[**www.linkedin.com/in/sowmyasrinivvasan/**](http://www.linkedin.com/in/sowmyasrinivvasan/) **| +1 2267983520**

[**sowmyasrinivvasan@gmail.com**](mailto:%20sowmyasrinivvasan@gmail.com)  **| Toronto, Canada**

**Sowmya Srinivasan**

**Cybersecurity Engineer | SOC Analyst**

**Azure Security | AWS | IAM | Penetration | SIEM| | Network Security |OWASP |Okta| Splunk | Wireshark**

**Professional Summary:**

* **12 years** of **IT** experience**,** including **4 years** as a **Cyber Security Analyst** specializing in **network security, cloud security (Microsoft Cloud), and ethical hacking, with expertise in cybersecurity tools, vulnerability scanners, and SIEM platforms,** along with **QA experience in test planning, defect** management, and team leadership
* Extensive hands-on experience **in Incident Response and Threat Hunting,** utilizing tools like **SIEM, and SOAR** to performvulnerability assessments**, exploit analysis, and security** hardening in alignment with **OWASP Top 10 and MITRE ATT&CK** frameworks
* Good at Improving real-time security alert accuracy by **45%** by optimizing **SIEM** configurations in **Splunk and QRadar**, enabling faster threat detection and incident response
* Real-time experience in conducting **50+ penetration tests** with **Nessus and Metasploit,** monitoring 3,000+ security events daily using Splunk, and utilizing forensic tools for data recovery and expertise in security governance, risk, and compliance, with a focus on protecting digital assets
* Proficient in **PowerShell** and **Linux programming,** developing custom cybersecurity **tools and scripts** to automate complex security tasks, optimize workflows, and increase overall operational efficiency
* Extensive experience with cloud-native security tools, including **AWS Guard Duty, Azure Security Center,** and Microsoft Sentinel, for continuous threat monitoring, compliance enforcement, and risk management.
* Collaborative in working with IT Infrastructure Teams to integrate **Privileged Access Management (PAM**) and **Identity Access Management (IAM)** solutions, ensuring seamless compliance with enterprise certification systems, security policies, and regulatory standards
* In-depth understanding of compliance frameworks & risk management, ensuring full adherence to **ISO 27001, NIST, PCI** **DSS, and GDPR standards,** conducting security audits, gap analysis, and remediation strategies
* Expertise in using **firewalls, Intrusion Detection/Prevention Systems (IDS/IPS),** proxy servers, and log aggregation technology to detect, analyze, and respond to network breaches, providing real-time insights into security threats.
* Extensive experience with **Wireshark f**or packet analysis to investigate security incidents, including **TCP/IP** traffic analysis and vulnerability assessments for web applications and network **penetration testing**
* Proficient in both **Agile and Waterfall methodologies,** leveraging **AI tools** to enhance project delivery efficiency, improve decision-making, and maintain effective team collaboration to meet organizational goals and security requirements

**Key Bootcamp Projects:**

* **VSI Custom Monitoring Environment :** Designed and implemented a Splunk-based monitoring solution for detecting and responding to security threats, leveraging log aggregation, correlation, and SPL for real-time monitoring
* **Malware Analysis in Isolated Sandbox :** Led setup of a malware analysis lab using VMware, FLARE-VM, and INetSim, conducting dynamic analysis and network traffic inspection to identify C2 communication and malicious behavior
* **Penetration Testing (CTF Style**) : Conducted penetration testing on web applications, Linux, and Windows servers, exploiting vulnerabilities like SQL injection and XSS, while compiling risk assessments and actionable security recommendations
* **Linux Server Hardening:** Secured Linux servers by applying best practices for user management, SSH configuration, and automation, enhancing security through key-based authentication and system updates
* **Cloud Security Project :** Deployed and secured a cloud-based application on AWS, implementing IAM, encryption, and security monitoring to ensure robust protection and compliance with best practices

**Education & Certifications:**

* **Cybersecurity Bootcamp** University of Toronto, Canada **Oct 2024 - April 2025**
* **Masters of Computer Technology,** Anna University ,India **Sep 2006 - May 2011**
* Certified in **CompTIA Security+**
* Completed Business Analysis Fundamentals

**Professional Experience:**

**IT Cyber security Analyst ACL Digital, India Mar 2022- Jan 2024**

* Ensured adherence to regulatory standards such as GDPR, ISO 27001, and PCI DSS, maintaining audit readiness and enforcing security policies to mitigate risks and enhance the security posture
* Performed comprehensive security assessments of internal systems and third-party vendors to ensure compliance with PCI DSS, ISO 27001, NIST, GDPR, and HIPAA frameworks
* Led thorough vulnerability assessments using tools like Nessus, Qualys, and Rapid7 Nexpose, identifying and remediating security vulnerabilities across IT infrastructures
* Implemented security policies, standards, and procedures to boost cybersecurity maturity, improve risk management, and ensure regulatory compliance
* Analyzed and responded to security incidents, conducted root cause analysis (RCA), and implemented remediation plans to prevent recurrence and reduce impact
* Configured and managed firewalls (Cisco ASA, Palo Alto Networks, Check Point) to strengthen network security and access controls
* Deployed and managed endpoint security solutions, including Microsoft Defender for Endpoint, Intune, Defender Antivirus, and SCCM, protecting endpoints against malware and unauthorized access
* Integrated and managed SIEM platforms such as Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Purview Audit for real-time threat detection, log analysis, and security incident monitoring
* Installed and operated security software, including firewalls and data encryption tools, while developing IT security best practices for the organization
* Led secure development initiatives focused on mitigating OWASP Top 10 vulnerabilities, conducting penetration tests and vulnerability assessments, and addressing security gaps
* Conducted regular security training sessions to improve team compliance and cybersecurity awareness, including phishing simulations and security awareness programs
* Performed security assessments and authored audit reports, identifying gaps in security controls and providing detailed remediation recommendations

**Lead I- Software Testing & IT Security Analyst UST Global, India July 2011-Mar 2022**

* Led a 15-member team to design, develop, and maintain the testing process for web applications, ensuring optimal efficiency and quality and Engaged in story grooming and evaluated story points for 75 epics, successfully completing most stories within the estimated timeline, meeting project deadlines.
* Collaborated with project management to understand project requirements and translated them into detailed test cases for accurate test execution.
* Ensured comprehensive test coverage to identify technology solution gaps and meet acceptance criteria, guaranteeing reliable and functional deliverables.
* Designed and managed complete regression test suites, each containing over 2,500 test cases, built from scratch, enhancing test coverage and effectiveness.
* Took responsibility for generating test cases and scripts based on business requirements and specifications, adhering to Agile practices and continuous improvement and Analyzed business requirements, identified gaps, and worked closely with project coordinators to clarify ambiguities and ensure alignment with stakeholder
* Provided real-time guidance on network configuration, security settings, and mitigation procedures based on security frameworks such as MITRE ATT&CK, Cyber Kill Chain, and NIST
* Conducted 24/7 SOC monitoring and log analysis, managing data from various devices including antivirus systems, firewalls, APTs, domain controllers, switches, routers, proxy servers, and VPNs
* Monitored dashboards, created reports and charts in SIEM tools, and monitored various servers and network devices for security events and anomalies
* Staying up to date with industry trends, Azure updates, and best practices in the field of Azure Cloud projects
* Developed cyber incident response plans, playbooks, and fine-tuned processes to enable rapid and effective incident responses using advanced platforms and management tools. Participated in cybersecurity awareness training programs to ensure all personnel knew their roles and responsibilities in maintaining security.
* Leveraged threat intelligence platforms such as Recorded Future, ThreatConnect, Anomali, and MISP to gather and analyze threat data, enhancing the organization’s proactive defense capabilities
* Utilized email security solutions such as Proofpoint, Mimecast, and Microsoft Defender for Office 365 to protect the organization from email-based threats, including phishing and malware

**Skill Matrix:**

* **Cybersecurity Fundamentals** :Network Security, Penetration Testing, Vulnerability Assessment, Incident Response, Risk Management, Ethical Hacking, Malware Analysis, Web & Email Security, Data Loss Prevention (DLP), Compliance (NIST CSF, ISO 27001, COBIT, GDPR)
* **Penetration Testing & Vulnerability :** Metasploit, Burp Suite, Nmap, SQLMap, Kali Linux, Nessus, OpenVAS, Qualys
* **Network & Traffic Analysis** : Wireshark, NetFlow Analyzer, TCP/IP, Snort, Security Onion
* **Cloud & Endpoint Security:** AWS Security Hub, Azure Security Center, Symantec Endpoint Protection, McAfee Endpoint Security, CrowdStrike Falcon
* **SIEM & IDS/IPS:** Splunk, ArcSight, QRadar, Cisco Firepower, Palo Alto Networks
* **Programming Languages:** Python, PowerShell, Linux
* **Identity & Access Management (IAM)** : Okta, Microsoft Azure AD, SailPoint
* **Firewalls & Encryption**: Palo Alto Networks, Fortinet FortiGate, Check Point, VeraCrypt, BitLocker, OpenSSL, PGP/GPG
* **Threat Intelligence & Incident Response:** Recorded Future, ThreatConnect, Anomali, MISP, INetSim, Procmon, Sysmon, Volatility, FLARE VM, Mimikatz, John the Ripper, Cobalt Strike
* **Collaboration, Presentation & Project Management:** Microsoft Office Suite (Word, Excel, Outlook, PowerPoint), Microsoft Teams, Webex, Agile Methodologies (Scrum), Software Test Lifecycle (STLC), Defect Management, JIRA, Trellod