

Course Title	Incident Response and Forensic Analysis				
Course Code	CYS635				
Course Type	Optional				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	1 <sup>st</sup> or 2 <sup>nd</sup> Year / 2 <sup>nd</sup> or 3 <sup>rd</sup> Semester				
Teacher's Name	TBA				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	<p>The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyze and respond to. The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Detecting these incidents therefore requires additional skills such as forensics, malware analysis and threat detection which help decipher how this threats operate and therefore how they can be prevented and mitigated. Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Define and describe the main phases of incident response</li> <li>• Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident</li> <li>• Identify different kinds of attacks methods to counter their effects</li> <li>• Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up</li> <li>• Explain the principles of evidence collection and the chain of custody</li> <li>• Identify and evaluate key forensic analysis techniques</li> <li>• Describe the application of such techniques to real situations and the connection with incident response</li> </ul>				

	<ul style="list-style-type: none"> <li>Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection.</li> </ul>		
Prerequisites	None	Co-requisites	None
Course Content	<p><u>Introduction:</u> Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles.</p> <p><u>Preparation:</u> Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates.</p> <p><u>Identification:</u> Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC).</p> <p><u>Containment:</u> Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation.</p> <p><u>Eradication:</u> Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully.</p> <p><u>Recovery:</u> Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process.</p> <p><u>Follow-up:</u> Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement.</p> <p><u>Digital Forensics Investigation Process:</u> Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures.</p>		

	<p><u>Technical forensics tools and techniques:</u> Hard disks, removable media and file systems, Windows forensics, duplication/imaging of forensic data, recovering deleted files and hidden or deleted partitions, steganography and image forensics, log analysis, password crackers, network device forensics, packet capture analysis, email tracking, mobile forensics, investigation of attacks, common tools (Encase, FTK, etc.)</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry, including law enforcement. Discussion normally focuses on the practicalities and challenges of incident response and the ways in which forensic analysis contributes to successful cybercrime prosecutions.</p>						
Teaching Methodology	Face – to – face						
Bibliography	<p><i>“Incident Response &amp; Computer Forensics, Third Edition”</i> by Jason T. Luttgens and Matthew Pepe</p> <p><i>“Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder”</i>, by Don Murdoch</p> <p><i>“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”</i>, by Leighton Johnson</p> <p><i>“The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics”</i>, by John Sammons</p> <p><i>“Digital Forensics with Open Source Tools”</i>, by Cory Altheide and Harlan Carvey</p> <p><i>“Digital Forensics Processing and Procedures”</i>, by David Lilburn Watson and Andrew Jones</p> <p>IEEE Journals and Magazines</p>						
Assessment	<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 5px;">Examinations</td> <td style="text-align: center; padding: 5px;">60%</td> </tr> <tr> <td style="padding: 5px;">Assignment(s)</td> <td style="text-align: center; padding: 5px;">40%</td> </tr> <tr> <td style="padding: 5px;"></td> <td style="text-align: center; padding: 5px;">100%</td> </tr> </table>	Examinations	60%	Assignment(s)	40%		100%
Examinations	60%						
Assignment(s)	40%						
	100%						
Language	English						