Ali Ahmed Dar

SECURITY ENGINEER

+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.
- Performed several Purple Teaming activities along with the Red Team to identify and cover any gaps in the logging, detections and response capabilities.
- Successfully integrated several essential log sources with centralized security tools, improving real-time threat visibility and reducing incident response time.
- Improved detection quality to cover a larger amount of attack vector and reduced the false positive noise.
- Implemented advanced security controls for endpoints and cloud environments, resulting in a decrease in security incidents and a reduction in potential data breaches.
- Designed and implemented several system hardening guidelines.
- Implemented a secure service delegation model between the organization’s Azure Sentinel and the service provider’s Azure AD.
- Formulated comprehensive incident response processes and procedures, automating responses using native Azure Logic apps and other 3rd party integrations.
- 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.

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 & Trainings

Certified Solutions Architect Associate | AWS 2022

Security Operations Analyst | Microsoft 2022

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