A Comprehensive Training Program for Cyber Defense, Risk Mitigation, and Incident Handling

INTRODUCTION

In today's rapidly evolving digital landscape, organizations face an increasing number of cyber threats that can disrupt business operations, compromise sensitive data, and impact financial stability.

This comprehensive Advanced Cybersecurity and Risk Management Framework courseware is designed to equip security professionals with the necessary knowledge and hands-on expertise to proactively identify, mitigate, and respond to cybersecurity risks and incidents.

The course follows a structured approach, covering fundamental risk management principles, business continuity planning, proactive threat monitoring, incident response, forensic investigation, and malware analysis.

By integrating real-world scenarios, industry best practices, and practical demonstrations, this training program ensures that cybersecurity professionals are well-prepared to handle evolving security challenges.

TOPICS

MODULE 1:Risk Management

MODULE 2:Business Continuity Management (BCM)

MODULE 3: Understanding the Cyber Attack Lifecycle(Complimentary)

MODULE 4:Security Operations Centre (SOC)

MODULE 5:Incident Response and Cyber Attack Handling

MODULE 6:Digital Forensics

MODULE 7:Malware Analysis

BRIEF SUMMARY OF EACH MODULES

MODULE 1: Risk Management

This module teaches students to identify, assess, and mitigate cyber risks.The students will be able to create effective risk response plans and implement relevant security controls. This will help strengthen the ability to proactively manage risks and improve overall cyber defense posture.

MODULE 2: Business Continuity Management (BCM)

Students will learn to develop and implement Business Continuity Plans (BCP) to ensure critical operations continue

during disruptions. The focus on business impact analysis (BIA) and post-disaster recovery will help to minimize downtime and quickly recover from cyber incidents, enhancing resilience and defense readiness.

MODULE 3: Understanding Cyber Attack life cycle(Complimentary)

This module covers the stages of a cyber attack from the hacker's perspective, focusing on the Cyber Kill Chain and various attack strategies. Through hands-on demos on endpoint, application, network attacks, and social engineering, students will see how attacks unfold. Case study discussions on recent cyber incidents provide real-world context. This module lays the groundwork for understanding the roles of SOC, Incident Response, Digital Forensics, and Malware Analysis in preventing, detecting, and responding to cyber threats.

MODULE 4: Security Operations Centre (SOC)

This module teaches students the core components of a Security Operations Centre (SOC), including the tools required (like SIEM), log management, and threat intelligence etc. Students will learn how these elements work together to enhance real-time threat detection and response,

strengthening the organization’s proactive defense capabilities.

MODULE 5: Incident Response and Cyber Attack Handling

Students will gain skills to handle cyber-attacks effectively by learning the stages of incident response—from preparation to post-incident analysis. This expertise enables them to mitigate damage, recover operations, and improve future defenses, ensuring quicker and more effective responses to security breaches.

MODULE 6: Digital Forensics

Focusing on forensic investigations, students will learn how to collect and analyze data from various systems, preserving evidence and uncovering cybercriminal activity. This knowledge aids in tracking attackers, supporting incident recovery, and enhancing the organization's overall response to security incidents.

MODULE 7: Malware Analysis

Students will learn to analyze and neutralize malware by performing static and dynamic analysis. This module covers infection vectors, reverse engineering, and current malware trends, equipping students with the skills to detect, counter, and prevent malware threats, thus bolstering the defense mechanisms.

CONTEXT

Effective cybersecurity and resilience begin with Risk Management, which identifies and evaluates threats, vulnerabilities, and potential impacts on an organization. This process informs the development of Business Continuity Management (BCM), ensuring that critical business functions can continue during and after a disruption. With risk and continuity plans in place, organizations establish a Security Operations Centre (SOC) to proactively monitor, detect, and mitigate threats in real time.

When an attack occurs, the Incident Response and Cyber Attack Handling process is activated, guiding teams through containment, eradication, and recovery strategies to minimize damage. Following an incident, Digital Forensics is crucial for investigating the attack, identifying perpetrators, and preserving evidence for legal or compliance purposes. Lastly, Malware Analysis plays a key role in understanding and neutralizing malicious software, providing insights that improve future threat detection and response strategies.

Together, these elements form a structured approach to cybersecurity, ensuring an organization remains resilient against evolving threats

WHO SHOULD ATTENED THIS TRAINING

This comprehensive training program is designed for professionals across different levels of an organization, ranging from strategic, tactical, to operational roles.

Strategic roles, such as CISOs, Chief Risk Officers, and senior leadership, will benefit by gaining a high-level understanding of risk management, business continuity planning, and incident response frameworks. They will be equipped with the knowledge to align cybersecurity and risk management strategies with business objectives and global regulatory standards, ensuring that the organization is prepared to mitigate and respond to cyber threats in a proactive and effective manner. These individuals can use the training to shape the overall cybersecurity posture, develop policies, and advocate for resources that address long-term threats.

Tactical and operational professionals, including security analysts, incident response teams, and digital forensic experts, will gain hands-on, practical skills crucial for day-to-day operations. They will be trained to implement risk management frameworks, respond to security incidents, and execute business continuity and disaster recovery strategies. Tactical teams will learn to set up and operate Security Operations Centres (SOC), leveraging SIEM tools for real-time monitoring and threat detection. Operational staff, such as forensic investigators and malware analysts, will develop expertise in analyzing and mitigating cyber-attacks, recovering critical data, and conducting thorough forensic investigations. This broad, cross-functional training ensures

that all roles are equipped to respond to cybersecurity challenges effectively and collaboratively.

CONTENTS OF THE MODULES

MODULE 1 : RISK MANAGEMENT

Topic 1: Risk Management Methodology

1.1 Quantitative vs. Qualitative Risk Assessment

1.2 Risk Evaluation Techniques

1.3 Types of Risk Response Strategies

1.4 Countermeasures and Security Controls

1.5 Risk Register and Documentation(with real world examples of sample documents)

1.6 Practical Demonstration of Risk Management Tool

Topic 2: Third-Party Vendor and Contractor Risk Management

2.1 Vendor Risk Assessment Frameworks

2.2 Key Security Clauses in Contracts

2.3 Compliance and Auditing Third-Party Services

2.4 Managing Supply Chain Security Risks

2.5 Case Studies on Third-Party Security Incidents

Topic 3: Regulatory Compliance and Policy Adherence

3.1 Understanding Global Data Protection Laws (GDPR, HIPAA, etc.)

3.2 Implementing ISO 27001 and NIST Standards

Topic 4: Risk Mitigation and Incident Response Planning

6.1 Developing a Risk Response Plan

6.2 Implementing Preventive, Detective, and Corrective Controls

6.3 Incident Response Frameworks

6.4 Cybersecurity Incident Handling and Reporting

6.5 Lessons Learned and Continuous Improvement in Incident Management

Topic 5: Continuous Monitoring and Risk Framework Implementation

8.1 Security Information and Event Management (SIEM) Overview

8.2 Implementing Audit Logs for Security Monitoring Overview

MODULE 2 :BUSINESS CONTINUITY MANAGEMENT

Topic 1: Introduction to Business Continuity Planning (BCP)

1.1 Understanding Business Continuity and Resilience

1.2 Importance of BCP in Risk Management

1.3 Legal and Regulatory Requirements for BCP

Topic 2: Business Continuity Planning Process

2.1 Project Scope and Planning

2.2 Organizational Review and BCP Team Selection

2.3 Identifying Resource Requirements

Topic 3: Business Impact Analysis (BIA)

3.1 Identifying Business Priorities and Critical Functions

3.2 Risk Identification and Threat Assessment

3.3 Likelihood and Impact Analysis

3.4 Resource Prioritization for Business Continuity

Topic 4: Business Continuity Strategy and Development

4.1 Developing Effective Continuity Strategies

4.2 Designing Provisions and Response Processes

4.3 Implementing Recovery Solutions for Critical Operations

Topic 5: Business Continuity Plan Approval and Implementation

5.1 Gaining Management Approval and Support

5.2 Plan Implementation and Execution

5.3 Training and Education for BCP Readiness

5.4 Documentation and Continuous Improvement

MODULE 3: Understanding the Cyber Attack Lifecycle

- Overview of Cyber Attacks and the Hacker's Perspective
- Exploring the Cyber Kill Chain and Attack Strategies
- Hands-On Demonstrations: Attacks on Endpoints, Applications, Networks, and via Social Engineering
- Analyzing Recent Cyber Attacks: Case Study Discussions

MODULE 4: SECURITY OPERATION CENTRE

Topic 1: Security Operation Management

- Importance of a Security Operations Center (SOC)

- SOC Functions and Responsibilities

- SOC Processes and Workflow

- Key Components of a SOC

Topic 2: Understanding Cyber Threats, Tactics, and Attack Methodologies

- Various Cyber Threats and Their Impact
- Tactics, Techniques, and Procedures (TTPs) in Cyber Attacks
- Attacks at Network, Host, and Application Layers
- Cyber Threat Indicators of Compromise (IoCs)
- Hacking Techniques and Strategies

Topic 3: Incidents, Events, and Log Management

- Common Sources of Security Logs
- Different Types of Log Data
- Log Formats and Their Importance

Topic 4: Incident Detection Using Security Information and Event Management (SIEM)

- Importance of SIEM in Cybersecurity
- SIEM Architecture and Core Components

- Detecting Incidents Through SIEM
- Insider Threat Detection Use Cases in SIEM
- Network-Based Incident Detection Use Cases
- Host-Based Incident Detection Use Cases

Topic 5: Threat Intelligence

- Categories of Threat Intelligence
- Advantages of Threat Intelligence for SOC Analysts
- Practical Threat Intelligence Applications for SOC Analysts

MODULE 5 : INCIDENT RESPONSE AND CYBER ATTACK HANDLING

TOPIC 1: Comprehensive Incident Response Framework

1. **Understanding Incident Response (IR)**

    - Introduction to Incident Response
    - Role and Structure of Incident Response Teams (IRT)
    - Key Responsibilities of IRT Members
    - Integrating IRT within an Organization's Framework
    - Comparison: SOC vs IRT
    - The Importance of IR in Cybersecurity

2. **Incident Response Process and Phases**

    - A Detailed Overview of the Incident Response Process
    - Key Phases of Incident Response
    - The Importance of Each Phase in Effective Incident Handling
    - A Step-by-Step Approach to Managing Incidents

TOPIC 2: Incident Response Process Breakdown

1. **Step 1: Preparation for Incident Response**

    - Crafting a Strong Incident Response Mission Statement
    - Essential Components of an IR Plan
    - Key Elements of an IR Policy
    - Structure of IR Procedures and Criteria
    - Setting Up Incident Readiness Procedures
    - Establishing a Computer Forensics Lab
    - Incident Reporting and Template Guidelines
    - Evaluating and Enhancing Security Posture
    - Implementing Security Awareness and Controls
    - The Role of Cyber Insurance in IR

2. **Step 2: Incident Recording and Ticket Assignment**

    - Logging Incidents in SOC Systems
    - The Role of Ticketing Systems and Tools
    - Managing Tickets and Tracking Incidents

3. **Step 3: Incident Triage and Analysis**
    - Incident Triage Process Flow
    - Incident Validation and Classification
    - Techniques for Risk and Severity Assessment
    - Prioritizing Incidents Based on Impact
4. **Steps 4-11: Incident Handling and Post-Incident Analysis**
    - Notification, Containment, and Evidence Collection
    - Eradication and Recovery Processes
    - Post-Incident Reporting, Analysis, and Documentation
    - Closing Investigations and Incident Disclosure

TOPIC 3: Handling Specific Network Security Incidents

1. **Unauthorized Access Incidents**
    - Containment and Eradication Strategies
    - Recovery Methods Post-Incident
2. **Inappropriate Usage Incidents**
    - Containment and Mitigation Measures
    - Recovery from Unauthorized Usage
3. **DoS/DDoS Attacks**
    - Containment Strategies for DoS/DDoS Incidents
    - Eradication and Blocking of Potential Attacks
    - Recovery and Post-Incident Analysis

TOPIC 4: Addressing Application Security Incidents

1. **Application Security Breaches**

    - Containment and Mitigation Strategies
    - Tools for Effective Containment (e.g., Whitelisting, Web Proxies)
    - Eradicating Web Application Security Attacks
        - Injection, XSS, Authentication, and Session Management Attacks
        - Sensitive Data Exposure and Access Control Vulnerabilities
        - Attacks Due to Misconfigurations and Known Vulnerabilities

TOPIC 5: Responding to Email Security Incidents

1. **Containing and Eradicating Email Security Incidents**

    - Steps for Containing Email-Based Attacks
    - Tools and Techniques for Email Threat Eradication
    - Recovery After Email Security Breaches

TOPIC 6: Handling Insider Threats in an Organization

1. **Containment and Mitigation of Insider Threats**

    - Containing Insider Threats Across Various Channels
    - Role of Human Resources and Network Security in Handling Insider Threats

- Privileged User Access Controls and Physical Security Measures

2. **Recovering from Insider Threats**

    - Post-Incident Recovery Procedures
    - Best Practices for Preventing Future Insider Threats

TOPIC 7: Malware Incident Response Strategies

1. **Malware Containment Techniques**

    - Steps for Containing Malware Threats
    - Tools and Methods for Effective Malware Containment

2. **Eradicating and Recovering from Malware Incidents**

    - Techniques for Malware Eradication
    - Recovery Procedures Following Malware Incidents

TOPIC 8: Case Studies ,Future of SOC and IR with AI ,Discussion on International Standards

1. **Key Cybersecurity Incidents of 2024: Emerging Threats**

    Generative AI: Leveraging AI to Exploit Cyber Threats

    Malware-Free or Fileless Attacks

Ransomware and Its Precursor Activities

Social Engineering and Help Desk Phishing

Cloud Security Threats: Misconfigured Cloud Resources and API Abuse

Identity-Based Attacks: MFA Bypass via Push Notification Fatigue

2. **Other Use Cases (Few Scenarios)**
    - Detection of Access Outside Business Hours
    - Lateral Movement Detection
    - Detection of Suspicious PowerShell Activity from Windows

3. **Future of SOC and IR with AI**

- AI in Threat Detection and Prevention
- Automated Incident Response
- AI-Powered Threat Intelligence
- AI-Driven Security Automation
- The Role of Machine Learning in SOC and IR
- AI for Predictive Analytics in Cybersecurity
- AI and Incident Triage
- Ethical and Privacy Concerns with AI in Cybersecurity
- Human-AI Collaboration in SOC and IR
- Challenges of Implementing AI in SOC and IR

4. **Discussion on NIST Standards for Incident Response**
    - NIST SP 800-61: Computer Security Incident Handling Guide
    - NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations
    - NIST SP 800-53A: Security and Privacy Control Assessment
    - NIST SP 800-92: Guide to Computer Security Log Management

MODULE 6:DIGITAL FORENSICS

Chapter 1 Digital Forensic Investigation Methodology

1.Exploring the significance of forensic Investigations

2.Delving into the preliminary investigation phase

3.Comprehending First Response Procedure

4.Navigating the investigation phase

5.Gaining Insight into the Post-Investigation Phase

Chapter 2 Hard Drive and File System Demystified

1.Types of Disk Drives and Their Features

2.Deciphering the Logical Structure of the Disk Drive

3.Boot process in Windows,Linux and MAC OS

4.Diverse file systems in Windows,Linux and Mac OS

5.File System Anlysis with Autopsy and The Sleuth Kit Tools

6.Exploring Storage System

7.Understanding Encoding Standards and Hex Editors

Chapter 3 Data Aquisition and Duplication

1.Understanding Data Aquisition Fundamentals

2.Understand Data Aquisition Methodology

3.Prepare an Image File for Examination

Chapter 4 Defending Against Anti-Forensics Tactics

1.Anti-Forensics Techniques Overview

2.Recovering Data from deleted files and bins

3.File Carving and deleted partition recovery

4.Cracking passwords and Bypassing Security

5.Spotting Data Concealment and Obfuscation

6.Counteracting Anti-Forensic measures

Chapter 5 Windows Based Digital Investigation

1.Data Collection:Volatile and Non-Volitile

2.Windows Memory and Registry Analysis

3.Browser Data Examination

4.Windows File and Metadata Inspection

5.Understanding ShellBags,LNK Files and Logs

Chapter 6: Investigating Linux and MAC Environment

1.Introduction to Linux and MAC Forensics

2.Data Collection and Preservation

3.Memory Analysis

4.File System and Disk Imaging

5.File Recovery and deleted data

6.Web Browser Forensics

Chapter 7: Network Forensics

1.Essentials of Network Forensics

2.Fundamentals of Logging and Network Forensics Readiness

3.Event Correlation Concepts in Network Forensics

4.Identifying Indicators of Compromise(IOCs) from Network logs

5.In-Depth Network Traffic Investigation

6.Incident Detection and examination using SIEM Tools

7.Wireless Network Attack Monitoring and detection

Chapter 8: Investigating Web Attacks

1.Understand Web Application Forensics

2.Understand Internet Information Services(IIS) Logs

3.Understand ApacheWeb Server Logs

4.Understand the Functionality of Web Application Firewall(WAF)

5.Investigate Web Attacks on Windows-based Servers

6.Detect and investigate various attacks on web applications

Chapter 9:Mobile Forensics

1.Exploring Mobile Device Forensics Significance

2.Unpacking Android and iOS Device Architecture

3.Step-by-step Mobile Forensic Process

4.Analyzing Cellular Network Data

5.SIM File System and Data Retrieval Techniques

6.Device locks,rooting and Jailbreaking Insights

7.Logical Data Aquisition on Android and iOS Device

8.Physical Data Extraction on Android and iOS Device

9.Navigating Mobile Forensics Challenge

10.Crafting Effective Investigation Reports

MODULE 7:MALWARE ANALYSIS

Chapter 1 Malware Fundamentals

1.Infection vectors

2.Malware discovery

3.Introduction to various file types: Non-PE (Doc, RTF, PDF, JS, VBS, PowerShell. PDF. JAR etc.) and PE.

4.Windows internals: User mode, kernel mode. service creation, mutex,Registry entries etc.

5.Tools used for analysis (ProcMon. RegMon. WireShark etc.)

Chapter 2 Preparing the ground for Analysis

1.In-depth discussion on PE file format and ELF File Format.

2.Introduction to compilers such as Visual Basic, DotNet. C++ etc. and compilation process.

3.Introduction to Assembly language. Registers and Flags, Identifying Key Assembly code structure. understanding Program control flow.

4.Extending Assembly Knowledge to include x64 Code Analysis.

Chapter 3 Initiating the analysis

1.Setup up environment for Malware analysis.

2.Examining static Properties of Suspicious Programs using tools such as Hiew.CFF. Process Explorer, Regshot etc.

3.Performing Behavioural Analysis of Malicious Windows Executables.

4.Performing Static and Dynamic Code Analysis of Malicious Windows Executables.

5.Reverse engineering using disassemblers like Ollydbg, x32dbg etc.

Chapter 4 Digging Deep

1.Continue discussion on malware families such as Emotet. Trickbot, Virus, Worm, Ransomware etc.

2.Learn about Process injection techniques. API Hooking

3.Recognizing packed samples and understanding the unpacking techniques.

4.Using Debuggers for dumping unpacked malware from memory.

5.File-less malwares and current trends (Extortion techniques)

6.Anti-VM. Anti-debug and anti-analysis tricks used by malware and how to bypass them.

7.Handling code misdirection techniques, including SEH. VEH and TLS Callbacks.

Chapter 5 Analyzing Malicious Documents & Reverse Engineering

1.Examining malicious Microsoft Office documents including Files with Macros

2.Analyzing malicious RTF documents.

3.De-obfuscating malicious JavaScript. Visual Basic using VisualStudio debugger.

4.PDF malware analysis.

5.Reverse engineering higher level languages (Python. Java and .NET bytecode)

6.Complete end to end attack chain illustration (initial attack vector)

7.Understanding things from Threat Actors perspective (knowledge on Exploits, Vulnerabilities).