INT244:SECURING COMPUTING SYSTEMS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: understand the fundamentals of security operations, incident response, and threat intelligence.

CO2 :: explain log analysis, network traffic analysis, and techniques for detecting security threats.

CO3 :: apply endpoint threat detection for, malware footprinting, and security monitoring.

CO4 :: demonstrate incident response automation to enable security, orchestration.

CO5 :: analyze security events to monitor cloud security incidents, compliance requirements, and regulatory reporting.

CO6 :: explore advanced threat hunting, SOAR, zero-trust security, and emerging SOC technologies.

Unit I

Introduction to SOC : overview of SOC, importance of SOC, challenges in SOC, role and responsibilities, models

SOC Pillars : introduction, definition of SOC pillars, importance of SOC pillars, levels of SOC analysis, prioritization and analysis, remediation and recovery, assessment and audit, threat intelligence

Security Incident Response : incident response lifecycle, handling and investigation technique, post incident analysis, information sharing is incident response, communication strategies, incident response in IT environment

Unit II

Log and Event Analysis : role of log and event analysis, advance log analysis techniques, detecting anomalies, integrating log analysis, enhancing log data security, reconstructing the attack chain, APIs for advanced threat detection, cross-platform log analysis, sporting cloud crypto jacking, integration of log analysis, evaluating log analysis

Network Traffic Analysis : traffic segmentation and normalization, threat intelligence integration, contextual protocol analysis, NIDS/NIPS, vulnerability validation, analyzing jarring signals, modelling protocol behavior

Unit III

End Point Analysis and Threat Hunting : end point detection and response, malware analysis and reverse engineering, data and asset-focused risk models, principles of endpoint security

Security Information and Event Management : fundamentals of SIEM, distributed processing, accelerated threat hunting, regulatory reporting with SIEM, infrastructure management, SIEM log retention strategies, automated response and remediation, threat hunting with SIEM, operational requirements

Security Analytics and Machine Learning in SOC : behavioral analytics and UEBA, ML-based security analytics, deployment of predictive models, anomaly detection in SOC

Unit IV

Incident Response Automation and Orchestration : introduction, evaluating the impact of automation in SOCs, the role of playbooks, threat-specific versus generic playbooks, gathering and application, collection from diverse sources, measuring the efficiency and effectiveness, improving SOC performance

SOC Metrics and Performance Measurement : advancing cyber resilience with insights, performance measurement, anomaly detection, metrics for evaluating incident response, skills investment gap assessment, financial metrics for evaluating, AI/ML, future trends in SOC metrics, core areas for SOC metrics

Unit V

Compliance and Regulatory Considerations in SOC : introduction, regulatory challenges across geographies, healthcare data breaches, financial services data security, energy and utility incident response, continuous incident readiness assessments, the role of SIEM in achieving

Cloud Security and SOC Operations : introduction, CASBs, container sandboxing, compliance validation and drift detection, data and key management for encryption, securing multicloud and hybrid cloud environments, the role of APIs in cloud security and SOC operations

Unit VI

Threat Intelligence and Advanced Threat Hunting : introduction, advanced threat-hunting methodologies, lifecycle intelligence for automated response, techniques for effective threat hunting in the cloud, behavioral analytics for detecting insider threats

Emerging Trends and the Future of SOC Analysis : introduction, emerging trends and the future of SOC analysis, the impact of cloud security on SOC operations, predicting future directions, SOAR, zero-trust security model

List of Practicals / Experiments:

List of practical's/experiment

- SOC Environment Setup: Set up the virtual machines, operating systems, log sources, and SOC tools required for all subsequent practicals.
- SIEM Configuration and Monitoring: Configure a SIEM platform to centralize logs and generate alerts based on collected events.
- Log and Event Analysis: Learn how to collect, filter, and analyze logs from Windows and Linux systems before configuring a SIEM.
- Network Traffic Analysis: Capture and analyze network traffic to understand normal and suspicious network behavior.
- Intrusion Detection and Prevention: Deploy IDS/IPS tools (Snort/Suricata) and monitor network attacks using the previously configured environment.
- Threat Intelligence Integration: Integrate external threat intelligence feeds (IOCs) into the SIEM and IDS for improved detection capabilities.
- Endpoint Detection and Response (EDR): Configure endpoint monitoring agents to detect suspicious processes, malware, and host-based attacks.
- Incident Response and Threat Hunting: Investigate alerts, collect evidence, perform threat hunting, and apply remediation techniques using SIEM, EDR, and MITRE ATT&CK.
- Cloud Security Monitoring: Extend SOC monitoring to cloud platforms by collecting and analyzing cloud audit logs and security events.
- SOC Dashboard and Compliance Reporting: Create dashboards, visualize SOC metrics, and generate compliance reports after all monitoring components are operational.

Text Books:

1. OPEN-SOURCE SECURITY OPERATIONS CENTER (SOC): A COMPLETE GUIDE TO ESTABLISHING, MANAGING, AND MAINTAINING A MODERN SOC by ALFRED BASTA, NADINE BASTA, WAQAR ANWAR, MOHAMMAD ILYAS ESSAR, WILEY

References:

1. SOC ANALYST CAREER GUIDE: BECOME HIGHLY SKILLED IN SECURITY TOOLS, TACTICS, AND TECHNIQUES TO JUMPSTART YOUR SOC ANALYST CAREER by KYLER KENT, PACKT PUBLISHING

2. BLUE TEAM HANDBOOK: SOC, SIEM, AND THREAT HUNTING (V1.02) by DON MURDOCH, independent publisher