INFRASTRUCTURE & SECURITY TRACK

With the increase in the use of the Internet in the tasks of our daily lives (such as electronic banking services, online shopping, social media, etc.), personal data has become increasingly vulnerable to electronic attacks, as attackers use modern methods and technologies to overcome traditional security controls. This is why cyber security has become an important field and is in high demand.

The cyber security track includes the techniques and mechanisms for ensuring the security of computer systems, data and networks and protecting them from various electronic attacks.

The educational objectives of the program are:

1. Developing the manpower required to protect Egypt from electronic threats, while ensuring that security priorities are aligned with the country's work needs and strategies
2. Empowering graduates with the technical knowledge and skills necessary to protect and defend computer systems and networks
3. Develop graduates who are able to identify, analyze and remedy computer security breaches
4. Develop graduates who can plan, implement and monitor cyber security mechanisms to help ensure that IT assets are protected

INFRASTRUCTURE AND SECURITY

1. Cisco Network Administrator
2. Cisco Cybersecurity Engineer
3. Fortinet Cybersecurity Engineer
4. Data Center Administrator
5. Huawei Network Administrator
6. Google Technical Support Specialist
7. Azure Cloud Solution Admin & Architect
8. AWS Cloud Solution Admin & Architect
9. Cyber Security Incident Response Analyst
10. Vulnerability Analyst / Penetration Tester
11. Information Security Analyst

INFRASTRUCTURE & SECURITY TRACK

1. Cisco Network Administrator

A Cisco Network Administrator is capable of the following using Cisco technologies; Designing, installing, configuring, and maintaining Cisco network devices, such as routers, switches, firewalls, access points, etc., Troubleshooting and resolving network issues, such as connectivity, performance, security, etc., Monitoring and optimizing network performance and availability using various tools and methods., Implementing and enforcing network security policies and standards, such as encryption, authentication, authorization, etc., Updating and upgrading network software and hardware in accordance with best practices and company procedures, Documenting and reporting network configuration, status, and changes, Providing technical support and guidance to network users and other IT staff, Collaborating with other network engineers, administrators, vendors, and stakeholders on network projects and initiatives.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
Cisco CCNA Routing and Switching (200-301 CCNA)	120
Cisco CCNP Enterprise (350-401 ENCOR)	60
Total	180

INFRASTRUCTURE & SECURITY TRACK

2. Cisco Cybersecurity Engineer

A Cisco Cybersecurity Engineer should be capable of the following using Cisco technologies; Planning, implementing, managing, monitoring, and upgrading security measures, in accordance with best practices and company procedures, for the protection of the organization's data, systems, and networks, such as encryption, authentication, authorization, etc., Troubleshooting security and network problems and responding to all system and/or network security breaches, Configuring and implementing intrusion detection systems and firewalls, documenting and reporting security configuration, status, and incidents, Maintaining firewalls, virtual private networks, web protocols, and email security and Creating virus and threat detection systems, performing vulnerability and risk assessments, and testing and checking the system for weaknesses in software and hardware.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
Cisco CCNA Routing and Switching (200-301 CCNA)	120
Cisco CyberOps Associate (200-201 CBROPS)	60
Total	180

INFRASTRUCTURE & SECURITY TRACK

3. Fortinet Cybersecurity Engineer

Fortinet Cybersecurity Engineer is capable of the following using Fortinet technologies; Planning, implementing, managing, monitoring, and upgrading security measures for the protection of the organization's data, systems, and networks, Troubleshooting security and network problems and responding to all system and/or network security breaches, Configuring and implementing intrusion detection systems and firewalls, Maintaining firewalls, virtual private networks, web protocols, and email security, Creating virus and threat detection systems and performing vulnerability and risk assessments, Testing and checking the system for weaknesses in software and hardware, Developing and implementing security policies and standards, such as encryption, authentication, authorization, etc., Updating and upgrading security software and hardware in accordance with best practices and company procedures, Documenting and reporting security configuration, status, and incidents, Providing technical support and guidance to security users and other IT staff, Collaborating with other security engineers, administrators, vendors, and stakeholders on security projects and initiatives.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
Cisco CCNA Routing and Switching (200-301 CCNA)	120
Fortinet NSE 4 - FortiOS 7.2 (NSE4_FGT-7.2)	48
Total	168

INFRASTRUCTURE & SECURITY TRACK

4. Data Center Administrator

A Data Center Administrator is capable of Monitoring server performance to ensure that it meets the organization's standards for speed and quality, Installing and configuring new network components such as switches, routers, firewalls, intrusion detection systems (IDS), load balancers, VoIP phones, wireless access points (APs), and other networking hardware devices, Coordinating with other IT staff members to ensure that all components of the data center are functioning properly, including power supply units (PSUs), cooling systems, fire protection systems, and security systems, Maintaining current knowledge of new technologies and industry trends in order to recommend new solutions or improvements to existing infrastructure, Handling security issues such as server failures, computer viruses, and unauthorized access attempts, Reviewing and updating disaster recovery plans in case of a major outage or security breach, Providing technical support for users who have questions about their accounts or who have technical problems with their computers, Designing and implementing new solutions based on company goals and objectives, as well as industry best practices.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
Huawei - HCIA-Datacom (Previously HCIA-Routing & Switching)	80
VMware - VCTA - Data Center Virtualization (VCTA-DCV 2023)	36
VMware - VCTA - Network Virtualization (VCTA-NV 2023)	12
VMware - VCTA - Security (VCTA-SEC 2023)	18
Total	146

INFRASTRUCTURE & SECURITY TRACK

7. Azure Cloud Solution Admin & Architect

Azure Cloud Solution Admin & Architect is capable of the following; Creating a well-informed cloud strategy and managing the adaptation process, Evaluating cloud applications, hardware, and software regularly, Developing and organizing cloud systems and working closely with IT security to monitor the company's cloud privacy, Troubleshooting and resolving cloud issues, such as connectivity, performance, security, etc., Implementing and enforcing cloud security policies and standards, such as encryption, authentication, authorization, etc., Updating and upgrading cloud software and hardware in accordance with best practices and company procedures, Documenting and reporting cloud configuration, status, and changes, Providing technical support and guidance to cloud users and other IT staff, Collaborating with other cloud engineers, administrators, vendors, and stakeholders on cloud projects and initiatives.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
Azure Fundamentals	6
Azure Data Fundamentals	6
Azure Administrator Associate	32
Azure Solution Architect Expert	32
Customer Data Platform Specialty	32
Azure Data Scientist Associate	36
Manage Resources in Azure	10
Deploy a website to Azure with Azur Virtual Machine	8
Total	162

INFRASTRUCTURE & SECURITY TRACK

8. AWS Cloud Solution Admin & Architect

An AWS Cloud Solution Admin & Architect is capable of the following using AWS technologies; Creating a well-informed cloud strategy and managing the adaptation process, Evaluating cloud applications, hardware, and software regularly, Developing and organizing cloud systems and working closely with IT security to monitor the company's cloud privacy, Troubleshooting and resolving cloud issues, such as connectivity, performance, security, etc., Implementing and enforcing cloud security policies and standards, such as encryption, authentication, authorization, etc., Updating and upgrading cloud software and hardware in accordance with best practices and company procedures, Documenting and reporting cloud configuration, status, and incidents, Providing technical support and guidance to cloud users and other IT staff, Collaborating with other cloud engineers, administrators, vendors, and stakeholders on cloud projects and initiatives.

The technical study plan proposed for this job profile is provided below:

Course Contents	Hours
AWS Cloud practitioner	34
SysOps Administrator Associate	40
Solution Architect Associate	40
Solution Architect Professional	40
Data Analytics	28
Architecting Solutions on AWS	18
Total	200

INFRASTRUCTURE & SECURITY TRACK

9. Cyber Security Incident Response Analyst

A Cyber Security Incident Response Analyst is capable of the following; Responding to incidents and threats tracked by the Incident Response Management System. Incidents may include phish, network, email, IDS, or antivirus alerts, Performing log, vulnerability, or compliance analysis/remediation, Collection, collating, and secure handling of evidence for storage and/or processing, Drafting reports and security briefs as needed, and Participation in intra-departmental meetings and projects in support of Network, Infrastructure, and Support groups as assigned.

Course Contents	Hours
Intro to Threats, Vulnerabilities, and Incident	20
Assessing Threats	20
Finding Security Vulnerabilities	20
Fixing Security Vulnerabilities	20
Preparing for Inevitable Attacks	20
Project: Navigating a Cybersecurity Incident	20
Total	120

INFRASTRUCTURE & SECURITY TRACK

10. Vulnerability Analyst / Penetration Tester

A Vulnerability Analyst / Penetration Tester is capable of the following; Ensuring that all Network security tests are conducted within the framework set at Mastercard, Ensure that all test cases and tools are used appropriately for testing of various network segment types, Ensuring that all help and guidance is provided to development teams on the vulnerabilities identified in their applications while performing security testing, Identify improvement areas in the security testing domain and implement learnings for the Globally located team, Coordinate with application development teams on their demands for security testing and provide a seamless experience with testing and reporting of penetration tests, and Working with a global team spread across time-zones and geographies.

Course Contents	Hours
Intro to Penetration Testing & Red Team Operations	20
Reconnaissance	20
Scanning & Research	20
Gaining Access	20
Maintaining Access	20
Covering Tracks & Reporting	20
Total	120

INFRASTRUCTURE & SECURITY TRACK

11. Information Security Analyst

An Information Security Analyst is capable of the following; Encrypting data transmission to conceal confidential information as it is being transmitted and keep out tainted digital transfers, Advising, implementing, and maintaining security systems, Analyzing and investigating intruder detection or other security systems, and Encrypting data at rest to conceal confidential information.

Course Contents	Hours
Fundamentals of Defending Systems	40
Analyzing Security Threats	40
Assessing Vulnerabilities and Reducing Risk	40
Monitoring, Logging and Responding to Incidents	40
Total	160