Shrutika Joshi

shrutika@workwebmail.com | (667) 406-7447 | USA | LinkedIn | GitHub

Summary

Information Security Analyst with 7+ years of experience in cybersecurity, specializing in threat detection, incident response, cloud security, and vulnerability management. Proficient in SIEM tools like Splunk and ElasticSearch, EDR platforms like CrowdStrike Falcon, and cloud security solutions across AWS, Azure, and GCP. Skilled in Python automation, compliance frameworks (NIST, GDPR, CMMC), and security auditing. Strong communicator with expertise in enhancing security posture and mitigating risks.

Technical Skills

- **SIEM & Security Monitoring**: Splunk, Kibana, ElasticSearch
- **Endpoint Security & Threat Detection**: CrowdStrike Falcon, Symantec DLP, AWS GuardDuty
- **Incident Response & Automation**: Python, ServiceNow, AWS (CloudTrail)
- **Cloud Security & Infrastructure**: AWS, Azure, GCP, IAM policies, Security Groups, Kubernetes, Container Security
- **Threat Hunting & Frameworks**: MITRE ATT&CK, Cyber Kill Chain, OWASP Top 10
- **Vulnerability Management & Risk Management**: CVSS, Risk Assessment, Threat Intelligence Reporting
- **Compliance & Auditing**: NIST, GDPR, CMMC, HIPAA, PCI DSS, ISO 27001, SOC 2
- **Forensic Tools:** Autopsy, FTK Analyzer, Ghidra, Volatility, Burpsuite, Encase, ProDiscover, NetworkMiner, Hydra

Professional Experience

Cyber Security Analyst, SynergisticIT 10/2024 – 03/2025 | Remote, USA

- Optimized SOC security monitoring and incident response by leveraging **Splunk** for centralized threat data aggregation, **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%.
- Used **AWS GuardDuty** and **CloudTrail** in the monitoring setup, improving threat detection and investigation abilities, **reducing false positives by 25%**, and providing enhanced 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.
- Collaborated with IT and security teams to gather requirements for **integrating ServiceNow into incident management**, ensuring effective tracking, resolution, and documentation of security incidents, **achieving 100% SLA** compliance for critical incident handling.
- Conducted detailed **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%.
- Delivered technical training on Splunk dashboards and Python-based automation tools, enhancing SOC team proficiency in threat identification and incident response. This training resulted in a 15% gain in operational response time and efficiency.

Information Security Analyst, VERITAS Technologies LLC 06/2019 – 01/2023 | Pune, India

- 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%.** Investigated attack patterns, **mapped adversary behaviors to MITRE ATT&CK**, and recommended security improvements, **conducted forensic analysis using Autopsy, Ghidra**.
- 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 the Crowdstrike Falcon EDR** platform by refining detection rules and threat intelligence feeds, 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 assessments, and ensuring compliance with standards such as **NIST, GDPR, and CMMC**, contributing to internal audits.
- 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.

- Contributed to the yearly **Security Tabletop exercise** to test and improve incident response strategies.

Associate Security Analyst, VERITAS Technologies LLC 06/2017 – 07/2019 | Pune, India

- 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 5000+** employees successfully reducing phishing attack success rates by 40% through simulated exercises, best practice guidelines, and company-wide security policy improvements.
- **Managed security for 3000+ systems**, proactively detecting and mitigating threats, leading to a 30% reduction in security incidents through continuous monitoring, risk assessment, and policy enforcement.
- **Leveraged Kibana and the ELK stack to monitor and analyze security logs**, enhancing threat detection and incident response, while working with IT teams to establish secure network architectures and improve endpoint security, strengthening defense mechanisms against potential cyber threats.

Associate Security Intern, VERITAS Technologies LLC 01/2017 – 06/2017 | Pune, India

- Worked on Commodity malware automation project. **Automated malware alerts from Splunk using Python** to respective users, which helped reduce 20% of manual work for the team.
- Gained foundational knowledge in incident response procedures, workflows, and worked on Symantec malware and phishing alerts.

Education

University of Maryland **Baltimore County, USA**
Master of Science in Cyber Security 01/2023 – 12/2024
Pune University **Pune, India**
M.Sc. in Computer Science 08/2015 – 04/2017

CERTIFICATES

- GIAC Certified Incident Handler (GCIH)
- CompTIA CySA+
- CompTIA Network+
- AWS Cloud Practitioner, AZ-900 Microsoft Azure Fundamentals
- SANS AIS247 – AI Security Essentials for Business Leaders

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
- Achieved fully funded **WiCyS – SANS security training scholarship** in partnership with SANS to pursue SANS courses SANS 275 AIS 247 – **GFACT, GSEC and GCIH certification**
- **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.