Abhishek Mule

mule.ab@northeastern.edu | +1(857)-961-9445 | https://www.linkedin.com/in/07abhishekmule/ | Boston, 02135 |
Available: May – December 2024

EDUCATION

Northeastern University, Boston, USA — Sept 2023 - Present
Master of Science in Cybersecurity — Expected Graduation: Dec 2025
Key courses: Cyberspace Technology and Applications, Decision Making for Critical Infrastructure, Foundations of Information Assurance, Computer System Security

University of Mumbai, Mumbai, India — Aug 2017 – Oct 2020
Bachelor of Engineering (Electrical Engineering)

SKILLS

Softwares/ Tools: Splunk, Microfocus ArcSight, Sentinel-One, Qualys, Nessus, Cisco IronPort, McAfee ePo, ServiceNow, Jira, Nmap, Wazuh
Programming Languages: Python, Bash,
Framework and Technologies: MITRE ATT&CK, OWASP Top 10, NIST, CSF, AES, RSA, SSL/TLS, Burp Suite
Brand monitoring Tools: CloudSEK XVigil, XMCO

PROFESSIONAL EXPERIENCE — India

Associate Information Security Consultant – IT | Anzen Technologies Pvt Ltd — **July 2022 – Apr 2023**

- Performed Active threat hunting by collecting data points using BRISK (Breach Response Investigation Software Kit) and created a baseline of the data actively checked for deviation and raised alerts with respective stakeholders
- Conducted malware analysis using advanced EDR tools, identifying and mitigating over 200 potential threats, resulting in decrease of successful cyber attacks
- Investigated and mitigated 20+ phishing attacks through comprehensive OSINT analysis, leveraging tools such as Proofpoint and Sentinel-One; reduced potential data breaches and safeguarded organizations information integrity
- Vigilantly monitored DLP alerts, promptly investigated incidents, and collaborated with the respective stakeholders to ensure swift resolution
- Facilitated regular training sessions to educate employees on DLP best practices, reducing incident frequency by 20%
- Spearheaded the analysis and investigation of 300+ IDS alerts from Darktrace sources, including MSSP alerts and ad hoc requests, resulting in accelerated incident response bolstering overall security posture by a great amount
- Coordinated with stakeholders to finetune a software module for the ticketing system, reducing resolution time by 10% and meeting SLAs 99.98% of the time, resulting in improved organization's satisfaction and retention rates

Management Trainee | DTDC Express Ltd — **Feb 2021 – July 2022**

- Analyzed large volumes of data using Splunk to detect and mitigate security threats, leading to a 46% reduction in average incident response time and a 7% decrease in overall security incidents identified
- Efficiently served as the initial point of contact for all security-related issues, delivering prompt support and issue resolution with a 100% response time adherence.
- Conducted thorough investigations, precise analysis, and detailed reporting of security events from diverse log sources, leading to a 20% reduction in unidentified incidents
- Expedited the incident management process by initiating ServiceNow tickets, achieving a 98% incident closure rate through persistent follow-up with stakeholders

PROJECTS

Created a Vulnerability Management Lab — **Nov 2020 - Jan 2021**

- Installed and configured Nessus essentials to perform credential vulnerability scan against windows hosts Implemented vulnerability management function on sandbox network with the following objectives - Discover, Prioritize, Assess, Report, Remediate, and verify

CERTIFICATIONS AND ACHIEVEMENTS

- Earned the prestigious Bravo Points recognition for streamlined triage process for SOC alerts at Anzen Technologies Pvt Ltd
- Successfully completed the IBM Cybersecurity Analyst Certification program
- Successfully achieved the Certified Ethical Hacker (CEH) certification from EC-Council, demonstrating proficiency in ethical hacking and cybersecurity techniques