Mehedi Hasan Nayem

Security Analyst | SIEM | Python | Problem Solver

mhnayem.n@gmail.com
/nayemmhn
+880 1312 - 132223

As an ambitious and motivated individual, I am seeking an opportunity to begin my career in the field of Cyber Security. I am eager to join a dynamic organization that encourages innovation and values strong interpersonal and leadership skills. My objective is to contribute to the growth of the company while enriching my knowledge and skills in a challenging and rewarding work environment. I am committed to advancing the company's goals and objectives and passionate about the field of Cyber Security. I am confident that I can be a valuable asset to the team and am eager to learn and grow in this exciting industry.

Technical Expertise

- Penetration Testing
- Vulnerability Management
- Open Source SIEM
- Python, Bash, Shell
- SOC, Vulnerability management, Incident Response
- Log Analysis
- Leadership, Teamwork &
- Adaptability

Tools-Tech & Working Env

Incident Response, & SIEM

- Wazuh
- Kibana
- Elasticsearch
- Vulners Agent
- Windows log

Professional Experiences

Adarsha January-1-2023 to Present

Technical Support Assistant | Security & Tech Team

Versatile technology, security, and digital asset management professional at Adarsha. There I worked to ensure the security and efficiency of digital assets and systems.

Core Responsibilities:

- Ensure Security for digital assets and technical infrastructure
- Provide necessary technical support
- Develop System and software base on demand
- Data sourcing, Management & analysis
- Maintaining Software, Services, Digital assets & Security
- Train employees about technical and security awareness
- Research, Analyze & test software, services
- Objective Key Result (OKR) Methodology

Cyber Security Training Assistant may-2022 to august-2022

I worked as a training assistant in a collaborative cyber security course organized by 'BYEAH' and 'Shorobor' in partnership with 'SecurityMindPro'. I Guided students, prepared tasks, and assessed assignments. Rewarding experience managing and nurturing aspiring cybersecurity professionals.

SecurityMindPro 2021 to Present

Associated

I learned and grew with my dedicated team. Together, we worked on various projects, wrote blogs, prepared cybersecurity services, and trained cybersecurity professionals. At SecurityMIndPro with my team I also lead the publication of CyberShield, the first Bengali cybersecurity magazine.

Notable Projects

DDoS Prevention System Based on Shannon Entropy

Explore POC august-2023

In 7 days, I successfully completed the DDoS prevention system Based on Shannon entropy with my team. There, snort captures network traffic & with Python analyzes its entropy to identify and block attackers.

S.	Category	Details
1	Programming Language	Python
2	Formula	Shannon Entropy
3	IDS Tools	Snort
4	Attacker OS	Kali
5	Attacking tools	hping
6	Host OS	Ubuntu
7	Web Server	Apache

Intrusion Detection System

- Snort

Penetration Testing tools

- Metasploit
- Burp Suite
- Nmap
- Nikto
- OpenVAS
- Owasp Zap

Network & Packet Analysis

- Wireshark

Programming languages

(For Problem-solving, Automation, and system development.)

- Python
- Bash
- shell scripting

Web scripting

- HTML
- CSS

OS and virtualization tools

- Kali (various distro)
- windows server
- Metasploitable-2
- VMware
- VirtualBox

Reference

Mashihoor Rahman

Cyber Security Analyst,
Cleanaway, Australia
Email: mashihoor@gmail.com
Cell: +61420760236

CyberShield : Bangla CyberSec Magazine

June - 2023

Pioneered CyberShield, the first Bangla cybersecurity magazine, to bridge the digital divide and empower Bengali speakers with cybersecurity knowledge and skills.

Windows Event Log Analyzer

March - 2022

Explore POC

windows Event Log is like a Blackbox we can investigate any issue by analyzing the event logs. This program gets logs from the Microsoft event viewer, analyzes logs, and sends a log summary with full details of logs in a CSV file to the given email.

s.	Category	Details
1	Programming Language	Python 3
2	Libraries & tools (For Sending Mail)	smtplib, MIMEMuliparts, MIMEText, MIMEBase, encoders
3	IDS Tools	Subprocess
4	Libraries & tools (For PowerShell command)	Kali
5	Programming Language	Python 3
6	Libraries & tools (For Sending Mail)	smtplib, MIMEMuliparts, MIMEText, MIMEBase, encoders
7	IDS Tools	Subprocess

WAZUH

July - 2022

AZUH is an open-source Security Information and Event Management (SIEM) solution. In this scenario, I used four operating systems (OS) in a Virtual Machine to simulate the WAZUH Implementation.

s.	OS	Services
1	Ubuntu 20.04.2	WAZUH manager and filebeat
2	Parrot 4.11.2	Elasticsearch
3	Ubuntu 20.04.2	Kibana and Agent-2
4	Windows xp	Agent-1

Professional Training & certifications

s.	Exam / Certifications	Vendor
1	AZ-900	Microsoft
2	CCNA Training	House of network
3	(ISC)² Candidate	(ISC)²
4	Foundations of operationalizing Mitre Attack	AttackIQ
5	bub bounty hunting	Udemy
6	Applied Linux command and shell scripting	Udemy
7	Python for Pentesters	Alison
8	Introduction to cyber security	Cisco
9	Introduction to IT and cyber security	Cybrary
10	Intro to Python	Cybrary
11	NDG Linux unhatched	Cisco

Education

Dhaka Polytechnic Institute

2021 to Present

Diploma In Engineering: Computer Science