

|                              |                                               |
|------------------------------|-----------------------------------------------|
| <b>Branch Name:</b>          | CYBER SECURITY                                |
| <b>Program Code:</b>         | ET207                                         |
| <b>Course Title:</b>         | Incident Response and Threat Intelligence     |
| <b>Course Code:</b>          | 2ET2070105T                                   |
| <b>Pre-requisite Course:</b> | Basic fundamental knowledge of cyber security |

**Course Objectives:** After successful completion of the course, student will be able to

1. To learn how to define an incident relating to cyber security.
2. To learn protocols for first on crime scene investigations.
3. Obtain basic knowledge on dealing with system security related incidents.
4. To learn basic fundamentals of cyber threat intelligence.
5. To demonstrate how cyber has changed the nature of intelligence collection.

**Teaching and Examination Scheme:**

| Credit | Teaching Scheme<br>Hours per week |   |   |       | Evaluation Scheme (Marks) |      |      |      |                   |      |      |      | Total (Marks) |
|--------|-----------------------------------|---|---|-------|---------------------------|------|------|------|-------------------|------|------|------|---------------|
|        |                                   |   |   |       | Theory (Marks)            |      |      |      | Practical (Marks) |      |      |      |               |
|        | L                                 | T | P | Total | SEE                       |      | CCA  |      | SEE               |      | CCA  |      |               |
|        |                                   |   |   |       | Min.                      | Max. | Min. | Max. | Min.              | Max. | Min. | Max. |               |
| 3      | 3                                 | - | - | 3     | 24                        | 60   | 16   | 40   | -                 | -    | -    | -    | 100           |

**Course Contents:**

| Unit No | Topics                                                                                                                                                                                                                                                                                                                                                       | Total Hours | Weight age (%) |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------|
| 1       | Cyber Incident Statistics, Computer Security Incident, Information as Business Asset, Data Classification, Information Warfare, Key Concepts of Information Security, Vulnerability, Threat and Attacks, Types of Computer Security Incidents, Examples of Incidents, Incidents Categorization, Low Level Incident, Mid Level Incident, High Level Incident. | 09          | 20             |
| 2       | Incident Prioritization, Incident Response, Incident Handling, Disaster Recovery, Technologies and Impacts, Virtualization and Impacts, Estimated Cost of an Incident, Incident Reporting Organizations, Vulnerability Reports, Incident Identification, Need for Incidents Response, Goals for Incident Response.                                           | 09          | 20             |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |    |    |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| 3 | Incident Response and Handling Process; Step 1: Identification; Step 2: Incident Recording; Step 3: Initial Response; Step 4: Communicating the Incident; Step 5: Containment; Step 6: Formulating a Response Strategy; Step 7: Incident Classification; Step 8: Incident Investigation; Step 9: Data Collection; Step 10: Forensic Analysis, Step 11: Evidence Protection; Step 12: Notify External Agencies; Step 13: Eradication; Step 14: System Recovery; Step 15: Incident Documentation; Step 16: Incident Damage and Cause assessment; Step 17: Review and Update the Response Policies. | 09 | 20 |
| 4 | Defining Cyber Threat Intelligence: The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor-and-respond strategy, Why the strategy is failing, Cyber Threat Intelligence Defined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence.                                                                                                                                                                                                                                   | 09 | 20 |
| 5 | Developing Cyber Threat Intelligence Requirements: Assets That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hacktivists. Intelligence Consumers: Tactical users, Operational users, Strategic users.                                                                                                                                                                                                   | 09 | 20 |

#### **Text Books:**

1. Luttgens Jason, Pepe Matthew, and Mandia Kevin, 2014, —Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, ISBN: 978-0071798686.
2. Friedman, J., & Bouchard, M. (2015). Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. CyberEdge Group.
3. Friedman, J., & Bouchard, M. (2015). Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. CyberEdge Group.

#### **Reference Books:**

1. Murdoch Don, 2016, —Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, CreateSpace Independent Publishing Platform, 2.2 Edition, ISBN: 978-1500734756
2. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge University Press.
3. Gourley Bob, 2014, —The Cyber Threat, Create space Independent Pub.

#### **Course Learning Outcomes (CLO):**

| Course Outcomes | Description | Bloom's Taxonomy Level |
|-----------------|-------------|------------------------|
|-----------------|-------------|------------------------|

|       |                                                                                                                                                              |                                   |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| COL 1 | Obtain basic knowledge <sup>1</sup> on dealing with system security related .                                                                                | Understanding (2)<br>Applying (3) |
| COL 2 | Increase knowledge <sup>1</sup> on potential defences and counter measures against common threat vectors/vulnerabilities.                                    | Applying (3)                      |
| COL 3 | Gain experience using tools and common processes in performing analysis <sup>4</sup> of compromised systems and dynamic malware analysis.                    | Applying (3)                      |
| COL 4 | Examine <sup>3</sup> the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection. | Applying (3)                      |
| COL 5 | Examine <sup>3</sup> the intelligence challenge of attribution in cyber-attacks.                                                                             | Applying (3)                      |

### Mapping of CLO with PO and PSO

| Course Learning Outcomes | Program Outcomes (POs) |      |      |      |      |      |      |      |      |       |       |       | Program Specific Outcomes(PSOs) |       |       |       |
|--------------------------|------------------------|------|------|------|------|------|------|------|------|-------|-------|-------|---------------------------------|-------|-------|-------|
|                          | PO 1                   | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 | PO 11 | PO 12 | PS O1                           | PS O2 | PS O3 | PS O4 |
| CLO1                     | H                      | M    | M    |      | M    |      |      |      |      |       |       |       |                                 |       |       |       |
| CLO2                     | H                      | M    |      |      | M    |      |      |      |      |       |       | L     |                                 |       |       |       |
| CLO3                     | H                      | M    | M    |      | M    |      |      |      |      |       |       |       |                                 |       |       |       |
| CLO4                     | M                      | M    | M    |      | M    |      |      |      |      |       |       | L     |                                 |       |       |       |
| CLO5                     | M                      | M    |      |      |      |      |      |      |      |       |       | L     |                                 |       |       |       |

**H: High, M: Medium, L: Low**