SHRUTIKA JOSHI

San Francisco Bay Area, CA - 94587 | 667-406-7447 | shrutjoshi75@gmail.com | www.linkedin.com/in/joshishrutika

PROFESSIONAL SUMMARY

Self-motivated cybersecurity professional with over six years of experience specializing in Security Operations and Incident Response. Proven expertise in monitoring, investigating, and responding to security incidents across cloud and enterprise environments. Adept at developing and enforcing security policies, conducting vulnerability assessments, threat hunting, and ensuring compliance with industry standards and regulations. Strong communication skills and a demonstrated ability to lead and collaborate effectively across teams.

EDUCATION

University of Maryland - Baltimore County | MS in Cyber Security, GPA – 3.6 — Jan 2023 – Dec 2024

Pune University | M.Sc. Computer Science, *GPA – 3.52* — Aug 2015 – April 2017

SKILLS

Programming	Python, JavaScript, MYSQL, SQL, PowerShell, Splunk query language
Security Tools	EDR (Crowdstrike Falcon), SIEM (Splunk, Qradar), Symantec DLP, SOAR, ServiceNow, KnowBe4, PhishER, Symantec Messagelab, Microsoft Defender Mediapro security Training platform, SCCM, JAMF, Qualys, Zscaler, Confluence, Microsoft Office Suite, Nmap, Wireshark, Metasploit, IDS, IPS, Snort rules, YARA rules, Docker, Kubernetes, Static and Dynamic malware analysis tools
Cloud	AWS, Azure, DevSecOps
Forensic Tools	Autopsy, Static and Dynamic malware analysis tools, FTK Analyzer, Ghidra, Volatility, Burpsuite, Encase, ProDiscover, NetworkMiner, Hydra
Security & Compliance	NIST 800-53, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27001, MITRE ATT&CK Framework, OWASP Top 10

CERTIFICATIONS

CompTIA CySA+, CompTIA Network+
AWS Cloud Practitioner, AZ-900 Microsoft Azure Fundamentals
SANS AIS247 – AI Security Essentials for Business Leaders
SANS SEC504 – Hacker Tools, Techniques, Incident Handling | GCIH – expected March 2025

WORK HISTORY

Information Security Analyst, VERITAS Technologies LLC, Pune, India — Jun 2019 – Jan 2023

- Led investigations into **advance security threats** based on **signature trends, log analysis and patterns** by leveraging tools **Crowdstrike Falcon, Symantec DLP, and Splunk, reducing false positive by 30%.** Investigated **attack patterns**, mapped **adversary behaviors** to **MITRE ATT&CK**, and recommended **security improvements**.
- **Created and fine-tuned Splunk correlation searches** to detect viruses and anomalous behavior. **Developed dashboards in Splunk** for real-time monitoring of suspicious events, **enhancing the overall security posture** of the organization.
- Managed and optimized **Crowdstrike Falcon EDR platform**, by refining **detection rules** and **threat intelligence feed**s, **reducing incident response time by 40%.**
- Enhanced **cloud security** by effectively responding to **alerts from AWS, GCP and Azure environments**, ensuring **real-time monitoring, detection, and resolution** of incidents in cloud infrastructure.
- Conducted **proactive threat hunting** using the **MITRE ATT&CK, Cyber Kill Chain framework**, identifying and mitigating **advanced threats and tracked APT groups.**
- Prepared **threat intelligence reports** by analyzing **threat advisories**, **attacker TTPs,** and recent threats. Coordinated with various teams to block **known IOCs** (Indicators of Compromise) and vulnerabilities, enhancing the organization's defensive capabilities.
- Assisted support in vulnerability management. Applied knowledge of **common vulnerability frameworks**, such as **CVSS and OWASP Top 10**, to evaluate the severity and impact of vulnerabilities.
- Participated in the **enforcement of internal security policies**, **conducting risk assessment** and ensuring **compliance** with standards such as **NIST, GDPR and CMMC**, contributing to **internal audits**.
- Led **knowledge transfer sessions** for over **10 plus employees and three interns**, accelerating their onboarding and enhancing team performance. Developed **security playbooks and workflows**, defining processes for security incidents, source code handling, GDPR and CMMC compliance, phishing and other security threats. Contributed to the yearly **Security Tabletop exercise** to test and improve **incident response strategies**.

Associate Security Analyst, VERITAS Technologies LLC, Pune, India — Jun 2017 – Jun 2019

- Provided **timely detection, investigation and mitigation** of **security incidents**, maintaining **100% SLA compliance by** Coordinating with MSSP, networking, governance risk & compliance, investigation, and security architecture teams to track and close security incidents using the **ServiceNow** ticketing system.
- Designed and delivered **annual security awareness** training for the entire organization around **5000+ employees** using **Mediapro and KnowBe4** platforms, fostering a culture of security awareness.
- Monitored and responded to **email security alerts, identifying and mitigating phishing scams** and spam using the **KnowBe4 tool and Microsoft Defender** Identified and successfully blocked phishing campaigns, preventing credential theft and data exfiltration attempts.
- Leveraged in-depth knowledge of technical security solutions, **including firewalls, SIEM, NIDS/NIPS/HIDS/HIPS, AVs, DLP, proxies, network behavioral analytics**, and endpoint/cloud security tools, to safeguard the organization's IT infrastructure.

Associate Security Intern, VERITAS Technologies LLC, Pune, India — January 2017 – June 2017

- Worked on Commodity malware automation Project- **Automated malware alert** from **Splunk using python** to respective users which helped in reducing 20% of manual work of the team
- Gained foundational knowledge in **Incident response procedures, and workflows** and worked on **Symantec malware** and **phishing alerts.**

EXTRA-CURRICULAR ACTIVITIES

WiCyS (Women in Cybersecurity) – Actively participating in all the events and CTF competitions held in WiCyS

- Participated in Target CTF Competition Tier 1 and moved to Tier 2 challenge. Achieved 40th place out of 700 participants — Aug 2024
- Achieved fully funded **WiCyS – SANS security training scholarship** in partnership with SANS to pursue SANS courses — SEP2024 - 2025
    - SANS 275 AIS 247 – **GFACT, GSEC and GCIH certification**
- Selected as an Mentor and Mentee in the Mentor and Mentee challenge

Grace Hopper Conference Volunteer – Organized and facilitated workshops, connecting with industry leaders and professionals. Engaged in sessions on AI for cyber threat intelligence and offensive testing.

SANS Volunteer – Supported cybersecurity training initiatives, providing insights and technical expertise to participants.