Ali Ahmed Dar

CyberSecurity Engineer

+923041079717
aliahmeddarhere@gmail.com
ali-ahmed-dar.github.io/
linkedin.com/in/ali-ahmed-dar/

SUMMARY

With extensive experience in a Security Operations Center (SOC), I specialize in cloud security, detection engineering, and incident response. I excel in crafting proactive strategies to mitigate risks and optimizing operations through automation. I've led initiatives like purple teaming, improved infrastructure visibility, and enhanced detection capabilities. I'm committed to continuous learning and cybersecurity principles, offering organizations valuable addition their security and resilience.

WORK EXPERIENCE

05/2022 – Present **Security Engineer** **Ebryx Pvt. Ltd**

- Continuous monitoring on several security tools and analysis of the alerts.
- Incident investigations for root cause identification and security improvements.
- Incident response to contain and remediate threats, minimizing potential impact.
- Development and improvement in threat detections.
- Gap identification in the organization's infrastructure for an improved overall security posture.
- Integration of essential log sources with centralized security tools.
- Formulating comprehensive incident response processes and procedures.
- Automation of incident responses and security processes.
- Advanced security controls for endpoints and cloud environments.
- Development of hardening guidelines for endpoints, cloud infra and software services.
- Purple Teaming activities to cover gaps in logging, detections, and response capabilities.
- Promoting efficiency and accuracy by automating daily operations for a smooth workflow.

CERTIFICATIONS

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

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

EDUCATION & PROFESSIONAL TRAININGS

• 2022	Bachelor in Software Engineering	NUST
• 2022	Security Operations Analyst	Microsoft
• 2022	Certified Solutions Architect Associate	AWS

INTERESTS

• Automobiles	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