Darshan Soni

darshan@dsoni.in | dsoni.in | linkedin.com/in/dsoni-in

Objective

Security & Compliance Analyst with hands-on experience in implementing security controls, deploying SIEM solutions, and managing application and infrastructure security. Skilled in translating compliance requirements into actionable engineering tasks and bridging the gap between business and technical teams. Experienced in building security tools, managing WAF/DNS, and enhancing security posture through automation.

Experience

Security & Compliance Analyst, KAS Cyber Ventures – Pune July 2025 – Present

- Aligned security projects with business goals by bridging the communication gap between engineers and executives.
- Collaborated with development teams to integrate security practices into application workflows, ensuring secure design and implementation without impacting delivery timelines.
- Deployed and configured Wazuh SIEM, including agent installation across endpoints, enabling centralized log collection and real-time threat monitoring.
- Designed and customized security dashboards for visibility into endpoint activity, improving detection and monitoring capabilities.
- Managed and configured WAF and DNS security using Cloudflare, implementing traffic filtering, domain protection, and attack surface reduction.
- Developed and Launched eDMARC, a DMARC analysis and management platform, achieving Top 20 ranking on Product Hunt Featured List.
- Designed and developed supporting utilities for core security products, including:
  - Continuous Threat Exposure Management (CTEM)
  - Risk Register
  - Business Impact Analysis (BIA) Application

Security Program Management Intern, KAS Cyber Ventures – Pune Jan 2025 – June 2025

- Mapped and analyzed multiple security standards including NIST CSF, IEC 62443 4-1/4-2, PCI-DSS and CIS Controls, identifying cross-framework commonalities to streamline compliance efforts.
- Created actionable security tasks and associated risk assessments for non-compliance scenarios to aid in effective risk management.
- Performed Web Application VAPT, successfully bypassing Cloudflare protection and identifying key vulnerabilities.
- Built a domain reconnaissance tool to identify and summarize critical domain security parameters such as DMARC/SPF settings, WAF presence, DNS records, WHOIS data, and SSL chain status.
- Deployed reconnaissance tool on a shared DreamHost server with no root privileges, alongside an existing PHP application to ensure seamless operation of both applications.

CTF CO-Lead, nCreeps – Pune Oct 2022 – June 2024

- Led the team to achieve national and international recognition, improving the team rank to AIR 9 in multiple CTF competitions.
- Designed and developed custom challenges in Web Exploitation category for ShunyaCTF, enhancing the learning experience for more than 500+ participants.
- Organized and hosted 5+ sessions on cybersecurity and CTFs, engaged more than 150+ participants, and fostering a thriving cybersecurity community.

Projects

Security Assessment University Placement Portal

- Discovered and responsibly disclosed an open redirect vulnerability in the college placement web application, which could have been exploited for phishing or malicious redirection attacks.
- Created a detailed video proof of concept (PoC) demonstrating the exploit, and submitted it to the technical team for clear understanding.

CipherX Darry1968/cipherx

- Built a web-based cryptanalysis tool to identify and decode ciphers (Caesar, AES, Base, etc.) using regex-based pattern detection for automated analysis.
- Technologies: Python, Flask, HTML, CSS, JavaScript.

ARGUS Darry1968/ARGUS

- Developed an API vulnerability scanner capable of detecting OWASP Top 10 API security flaws such as Injection, Broken Authentication, and Broken Object Level Authorization (BOLA).
- Integrated a reporting module to generate human-readable vulnerability assessments from target URLs.
- Technologies: Python, Flask, argparse, requests, base64, pycrypto.

Education

MIT ADT University, Pune(Maharashtra) 2021 - 2025
B. Tech in Computer Science and Engineering, specialized in Cybersecurity and forensics

- CGPA: 8.75

Nowrosjee Wadia Junior college, Pune(Maharashtra) 2019 - 2021
High School

- Percentage: 87.60

Technologies

Security Standards: NIST CSF, IEC 62443, CIS controls, CSCRF, PCI-DSS.

Languages: Bash, Python, PowerShell scripting.

Developer Tools: Git, Docker, VS code, Postman, Regex.

Security: BurpSuite, OWASP ZAP, Wireshark, Nmap, Nessus, Snort.

Certificates

Google Cybersecurity Professional Certificate Google, Coursera

Cisco Certified Support Technician Cybersecurity CISCO

Career Essentials in Cybersecurity Microsoft and LinkedIn

Achievements

Academic: Achieved second rank in the B.Tech CSE program with specialization in Cybersecurity

Award: Recognized as Best Outgoing Student for outstanding academic performance

CTF experience: Led nCreeps CTF team to AIR 9 ranking and Hosted a national level CTF event called ShunyaCTF.

Tool Demo at IIT Bombay: Demonstrated a Passive Domain Misconfiguration Analyzer at IIT Bombay Trust Lab.

Workshop: Conducted AI & cybersecurity workshops at C0C0N, Kerala's premier cybersecurity conference

Speaker of Blackout: Explained Different domains of cybersecurity and CTFs.