SILVER OAK UNIVERSITY

Silver Oak College of Computer Application

Master of Science Cyber Security & Digital Forensics

Course Name: Security Monitoring

Course Code: 1040147201

Semester: 3rd

Prerequisite: Network security and working sensors, Fundamentals of IPS and IDS, Understanding of Snort and Suricata, Log analysis for Firewalls

Course Objective: The Security Monitoring is part of Security Operation Center where a process is set to detect, analyze, and respond to cybersecurity incidents using a combination of technology and tools and a strong set of processes.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	1	0	4	4

Contents:

Unit No.	Course Contents	Teaching Hours	% Weightage
1	**Security Monitoring fundamentals:** What is Security Operations, Finding the sweet spot, Security and Control, Security Goals, Reliability vs Security, Typical Security Flaws, Basics of SOC infrastructure	8	20
2	**Log management:** Computer Security, Log Management, Log Management Infrastructure, Log Management Planning, Log Management Operational Process	8	20
3	**Security Information & Event Management:** Introduction to SIEM, SIEM Architecture, Logs and Events, Understanding logs, Various formats, Log Baselining, Aggregation and normalization, Event Collection and Event Correlation, Correlation Rules	12	28
4	**Incident Response Plan :** Purpose of Incident Response Plan, Requirements of Incident, Response Plan Preparation, Incident Recording, Initial Response, Communicating the Incident, Incident Documentation, Incident Damage and Cost Assessment, Review and Update the Response Policies	7	16

5	**Log Management and Analysis** Importance of Log Management, Centralized log collection and management.Compliance and regulatory requirements for log retention.Log Analysis Techniques, Automated log analysis and correlation.Using log data for threat hunting and forensic analysis. Advanced Monitoring Techniques, User and Entity Behavior Analytics (UEBA).	7	16

Course Outcomes:

Sr. No.	CO Statement	Unit No
CO-1	Define security operations, delineate the relationship between security and control, and articulate security goals, distinguishing between reliability and security.	1
CO-2	Implement log management infrastructure by understanding its components, planning, and operational processes.	2
CO-3	Utilize SIEM tools for event collection, correlation, and rule creation, enhancing the ability to detect and respond to security incidents.	3
CO-4	Assess incident damage and cost, evaluate response strategies.	4
CO-5	Apply centralized log collection techniques to enhance operational efficiency and accelerate incident response.	5

Teaching & Learning Methodology:

1. The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
2. Lectures with live practical example using Projector and Computer
3. Experiments shall be performed in the laboratory related to course contents

List of Tutorials: **Total Hours: 14**

Sr. No.	Tutorial Name
1.	Perform Installation deployment of SIEM systems like Qradar, Splunk, Arcsight.
2.	Perform operations to collect logs at a centralized location using a logger.
3.	Perform operations with smart connectors to manage IT assets.
4.	Perform security operations/investigations on different types of security events.
5.	Perform threat hunting using Splunk.
6.	Perform vulnerability management using SIEM.
7.	Perform orchestration of common security related events and investigations.
8.	Perform incidence recovery for threat mitigation using SIEM.

Major Equipment:

1. Computer System
2. LAN cable

Books Recommended:

1. Caroline Wong, **"**Security Metrics, A Beginner's Guide"
2. N. K. McCarthy, Matthew Tod, Jeff , Klaben, "The Computer Incident Response Planning Handbook"
3. Richard Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response"
4. Corey Schou, Steven Hernandez, "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"

CO-PO-PSO MATRIX:

Co. No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	2	3	2	2				1	2
CO-2	1	2	1	1	2			2	2
CO-3	2	1	2	2				2	3
CO-4	3	2	1	1				3	3
CO-5	1	2	2	2				2	2