SUVAM BARUI

5852868666 ◇ sb9895@rit.edu ◇ LinkedIn ◇ GitHub ◇ HTB

WORK EXPERIENCE

Securely Yours LLC Security Engineer Intern (Generalist) *(Bloomfield Hills, Michigan)* May 2025 - present

- Conducted over 10 comprehensive webapp penetration tests using tools like Burp Suite, ZAP Proxy, XSStrike, SQLMap and Nuclei; identified 50+ critical and high-severity vulnerabilities, delivering detailed reports with CVSS scores, risk ratings, and remediation guidance.
- Engineered a secure SOAR automation architecture using Shuffle workflows and USM Central APIs resulting in a 20% reduction in incidence response time and aligning with NIST and MITRE D3FEND best practices.
- Automated 10+ security orchestration playbooks for incident response by leveraging USM Central and USM Anywhere APIs, which improved response consistency and reduced manual effort by 30%.
- Analyzed and optimized over 10 million firewall and network logs, filtering and suppressing redundant or low-value entries, boosting SIEM query speed by 35% and reducing storage usage by 25% for multiple clients.
- Integrated VirusTotal API into alert enrichment pipelines, accelerating threat intelligence correlation and decision-making by 30%; generated 50+ OTX write-ups for client-facing reports, cutting report turnaround time by 50%.

Securely Managed LLC Security Operations Center (SOC) Intern *(Bloomfield Hills, Michigan)* Feb 2025 - May 2025

- Monitored over 100,000 security events and performed real-time threat detection using AlienVault (LevelBlue); analyzed logs from SIEM, EDR, and firewalls, leading to the identification and mitigation of 200+ potential threats including malware, unauthorized access, and misconfigurations.
- Investigated and responded to 75+ security incidents, executing containment and recovery procedures; implemented preventive measures such as rule tuning, threat intelligence enrichment, and policy updates, resulting in a 30% reduction in recurring incidents.
- Researched 25+ emerging threats monthly, including CVEs, threat actor TTPs, and malware campaigns; published internal threat briefings and provided proactive security recommendations that improved threat awareness across teams and enhanced the organization's detection capabilities.

Rochester Institute of Technology Graduate Teaching Assistant (Hacking for Defense) *(Rochester, New York)* Jan 2023 - Jul 2024

- Guided and supported 120+ students across 3 semesters as a Graduate Teaching Assistant, actively facilitating classroom discussions and hands-on problem-solving related to real-world challenges faced by government agencies like DoS and DoD.
- Mentored 15+ student teams on project execution for government-sponsored problem statements, providing technical and strategic guidance that improved project efficiency by 40% and led to adoption of multiple student-proposed solutions by federal stakeholders.

CERTIFICATIONS

- Offensive Security Certified Professional OSCP+ | OSCP — Jul 2028
- HTB Certified Penetration Testing Specialist HTB CPTS — Jun 2025
- AWS Certified Cloud Practitioner AWS CCP — Feb 2028
- CompTIA Security+ SYO-601, COMP001021892318 — Jul 2027

EDUCATION

Rochester Institute of Technology *MS in Computing Security* GPA: 3.8/4.0 — Rochester, NY [Aug 2022 - Dec 2024]

Haldia Institute of Technology (MAKAUT) *B. Tech in Computer Science and Engineering* — Kolkata, India [Aug 2015 - May 2019]

PROJECTS

Network Recon & Vulnerability Automation | Github

- Developed an automated multi-stage Nmap recon framework using Bash, streamlining top-TCP and common-UDP scans into full-port sweeps, reducing manual effort by 70%.
- Engineered dynamic port parsing logic to extract open ports from initial scans and perform targeted version detection and NSE vulnerability checks, cutting redundant scan time by 40%.
- Optimized scan sequencing for efficiency, prioritizing faster recon while preserving deep analysis for later stages-improving critical service identification time by 50%.

Cloud SOC Lab Design and Deployment (AWS-Based)

- Deployed a scalable SOC lab environment on AWS, provisioning over 10 EC2 instances across isolated VPCs, including Wazuh (SIEM/EDR), ELK Stack, Suricata (IDS/IPS), Zeek, and an Active Directory domain controller; simulated a mid-sized enterprise network with segmented Windows endpoints and a virtual pfSense firewall.
- Executed 30+ Atomic Red Team attacks mapped to MITRE ATT&CK; achieved 90% detection rate and automated 15+ response workflows with Shuffle, MISP, and OpenVAS.
- Managed 50+ simulated security incidents using TheHive and Cortex hosted on AWS EC2, integrated with Wazuh alerts; enhanced enrichment and correlation via custom Python scripts, resulting in 40% faster alert handling and a 25% increase in automation coverage across recurring threat patterns.

ACHIEVEMENTS & AWARDS

- Top 500 Global on HackTheBox with 101 user + root owns across challenges.
- Member of HTB Team [REDACTED], ranked Top 10 Worldwide.
- Ranked 326/9,300 - HTB Season 7 (VICE), Jan–Apr 2025.
- Ranked 81/7825 HTB Season 5 (Anomalies), Apr-Jun 2024.
- Ranked Top 1% on TryHackMe
- CTF Team RaptX - 29/1528 in IrisCTF 2025.

SKILLS

Interests: Offensive Security, Security Operations, Security Automation, Cloud Security, Purple Teaming
Programming & Scripting: C, C++, Java, Python, SQL, Bash, Powershell
Cloud Security: Amazon Web Services, Microsoft Azure, Google Cloud Platform, CloudTrail, CloudWatch, IAM
Security Tools: Metasploit, BurpSuite, Nmap, Bloodhound, Nessus, Snort, Wireshark, Splunk, LevelBlue (Alienvault)
Core Competencies: Web Application Penetration Testing, SOAR Automation, Incident Response ,Threat Modeling
Operating Systems & Technologies: Windows, Kali, Ubuntu, macOS; BGP, OSPF, TCP/IP, IPv4, VPN, IPSec, HTTP, DNS, DHCP, OSI Model
Compliance & Frameworks: MITRE ATT&CK, Cyber Kill Chain, MITRE D3FEND, NIST, SOC2, GDPR, HIPAA, PCI-DSS, ISO 27001, FedRAMP
Soft Skills: Problem Solving, Critical Thinking, Attention to Detail, Team Collaboration, Time Management, Continuous Learning, Conflict resolution, Stakeholder management, Adaptability, Creative thinking skills, Leadership skills, Emotional intelligence