Amruta Pandhare

Room No : 702, Wing : D, Balaji Angan Society, Sector 3, Kharghar,
Navi Mumbai, Maharashtra - 410210.

9152111757
pandhareamruta23@gmail.com
https://www.linkedin.com/in/amruta-pandhare-283bb91a8/

ABOUT ME

I'm Amruta, I have worked as a SOC Analyst for a year and a half. My job is to ensure the security of a network by monitoring, analyzing, and responding to security issues. I'm proficient in using ElasticSearch SIEM tool for this purpose.

In my role, I keep a watchful eye on the network for any signs of an attack. If an attack is detected, I investigate and report it promptly. I also enjoy analyzing various log sources and developing use cases to improve our monitoring capabilities.

One of my strengths is documentation, which comes in handy when creating Threat Advisory reports that detail vulnerabilities, emerging threats, and other cybersecurity risks. To stay up to date with the latest trends in cybersecurity, I regularly consult Threat Intel.

I've also had the opportunity to work on a client project that was entirely based on AWS, which has helped me develop my expertise in this area. Additionally, my strong communication and management skills have been valuable assets in my interactions with clients and colleagues on a daily basis.

Moreover, I am continuously learning about web application security and aim to transition to VAPT (Vulnerability Assessment and Penetration Testing) as I want to broaden my knowledge of all areas in cybersecurity.

SKILLS & PROFICIENCIES

- Team management
- Strategic and Proactive at work
- Proficient in using SIEM tool
- Excellent communication skills
- Very organized and disciplined
- Always striving to learn things

WORK HISTORY

SOC Analyst L1
CyberNX Technologies Pvt Ltd.
October *2021 to Present*

1. Familiarity with ElasticSearch SIEM tool and expertise in log analysis.
2. Monitoring, analyzing, and investigating security alerts to ensure comprehensive threat detection.
3. Creating and documenting incidents, accurately reporting on the incident response process.
4. Providing recommendations for appropriate actions and solutions based on incident investigation and analysis.
5. Developing use cases and producing reports to support security operations.
6. Conducting noise reduction techniques to minimize false positives and optimize threat detection.
7. Crafting Threat Advisories and conducting Threat Intelligence to inform proactive security measures.
8. Maintaining regular communication with clients and serving as their primary point of contact.
9. Being a dedicated SPOC for a specific client, providing personalized attention and support.
10. Directing and supervising a team of 10-12 security professionals.

EDUCATIONAL BACKGROUND

Vidyalankar Institute of Technology, Mumbai — Degree in Computer Engineering
2018 - 2021
Marks : 74.78% (8.23 CGPI)

VPM's Polytechnic, Mumbai — Diploma in Computer Engineering
2015 - 2018
Marks : 85.44%

Vidya Mandir, Titwala, Mumbai Suburban — SSC
2015
Marks : 87.40%

CERTIFICATION & COURSES

- **Certified AppSec Practitioner (CAP) — The SecOps Group**

Certified Appsec Practitioner (CAP) is an intermediate-level exam to test attendees' knowledge on the core concepts of application security.

- **Web Fundamentals Learning Path — Try Hack Me**

The aim of this path is to teach you how to successfully attack and exploit web applications. Knowledge of OWASP Top 10, and BurpSuite, etc.

- **Practical Ethical Hacking — TCM Security**

This course covered the practical side of ethical hacking and using tools like Nmap, Nikto, Burp suite, etc.

- **Introduction to Network Analysis — Security Blue Team**

This course covered understanding of basic networking fundamentals and the skills to analyze malicious traffic from a mock compromised system PCAPS using Wireshark and TCPDump.

- **Python Data Structure — University of Michigan**

This course introduced the core data structures like Strings, Files, Lists, Dictionaries, Tuples, etc.

- **Programming for everybody (Getting started with Python) — University of Michigan**

This course introduced the basics of Python like variables, functions, loops, etc.

- **First Step Korean— Yonsei University**

This was an elementary-level Korean language course and it covered basic consonants, vowels, and expressions used in everyday life, such as greetings, talking about family, and so on.

- **Meditation: A way to achieve your goals in your life— KAIST**

An interesting and thought-provoking course on how self-reflective meditation can help achieve life's goals such as peace and contentment.

EXPERTISED AREAS

- Incident Response
- Ethical Hacking
- AWS (Amazon Web Services)
- Kali Linux
- Computer Network
- Threat Intel
- Python

USED TOOLS

- Nessus
- BurpSuite
- Metasploit
- Nmap
- Nikto, dirb, Hydra, etc.

LANGUAGES

- English
- Hindi
- Marathi

HOBBIES

- Reading Novels
- Watching True Crime Documentaries
- Listening Podcasts
- Learning New Languages

PROJECTS

OMR Evaluator Using Python — Image Processing

OMR sheets have been widely used across the globe for grading purposes. This project suggests an accurate and cost efficient system for the evaluation of the OMR sheet. Based on the image and answers provided by the user the system successfully calculates the results and stores the result in a CSV file. The user can scan one sheet at a time or can scan the entire folder according to his/her needs.