

## Managing and Defending against current Threats

**Duration: 3 Days    Course Code: MDT**

---

### Overview:

This is a deep dive course on security operations: vulnerability management, anomalies detection, discovery of industry attacks and threats, understanding how compromised system or solution looks like, defining the indicators of the attack, incident handling.

---

### Target Audience:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

---

### Objectives:

- |  |  |
|--|--|
| ■ On completion of this course you will be able to:        | ■ Prepare a risk assessment for your organization        |
| ■ Analyze emerging trends in attacks                       | ■ Report and recommend countermeasures                   |
| ■ Identify areas of vulnerability within your organization | ■ Develop a threat management plan for your organization |
- 

### Prerequisites:

■

---

## Content:

### Module 1: Identifying Areas of Vulnerability (Day 1)

This part introduces the new cybersecurity challenges and trends, emphasizing on data security and integration through and into the cloud and the challenges of the coordination of the cloud and on-premise security solutions. Security is a business enabler, and it is only when it is viewed from a business perspective that we can truly make the right decisions. You will learn how to define values of your company which needs to be protected or restricted. You will know how to find obvious and not so obvious sensitive information which can be monetized by adversaries. Having that scope defined and knowing your resources you will know where the biggest gaps in your security posture are.

1. Defining the assets which your company needs to protect
2. Defining the other sensitive information that needs to be protected

### Module 2: Modern Attack Techniques (Day 1)

1. OS platform threats and attacks
2. Web based threats and attacks
3. E-mail threats and attacks
4. Physical access threats and attacks
5. Social threats and attacks
6. Wireless threats and attacks

### Module 3: Identity Attacks (Day 1)

There are many methods widely in use today to steal personal information. These attacks on confidential data can be extremely high-tech, involving the latest technologies and most recent security exploits. Many of the attack methods, however, are very low-tech, involving little or no technology at all. By taking a detailed look at the various types of attacks, you will

### 3. Persistence methods

#### 4. Hiding traces

#### 5. Case study: ransomware examples

### Module 5: Discovery and Analysis of the Modern Attacks (Day 3)

Most computer vulnerabilities can be exploited in a variety of ways. Hacker attacks may use a single specific exploit, several exploits at the same time, a misconfiguration in one of the system components or even a backdoor from an earlier attack. Due to this, detecting hacker attacks is not an easy task. This module gives a few basic guidelines to help you figure out either if your machine is under attack or if the security of your system has been compromised.

1. Defining Critical Security Controls
2. Incident response checklist
3. Suspicious Activities Time Line
4. Filtering Suspicious Activities Network traffic inspection
5. Malware analysis tools
6. Host, Port and Service Discovery
7. Vulnerability Scanning
8. Monitoring Patching, Applications, Service Logs
9. Detecting the most common attacks:
  - a. DNS Reconnaissance
  - b. Directory Service Enumeration
  - c. Enumerating high privileges accounts

### 12. Scripting and Automation

#### 13. PowerShell for extraction and information gathering

#### 14. Industry Best Practices

### Module 6: Designing and Implementing Endpoint Security (Day 4)

In Enterprise level organizations IT landscape is divided into smaller parts based on their primary function or localization in IT environment. Sometimes you cannot implement security controls globally and you will need a deep understanding of current security posture of each element to wisely put additional layers of security. Having full environment divided into functional parts is also a better approach from financial point of view. Getting internal sponsor acceptance is easier if the benefit is delivered quicker.

1. Strategy for protecting Internet facing systems
2. Strategy for protecting internal systems
3. Strategy for protecting users' workstation
4. Strategy for protecting (against) BYOD devices
5. Implementing automation and access control (Just Enough Administration, Desired State Configuration)
6. Application whitelisting (AppLocker, Device Guard etc.)
7. Configuring firewalls
8. Privileged accounts
9. Securing authentication
10. Storage and full disk encryption
11. Control Folder Access

become familiar with the techniques used by cybercriminals.	d. SMB Session Enumeration	12. Application Guard
1. Performing the identity attacks	e. Enumerate Credentials stored in memory	Module 7: Securing the Communication Channel Approach (Day 5)
2. Cached logons (credentials)	f. Overpass – the – hash	In some organizations there is no strict architecture design defined. Especially in modern approach where most of the services are Cloud-based. This module will focus on systems communication channel rather than systems placement or role in the organization. This method is best for smaller companies as well as organizations which are in the transition phase or are changing significantly its structure.
3. Data Protection API (DPAPI) for user's secrets protection	g. Harvesting Credentials	
4. Credential Guard in details	h. Pass – The – Ticket	
5. Performing the LSA Secrets dump and implementing prevention	i. Remote Code Execution	
6. Active Directory and Azure AD security	j. Compromise KRBTGT Account	
7. Authentication Mechanism Assurance	k. Golden Ticket	1. Implementing tunneling
8. Using virtual smart cards	10. Using Sysmon in the advanced monitoring configuration	2. Designing secure access
9. Multi-factor Authentication	11. Log Collection	3. Sniffing the network techniques
Module 4: Malicious Software Techniques (Day 2)		4. The meaning of partitioning the network
The hacker can run a malicious program which the user believes to be authentic. This way, after installing the malicious program, the hacker gets unprivileged access. Techniques are becoming more sophisticated than ever. In this module you will learn how modern malware works and what are the ways to discover its operations.		5. Ensuring confidentiality with encryption
1. Types of the attacks		6. Searching for rogue servers
2. Points of entry		7. Securing networking services
		8. Limiting the impact of common attacks

## Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

[training@globalknowledge.com.eg](mailto:training@globalknowledge.com.eg)

[www.globalknowledge.com/en-eg/](http://www.globalknowledge.com/en-eg/)

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo