Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025	
Date: 27-10-2025	**Time:** 11.00am to 12.30pm

School: SOCSE/SOE	**Program:** B.Tech	
Course Code: CCS3411	**Course Name:** Security Information and Event Management (SIEM)	
Semester: VII	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**26**	**24**			

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **5Q x 2M=10M**

1	What do you mean by Misconfigurations and how can you prevent it?	**2 Marks**	**L1**	**CO1**
2	What is Homegrown SIEM?	**2 Marks**	**L1**	**CO2**
3	What do you mean by event correlation engine.	**2 Marks**	**L1**	**CO2**
4	What is Tactical threat intelligence.	**2 Marks**	**L1**	**CO1**
5	What is HIPPA and FISMA act.	**2 Marks**	**L1**	**CO1**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Explain event correlation in detail with techniques and examples.	**10 Marks**	**L2**	**CO 2**
		Or			
7.	**a.**	Discuss Commercial SIEM tools for SMEs with the selection criteria.	**10 Marks**	**L2**	**CO 2**

8.	**a.**	Explain CIA with industrial examples and its importance.	**10 Marks**	**L2**	**CO 1**
		Or			
9.	**a.**	Explain threat intelligence with its various types, sources and benefits in SIEM.	**10 Marks**	**L2**	**CO 1**

10.	**a.**	Explain various types of Threats in detail with its sub-types.	**10 Marks**	**L2**	**CO 1**
		Or			
11.	**a.**	Explain various types of Attacks in SIEM with examples.	**10 Marks**	**L2**	**CO 1**

12.	**a.**	What do you mean by log management and explain the types of logging solution with tools as examples.	**10 Marks**	**L2**	**CO 2**
		Or			
13.	**a.**	What is SIEM and how it is used in SME with its major components.	**10 Marks**	**L2**	**CO 2**