals | Cloud Security Fundamentals, Certified Cybersecurity Practitioner, Network Security Funda mentals | 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

EXPERIENCE

Centene Health, USA | SOC Analyst **Jun 2025 - Present**

- Supported IT Compliance initiatives for healthcare infrastructure, ensuring adherence to HIPAA, SOX, ITGC (COBIT), FedRAMP, and NIST 800-53 standards, conducted third-party vendor risk assessments and Azure cloud compliance reviews for secure adoption of healthcare applications.
- Monitored and triaged security alerts in Splunk, QRadar, AWS Security Hub, and CrowdStrike Falcon using custom SPL, RegEx, and MITRE ATT&CK, reducing false positives by 30% and accelerating incident response across healthcare IT environments.
- Investigated Indicators of Compromise (IOCs) and performed threat attribution using Wireshark, Osquery, Axiom Cyber, MISP, and OSINT tools, conducted packet-level forensics, persistence checks (WMI, registry keys), and mapped findings to MITRE TA0003 and CIS controls to protect sensitive patient health data.
- Conducted vulnerability assessments with Nessus (CVSS, EPSS, KEV), automated CVE-CMDB enrichment with Python/Bash, and improved MTTD/MTTR by 40% while enhancing firewall policies to prevent C2 traffic and lateral movement, ensuring HIPAA, HITRUST, and HITECH compliance.
- Executed Data Loss Prevention (DLP), encryption, and threat monitoring strategies to safeguard Protected Health Information (PHI), leveraged forensic tools (EnCase, FTK, Cellebrite, Gargoyle, IEF) for healthcare security investigations and supported migration of hospital security infrastructure to Fortigate FG 100D.

KPIT, India | Cyber Security Engineer **Jun 2020 - Sep 2023**

- Integrated Veracode SAST/DAST into CI/CD pipelines and enforced secure coding practices, reducing post-deployment vulnerabilities by 60% across BFSI and healthcare software solutions.
- Configured and managed HashiCorp Vault for cryptographic secrets management, automated access control enforcement, and secure key lifecycle management to protect sensitive application data.
- Conducted forensic investigations across memory, disk, and network layers, led SOC response for application-level incidents, and deployed micro-segmentation and IDS/IPS controls to mitigate lateral movement in client development and test environments.
- Tuned DLP policies, developed OSINT-driven threat intelligence feeds mapped to MITRE ATT&CK, and executed third-party vendor risk assessments, ensuring compliance with ISO 27001, NIST, and client security SLAs.
- Hardened application servers, containers, and APIs using CIS Benchmarks, secured WAFs against OWASP Top 10 vulnerabilities, mentored junior engineers in secure coding and threat hunting, and delivered Splunk-powered cyber risk dashboards to leadership for real-time visibility.
- Developed advanced detection use cases leveraging Windows Event Logs, Osquery, and MITRE ATT&CK mapping, enforced CIS Control 8 and ISO 27001 A.12.4 standards to strengthen application logging, monitoring, and early threat detection across software development environments.
- Integrated privileged identity management with CyberArk and automated IAM workflows with Saviynt for AD/Azure AD, reducing provisioning errors by 80% and improving secure access management within hybrid development ecosystems.
- Supported secure SDLC practices and CI/CD pipeline security by enforcing PCI DSS and ISO 27001 controls for logging, access reviews, and incident response, ensuring audit readiness for client software projects.