Training includes the following topics:

· Knowledge of cybersecurity, including the impact of threats.

· Recognize the evolving cyber threat landscape, including different characteristics of cyberattacks, malware and cryptocurrency.

· Protection of data using authentication, encryption and backup.

· Learn what networks do and how they operate.

· Essentials of network devices and how to configure them.

· Understanding of core networking concepts (TCP/IP, DNS, DHCP, HTTP/S, SSH) and network troubleshooting (tcpdump, wireshark)

· Characteristics and benefits of Cloud and Virtualization technologies.

· Security and Risk Management

· Asset Security

· Security Architecture and Engineering

· Communication and Network Security

· Identity and Access Management (IAM)

· Security Assessment and Testing

· Security Operations

· Software Development Security

This training module is organized in a way that includes theory-focusing lessons, lab activities as well as practice-oriented exercises.

Expected Results from Academy Program

Successful Candidate should be able to engage responsibilities below:

· Global implications of cyber threats

· Ways in which networks are vulnerable to attack

· Impact of cyber-attacks on industries

· Approach to threat detection and defense

· Why cybersecurity is a growing profession

· Opportunities available for pursuing network security certifications

· Describe the tactics, techniques and procedures used by cybercriminals.

· Describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.

· Describe technologies, products and procedures used to protect confidentiality, ensure integrity and provide high availability.

· Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.

· Explain the purpose of laws related to cybersecurity.