SYLLABUS

1. Information regarding the programme

1.1 Higher education institution	**Babeş-Bolyai University**
1.2 Faculty	**Faculty of Mathematics and Computer Science**
1.3 Department	**Department of Computer Science**
1.4 Field of study	**Computer Science**
1.5 Study cycle	**Master**
1.6 Study programme / Qualification	**Distributed Systems in Internet**

2. Information regarding the discipline

2.1 Name of the discipline (en) / (ro)			**Extended Detection and Response /** **Detecție extinsă și răspuns la incidentele de securitate**				
2.2 Course coordinator			**Ionuț-Marcel Breta**				
2.3 Seminar coordinator			**Ionuț-Marcel Breta**				
2.4. Year of study	**1**	2.5 Semester	**1**	2.6. Type of evaluation	**VP**	2.7 Type of discipline	Facultative
2.8 Code of the discipline		MME8208					

3. Total estimated time (hours/semester of didactic activities)

3.1 Hours per week	4	Of which: 3.2 course	2	3.3 seminar/laboratory	1 lab + 1 project
3.4 Total hours in the curriculum	56	Of which: 3.5 course	28	3.6 seminar/laboratory	28
Time allotment:					hours
Learning using manual, course support, bibliography, course notes					10
Additional documentation (in libraries, on electronic platforms, field documentation)					24
Preparation for seminars/labs, homework, papers, portfolios, and essays					20
Tutorship					5
Evaluations					10
Other activities:					

3.7 Total individual study hours	69
3.8 Total hours per semester	125
3.9 Number of ECTS credits	5

4. Prerequisites (if necessary)

4.1. Curriculum	• Web mechanics - https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics • HTTP - https://developer.mozilla.org/en-US/docs/Web/HTTP • HTML - https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/HTML_basics • CSS - https://developer.mozilla.org/en-US/docs/Web/CSS • JavaScript - https://developer.mozilla.org/en-

	US/docs/Web/JavaScript • REST APIs - https://www.codecademy.com/article/what-is-rest • Node.js - https://nodejs.dev/en/learn/ OR PHP - https://www.php.net/ OR any other server-side language • MongoDB - https://www.mongodb.com/docs/manual/ OR any other non-relational DB
4.2. Competencies	• Networking basics and HTTP • Web development basics • APIs basics (usage) • Database knowledge

5. Conditions (if necessary)

5.1. For the course	• N/A
5.2. For the seminar /lab activities	• Office 365 Developer account

6. Specific competencies acquired

Professional competencies	• Basic cybersecurity and XDR knowledge • Enhanced network applications development knowledge and techniques
Transversal competencies	• Teamwork

7. Objectives of the discipline (outcome of the acquired competencies)

7.1 General objective of the discipline	• Understanding basic cybersecurity and XDR knowledge • Enhancing network applications development knowledge and techniques
7.2 Specific objective of the discipline	• Implement and deliver a simple XDR platform with a web interface

8. Content

8.1 Course	Teaching methods	Remarks
1. Introduction to cybersecurity	Presentation & open discussion	
2. Need for Extended detections & how XDR works	Presentation & open discussion	
3. Managing collectors	Presentation & open discussion	
4. Gathering data from collectors – from on-premise services	Presentation & open discussion	
5. Gathering data from collectors – from cloud services	Presentation & open discussion	
6. Storing data from collectors	Presentation & open discussion	
7. Incidents – introduction	Presentation & open discussion	

8. Detecting incidents – based on attack scenarios	Presentation & open discussion	
9. Detecting incidents – based on anomalies	Presentation & open discussion	
10. Detecting incidents – correlating events	Presentation & open discussion	
11. Displaying incidents	Presentation & open discussion	
12. Generating recommended actions	Presentation & open discussion	
13. Executing recommended actions	Presentation & open discussion	
14. Project presentation and review	Evaluation	To be coupled with the 7th seminar (Project presentation and review)
Bibliography • From Silos to Symphony: XDR and the New Age of Cyber Resilience, https://businessresources.bitdefender.com/ebook-from-silos-to-symphony-xdr-and-the-new-age-of-cyber-resilience • The Essential Guide to XDR, https://www.paloaltonetworks.com/resources/ebooks/cortex-ebook_the-essential-guide-to-xdr • Extended Detection and Response (XDR) For Dummies, https://www.cisco.com/c/en/us/products/security/xdr/xdr-for-dummies.html • What is extended detection and response (XDR)? https://www.ibm.com/topics/xdr		
8.2 Seminar / laboratory	Teaching methods	Remarks
1. Prepare a base for the application	• Expose problem • Discuss solutions • Present example	
2. Manage credentials for sensor	• Expose problem • Discuss solutions • Present example	
3. Retrieve and store data for sensor	• Expose problem • Discuss solutions • Present example	
4. Detect incidents out of stored data	• Expose problem • Discuss solutions • Present example	
5. Display incidents	• Expose problem • Discuss solutions • Present example	
6. Generate recommended actions	• Expose problem • Discuss solutions • Present example	
7. Project presentation and review	• Expose problem • Discuss solutions • Present example	
Bibliography • Office 365 APIs, https://learn.microsoft.com/en-us/previous-versions/office/office-365-api		

9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

- Bitdefender
- Palo Alto
- Cisco
- IBM
- CrowdStrike
- Microsoft
- Trend Micro
- VMware

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Share in the grade (%)
10.4 Course			0%
10.5 Seminar/lab activities	• Implement a simple XDR platform	• Project review	100%
10.6 Minimum performance standards			
For the project to be graded with 5: ○ Implement one data collector ○ Ability to detect at least one incident type ○ Ability to display incidents			

Date ....

Signature of course coordinator ....

Signature of seminar coordinator ....

Date of approval ....

Signature of the head of department ....…............................