KAMARAJ®
COLLEGE OF ENGINEERING & TECHNOLOGY
(An Autonomous Institution - AFFILIATED TO ANNA UNIVERSITY, CHENNAI)
S.P.G.Chidambara Nadar - C.Nagammal Campus
S.P.G.C. Nagar, K.Vellakulam – 625 701 (Near VIRUDHUNAGAR).

IZAPY®

# Department of Computer Science and Engineering

## Industry-certified Value-Added Course

## On

## "Cyber Guardian: Mastering Threats Intelligence, Cloud Security and Access Control"

**14.07.2025 to 19.07.2025**

**Course Objectives**

CO 1 To Learn the basics of cybersecurity, types of attacks, and how to stay protected.

CO 2 To get hands-on practice in finding & testing computer and website weaknesses (VAPT)

CO 3 To learn how attackers (red team) and defenders (blue team) work in real situations.

CO 4 To understand how security teams (SOC) monitor and respond to threats using logs.

CO 5 To Learn how to break down an attack using step-by-step methods like the Cyber Kill Chain.

**UNIT I – Fundamentals of Cybersecurity and Cloud Security**

Introduction to Cybersecurity – CIA Triad – Threat Landscape Overview – Types of Attacks: Phishing, Malware, Ransomware, Insider Threats – Overview of Cloud Computing – Shared Responsibility Model – Cloud Service Models (IaaS, PaaS, SaaS) – Identity and Access Management (IAM) Concepts – Cloud Security Best Practices – Introduction to Cloud Compliance Standards: ISO 27001, NIST, CIS – Cloud Security Controls (Theory Only, No Hands-on Practice).

**UNIT II – Vulnerability Assessment and Penetration Testing (VAPT)**

Introduction to VAPT – Difference Between Vulnerability Scanning and Penetration Testing – VAPT Methodologies and Phases – Footprinting and Reconnaissance – Scanning and Enumeration – Introduction to Tools: Nmap, Nikto, Nessus – Manual Testing Techniques – OWASP Top 10: SQL Injection, XSS, CSRF, Broken Authentication, IDOR – Safe Lab Simulation and Report Writing.

## UNIT III – Red Team Concepts and Offensive Techniques

Introduction to Red Teaming – Objectives and Rules of Engagement – Attack Lifecycle: Initial Access, Privilege Escalation, Lateral Movement – Social Engineering and Phishing Attacks – Payload Creation and Delivery – Introduction to Metasploit Framework – Usage of Social-Engineer Toolkit (SET) – Basic Exploitation Demonstrations – Ethical Considerations in Offensive Security.

## UNIT IV – Blue Team Concepts and SOC Operations

Introduction to Blue Team Roles – SOC Structure and Tier Responsibilities – Alert Monitoring and Escalation Flow – Basics of Log Analysis and Event Correlation – Overview of SIEM Tools: Splunk, Wazuh – Threat Intelligence: IOCs, IOAs – Writing Detection Rules and Playbooks – Incident Response Lifecycle – Hands-on Log Investigation (Simulated Environment).

## UNIT V – Cyber Kill Chain, MITRE ATT&CK and System Threats

Introduction to Cyber Kill Chain – Seven Stages: Reconnaissance to Actions on Objectives – Real-world Attack Mapping – Introduction to MITRE ATT&CK Framework – Mapping Tactics and Techniques – Malware Behavior and Fileless Attacks – Insider Threats – Endpoint Exploits – System Hardening Practices – OS Baseline Configurations – Patch Management – Detection and Mitigation Strategies.

## Course Outcomes

After successful completion of the course, the students will be able to

| CO. No. | Course Outcome | Knowledge Level |
|---|---|---|
| CO1 | Identify the fundamental cybersecurity concepts, threat types, and the impacts of risk. | K3 - Apply |
| CO2 | Develop cloud security principles, IAM models, and compliance frameworks. | K3 - Apply |
| CO3 | Make use of cyberattacks using the Cyber Kill Chain and propose appropriate defenses. | K3 - Apply |
| CO4 | Simulate red and blue team operations to understand offensive and defensive strategies. | K3 - Apply |

| | | |
|---|---|---|
| CO5 | Apply basic vulnerability assessment and penetration testing using common tools. | K3 - Apply |

## PROGRAMME SPECIFIC OUTCOMES (PSOs):

### PSO1:

Professional Skills: The ability to understand, analyze and develop computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient design of computer-based systems of varying complexity.

### PSO2:

Problem-Solving Skills: The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.

| Course Name | CO. No. | POs | | | | | | | | | | | | PSOs | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | 1 | 2 |
| VAC – Cyber Guardian | CO1 | 1 | - | - | - | 2 | - | 2 | - | 1 | - | - | | - | 2 |
| | CO2 | 1 | 2 | 1 | - | 3 | 2 | - | - | - | - | - | | - | 2 |
| | CO3 | 1 | 2 | - | 2 | 3 | 2 | 2 | 2 | - | - | - | | 1 | - |
| | CO4 | 1 | 2 | - | - | 2 | 2 | 3 | - | - | - | 3 | | 1 | - |
| | CO5 | 1 | 2 | 2 | - | 1 | 1 | 2 | 2 | - | - | 2 | | - | 2 |

1 - low, 2 - medium, 3 - high, '- "- no correlation

| VAC | SDGs1 - low, 2 - medium, 3 - high, '-"- no correlation | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Cyber Guardian | | | | ✓ | | | | | ✓ | | | | | | | ✓ | |

| TRAINER (S) | COURSE CO-ORDINATOR(S) | VAC CO-ORDINATOR'S | HOD |
|---|---|---|---|
| Mr. C. Sai Gautam<br>Ms. J. Jana Sorupaa | Mrs. E. Vijayalakshmi – AP/CSE<br>Mrs. S. Archana Devi– AP/CSE | Mrs. S. Athilakshmi – AP/CSE<br>Mrs. S. Archana Devi – AP/CSE | Dr. A. Meenakshi<br>Professor& Head-CSE |