Ali Ahmed Dar

SECURITY ENGINEER

+923041079717

aliahmeddarhere@gmail.com

https://ali-ahmed-dar.github.io/

linkedin.com/in/ali-ahmed-dar/

Experience

Security Engineer | Ebryx Pvt Ltd **05/2022 – present**

- Continuous monitoring on several security tools and analysis of the alerts to swiftly detect and mitigate security threats.
- Contribution to incident investigations by identifying root causes and collaborating on security improvements.
- Collaboration in incident response efforts to contain and remediate threats, minimizing potential impact and safeguarding the organization.
- Development and improvement detections to cover a broader range of attack vectors and reduced false positive noise.
- Gap identification and analysis in the organization's infrastructure and systems, leading to an improved overall security posture.
- Integration of essential log sources with centralized security tools, enhancing real-time threat visibility and reducing incident response time.
- Formulating comprehensive incident response processes and procedures, automating responses using native automations and other 3rd party integrations.
- Advanced security controls for endpoints and cloud environments, resulting in decreased security incidents and potential data breaches.
- Design and implementation of system hardening guidelines for endpoints, cloud environments and software services.
- Purple Teaming activities with the Red Team to identify and cover gaps in logging, detections, and response capabilities.
- Secure service delegation between the service providers and customers.
- Use of Terraform Infrastructure as Code (IAC) to transform cloud infrastructure to code, enhancing security, stability, and compliance standards.
- Promoting efficiency and accuracy by automating daily operations for the benefit of the organization and a smooth workflow.

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 | WAF – [Sentinel | QRadar | Wazuh | ELK | Microsoft Defender | CrowdStrike | Cloudflare]
- **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 | Git, GitHub

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 & Professional Trainings

- Certified Solutions Architect Associate | AWS 2022
- Security Operations Analyst | Microsoft 2022
- Bachelors in Software Engineering | NUST 2018-2022

Interests

- **Cars** – A car enthusiast, interested in driving and understanding automobiles
- **Psychology** - Fascinated by human psychology – analyzing human behaviors
- **Social work** - I find happiness in helping out others whenever I can