Abhijeet Pawar

(312) 678 - 8671 | abhidotsh@gmail.com | LinkedIn

SUMMARY

Cybersecurity professional with over 3 years of experience in security incident response and security engineering. Skilled in cloud security, detection and response, vulnerability assessments, and automated detection models. Personal achievements include top placements in cybersecurity competitions and published research on third-party risk management and cyber-attack simulations.

WORK EXPERIENCE

Security Detection and Response Engineer Intern | *Circle Internet Financial – USA* MAY 2024 – DEC 2024

- Led 150+ security investigations, managing on-call to identify root causes, taking corrective actions, and document findings on various threats (malicious phishing campaigns, cloud anomalies, endpoint activity, emerging threats).
- Developed a Python-based "Sigma Converter" tool to automate 100+ Sigma rule conversions into detection rules for Panther SIEM and SentinelOne STAR, reducing deployment time by 50% and enhancing threat detection coverage by 15%.
- Implemented 25+ detection rules for recent incidents, data leaks, and emerging threats, including excessive OnePassword login attempts and Okta admin misuse, resulting in the detection of 8 unknown threats and a 10% reduction in false positives.
- Secured 1,550+ Google OAuth applications and Chrome extensions, blocking 80 unauthorized apps and implementing secure configurations to reduce the attack surface by an estimated 5% and prevent potential data breaches.
- Led threat hunting efforts for the Polyfill supply chain attack, removing malicious components, identifying 30 vulnerabilities across 10 repositories, and driving remediation, successfully preventing a potential compromise.
- Utilized Anomali, VirusTotal, URLScan, Google Admin Console, and Proofpoint to block ~20 phishing attempts/month and reduce successful attacks by 5%.
- Leveraged SentinelOne EDR and Snowflake for incident investigation, utilizing Python and Power Query to analyze data and identify indicators in alignment with the MITRE framework.

Cyber Security Consultant | *Atos – India* AUG 2021 – JUNE 2023

- Spearheaded 50+ application security assessments to identify and remediate vulnerabilities, using HCL AppScan, Nessus, Dependency Checker, and Burp Suite.
- Mitigated web application vulnerabilities by applying OWASP Top 10 principles, using DAST and SAST methodologies to address 5 critical issues and reduce risk by 25% within 6 months.
- Designed a cybersecurity awareness program for 200+ employees, highlighting phishing via social media.
- Developed and implemented 10 Splunk detection rules leveraging the MITRE ATT&CK framework to identify adversary TTPs improving proactive threat detection by 20%. Collaborated with cross- functional teams to address detection gaps and reduce risk.

JavaScript Developer | *Confiable Solutions – India* JUNE 2020 – JUNE 2021

- Managed profitable client relationships by developing and maintaining websites and creating dashboards for risk scorecards for international clients using HTML, CSS, and JavaScript.
- Conducted peer code reviews to ensure quality and adherence to best practices.

Cyber Security Intern | *SSP Technology – India* JAN 2020 – JUNE 2020

- Provided support in managing and securing Windows Active Directory (AD) environments, including provisioning, access control, and group policy configurations to enhance security and compliance.
- Assisted in monitoring and responding to security incidents, analyzing system logs and network traffic to identify potential threats and mitigate risks in real-time.

TECHNICAL SKILLS

Programming Languages: Python | C++ | Bash | SQL | PowerShell
Tools: Splunk | SentinelOne | Burp suite | Tines (SOAR) | Nessus | Google Admin Console | Panther SIEM | Snowflake | OWASP ZAP | Wireshark | Metasploit | Nmap | Zscaler (WAF)
Systems and Platforms: Windows | Mac | Linux | Microsoft Office | Git | Jira | Docker | AWS | Azure
Security Frameworks: ISO 27001| NIST Framework | MITRE ATT&CK Framework | CIS Critical Security Control

EDUCATION

Master of Applied Science, Cyber Forensic and Security
Illinois Institute of Technology, Chicago, IL MAY 2025

Bachelor of Engineering, Information Technology
University of Pune, India OCT 2020

PROJECTS

AI-Based Phishing Detection Tool

- Developed an AI-based phishing detection tool using machine learning to classify emails as phishing or legitimate based on content, subject lines, and sender information.
- Utilized Python and machine learning libraries like Scikit-learn and NLTK for natural language processing (NLP) to extract features from email data.
- Integrated VirusTotal for scanning email attachments for malware and used SentinelOne for endpoint detection of phishing-related threats.

Security Operations Center (SOC) Automation Lab

- Orchestrated a comprehensive SOC automation lab project, integrating SIEM (Wazuh) and SOAR (Shuffle) technologies to monitor and respond to security events such as Mimikatz detection.
- Configured Wazuh agent to detect and alert security events, ensuring the capture of critical telemetry with Sysmon integration.

Acme Coffee Penetration Testing

- Performed password cracking using John the Ripper and Hashcat to gain access to the virtual machine and retrieve the system information with root privileges.
- Emulating real-world attacks, a pen test of Acme Coffee utilized Nmap and Metasploit for network mapping and exploitation, identifying open ports, and fetching information.
- Executed SQL injection using sqlmap to retrieve database information, and version to determine the vulnerabilities which provided database details.

Active Directory Penetration Testing

- Established a virtual lab with a domain controller and two user machines, mirroring real-world network scenarios to assess to improve logging, threat detection, and reduce attack potential.
- Performed simulated cyber-attacks like LLMNR poisoning, SMB relay, keberoasting, AS-REP roasting and pass-the-ticket attacks to evaluate and improve security controls.

RESEARCH WORK

- Enhancing Cybersecurity through Effective Third-Party Risk Management and Supply Chain Security, Illinois Tech
- Design And Implementation of a Devs-Based Cyber-Attack Simulator for Cyber Security, IJIRCC

CERTIFICATIONS and COMPETITONS

Certifications:

- CompTIA Security+
- CompTIA Network+(Pursuing)
- ISC2 Certified in Cybersecurity
- Practical Ethical Hacking by TCM Security
- Qualys: Vulnerability Management

Competitions

- Led and secured 2nd position at NCAE Cybergames 2024
- Top 10% in TCM Security CTF
- Ranked in the top 10% in National Cyber League 2023
- Solved anomalies for team Tailwinds at Cyber Force 2023