

Holds a B. Sc. in Electronics & Communications Engineering and a Diploma in Cybersecurity. Has over 7 years experience working in cyber security.

PERSONAL DATA

Nationality : Egyptian
Gender : Male

EDUCATION

- : B. Sc. in Electronics & Communications Engineering, Arab Academy for Science and Technology and Maritime Transport, 2013
- : Diploma in Cybersecurity track intake 38, Information Technology Institute, 2018

LANGUAGES

Arabic : Native Language
English : Very Good

COMPUTER SKILLS

- : Windows, MS Office, Internet

TRAINING COURSES AND CERTIFICATIONS

- : Cisco Certified Network Associate (CCNA) course & IT-Essential course, ITTA Cisco Networking Academy (Jan. 2014 – Dec. 2015).
- : ICS Cyber Security 301 V and 410 V.
- : McAfee Network Security Platform (IPS) Essential.
- : Introduction to Machine learning with Python.
- : Certified Ethical hacker v10 (CEH V10) - ECC4869207351.
- : ITIL Foundation certificate in IT Service Management - GR671081566MK.
- : Certified CCNA Cyber OPS.
- : Cisco Certified Network Associate (CCNA R&S) (Mar. 2016) - verification No. LDRXC3HD7PE416CN.
- : Intern - home using real Cisco gears (Jan. 2016 – Jun. 2016):
 - Design and implement a local area network in the branch office that can serve up to 40 users.
 - Upgrade IOS on switches, and routers (2821, 3550, 877).
 - Configure routers and switches.
 - Setup Wi-Fi with Vlans for public and private clients, configured Access Points (Cisco wap4410).

- Set up switches to handle both VOIP and data from clients.
 - Set up a VPN connection between the branch and corporate office.
 - Documentation for all the work.
- : Intern - Vodafone (spring 2013):
- Overview of GSM, UMTS, LTE network.
 - Overview of computer network.
 - Overview of transmission concept.
- : Intern - Alexandria Mineral Oils Co. (AMOC) (spring 2015):
- PLC & SCADA system training.
 - Business of sector Petroleum Industry.
 - Overview of Computer Networks in the company.

CHRONOLOGICAL EXPERIENCE RECORD

- Dates** : From Jun. 2023 till now
- Employer** : PWC ETIC
- Job title** : OT / IT Senior Consultant
- Job Description** :
- Assess customers based on NIST CSF and create the remediation activities plans and projects.
 - Collaborating with Senior managers to define and create the OT Target Operating Model (OT TOM) for our customers.
 - Collaborating in defining and creating OT vulnerability Management 's Target operating model.
 - Define the reference OT architecture based on the Purdue Model.
 - Define the roadmap for the Target state.

- Dates** : From Dec. 2021 till Jun. 2023
- Employer** : Orange Business Service
- Job title** : Active Prevention & Threat Intelligence Security Solution Engineer
- Job Description** :
- Design and develop new Security Solutions for all security services handled by the team including on- premises and on-cloud services such as (AWS, Microsoft AZURE, and Google Cloud Platform) or private cloud such as (ESXI).
 - In-lab design and test of overall architecture and components.
 - Develop and execute test plans.
 - Perform systems integration across multiple platforms such as (Backup system, PAM, firewalls, ...).
 - Provide Operations, Pre-sales, Sales, and Marketing with the appropriate support, documentation, and training and lead them during the rollout and deployment.
 - Perform operational-like tasks during pilot phases to assist operations.
 - Test and validate new features for customized and generic solutions in the lab from specifications.
 - Design and test complex customer security solutions and architectures.
 - Work closely with Customer Solutions, Professional Services, Service Delivery, and Operations to design, develop, and support Security solutions and on critical strategic occasions directly with Orange's customers.
 - Provide L3 support for security operation teams.

- If necessary, identify and raise risks to management regarding the current service and future enhancements.
- Working on OT Security systems such as Nozomi, and MS Defender for IoT.

Dates : From Sep. 2020 till Dec. 2021

Employer : Alex Bank

Job title : Senior IT Security Engineer

Job Description :

- Implement Alex Bank IT Security Policy across systems with different teams within ICT.
- Monitor the security patching process and deployment across all appliances/servers connecting to the Alex Bank network to prevent possible intrusions/vulnerabilities/risks.
- Perform an internal audit on ICT's Software/Systems and act as a focal point for external audit.
- Track security rule changes and review changes on firewalls, anti-virus software, and password parameters, to identify any risk points that might make information systems vulnerable to attacks.
- Assist in recommending changes that will improve aspects of Alex's bank security.
- Proactively monitor networks and equipment behaviors; Analyze reports generated by the monitoring system to identify trends that might indicate a future risk.
- Maintain Security Control measures in place among ICT.
- Maintain and review Users' identities and logical access management through received role-based access matrix and selected solutions.
- Review of the risks that affect Alex Bank ICT Software/Systems, monitoring audit logs for changes to threats, vulnerabilities, and available security controls.
- Ensure that the high-level network and security design is supportive of the defense-in-depth concept with critical systems located at the core and a variety of security control technologies used, and Ensure confidentiality, integrity, and availability are considered when designing the network.
- Participate in post-security incident reviews and identify and manage follow-up actions where required.
- Report security and access violations trade-off studies to recommend methods for countering threats to systems.
- Prepare monthly Security incidents, assessments, and activities tracking reports.
- Administrate Security products such as "Mail Gateway, Antivirus, Web Proxy, Firewall Monitoring, Forensics tool, Privileged Access Management, Sandbox, Network Analyzer".
- Assist in choosing and Performing POC on different security products such as "Antivirus, EDR, and IPS.

Dates : From Jun. 2018 till Aug. 2020

Employer : Aman for E-Payment

Job title : Senior Information Security Engineer

- Job Description** :
- Act as technical lead for PCI-DSS 3.2.1 and successfully get the certificate.
 - Creating Hardening Standards based on CIS for different (Operating Systems, Applications, and Databases).
 - Create policies and procedures for AMAN E-Payment.
 - Review and Assess changes on different applications (Android, web) from a security perspective based on OWASP top 10 and securing web application technology checklist (SWAT) and PCI-DSS requirements.
 - Advise and consult with stakeholders regarding new product/application changes in each iteration phase on risk assessment, threat modeling, code review through SonarQube, and vulnerability remediation.
 - Reviewing application data flow diagram and ensuring documentation of transaction flows and valid business justification for logged data and avoiding insecure ports.
 - Reviewing Network Diagrams to ensure network segmentation and segregation.
 - Perform Pentest, Vulnerability Assessment, and Firewall rules reviews on all Aman assets.
 - Implement and integrate Source code review solution with CI/CD tool (Jenkins) to automate and accelerate the development life cycle and enhance security to achieve and maintain DevSecOps.
 - Deploy and administer Security Solutions such as ("SIEM", "FIM", "Vulnerability assessments", "Static code Analysis").
 - Assess, Deploy, and manage Next-Generation Firewall.
 - Assess and deploy Antivirus solutions.
 - Deploy and manage a two-factor authentication solution.
 - Follow up with IT teams as Security Consultant on all new projects.
 - Design a New Network for AMAN E-Payment for Acceptance project which achieves PCI-DSS requirements and is based on Industrial best practice.
 - Perform Risk Assessment among Aman environments.
 - Implement a user access matrix on all applications, Operating systems, and databases and review user access based on this access matrix.
 - Implement and maintain Assets list.
 - Acting as Focal point for all external audits.

Dates : From Aug. 2016 till May 2018

Employer : Etisalat Misr

Job title : Network Operations Front Office Engineer

- Job Description** :
- 24x7 Network real-time monitoring for all Etisalat ISP Network Alarms, Events, and Faults and taking the proper action with concerned teams.
 - Interfacing with Telecom Egypt to solve Transmission Link failures and TE Power Failures.
 - Implement End-to-End Network TT management function (starting from problem appearance till final service restoration).
 - Keeping all stakeholders notified of any experienced Network Failure.
 - Follow Trouble tickets flow to ensure resolution within SLA.
 - Act as a single point of contact for the Network Operations Center and it is the gateway for all Network TTs.
 - Create Network Incidents and execute 1st level troubleshooting either to

forward to the next level or restore the problem.

- Handle all faults that need field intervention & and take the proper actions to resolve & and dispatch smoothly to the next level of supporting functions.
- Change Implementation for some Network Related Activities like (BW Upgrade and traffic Transfer...).
- Configure RFS DSLAMs/Cards after the Acceptance Phase.
- Add Tx Configuration for Tx Links during the installation Phase.
- Create ADSL Service Traffic Path through the Core Network for new RFS sites.
- Assigning and guiding Field Maintenance on site till problem restoration.
- Create Connectivity Graphs for fixed Network Sites with cooperation with Back Office.

- Field of experience :**
- Deep knowledge of PCI-DSS 3.2.1.
 - Knowledge of firewall technology, work as a teacher assistant in a firewall course in ITI.
 - Knowledge of Web, Android Applications, and network pen-testing.
 - Knowledge of Cisco Certified Network Professional knowledge (CCNP R&S).
 - Knowledge of Cisco certification network associate security (CCNA Sec).
 - Knowledge of RHCA and MCSA.