





# Arsalan Husain

 [LinkedIn](#) |  978-460-4978 |  arsalanhusain15@gmail.com |  [GitHub](#)

## Objective

Dedicated and tech-savvy professional with a successful track record in Human Resources, seeking to leverage my skills and transition into a Cybersecurity SOC Analyst role.

## Cybersecurity Skills

SIEM | Azure Sentinel | Splunk | Firewalls | Windows Administration | Kali Linux | Wireshark | Digital Forensics | Metasploit | Bash | Python | Burp Suite/Beef | John The Ripper | Decryption/Analysis | Autopsy | OWASP | MITRE Framework | Nessus Vulnerability Scanner | TCPdump |

## Education

### Cybersecurity Bootcamp

Columbia University

New York, NY, USA

08/2022 - 02/2023

- 24 Week Cybersecurity Bootcamp Certificate

## Cybersecurity Projects

### [Managing a SIEM Through Splunk](#)

- Utilized system logs to monitor and detect attacks on company infrastructure.
- Established baseline behavior to evaluate system alarms in the event of a breach due to unusual behavior.
- Derived actionable insights to enhance prevention strategies based on generated reports from Splunk.
- Provided crucial evidence for incident response and ensured compliance with security policies.

### [Using Splunk To Detect Attacks](#)

- Analyzed the company outage and determined the time frame for system downtime and recovery after the DDOS through event monitoring.
- Depicted the critical vulnerabilities with a Splunk report, and set a custom daily alert to send to the SoC analyst when any vulnerabilities are detected.
- Identified the time frame for the brute force attack, and established a baseline and threshold of bad logins for active hourly alert.

### [Azure Sentinel MAP with LIVE CYBER ATTACKS!](#)

- Used Azure Sentinel (SIEM) and connected it to a live virtual machine acting as a honey pot.
- Observed live attacks (RDP Brute Force) from all around the world.
- Used a custom PowerShell script to look up the attackers Geolocation information and plot it on the Azure Sentinel Map.

## Certifications

- CompTIA Security+
- Currently pursuing CompTIA Network+ - Estimated Completion by December 2023

## Work Experience

### Talent Acquisition Coordinator

EOS Accountants LLP

New Jersey

07/2021 - Present

- Collaborated closely with key stakeholders to implement and enforce security protocols within the recruiting process, safeguarding sensitive candidate information and mitigating potential risks.
- Implemented and established recruiting programs from inception, including the system architecture, infrastructure and process.  
**Saving \$150,000 for the firm within 2 years.**
- *Developed and created technical documentation for all best practices, policies, and procedures.*

### HRIT Analyst

C&S Wholesale Grocers

New Hampshire

07/2019 - 03/2021

- Managed Windows administration and Active Directory functions for the HR team, ensuring smooth operations and system stability.
- Implemented and managed user accounts, security groups, and access controls within Active Directory, data integrity and privacy.

## Other Education

### Bachelor of Science

Virginia Tech

Blacksburg, VA, USA

08/2015 - 05/2019

- Major in Business Management and Human Resources