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	SIEM is used to collect, monitor, and correlate security events and logs from different IT systems. It helps organizations identify suspicious activities, detect security incidents, and support timely response to threats.	2	CO1	BT2
2	Originate from within the organization.May involve employees or authorized users..Example: misuse of access privileges. Originate from outside the organization..May involve attackers or malicious external entities..Example: phishing or external network attack..	2	CO1	BT2
3	Threat intelligence provides information about known threats, attackers, malicious activities, and indicators of compromise. It helps security teams understand potential threats and improve threat detection and response.	2	CO1	BT2
4	Homegrown SIEM Developed and customized by the organization.Offers greater customization.Requires internal resources for maintenance Developed and provided by a security vendor..Provides ready-made features and vendor support.Usually includes professional support and updates.	2	CO2	BT2
5	Log correlation combines and compares related events from different sources to identify meaningful security patterns. It helps SIEM detect suspicious activities that may not be visible from a single log.	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	SIEM architecture consists of several components that work together to monitor and manage security events. Major components: Data Sources: Firewalls, servers, applications, endpoints, and network devices generate security logs and events.Log Collection: Collectors or agents gather logs from different sources.Log Management: The collected logs are stored and organized for further processing.Event Processing: SIEM processes and normalizes events received from different systems.Event Correlation: Related events are correlated to identify suspicious patterns.Threat Detection: Rules and security information are used to detect possible security incidents.Monitoring and Alerts: Security teams receive alerts when suspicious activities are detected.Reporting: SIEM generates reports and dashboards for monitoring, investigation, and compliance.Basic flow: Data Sources → Log Collection → Processing & Correlation → Threat Detection → Alerts & Reporting Thus, SIEM provides centralized security monitoring of an organization's IT environment.	10	CO1	BT2

ANSWER KEY

PTO (Please Turn Over)

7	Logs are records generated by IT systems that contain information about activities and events. Event management involves collecting and processing these events to identify security-related activities. Process: Event Generation: Servers, firewalls, applications, and endpoints generate logs.Collection: SIEM collects logs from different sources.Centralized Storage: Logs are stored in a common SIEM platform.Normalization: Logs from different formats are converted into a common format.Event Correlation: Related events are combined to identify meaningful patterns.Analysis: SIEM checks events against predefined rules and security conditions.Alert Generation: Suspicious activities generate alerts for security teams.Investigation: Security personnel use the collected logs to understand the incident.For example, multiple failed login attempts followed by a successful login may indicate suspicious activity.	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
8	A SIEM system consists of several components that work together to collect, process, store, and analyze security information. Major components: Source Devices: Servers, firewalls, routers, applications, and endpoints generate logs.Log Collection: Logs are collected from different source devices.Parsing and Normalization: Logs from different formats are converted into a common format.Rule Engine: Applies predefined rules to identify specific security conditions.Correlation Engine: Combines related events to identify suspicious patterns.Log Storage: Stores collected logs for investigation and future reference.Alerting: Generates alerts when suspicious activities are detected.Incident Response: Helps security teams investigate and respond to detected incidents.Basic flow: Source Devices → Log Collection → Parsing/Normalization → Rule & Correlation Engine → Storage/Alerts → Incident Response	10	CO2	BT2
9	A Homegrown SIEM is a security monitoring solution developed by an organization using its own tools, scripts, and infrastructure instead of depending completely on a commercial SIEM product. Major components include: Log Collectors: Collect logs from servers, applications, and network devices.Log Storage: Stores security events for monitoring and investigation.Parsing/Normalization: Converts different log formats into a common structure.Correlation: Identifies relationships between events.Rule Engine: Detects predefined security conditions.Alerting: Notifies security personnel about suspicious activities.Dashboard/Reporting: Displays security information and generates reports.Implementation considerations: Availability of skilled technical staff.Storage and processing requirements.Development and maintenance effort.Scalability of the solution.Security requirements of the organization.A Homegrown SIEM provides flexibility and customization, but it requires continuous development and maintenance.	10	CO2	BT2

PART D: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
10	hreats and vulnerabilities can occur due to technical weaknesses, human mistakes, or malicious activities. TypeDescriptionExampleMisconfigurationIncorrect security settings that create weaknesses.Open network ports or weak access permissions.User MistakesUnintentional actions by users that affect security.Clicking a suspicious link or using a weak password.Malicious ContentHarmful software or content intended to damage or compromise systems.Malware, ransomware, or malicious attachments.Internal ThreatsThreats originating from authorized users within an organization.Employee misusing confidential information.External ThreatsThreats originating outside the organization.Phishing, network attacks, or unauthorized access attempts.These threats can lead to data loss, unauthorized access, service disruption, and financial or operational damage. Proper security controls, user awareness, monitoring, and SIEM can help in detecting and managing such threats.	10	CO1	BT2

ANSWER KEY

11	The CIA triad represents three basic objectives of information security: Confidentiality: Ensures that information is accessible only to authorized users.Integrity: Ensures that information remains accurate and is not modified without authorization.Availability: Ensures that systems and information are available to authorized users when required.Role of SIEM SIEM continuously monitors security events from different IT systems.It helps detect unauthorized access and activities affecting confidentiality.Log monitoring can help identify unauthorized changes affecting integrity.Monitoring system failures and unusual activities supports availability.SIEM maintains and organizes security logs that can be useful for audits.It can generate reports required for security monitoring and regulatory compliance.Alerts help security teams respond to incidents in a timely manner.Thus, the CIA triad provides fundamental security objectives, while SIEM supports organizations in monitoring, detecting, investigating, and documenting security-related activities.	10	CO1	BT2

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	ncident Response (IR) is the process of identifying, handling, and recovering from security incidents. SIEM supports IR by providing centralized logs, alerts, and security information. Major steps: Preparation: Establish security policies, tools, and response procedures.Detection: SIEM identifies suspicious events and generates alerts.Analysis: Security teams examine related logs and events to understand the incident.Containment: Steps are taken to limit the impact of the incident.Eradication: The cause of the incident is identified and removed.Recovery: Affected systems are restored to normal operation.Review: The incident is documented and lessons are used to improve future security.Role of SIEM: Logs → Event Correlation → Alert → Investigation → Incident Response Thus, SIEM helps security teams detect incidents quickly and provides useful information throughout the response process.	10	CO2	BT2
13	SIEM can support both regulatory compliance and Business Intelligence by collecting and analyzing security-related information from different IT systems. SIEM and Regulatory Compliance: Collects and stores security logs.Provides centralized monitoring of system activities.Helps maintain records required for security audits.Generates reports related to security events and user activities.Helps identify activities that may violate security policies.SIEM and Business Intelligence: Collects security data from multiple sources.Organizes the data for analysis.Uses dashboards and reports to present security information.Helps identify trends and recurring security events.Provides information that can support security and risk-related decisions.Basic flow: Security Data → SIEM Collection → Processing & Analysis → Reports/Dashboards → Security Insights Thus, SIEM converts security data into useful information for compliance monitoring, reporting, and organizational security management.	10	CO2	BT2

ANSWER KEY