	Introduction to Cyber Security	L	T	P	C
		3	0	0	3
Pre-requisites/Exposure	--				
Co-requisites	--				

Course Objectives

1. To covers foundation knowledge and essentials skills in all security domains.
2. To enable students to understand Security Monitoring, Cryptography and Data Analysis.

Course Outcomes

On completion of this course, the students will be able to

CO1. Describe the tactics, techniques and procedures used by cyber criminals.
CO2. Analyze Cybersecurity Threats, Vulnerabilities and Attacks.
CO3. Protecting a Cybersecurity Domain.
CO4. Learning of Cryptography and the Public Key
CO5. Describe Security Monitoring and Data Analysis

Catalog Description

The course introduces participants to the foundation knowledge and essentials skills in all security domains in the cyber world - information security, systems security, network security, mobile security, physical security, ethics and laws, related technologies, defense and mitigation techniques use in protecting businesses. Also, to investigate endpoint vulnerabilities and attacks. Analyze network intrusion data to identify compromised hosts and vulnerabilities

Course Content

Unit I : Cybersecurity: A World of Experts and Criminals

The Cybersecurity World, Cyber Criminals versus Cybersecurity Specialists, Common Threats ,Spreading Cybersecurity Threats, Creating More Experts, The Cybersecurity Cube, The Three Dimensions of the Cybersecurity Cube ,CIA Triad, States of Data, Cybersecurity Countermeasures, IT Security Management Framework.

Unit II : Cybersecurity Threats, Vulnerabilities and Attacks

Malware and Malicious Code , Deception , Attacks , Cryptography, Access Controls , Obscuring Data , Types of Data Integrity , Controls , Digital Signatures , Certificates , Database Integrity Enforcement.

Unit III : Protecting a Cybersecurity Domain
Defending Systems and Devices, Server Hardening, Network Hardening, Physical and Environmental Security, High Availability, Measures to Improve Availability, Incident Response, Disaster Recovery, Cybersecurity Domains.

Unit IV : Cryptography and the Public Key
Infrastructure, Network security monitoring, Cryptography, Tools to encrypt and decrypt data, Public Key Cryptography, Public key infrastructure (PKI), Endpoint Protection, Endpoint Vulnerability.

Unit V : Security Monitoring and Data Analysis
Technologies and Protocols, Log Files, Security monitoring, Intrusion Data Analysis, compromised hosts, Vulnerabilities, Data Collection Security-related data, Data Preparation, Arrange a variety of log files , Data Analysis.

Modes of Evaluation: Quiz/Assignment/ presentation/ extempore/ Written Examination
Examination Scheme:

Components	**Internal**	**Mid Term**	**ESE**	**Total**
Weightage (%)	**30%**	**20%**	**50%**	**100%**

Relationship between the Program Outcomes (POs), Program Specific Outcomes and Course Outcomes (COs)

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PSO1	PSO2
CO1												
CO2												
CO3												
CO4												
Average												

1. WEAK 2. MODERATE 3. STRONG