DARSH TURAKHIA

Brampton, Ontario, +1 (437) 669-2938, darshturakhia@gmail.com

LinkedIn **Website**

PROFILE

Dynamic cybersecurity professional with expertise in SIEM tools, system administration (Red Hat), and various programming languages. Effective communicator and collaborative leader. Passionate about driving cybersecurity initiatives for organizational success.

SKILLS

Operating System: Windows, Linux
Database: MySQL, Sql, DB Browser
Monitoring Tools: Splunk, Securonix, Seceon AI, Wazuh
EDR Solutions: CrowdStrike EDR
Servers: XAMPP, Tomcat
Programming Language: C, C++, Python, Java
Web Language: HTML, CSS, JavaScript
Interpersonal: Communication, Collaboration, Proactivity, Time management, Adaptability, Leadership

WORK HISTORY

Security analyst, SOC, Techdefence labs, India — January 2023 - May 2023

- Leveraged cutting-edge SIEM tools to monitor, detect, and respond to cyber threats targeting organization's network and systems, reducing potential risks by 18% within first three months of tenure.
- Prevented a potential loss of $100K by detecting a real-world brute force attack by leveraging SIEM capabilities, mitigating potential damage and ensuring uninterrupted business operations.
- Collaborated cross-functionally with teams to implement and enhance security measures and protocols, resulting in a 36% improvement in incident response time.
- Played a pivotal role in incident response activities, providing timely and effective resolutions to security incidents, with a 10% decrease in incident severity over course of employment.
- Received recognition and an award from company for outstanding performance and dedication to cybersecurity excellence.

System administrator, Electromech Corporation, India — May 2021 - July 2021

- Demonstrated expertise in administering and maintaining IT systems and infrastructure, utilizing skills acquired through the Red Hat Certified System Administrator (RHCSA) certification.
- Deployed and configured Red Hat Enterprise Linux systems, ensuring optimal performance and security in alignment with industry best practices.
- Spearheaded a project leveraging Docker technology to streamline application deployment processes, resulting in a 20% improvement in efficiency and resource utilization.

EDUCATION

CYBER SECURITY AND COMPUTER FORENSICS — January 2024 - Present
Lambton College, Mississauga, Ontario

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING July 2019 - May 2023

Ganpat University, India

- Major of Cyber Security, GPA 3.5 / 4.0
- Awarded Director General Award for student excellency

PROJECTS

- Security Incident & Event Management Automation
  Developed a fully automated SIEM solution integrating Windows Event Viewer logs into Splunk with CSV encryption for heightened security.

- Analysis of a Malware
  Conducted an in-depth analysis of the Pony Stealer malware showcasing advanced malware analysis skills.

- Exploiting a physical machine
  Demonstrated proficiency in system deployment and penetration testing by documenting the deployment and subsequent root access to the Stapler machine.

- Aerospace Industry
  Successfully implemented IBM's ISIM tool for organizational enhancement in the aerospace industry.

- GitHub Analytics
  Created a web app offering insights into GitHub activity from 2011-2021, filtering by programming languages utilized.

- Fraud Detection System
  Designed an online transaction app with robust fraud detection features including data protection, email notifications, and API security measures.

- Expense Manager
  Engineered a website enabling multiple users to manage expenses, bills, and goals with personalized tables and graphical representations.

- Library Management
  Constructed a PHP-based library management system with secure admin and member functionalities, featuring database structuring and password protection.

CERTIFICATIONS

300 Certified SNYPR Security Analyst 6.3.1 **Securonix**

Demonstrates expertise in analyzing and securing networks using SNYPR with version 6.3.1.

300 Certified SNYPR Administrator 6.3.1 **Securonix**

Proficient in administrating and managing SNYPR security systems version 6.3.1 for robust network defense.

Red Hat Certified System Administrator (RHCSA) **RedHat**

Validates strong foundational skills in system administration, including security aspects, within Red Hat Linux environments.

CCNA: Switching, Routing, and Wireless Essentials **CISCO**

Confirms adeptness in essential networking tasks, including switching, routing, and wireless technologies, crucial for securing network infrastructures.

Data Privacy Fundamentals **IBM**

Demonstrates fundamental knowledge and skills in safeguarding sensitive data and ensuring compliance with data privacy regulations.

NSE 2 Network Security Associate **Fortinet**

Signifies proficiency in foundational network security concepts, strategies, and technologies, essential for securing modern network environments.

VOLUNTEER WORK

Team Lead, Karma Foundation, India May 2020 - July 2020

- Initiated and managed outreach to around 220 authors and storytellers, soliciting short video clips for promotional materials.
- Orchestrated editing and merging of more than 100 video submissions into cohesive promotional content for organization's initiatives.