Faculty Name/s: **Dr. Pavithra A C**								Academic Year: **2025-26**
Department: **CSE-CYBER SECURITY**								
Course Code	Course Title	Core/Elective	Prerequisite	Teaching Hours/Week				Total Hrs/ Sessions
				L	T	P	S	
BCY456B	**Managed Detection and Resolution (MDR) in Cyber Security**	**PCC**	Cyber Security Intro	**1**	**-**	**-**	**-**	**14**

Course objectives: This course (BCY456B) will enable students to:

CLO1: Understand importance of MDR in cyber security

CLO2: Distinguish between MDR, MSSP and SIEM.

CLO3: Understand advantages of MDR.

Topics Covered as per Syllabus

MODULE-I

Introduction to Managed Detection and Resolution (MDR): Definition and importance of MDR. Advantages of using MDR in Cyber security.

MODULE-2

Introduction to MSSP and SIEM: Services offered by Managed Security Service Providers (MSSP).Limitations of using MSSP. Definition and offerings of SIEM (Security and Information Event Management). Limitations of using SIEM

MODULE - 3

Key Components of MDR solutions: Endpoint detection and response (EDR), Threat Intelligence,SOAR (Security Orchestration, Automation and Response), Expert Security Analysts.

MODULE-4

Factors to consider during selection of MDR Provider – Security compliance with industry standard security regulations like HIPAA, PCI-DSS and GDPR. Service Level Agreements (SLA), Incident response procedures, Reporting

MODULE-5

Key services provided by MDR Provider – Advanced Threat detection, Proactive threat hunting, Rapid Incident response, seamless integration with existing security tools and processes

List of Text Books
1. Managed Detection and Response (MDR), by James Sullivan and Kenneth Hess, ISBN 978-1-394-25277-0, John Wiley & Sons.

Reference Books:

1. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, by Kenneth J Knapp, ISBN 978-1-60566-326-5, Information Science Reference (an imprint of IGI Global)

Web links and Video Lectures (e-Resources): Web links and Video Lectures (e-Resources):
●https://www.youtube.com/watch?v=TqXsHBGcuDg – Sophos MDR - Threat Response Demonstration by Sophos Support

Course Outcomes: Students will be able to

CO1: Explain the need of changing Cyber Security landscape and need for MDR	**L1, L2**
CO2: Explain Managed Detection and Response solutions	**L1, L2, L3**
CO3: Illustrate the importance of proactive cyber threat hunting, detection and mitigation	**L1, L2**

Internal Assessment Marks (50): SEE paper shall be set for 50 questions, each of the 01 marks. The pattern of the question paper is MCQ (multiple choice questions). The time allotted for SEE is 01 hour. The student has to secure a minimum of 35% of the maximum marks meant for SEE.

The Correlation of Course Outcomes (CO's) and Program Outcomes (PO's)

Subject Code:	**BCY456B**	**Managed Detection and Resolution (MDR) in Cyber Security**			**Faculty Name:**		**Dr. Pavithra A C**					
List of Course Outcomes	**Program Outcomes**												**Total**
	PO1	**PO2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	
CO-1	1	1	1	-	-	1	-	-	-	-	-	1	**5**
CO-2	1	1	1	-	-	1	-	-	-	-	-	1	**5**
CO-3	1	1	1	-	-	1	-	-	-	-	-	1	**5**
Total	**3**	**3**	**3**	**0**	**0**	**0**	**0**	**3**	**0**	**0**	**0**	**3**	**15**

Note: 3 = Strong Contribution 2 = Average Contribution 1 = Weak Contribution - = No Contribution