Ali Ahmed Dar

Security Engineer

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

SUMMARY

CyberDefense professional with experience in cloud security, detection engineering, and incident response, adept at risk mitigation, automation, and enhancing security and infrastructure visibility

WORK EXPERIENCE

05/2022 – Present Security Engineer Ebryx Pvt. Ltd

Contributed to SOC team in an MSSP, with clients across EU, US, and Middle East, also provided dedicated support to the in-house Security team of a prominent EU-based organization as a detection engineer, identifying and mitigating security threats within their hybrid IT infrastructure.

- Log collection from several services – AWS (through CloudTrail & CloudWatch), Azure (Monitor), on-prem devices (EDRs/agents), firewalls and other 3rd party software to ensure comprehensive security monitoring.
- Research on threat actors and purple teaming activities – designing & implementing detection rules on SIEMs and using native services like AWS GuardDuty, Security Hub, Microsoft Defender, as well as third-party software like Wiz, Prisma, and network firewalls.
- Monitoring and analysis of alerts on SIEMs, firewalls, native and third-party cloud security solutions, conducting investigations and root cause analysis, providing suggestions for security improvements, and executing incident response to contain and remediate threats.
- Conducted comprehensive gap identification in the organization's infrastructure, suggesting and implementing new security rules, robust infrastructure configurations, and advanced security measures, significantly enhancing the overall security posture.
- Developed and implemented robust protocols for modern cloud infrastructure and services, aligning with ISO 27001 compliance standards, while also creating hardening guidelines for endpoints, cloud infrastructure, and software services.
- Automated incident response mechanisms and daily workflows using collaborative tools such as Jira, Slack, and spreadsheets, streamlining processes and enhancing efficiency.
- Implemented advanced security controls for endpoints and cloud environments, including but not limited to network policies, security groups, ACLs, and Zero-Trust principles, ensuring comprehensive protection against evolving threats.
- Converted cloud instances, networking, IAM & firewall configurations, and automations on AWS and Azure into Terraform code, for management, efficiency and reliability.
- Developing an in-house cloud security posture, vulnerability & (mis)configuration scanner.
- Managed IAM in both AWS and Azure, alongside overseeing Okta as an Identity Provider (IDP), spearheaded onboarding/offboarding automation initiatives and devised access-granting methods spanning across multiple cloud tenants.

07/2021 – 02/2022 Security Intern NCSAEL

- Developed security monitoring & detection solutions leveraging firewalls, EDRs, and SIEMs.
- Used Python and external APIs for network scanning to discover and identify vulnerabilities.
- Secured network perimeters to safeguard against unauthorized access and potential threats.

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 – Sentinel, QRadar ,Wazuh ,ELK (ElasticSearch) , VIPRE
  - EDR & XDR – Microsoft Defender CrowdStrike, Cloudflare Warp Zero Trust
  - Firewall/WAF – Cloudflare, AWS WAF
- Cloud Security Posture Management
  - Microsoft Azure – Sentinel (Detections & investigations, monitoring dashboards, automations), Defender (Cloud, Apps, Endpoints & Emails), Vaults, IAM and networking
  - AWS – CloudTrail, GuardDuty, CloudWatch, SecurityHub, SecurityGroups, WAF
  - Lacework, Prisma Cloud & Wiz
- Programming, Scripting & Automation
  - Python
  - BASH & Batch (CMD)
  - Infrastructure as Code – Terraform

EDUCATION & PROFESSIONAL TRAININGS

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