Tanishq Borse

New York • (585)406-8869 • tanishqborse@gmail.com • LinkedIn • Portfolio

Passionate and proactive Cyber Security Engineer with 2+ years' experience in secure software design, development, security operations, threat modelling, automation, incident response, data analysis and risk management. Looking for full-time opportunities starting July 2025.

EDUCATION

Masters in Cybersecurity at Rochester Institute of Technology (3.9/4 CGPA)   *May 2025*
B. Tech in Computer Science and Engineering at MIT WPU (8.5/10 CGPA)   *July 2022*

RELEVANT EXPERIENCE

Co-Founder at CAMA Security Inc.   *New York |May. 24 – Present*
- Received a $15K award for Innovation in defense by Lockheed Martin for developing a lightweight cryptographic attestation scheme for runtime verification of firmware integrity on 10k+ resource constrained embedded devices in contested environments.
- Led market research, product roadmap development, threat modelling, and created investor pitch decks to drive strategic growth.

Teaching Assistant at Rochester Institute of Technology   *New York | Jan. 23 – May 24*
- Assisted over 300 students in 50+ lab sessions covering authentication and security principles (AD attacks, OAuth2, SELinux, MFA, SSO, Biometric Auth using ML), strengthening understanding of access control principles used in security infrastructure.

Cybersecurity Engineer Co-op at Poseidon Systems   *Victor, New York |May 23 – Dec. 23*
- Led the management and deployment of a centralized open-source SIEM platform, implementing custom correlation rules, real time
- threat enrichment, anomaly detection, and ML driven analytics (UEBA, unauthorized DNS request detection) to streamline response.
- Implemented SOC playbooks for endpoint isolation, alert enrichment, and ticketing system integration mapped to MITRE ATT&CK.
- Automated vulnerability management tasks across on-prem and multi cloud environments using Qualys, Nessus, and Wiz.
- Reduced security operations workload by 35% and accelerated IT support & issue resolution across the organization.
- Discovered and reported critical vulnerabilities in Web Application and IOT sensor through SAST/DAST tools and manual pentesting.
- Supported SSDLC through threat modelling, secure code reviews, debugging, and performance optimization.
- Supported deployment, maintenance and security hardening initiatives for firewalls, IDS/IPS and network switches.
- Reviewed and refined internal security policies for compliance with regulatory frameworks like NERC, CMMC and ISO 27001.

Application Security Engineer at Infopercept Consulting   *India | June 21 – Dec 21*
- Fortified application security posture for multiple financial and NBFC's through vulnerability analysis and pentesting to identify and remediate critical vulnerabilities (OWASP Top 10, PCI DSS) using automated (Nessus, Acunetix) and manual (Burp Suite, Nmap) tools.

SKILLS
- **SIEM** (Splunk, Qradar, Graylog), EDR (Falcon, Defender), **Firewalls** (CISCO, Palo Alto, Fortinet), **IDS/IPS** (Snort, Suricata, Zeek), TCP/IP
- **Compliance & Risk Management:** NIST SP 800-53, PCI DSS, HIPAA, NERC CIP, ISO 27001, CSF, CIS, GLBA, GDPR, OWASP
- **Vulnerability & Threat Management**: Burp Suite, Nessus, Tenable, TheHive, Trivy, Semgrep, Synk, Wiz
- **Cloud & Automation**: AWS Security, Kubernetes Security (Falco, Kube-bench), Terraform, GitLab CI/CD
- **Programming & Scripting:** Python, PowerShell, Bash, Go, SQL, PostgreSQL, JavaScript, Typescript, React, Jupyter Notebook
- **Certifications:** Certified Ethical Hacker (**CEH**), ISC^2 CC, AWS CLF-02, OSCP+ (ongoing)

PROJECTS
- **AI-Driven Dynamic Malware Detection** | Python, PyTorch
  Reduced security analyst efforts significantly through SHAP AI explainability for deep learning model with 95% accuracy at low FPR by using self-supervised transformer-based model. Performed ETL for preprocessing sequential dynamic logs with domain knowledge.
- **Secure Web shield** | Python, PHP, MySQL
  Developed a custom Python web server with robust API security protocols, performed web application server security audits and hardening. Automated deployment using Ansible and integrated secure CI/CD pipelines, significantly enhancing security posture.
- **Kubernetes Security Hardening**
  Developed an automated Kubernetes security monitoring pipeline (Falco, Kube-bench, Semgrep, GitLeaks, Trivy), improving runtime threat detection by 30% and reducing manual vulnerability management by 30%, significantly mitigating supply-chain security risks.
- **Multimedia in Next-Gen 911 – sponsored project by Cybersecurity and Infrastructure Security Agency (CISA)**
  Led research for identifying underlying risks for implementing Multimedia in Next Gen 911 Systems with 100+ stakeholders, presented findings to the U.S. Congress (House & Senate), resulting in nationwide policy changes impacting the lives of millions of Americans.

LEADERSHIP & ACTIVITIES
- **CTF Player:** Winner 2nd place in MetaCTF at BSides Security Conference. | Hack the Box, Tryhackme, Pentesterlab
- **Active Member:** RITSEC, ISACA, ISC^2 | **Volunteer:** Rochester Security Summit '24 | BSides '25