Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 05/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CCS3411 **Course Name:** Security Information and Event Management (SIEM)

Semester: Sevent Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	46	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Describe the need for Security Information and Event Management (SIEM) in modern IT systems.	2	CO1	BT2
2	Differentiate between internal and external threats to an IT system.	2	CO1	BT2
3	Summarize the role of threat intelligence in identifying and understanding security threats.	2	CO1	BT2
4	Differentiate between a Homegrown SIEM and a Commercial SIEM solution.	2	CO2	BT2
5	Summarize the role of log correlation in a SIEM system.	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Describe the architecture of a typical SIEM system and explain the functions of its major components in collecting, processing, and monitoring security events.	10	CO1	BT2
7	Illustrate the role of logs and event management in SIEM. Describe how security events are collected, analyzed, and used for identifying suspicious activities.	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Describe the major components of a SIEM system and illustrate the flow of security information from source devices to incident detection.	10	CO2	BT2
9	Summarize the concept of Homegrown SIEM and describe its major components and implementation considerations for an organization.	10	CO2	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Classify the major types of threats and vulnerabilities in IT systems, including misconfiguration, user mistakes, malicious content, internal threats, and external threats, with suitable examples.	10	CO1	BT2
11	Summarize the importance of the CIA triad and explain how SIEM supports security monitoring and regulatory compliance in IT systems.	10	CO1	BT2

PART E: Answer Any 1 Following Questions. 10 M

PTO (Please Turn Over)

Q.N.	Questions	M	CO	BT
12	Illustrate the role of SIEM in incident response and describe the major steps involved in handling a security incident.	10	CO2	BT2
13	Explain how SIEM can support regulatory compliance and Business Intelligence (BI) in an organization.	10	CO2	BT2