GANPAT UNIVERSITY									
FACULTY OF ENGINEERING & TECHNOLOGY									
Programme	Bachelor of Technology					Branch/Spec.	Computer Science & Engineering (CS)		
Semester	VII					Version	1.0.0.0		
Effective from Academic Year	2021-22					Effective for the batch Admitted in	June 2018		
Subject code	2CSE708		Subject Name			SECURITY INCIDENT & EVENT MANAGEMENT			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	2	0	5	Theory	40	60	100
Hours	3	0	4	0	7	Practical	60	40	100

Pre-requisites:

SQL, Linux Commands, Data protection and IT Security Fundamentals

Learning Outcomes:

After Successful completion of the course, students will be able to:

- Identify and recognize potential known and unknown threats
- Monitor and analyse the activities of authorised users and review their privileged access to various resources
- Demonstrate and extrapolate understanding and working of SIEM
- Implement secure and non vulnerable SIEM

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Security Intelligence & Event Management** Security technologies implemented in the IT Industry, SIEM Evolution, Introduction to SIEM, SIEM Architecture and its components, General Security Practices, Correlation - Brute Force Detection, DDos Attack, File Copying, File Integrity Change	8
2	**Security Operations Center and Network Security Monitoring** What is SOC, SOC Components, Awareness of assets, aggregation and correlation, Log Collection, Monitoring & Reporting, Threat Intelligence, Alerts, Defence and Compliance, Introduction to Firewall, Switches, IPS & Directories, Collection, Detection and Analysis, Security Policies, Topologies	8
3	**Investigating the Events of an Offence, Using Asset Profiles to investigate Offences & Investigating offences triggered by Flows** Events, Asset Profiles, Flows and Investigating Offences	7
4	**Using Rules and Using the Network Hierarchy** Navigate rules and rule groups, Locate the rules that fired for an event or flow, and triggered an offense, Investigate which test conditions caused a rule to fire, Investigate building blocks and function tests, Examine rule actions and responses, examine for which indicators anomaly detection rules can fire, Locate and explain the structure of the Network Hierarchy, Use networks in investigations, Use Flow Bias and Direction in investigations	11

5	**Index and Aggregated Data Management, Dashboards and Reports** Index Management administration, Aggregated Data Management, Navigate the Dashboard tab, Customise dashboard items, Generating reports , Applying filters	**11**

Practical content
Practical contents will be based on following concepts: QRadar SIEM user interface, Investigating the local DNS scanner offence,events that contribute to an offence, offence that is triggered by flows, rules exercise, Network Hierarchy exercise, Index and Aggregated Data Management exercise, Using Dashboards exercises, Creating reports exercises

Text Books	
1	IBM Security QRadar SIEM by Gerardus Blokdyk

Reference Books	
1	QRadar A Complete Guide by Gerardus Blokdyk
2	Security Information and Event Management by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Course Outcomes:	
COs	Description
CO1	Identify and recognize potential known and unknown threats
CO2	Monitor and analyse the activities of authorised users and review their privileged access to various resources
CO3	Demonstrate and extrapolate understanding and working of SIEM
CO4	Implement secure and non vulnerable SIEM

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	0	1	1	0	1	1	1	1	2	1
CO2	3	2	0	1	1	1	2	2	1	1	2	1
CO3	3	3	3	3	3	2	3	3	2	1	2	2
CO4	2	1	1	3	1	1	2	2	1	0	1	1