Ali Ahmed Dar

SECURITY ENGINEER

| Pakistan | +923041079717 | aliahmeddarhere@gmail.com | linkedin.com/in/ali-ahmed-dar/ |

Experience

Security Engineer | Ebryx Pvt Ltd

Detection & Response **05/2023 – present**

- Identified critical gaps in the organization's infrastructure and systems, leading to an improved overall security posture.
- Successfully integrated several essential log sources with centralized security tools, improving real-time threat visibility and reducing incident response time.
- Implemented advanced security controls for endpoints and cloud environments, resulting in a decrease in security incidents and a reduction in potential data breaches.
- Formulated comprehensive incident response processes and procedures, automating responses.
- Leveraged Terraform Infrastructure as Code (IAC) to transform cloud infrastructure, enhancing security, stability and compliance standards.

SOC Analyst **05/2022 – 04/2023**

- Conducted continuous monitoring and analysis to swiftly detect security attacks, leading to the development of innovative detection techniques to bolster threat identification.
- Contributed to incident investigations by identifying root causes and collaborating on security improvements.
- Collaborated in incident response efforts to contain and remediate threats, minimizing potential impact and safeguarding the organization.
- Actively promoted efficiency and accuracy by automating daily operational workflows, including security detection and response components, for the benefit of the organization.

Part-Time Consultant | SecureX AI Inc. (Startup) 05/2022 – 01/2023

- Innovated data gathering methodologies to efficiently collect vulnerability and risk data for various software and products from diverse sources such as CVE, NVD, and NIST, enabling comprehensive threat assessments and informed decision-making.
- Delivered consultancy services, empowering teams with secure work practices knowledge, specifically focusing on secure data transfer and storage techniques, enhancing overall data protection and risk mitigation strategies.

Computer Networks & Security Intern | NCSAEL 07/2021 – 02/2022

- Designed and established a secure network perimeter.
- Developed monitoring solutions and effective detection techniques.
- Performed network scanning and in-depth vulnerability analysis.

Skills

- **Security Monitoring, Detections & Incident Management**
  SIEM | SOAR | EDR | XDR – [Sentinel | QRadar | Wazuh | ELK | Microsoft Defender | CrowdStrike]
- **Cloud Security**
  Microsoft Azure | GCP | AWS
- **Security Posture Management**
  Lacework | Prisma | Cloudflare Warp Zero Trust | Wiz
- **Identity & Access Management**
  Okta | Azure AD IAM
- **Network Security**
  Packet Capture | Traffic Analysis
- **Programming, Scripting & Automation**
  Python | BASH | Batch (CMD) | Infrastructure as Code - Terraform

Certifications

- Microsoft Certified | Security, Compliance, and Identity Fundamentals 09/2023
- The SecOps Group | Certified Cloud Security Practitioner (CCSP - AWS) 04/2023
- The SecOps Group | Certified Network Security Practitioner (CCSP - AWS) 04/2023
- ARC-X | Cyber Threat Intelligence (CTI-101) 03/2023
- MITRE | ATT&CK Defender ATT&CK Adversary Emulation 11/2022
- ISC2 | Certified in Cybersecurity (CC) 11/2022

Education

Bachelors in Software Engineering | NUST 2018-2022

Interests

- **Cars** - I love driving and learning about cars
- **Human psychology** - A human brain charms me like nothing else
- **Social work** - I find happiness in helping out others whenever I can