Ahmed Mohamed Ahmed Azhary

Cell: +201552222583

E-mail: Alazhary.ahmed@gmail.com

LinkedIn: https://www.linkedin.com/in/ahmed-azhary-a1999270/

Professional Summary

Accomplished information security professional with over a decade of experience in designing, implementing, and supporting security initiatives in fast-paced, customer-facing environments. Expertise in developing and implementing robust security policies and procedures to mitigate emerging threats and vulnerabilities. Skilled in maintaining long-term customer relationships and staying up-to-date with the latest technologies, ensuring organizations are equipped to tackle evolving security challenges.

Professional Experience

National Bank of Kuwait Egypt | Head of SOC & Information Security and Incident Response Manager

January 2024 – Present

- Develop and implement information security policies and procedures to protect the bank's information assets from unauthorized access, theft, or damage.
- Managed the Security Operations Center (SOC) across many countries, including Egypt, ensuring efficient and continuous monitoring and protection of critical assets.
- Developed and implemented regional security strategies tailored to the specific needs of each country under your administration, while ensuring alignment with NBK Group policies
- Directed and coordinated a larger SOC team, ensuring operations aligned with business objectives and regulatory compliance across different regions.
- Enhanced threat detection and response systems, improving the overall security posture across all managed countries.
- Led SOC training programs to strengthen incident response capabilities for international teams.

National Bank of Kuwait Egypt | Information Security and Incident Response Manager

February 2023 – December 2023

- Develop and implement information security policies and procedures to protect the bank's information assets from unauthorized access, theft, or damage.
- Conduct regular security assessments and audits to identify vulnerabilities and potential threats to the bank's information systems.
- Develop and implement incident response plans to minimize the impact of security breaches and other incidents on the bank's operations and reputation.
- Collaborate with other departments and stakeholders to ensure compliance with relevant regulations and industry standards for information security.
- Stay up-to-date on emerging security threats and trends and continuously improve the bank's security posture.
- Manage and train a team of security professionals responsible for monitoring, detecting, and responding to security incidents.
- Ensure the security of customer data and personal information, and maintain customer trust in the bank's ability to protect their confidential information.
- Provide regular security awareness training to employees to promote a culture of security within the bank.

Vodafone Egypt | Cyber Security Defense Tech Lead

November 2020 – February 2023

- Provided mentorship and training, improving team performance and incident handling skills.
- Provide immediate supervision to a team of Incident Response Analysts
- Responding to critical incidents, threats, vulnerabilities and bring these issues to resolution
- Continually create new knowledge base articles and pattern discovery to be used for discovery, analysis, and detection
- Communicator/coordinator with internal and 3rd party teams during high severity incidents
- Communicator/coordinator for annual table-top exercises
- Develop new, repeatable methods for finding malicious activity across Blackbaud networks, systems, and products - create alert content as needed from findings
- Design, document, and implement incident response processes, procedures, guidelines, and solutions. Responsible for technical and executive level reports on incident response issues
- Able to perform case management duties
- Lead and work together with the analyst team on executing threat hunting and threat intel activities
- Provide mentoring and training sessions for the Threat Detection and Response team

- Perform basic programming and develop scripts in support of/as needed for Incident Response and Security Operations
- Position includes on call responsibilities

Telecom Egypt | Senior Network Security Engineer

January 2019 – October 2020

- Planning, engineering, and monitoring the security arrangements for the protection of the network systems.
- Identifying, monitoring, and defining the requirements of the overall security of the system.
- Creating different ways to solve the existing threats and security issues.
- Configuring and implementing intrusion detection systems and firewalls.
- Testing and checking the system for weaknesses in software and hardware.
- Maintaining firewalls, virtual private networks, web protocols, and email security.
- Creating virus and threat detection systems.
- Configuring and installing security infrastructure devices.
- Investigating intrusion and hacking incidents, collecting incident responses, and carrying out forensic investigations.
- Determining latest technologies and processes that improve the overall security of the system.
- Using industry-standard analysis criteria to test the security level of the firm.
- Developing tracking documents to note system vulnerabilities.
- Reporting the security analysis and monitoring findings.
- Supervising the configuration and installation of new software and hardware.
- Implementing regulatory systems in accordance with IT security.
- Informing the company about the security incidents as soon as possible.
- Modifying the technical, legal, and regulatory aspects of the system security.
- Defining and maintaining security policies.
- Occasionally replacing the security system protocol and architecture.
- Maintaining switches and servers.

Pfizer | IT Security Operations Backline Engineer

August 2016 – December 2018

- First line Tel. & IT Security on line activities and actively monitors & analysis security alerts and provides early alerting and basic troubleshooting when needed.
- Provides monitoring and alerting for security services & malicious activities; takes mitigation actions & escalates urgent cases to the on-call security engineer.
- Responsible for implementation of user access profiles defined & approved by the production system and data owners.
- Responsible for implementing the approved and assigned security request for changes.
- Provides initial troubleshooting and diagnostics for security related incidents.

- Handles incidents communications within the team and with other teams when necessary.
- Provides Data Security analytics & correlations using approved systems.
- Reported incidents are escalated & resolved based on agreed SLA.
- Responsible for doing analysis to produced alerts and creates used cases based on investigations.

Malomatia – ICT | L1 Network Support Engineer

August 2012 – August 2016

- Supported network environments for the Government Network of Qatar, handling security and network operations.
- Provided first-line troubleshooting, ensuring rapid incident resolution.
- Progress service / change requests, incidents and problems, determine root cause and communicate to internal and external stakeholders
- Provision and maintenance of user accounts and access rights across multi-vendor hardware and Applications
- Monitoring internal and remote network environments initiating first line troubleshooting / triage procedures
- Communication, delegation and escalation with internal and external support tiers
- Identification and mitigation of various security threats

Key Projects

- Fortigate, Palo Alto, Forcepoint, Cisco ASA, and SRX Firewall installation and migration projects.
- VPN and NAC system deployments using Pulse Secure and Cisco ISE.
- Migrated proxy systems from Forcepoint to Blue Coat.
- Led cloud security and DLP implementations across multiple sites.

Technical Skills

- Security Information and Event Management (SIEM): Expertise in QRadar, ArcSight, Splunk, and LogRhythm.
- Firewall Configuration and Management: Proficient with Cisco ASA, Palo Alto, Fortinet, SRX, Check Point.
- Threat Intelligence and Incident Response: Skilled in threat hunting, malware analysis, and forensic investigations using MITRE ATT&CK and Threat Intelligence Platforms (TIPs).
- Vulnerability Management and Penetration Testing: Experience with tools like Nessus, Qualys, OpenVAS, and Kali Linux.
- Intrusion Detection/Prevention Systems (IDPS): Configured and monitored Snort, Suricata, and Cisco Firepower.

- Identity and Access Management (IAM): Proficient in Active Directory, Okta, and Azure AD.
- Data Loss Prevention (DLP): Implemented and managed DLP solutions using Symantec, Forcepoint, and McAfee.
- Encryption and Endpoint Security: Experience with BitLocker, McAfee Endpoint Protection, and Symantec Endpoint Protection.
- Cloud Security: Secured cloud environments on AWS, Azure, and Google Cloud.
- Disaster Recovery and Business Continuity Planning: Developed and tested recovery plans, ensuring minimal disruption during incidents.
- Programming and Scripting: Skilled in scripting with Python, Bash, and PowerShell to automate security operations and incident responses.

Certifications

- Certified Information Systems Security Professional (CISSP)
- Palo Alto Networks Certified Network Security Engineer (PCNSE)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Professional Security (CCNP Security)
- Red Hat Admin 1
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Systems Engineer (MCSE)

Education

B.Sc. in Information Systems, New Cairo Academy (2011)

Personal Information

Nationality: Egyptian
Date of Birth: 28/11/1988
Marital Status: Married
Languages: Arabic (Native), English (Fluent)