[redacted]

m[redacted]gmail.com | (+91)[redacted] |linkedin.com/in/[redacted]

PROFESSIONAL SUMMARY

Cyber security professional with **3.5 years** of experience and strongly interest in security monitoring and application security. **OSCP** certified and working as a **Technology Associate** in **Deloitte's USI.**

Experience

APRIL 2022 – PRESENT | TECHNOLOGY ASSOCIATE | DELOITTE TOUCHE TOHMATSU LIMITED

- Leading an entire pool of Security Operations Center (SOC) L1 analysts. Responsible for assessing escalated outputs and alerts from Level 1 Analysts. Update processes, run books, templates, and procedures based on experience for best practice.
- Working with SIEM engineering teams to develop innovative and cutting-edge detection content aligned with MITRE ATT&CK and Cyber Kill Chain to optimize the detection capability using existing logging.
- Identifying any gaps in any of the detection solutions and assist with building new detections.
- Evaluating already deployed SIEM rules, filters, events, and use cases and adapt to meet the business requirements.
- Documenting weekly and monthly reports of the security incidents. Also, performing rule tuning to reduce the number of false security incidents and conduct proactive hunts using SIEM and EDR tools.
- Conducting team knowledge transfer sessions on new tools and technologies.

NOVEMBER 2020 – MARCH 2022 | TECHNOLOGY ANALYST | DELOITTE TOUCHE TOHMATSU LIMITED

- Providing detection, analysis, research, and data gathering for security alerts. Performing event Analysis on Base & correlated Events using Splunk.
- Categorizing the events & raising necessary cases such as Operational, Health, Tuning, and Content request aspects along with security incidents for the issue resolution/security investigation/mitigation.
- Serving Ad-hoc requests for clients by helping them in finding the logs and assisting with an internal investigation on malicious activity & forensics. Improving the TP/FP ratio through consistent analysis and reporting fine-tuning opportunities.

APRIL 2020 – NOVEMBER 2020 | INDEPENDENT RESEARCHER | BUGCROWD

- Performing Regular Pentest on Web Applications, APIs.
- Reporting & Documentation
- Comes in Monthly Leader Board for reporting high severity vulnerability.
- Global Ranking 840, Link: https://bugcrowd.com/[redacted]
- Received Acknowledgements and Hall of Fame from some renowned Companies like
    - Apple
    - Google
    - Microsoft
    - Hack the Box (HTB)
    - Unilever
    - Western Union many more...

JANUARY 2020 – APRIL 2020 | INTERN | DELOITTE TOUCHE TOHMATSU LIMITED

- Works with Application Security Analyst
- Providing web application security to TMT and Financial clients including Threat Modeling, Penetration testing, reporting threats, vulnerabilities, and bugs as per OWASP Top 10 standards.
- Vulnerability Management on Qualys Cloud Platform for a healthcare client. Classifying network assets according to the business requirements for managing Qualys Vulnerability Dashboard.

Education

B.E IN COMPUTER SCIENCE | Chandigarh University

- 2016-2020
- CGPA 7.4
- Grand-Finalists (TOP-10) in CCTC- DELOITTE
- INCTF is a CTF competition organized by team BI0S (India's Best CTF Team). In the following, I and my team placed 13 ranks.

HANDS ON TOOLSET

- Security Information and Event Management(SIEM) Tool: Splunk.
- Security Tool: Windows Defender Advanced Threat Protection (ATP), Carbon Black, Symantec,Crowdstrike Falcon
- Cloud: Azure.
- Incident Management Tools: JIRA, ServiceNow.
- Vulnerability Scanner- Tenable Nessus, Acunetix, Qualys.
- Exploitation Tools- Metasploit, Burp Suite, SqlMap and other used in Bug bounty.

SKILLS

- Security Operations and CyberThreat Hunting
- SOC Testing and Playbook creation
- Cloud compliance and Security monitoring

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (CEH)

OTHER RELEVANT INFORMATION

- Additional Languages: Hindi (Native), English (Fluent)
- Date of birth: 10/07/1997
- Sex: Male
- Address: 1no. Darpo Narayan Tagore Street, Kolkata (Pin - 700006)