Shrutika Joshi

shrutika@workwebmail.com | +1 (667) 406-7447 | USA | www.linkedin.com/in/joshishrutika | https://shrutjoshi.github.io/Shrutika_Portfolio

Summary

Cybersecurity Professional with 7+ years of experience across diverse domains including threat detection, incident response, cloud security, security operations, and risk & compliance. Proven track record of securing IT and cloud environments using tools like Splunk, CrowdStrike, AWS GuardDuty. Skilled in Python scripting, automation, and applying frameworks such as NIST, GDPR, and CMMC. Strong communicator with a passion for solving complex security challenges and collaborating across teams. **Certified in GCIH, GFACT, CySA+, and AWS Cloud Practitioner**, with a commitment to continuous learning and staying current with emerging threats.

Technical Skills

- **SIEM & Security Monitoring**: Splunk, ElasticSearch, ServiceNow
- **Endpoint Security & Threat Detection**: CrowdStrike Falcon, Symantec DLP, AWS GuardDuty
- **Cloud Security & Infrastructure**: AWS, Azure, GCP, IAM policies, Security Groups, CloudTrail, AWS Security Hub
- **Security & Compliance:** NIST 800-53, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27001, MITRE ATT&CK, Cyber Kill Chain
- **Vulnerability Management & Compliance**: CVSS, Qualys, NIST, GDPR, CMMC, Risk Assessment
- **Application Security** OWASP Top 10, Threat Modeling, Secure Code Review, SAST, DAST
- **Programming & Automation:** Python, JavaScript, MYSQL, SQL, PowerShell,SPL
- **Forensic Tools:** Autopsy, FTK Analyzer, Ghidra, Volatility, Burpsuite, Encase, ProDiscover, NetworkMiner, Hydra, Static and Dynamic malware analysis
- **AI & Machine Learning:** Jupiter notebook, LLM Security, Prompt Engineering, Generative AI (AWS SageMaker)

Professional Experience

SynergisticIT (Remote, USA)

Cyber Security Analyst [October 2024 - May 2025]

- Optimized SOC security monitoring and incident response by leveraging **Splunk** for centralized threat data aggregation from network traffic, endpoints, and servers, improving threat detection capabilities and reducing alert response times by 30%.
- Developed an automated **incident response system using Python**, integrating **CrowdStrike** for real-time malware detection and response automation. Streamlined threat mitigation, reducing manual intervention and accelerating incident resolution by 40%.
- Integrated **AWS GuardDuty and CloudTrail** into the monitoring setup, enhancing threat detection and investigation capabilities. This implementation improved security auditing, reduced false positives by 25%, and provided greater visibility into potential compromises.
- Implemented **AWS IAM policies and security groups** to enforce least privilege access, mitigating insider threats and unauthorized access. Strengthened cloud security posture by regularly auditing permissions and integrating **AWS Security Hub** for centralized security monitoring.
- Conducted in-depth post-incident analysis and root cause investigations using **Splunk and ElasticSearch**, identifying attack vectors and key vulnerabilities. These findings led to targeted remediation, improving proactive threat detection and system security by 20%.

VERITAS Technologies LLC (Pune, India)

Information Security Analyst [June 2019 - Jan 2023]

- Led investigations into advanced security threats based on signature trends, log analysis, and patterns by leveraging tools. such as **Crowdstrike Falcon, Symantec DLP, and Splunk, reducing false positives by 30%**.
- Built and tuned **10+ Splunk dashboards and correlation searches** for real-time threat monitoring.
- **Reduced EDR** alert triage time **by 40%** by optimizing **Crowdstrike Falcon detection** rules and threat feeds.
- Investigated and triaged security alerts across **AWS (GuardDuty, CloudTrail), GCP** (Security Command Center)**, and Azure** (Defender for Cloud), leading to the containment of multiple credential misuse and misconfiguration incidents.
- Integrated real-time detection rules with SIEM platforms like Splunk, reducing false positives by 30% and improving mean time to response (MTTR) by 25%.
- Conducted proactive threat hunting using the **MITRE ATT&CK, Cyber Kill Chain** framework**.**

- 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.
- Led knowledge transfer sessions for over 10 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.
- Participated in the **enforcement of internal security policies**, conducting risk assessments, and ensuring compliance with standards such as **NIST, GDPR, and CMMC**, contributing to internal audits.
- Contributed to the yearly **Security Tabletop exercise** to test and improve incident response strategie**s**

Associate Security Analyst [June 2017 - June 2019]

- Performed **security audits and vulnerability assessments** for 10+ applications, ensuring compliance and influencing security best practices for 15+ team members to strengthen the organization's cybersecurity posture.
- Led **security awareness training** for 200+ employees successfully reducing phishing attack success rates by 40% through simulated exercises, best practice guidelines, and company-wide security policy improvements.
- Managed security for 100+ systems, proactively detecting and mitigating threats, leading to a 30% reduction in security incidents through continuous monitoring, risk assessment, and policy enforcement.
- Investigated **web application security alerts**, analyzing logs for potential SQL injection, cross-site scripting (XSS), and authentication bypass attacks, and worked with developers to implement secure coding practices.

Associate Security Intern [Jan 2017 - June 2017]

- Automated malware alerts from **Splunk using Python**, reduced manual work load by 20%.
- Managed security for 3000+ systems, detecting and mitigating threats, leading to a 30% reduction in security incidents.

Education

M. S. Cyber Security, University of Maryland (Baltimore County, USA), [GPA: 3.4] - December 2024

M. S. Computer Science, Pune University (Pune, India), [GPA: 3.6] **-** April 2017

B. S. Computer Science, Pune University (Pune, India) - April 2015

Certificates

- SANS Institute – GCIH, GFACT, GSEC (Appearing), AIS247 – AI Security Essentials for Business Leaders
- CompTIA – CySA+, Network+
- AWS – Certified Cloud Practitioner
- Udacity – Introducing Generative AI with AWS

Projects

University of Maryland Baltimore County

- One National Investments – Conducted In-depth **Risk Assessment** and created detailed document
- Conducted **Forensic analysis** and Ethical hacking of a system and created detailed reports on the findings

WiCyS (Women in Cybersecurity)

- Participated in **Target CTF** Competition - Achieved 40th place out of 700 participants
- Achieved fully funded **WiCyS – SANS** security training scholarship to pursue GFACT, GSEC and GCIH certification