

Information Security Operations Center

Prepared by
Dr. Ibrahim Gomaa

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture - Intro



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY
BY EVERYONE'S SMART UNIVERSITY

Dr. Ibrahim Gomaa

ibrahim.gomaa@midocean.ae



MIDOCEAN
UNIVERSITY

Assistant Prof.



Assistant Prof.
NTI, MCIT, Egypt

SANS
INSTITUTE

hp

Microsoft

Linux

Information Security
Network Security
Cloud Security
Internet of Things
Blockchain Technology

Certified trainer for the following academies:

cisco

amazon

HUAWEI

vmware

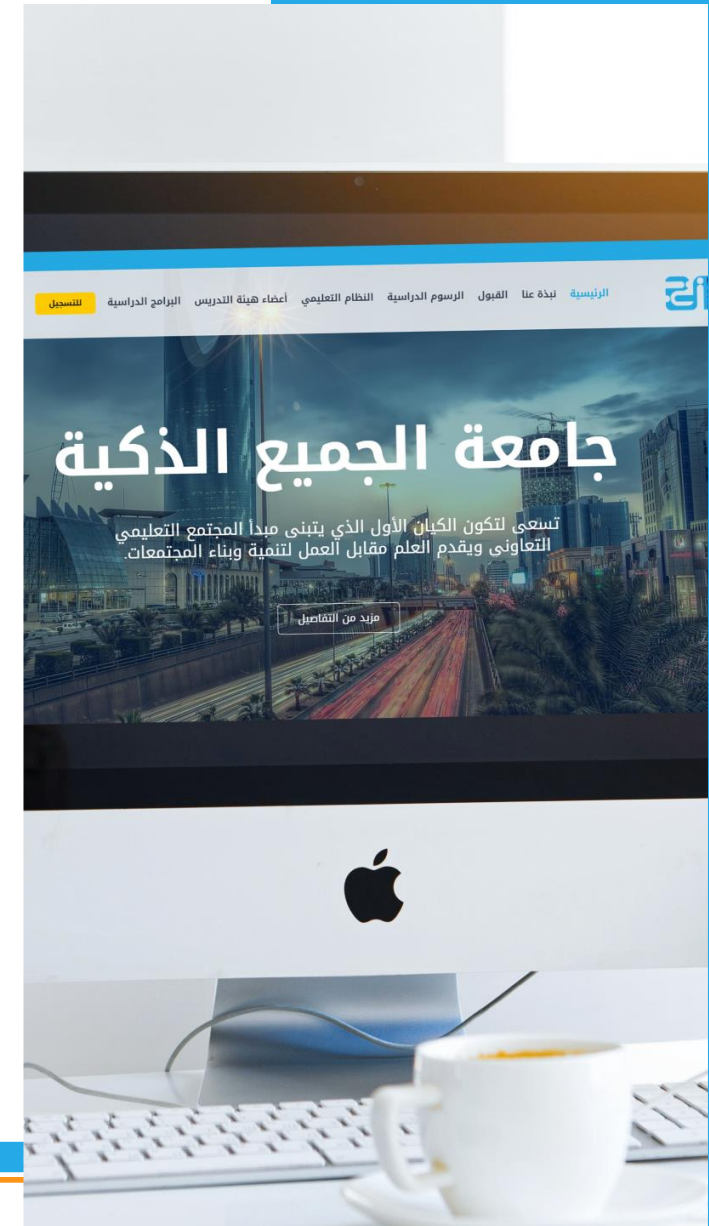
FORTINET

Information Security Operations Center (SOC)



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

The course covers the knowledge and skills needed to
successfully handle
the tasks, duties, and responsibilities
of an associate-level Security Analyst working in
a Security Operations Center (SOC).

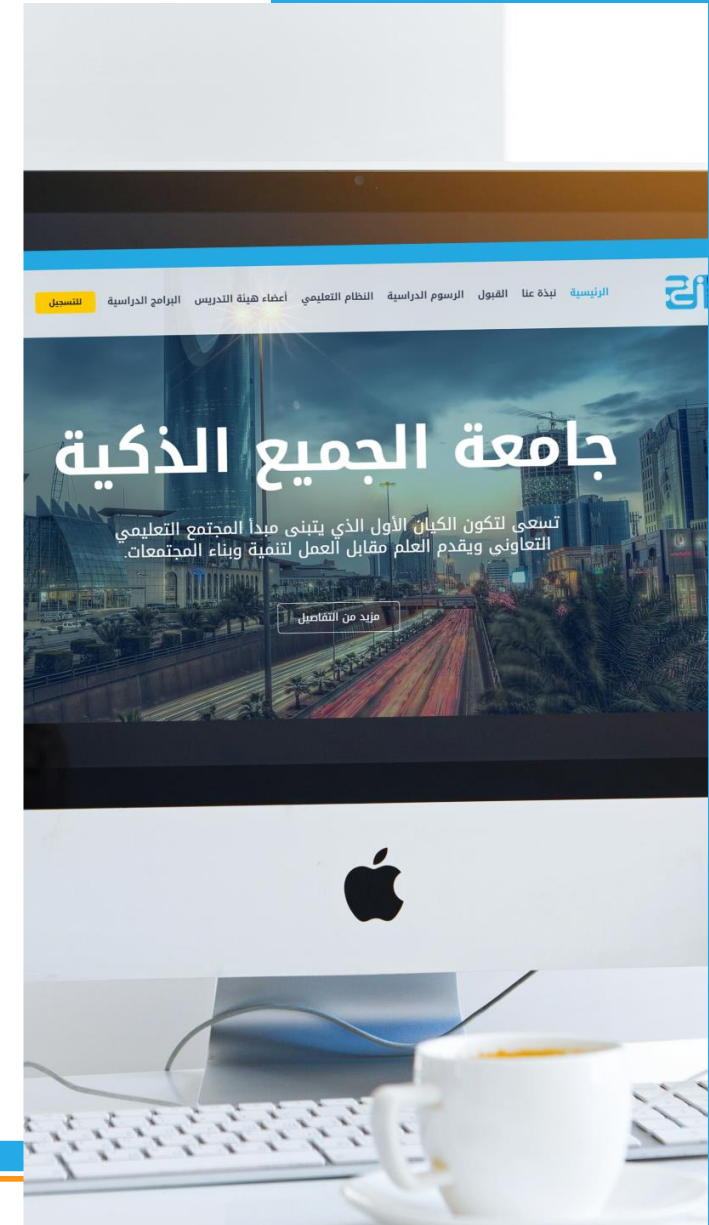


General required knowledge

IT Technical Knowledge

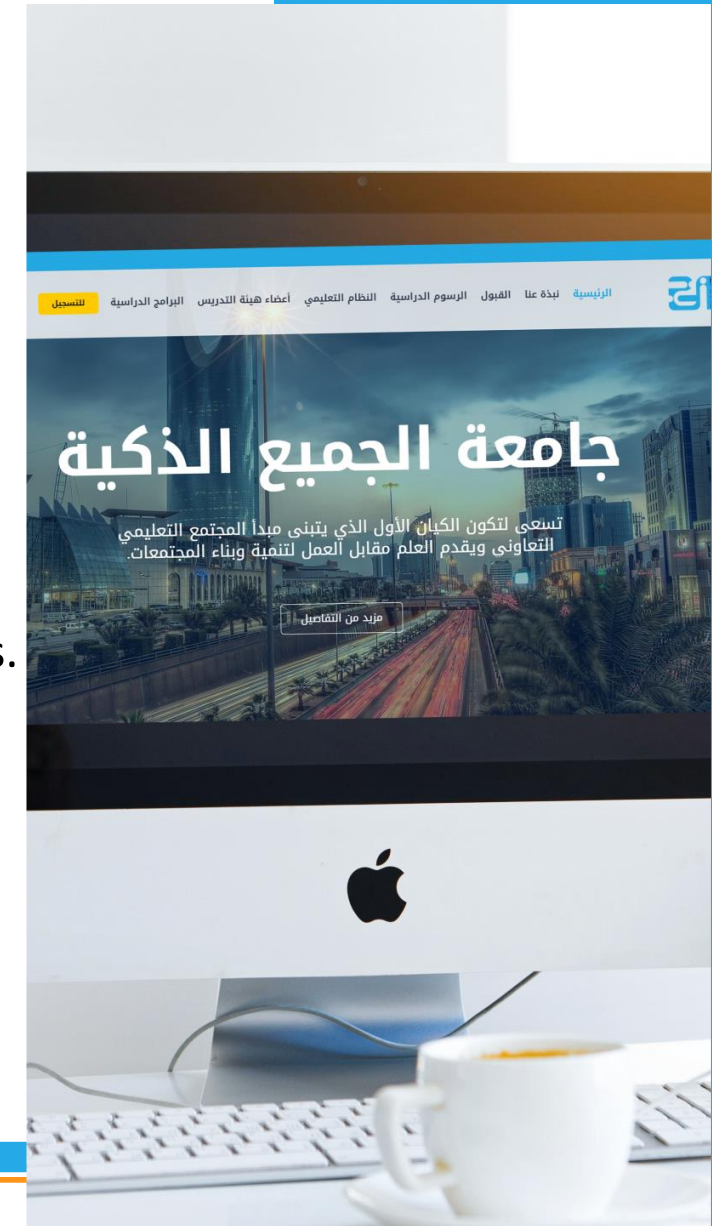
Preferred knowledge

- Familiarity with operating system concepts
- Working knowledge of information security
- Familiarity with general networking concepts



After completing this course, you should be able to:

- Security Operations Center (SOC) operation and structure.
- Linux Operating System features needed for cybersecurity analysis.
- Analyze the operation of network protocols and services.
- Identification of attacks against network protocols using network monitoring tools.
- How to prevent malicious access to computer networks, hosts, and data.
- Understanding the impacts of cryptography on network security monitoring.
- How to investigate endpoint vulnerabilities and attacks?
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.



Lecture – Intro

Lab Environment

In this course,

two virtual machines (VM) are used:

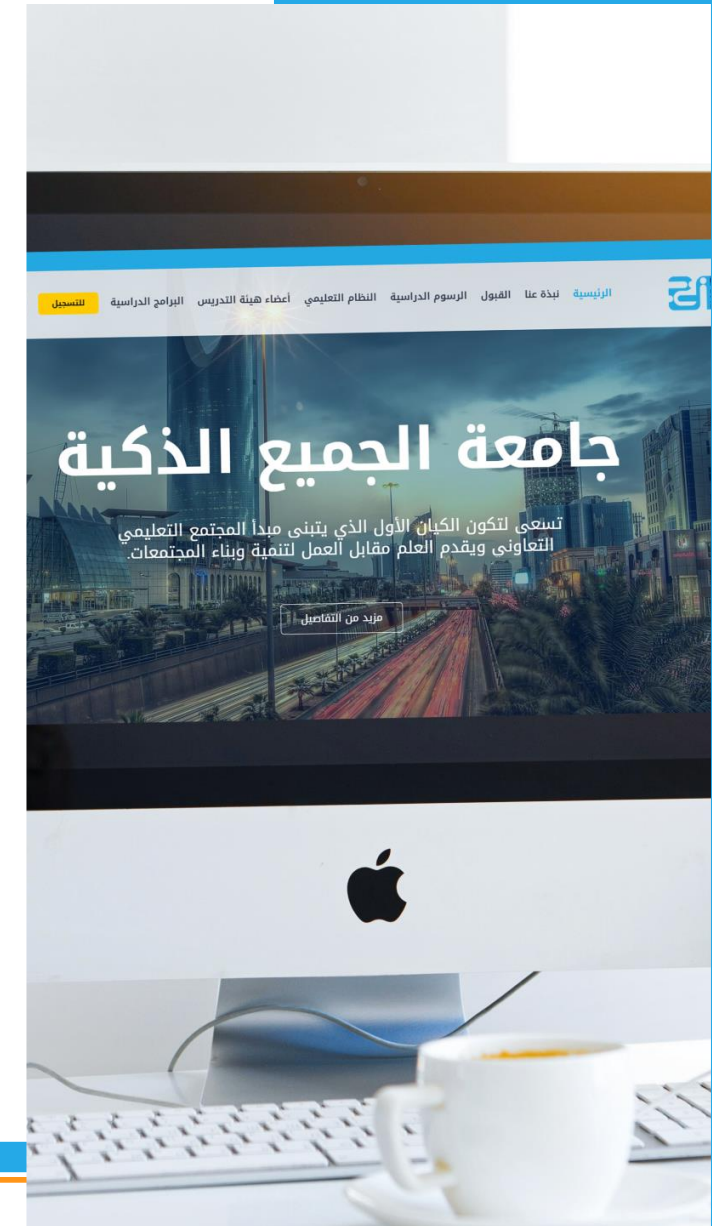
[CyberOps Workstation](#) and [Security Onion](#).

These VMs provide all of the applications and latest security monitoring and network intrusion analysis capabilities needed for the course.

The minimum RAM memory requirement to run CyberOps Workstation virtual machines is **1 GB**. However, for the Security Onion virtual machine, **4 GB** RAM is recommended.

The RAM memory recommendation on Security Onion VM allows the services, such as network security monitoring (NSM), to function properly.

Installation labs are available in the course and provide detailed steps to properly set up your VMs and the lab environment.



- **Lecture 1:** Network Security Monitoring
- **Lecture 2:** The features and characteristics of the Linux Operating System
- **Lecture 3:** Network protocols and services analysis
- **Lecture 4:** Types of network attacks
- **Lecture 5:** Investigate endpoint vulnerabilities and attacks
- **Lecture 6:** Preventing malicious access to computer networks, hosts, and data
- **Lecture 7:** The impacts of cryptography on network security monitoring.
- **Lecture 8:** Evaluate network security alerts
- **Lecture 9:** Analyze network intrusion data to identify compromised hosts and vulnerabilities
- **Lecture 10:** Apply incident response models to manage network security incidents



Lecture 1: Network Security Monitoring

Topic Title	Topic Objective
Introduction	Monitoring, Alerting, and what they can do for you.
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.
The Modern Security Operations Centre	Explain the mission of the Security Operations Center (SOC).
Becoming a Defender	Describe resources available to prepare for a career in cybersecurity operations.

Lecture 2: The features and characteristics of the Linux Operating System

Topic Title	Topic Objective
Linux Basics	Explain why Linux skills are essential for network security monitoring and investigation.
Working in the Linux Shell	Use the Linux shell to manipulate text files.
Linux Servers and Clients	Explain how client-server networks function.
Basic Server Administration	Explain how a Linux administrator locates and manipulates security log files.
The Linux File System	Manage the Linux file system and permissions.
Working in the Linux GUI	Explain the basic components of the Linux GUI.
Working on a Linux Host	Use tools to detect malware on a Linux host.

Lecture 3: Network protocols and services analysis

IPv4 and IPv6	Explain how the IP protocol supports network communications.
ICMP	Explain how ICMP is used to test network connectivity
ARP and ARP Issues	Explain how ARP requests impact network and host performance as well as potential security risks.
DHCP	Explain how DHCP services enable network Functionality
DNS	Explain how DNS services enable network Functionality
NAT	Explain how NAT services enable network Functionality
Email and HTTP	Explain how Email and HTTP services enable network Functionality

Topic Title	Topic Objective
Who is Attacking our Network	Explain how network threats have evolved.
Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
Malware	Describe types of malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering, DoS, DDoS	Explain reconnaissance, access, social engineering network attacks, DoS and DDoS

Lecture 5: Investigate endpoint vulnerabilities and attacks

Topic Title	Topic Objective
Antimalware Protection	Explain methods of mitigating malware
Host-based Intrusion Prevention	Explain host-based IPS/IDS log entries
Application Security	Explain how a sandbox is used to analyze malware
Network and Server Profiling	Explain the value of network and server profiling.
Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.

Lecture 6: Preventing malicious access to computer networks, hosts, and data

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.
Access Control Concepts	Explain how access control protocols network data.
AAA Usage and Operation	Explain how AAA is used to control network access.
Information Sources	Describe information sources used to communicate emerging network security threats.
Threat Intelligence Services	Describe various threat intelligence services.

Lecture 7: The impacts of cryptography on network security monitoring

Topic Title	Topic Objective
Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity of data.
Confidentiality	Explain how cryptographic approaches enhance data confidentiality.
Public Key Cryptography	Explain public key cryptography.
Authorities and the PKI Trust System	Explain how the public key infrastructure functions.
Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.

Topic Title	Topic Objective
Types of Security Data	Describe the types of data used in security monitoring.
Source of Alerts	Identify the structure of alerts.
Overview of Alert Evaluation	Explain how alerts are classified.

Lecture 9: Analyze network intrusion data to identify compromised hosts and vulnerabilities

Topic Title	Topic Objective
A Common Data Platform	Explain how data is prepared for use in a Network Security Monitoring (NSM) system.
Investigating Network Data	Use Security Onion tools to investigate network security events.
Enhancing the Work of the CyberSecurity Analyst	Describe network monitoring tools that enhance workflow management.

Lecture 10: Apply incident response models to manage network security incidents

Topic Title	Topic Objective
Evidence Handling and Attack Attribution	Explain the role of digital forensics processes
The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain
The Diamond Model of Intrusion Analysis	Classify an intrusion event using the Diamond Model
Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario

Thanks

