COURSE CATEGORY: DIGITAL FORENSICS
COURSE LEVEL:  ADVANCED
COURSE CODE: IFIS CDE/05
COURSE NAME: CONTINUOUS MONITORING AND SECURITY OPERATIONS

0101
010 IFIS
Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

## About this Course

This course will best position your organization to analyse threats and detect anomalies that could indicate cybercriminal behaviour. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether.

## Learning Outcomes

- Increase your understanding and enhance your skills in implementing Continuous Monitoring.
- Timely incident detection
- Combat cyber threats and prevent cyber attacks

## Course Outline

**Topic 1: Current State Assessment, Security Operations Centers, and Security Architecture**

The prevention-dominant security model has failed. Given the occurrence and degree of noteworthy intrusions, this should not come as a shock.
In order to address the root of the problem, we must understand the current architecture and the design gaps that facilitate the adversary's dominance.

Overview
- Traditional Security Architecture
- Perimeter-focused
- Addressed Layer 3/4
- Centralized Information Systems
- Prevention-Oriented
- Device-driven
- Traditional Attack Techniques

Modern Security Architecture Principles
- Detection-oriented
- Post-Exploitation-focused
- Decentralized Information Systems/ Data
- Risk-informed
- Layer 7 Aware
- Security Operations Centers
- Network Security Monitoring
- Continuous Security Monitoring
- Modern Attack Techniques
- Adversarial Dominance

Frameworks and Enterprise Security Architecture
- Enterprise Security Architecture
- Security Frameworks

Security Architecture - Key Techniques/ Practices
- Threat Vector Analysis
- Data Exfiltration Analysis
- Detection Dominant Design
- Zero Trust Model
- Intrusion Kill Chain

- Visibility Analysis
- Data Visualization
- Lateral Movement Analysis
- Data Ingress/Egress Mapping
- Internal Segmentation
- Network Security Monitoring
- Continuous Security Monitoring

Security Operations Center (SOC)

- Purpose of a SOC
- Key SOC roles
- Relationship to Defensible Security Architecture

### Topic 2: Network Security Architecture

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient. A detailed roadmap to bridge the gap between the current and desired state is needed. This topic introduces and details the components of our infrastructure that become part of a defensible network security architecture and Security Operations Centre. We are long past the days where a perimeter firewall and ever-present antivirus was sufficient security. Many pieces and moving parts comprise a modern defensible security architecture.

SOCs/Security Architecture - Key Infrastructure Devices

- Traditional and Next Generation Firewalls, and NIPS
- Web Application Firewall
- Malware Detonation Devices
- HTTP Proxies, Web Content Filtering, and SSL Decryption
- SIMs, NIDS, Packet Captures, and DLP
- Honeypots/Honeynets
- Network Infrastructure - Routers, Switches, DHCP, DNS
- Mobile Devices and Wireless Access Points
- Threat Intelligence

Segmented Internal Networks

- Routers
- Internal SI Firewalls
- VLANs
- Detecting the Pivot

Defensible Network Security Architecture Principles Applied

- Internal Segmentation
- Threat Vector Analysis
- Data Exfiltration Analysis
- Detection Dominant Design
- Zero Trust Model (Kindervag)
- Intrusion Kill Chain
- Visibility Analysis
- Data Visualization
- Lateral Movement Analysis
- Data Ingress/Egress Mapping

### Topic 3: Network Security Monitoring

In this topic, we will help you figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise. However, to do that, you must first understand the approach and goals of monitoring and define a methodology for analysis

Continuous Monitoring Overview

- Defined
- Network Security Monitoring (NSM)
- Continuous Security Monitoring (CSM)
- Continuous Monitoring and the 20 Critical Security Controls

Network Security Monitoring (NSM)

- Evolution of NSM
- The NSM Toolbox
- NIDS Design
- Analysis Methodology
- Understanding Data Sources;
  - Full Packet Capture
  - Extracted Data
  - String Data
  - Flow Data
  - Transaction Data
  - Statistical Data
  - Alert Data
  - Tagged Data
  - Correlated Data

Practical NSM Issues

Cornerstone NSM

- Service-Side and Client-Side Exploits
- Identifying High-Entropy Strings
- Tracking EXE Transfers
- Identifying Command and Control (C2) Traffic
- Tracking User Agents
- C2 via HTTPS
- Tracking Encryption Certificates

## Topic 4: Endpoint Security Architecture

This topic details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities. Modern attacks put an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us.

Security Architecture - Endpoint Protection

- Anti-Malware
- Host-based Firewall, Host-based IDS/ IPS
- Application Whitelisting, Application
- Privileged Accounts, Authentication, Monitoring, and UAC
- Whole Disk Encryption
- Virtual Desktop Infrastructure
- Browser Security
- EMET

Dangerous Endpoint Applications

- Java
- Adobe Reader
- Flash
- Microsoft Office
- Browsers

Patching

- Process
- To Test or Not to Test
- Microsoft
- Third Party

## Topic 5: Automation and Continuous Security Monitoring

This course focuses on continuous monitoring rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed. Continuous monitoring proactively and repeatedly assesses and reassesses the current security posture for potential weaknesses that need be addressed.

Overview

- Continuous Security Monitoring (CSM) vs. Continuous Diagnostics and Mitigation (CDM) vs. Information Security Continuous Monitoring (ISCM)
- Cyberscope and SCAP

Industry Best Practices

- Continuous Monitoring and the 20 Critical Security Controls
- Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions

Winning CSM Techniques

Maintaining Situational Awareness

Host, Port, and Service Discovery
Vulnerability Scanning
Monitoring Patching
Monitoring Applications
Monitoring Service Logs

- Detecting Malware via DNS logs

Monitoring Change to Devices and Appliances
Leveraging Proxy and Firewall Data
Configuring Centralized Windows Event Log Collection
Monitoring Critical Windows Events

- Hands on: Detecting Malware via Windows Event Logs

Scripting and Automation

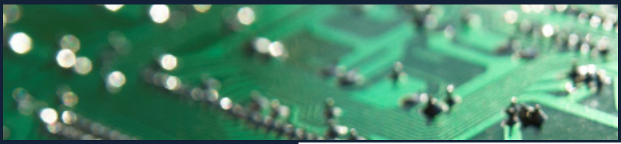
- Importance of Automation
- PowerShell
- Hands-on: Detecting Malicious Registry Run Keys with PowerShell

## Prerequisites

- Basic understanding of network protocols and devices
- Experience with Linux and Windows from the command line

## Target Audience

- Security Architects
- Senior Security Engineers
- Technical Security Managers
- SOC Analysts
- SOC Engineers
- SOC Managers
- CND Analysts
- Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)



## Application/ Relevance of this course

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/ Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

## Duration and Fees

**Duration:** 10 days

**Pricing:** $1200

**For Inquiries, booking and more information,**

**Call Admissions on 0393517236/0783517236 or Email: admissions@forensicsinstitute.org**