Vaishnavi Sonagra

vaishnavi.sonagra@kellogg.ox.ac.uk | www.linkedin.com/in/vaishnavisonagra/

EDUCATION

University of Oxford (United Kingdom) **Expected 2025**

MSc. Software and Systems Security

- Invitee of the British Computer Society (BCS) review
- Elected as student representative for the programme
- Relevant Coursework: Understanding and Mitigating Malware, Cloud Security, Security in Wireless Networks, Mobile System Security, and Security Principles (Applied Cryptography)
- Thesis Topic: Predictive Threat Intelligence (In-progress)

2016-2020

Cummins College of Engineering for Women, Pune (India)

B.Tech Electronics and Telecommunication

- Relevant Coursework: Computer Networks, AI and Big Data Analytics, Real Time Operating Systems

PROFESSIONAL EXPERIENCE

Security Consultant → Assistant Manager, Incident Response - PwC India **2021-present**

- **Incident Response:**
  - Led IR investigations as a **first-responder** for highly-escalated incidents within unfamiliar client environments to identify the root cause, impact and modus operandi of advanced threat actors and assisted the clients minimising the impact with rapid recovery. Finally, produced detailed reports with **MITRE ATT&CK** mapped TTPs and recommendations
  - Conducted intrusion analysis, triage and **deep-dive forensics** and performed log correlation for large datasets, memory analysis and artefact analysis to perform timeline analysis & ascertain the root cause of incidents such as ransomware (Conti, LockBit all versions, BlackCat (ALPH-V), etc), Data Theft, ATM cashouts, and Phishing among others
- **SOC (Security Engineering)**:
  - Led SOC implementation and management projects using security solutions (such as SIEM/SOAR, EDR/XDR, Firewalls, WAF, etc.) ensuring **24X7X365 support** with log management and disaster recovery strategies.
  - Spearheaded assignments to enhance client's current SOC environment in terms of threat detection and response by performing activities such as migrations, **SIEM use-case fine-tuning, threat intel generation** and api integration with security tools; and **SOAR automation**
- **Red Teaming:**
  - Performed proactive Active Directory red teaming assessments to identify threats affecting AD health (**On-prem as well as Azure**) and domain trust relationships and assisted clients perform enhancements by reconfiguring, group policies, ACLs and other mechanisms
- **CSIRT setup:**
  - Developed an app for orchestration of a immersive **simulation-based tabletop** exercise to train muscle-memory of incident response stakeholders including technical and executive teams
  - Formulated custom security incident management policies and governance policies for clients based on industry standards such as **ISO 27001, NIST SP 800-61r2, ENISA,** etc. and delivered trainings to teams

TOOL EXPERTISE

- Cloud environment expertise: Microsoft Azure and Aws
- Programming and Scripting experience: Python (LeetCode Rank ~6 Lakh), Powershell, KQL and SQL
- Tools Expertise: Microsoft Sentinel, Google Chronicle, Datadog, Securonix, IBM Qradar, Microfocus, Splunk, ELK, Crowdstrike Falcon XDR, Palo Alto Cortex XDR, Demisto SOAR, EnCase Forensics, Magnet AXIOM, Volatility, Velociraptor, KAPE, Kansa, Relativity, FTK, OS forensics, MISP, Thor, Loki, and open source tools

CERTIFICATIONS

- EC-Council Certified Ethical Hacker (CEH v11)
- SANS GCFA (In-preparation - planned for 2025)
- Palo Alto Networks Cybersecurity Specialization (Coursera)
- University of Michigan - Python Specialization (Coursera)

ACHIEVEMENTS AND RECOGNITIONS

- Awarded the PwC IN's first ever Chairperson award for creating simulation based tabletop exercise
- WiCyS Student and volunteer Scholar 2024 (Tennessee, USA)
- SANS Global Community CTF: BootUp 2021 (Ranked 625th for beginner track)
- SANS Global Community CTF: Mini Boot Up 2021 (Ranked 515th)
- Top 15% on TryHackMe
- Received two PwC's above and beyond individual awards

MOOCS

- Microsoft Learning: Fundamentals AI concepts
- Microsoft Learning: Understand Data Science for Machine Learning
- Microsoft Learning: SC 200 Defender for endpoint, Mitigate threats using Microsoft Defender XDR
- Cybrary.it: Penetration Testing and Ethical Hacking
- Cybrary.it - Developing Ethical Hacking tools using Python
- Cybrary.it - CompTIA CySA+ (CS0-002) preparation certification
- Cybrary.it - Certified Information Systems Security Professional (CISSP) preparation certification