Aum Amriteshwaryai Namah

AMRITA VISHWA VIDYAPEETHAM | AHEAD Online

25CSA552A Fundamentals of Cybersecurity Operations (3- 0 -2– 4)

Course Description:

- The course teaches students security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents.
- Students will learn how to monitor alerts and breaches and become a contributing members of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities

Course Outcomes:

CO1	Students should be able to understand the functionalities of various SOC generations.
CO2	Understand different data collection, data analysis, and security analysis techniques as part of SOC technologies.
CO3	Understand the vulnerability management techniques and threat intelligence methodologies.
CO4	Assess the SOC capabilities using different SOC tools and techniques.
CO5	Learn how SOC helps in business continuity and disaster recovery plan.

CO-PO Affinity Map

PO/ PSO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	**PO8**	**PSO3**
CO1	1	1	2	3	-	-	-	3	2
CO2	2	1	3	3	1	-	-	3	3
CO3	2	2	2	3	-	-	-	2	3
CO4	2	2	3	3	1	-	-	2	3
CO5	1	2	2	3	1	1	1	2	3

Syllabus:

Unit I

Information security incident management (Incident detection, triage and incident categories, Incident severity, resolution, Closure, Post-incident)

Unit II

Security Operations Center (SOC) Generations (First-generation, second, third and fourth generation SOC), SOC Maturity models (Introduction to maturity models, and applying maturity models in SOC),

Unit III

SOC and SIEM – Introduction (Role of SIEM in SOC), SOC and Splunk (Splunk architecture & SOC, Splunk Rules, Splunk log management, Splunk correlation), SOC and Health Care - A Case study (SOC Considerations for a HealthCare situation), SOC and Application security (OWASP, Application security and SOC).

Unit IV

SOC - Business Continuity, Disaster recovery (Importance of BCP and DR processes, and its interface to SOC), Security event generation and collection (Cloud Security, IDPS, Breach Detection),

Unit V

SOC Technologies-1 (Data collection and analysis, syslog protocol), SOC Technologies-2 (Telemetry Data, Security analysis, Data enrichment), Vulnerability Management (Broad introduction), Threat intelligence (Broad introduction), Assessment of SOC capabilities (Business and IT Goals, Assessing capabilities & IT processes),

Textbooks / References:

1. Security Operations Center: Building, Operating, and Maintaining Your SOC, Book by Gary McIntyre, Joseph Muniz, and Nadhem AlFardan
2. Designing and Building Security Operations Center, 2015, Book by David Nathans
3. Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, 2018, Book by Arun E Thomas
4. The Modern Security Operations Center, 2021, Book by Joseph Muniz
5. Principles for Cyber Security Operations, 2020, Book by Hinne Hettema

AMRITA VISHWA VIDYAPEETHAM

Amrita Online - Course Plan

Week	Topic	Learning Objectives	eLearning Content	Video Lectures	Assessments
1	**The Danger**	Why networks and data are attackedand how to prepare for a career in cybersecurity operations.	8 Videos	War Stories	Quiz - 1
				Threat Actors	
				Threat Impact	
				The Danger - Summary	
				The Modern Security Operations Center	
				Becoming a Defender	
				Fighters in the War Against Cybercrime – Summary	
				Introduction to netacad	
2	**Windows and Linux**	Gain knowleddge on Security features of the Windows operating system & Implement basic Linux security.	13Videos	Windows History	Quiz - 2
				Windows Architecture and Operations	
				Windows Configuration and Monitoring	
				Windows Security	
				The Windows Operating System Summary	
				Linux Basics	
				Linux Shell	
				Linux Servers and Clients	
				Basic Server Administration	
				The Linux File System	
				Linux GUI	
				Linux Host	
				Linux Summary	
3	**Network Protocols**	Detailed explanation how protocols enable network operations & how the Ethernet and IP protocols support network communication.	13 videos	Network Communications Process	Quiz – 3 Lab - 1
				Communication Protocol	
				Data Encapsulation	
				Network Protocols Summary	
				Ethernet	
				IPv4	
				IP Addressing Basics	
				Types of IPv4 Addresses	
				The Default Gateway	
				IPv6	
				Ethernet and IP Protocol Summary	
				ICMP	
				Connectivity Verification Summary	
4	**ARP&SOC**	Analyze address resolution protocol PDUs on a network.and roles and responsibilities in SOC	8 Videos	MAC and IP	Quiz - 4
				ARP	
				ARP issues	
				Address Resolution Protocol Summary	
				Roles and responsibilities in SOC -part a	
				Roles and responsibilties in SOC -part b	
				Roles and responsibilties in SOC -part c	
				Roles and responsibilties in SOC -part d	

5	**The Transport Layer & Network Services**	How transport layer protocols support network functionality and how network devices enable wired and wireless network communication	13 Videos	Transport Layer Characteristics	Quiz - 5
				Transport Layer Session Establishment	
				Transport Layer Reliability	
				The Transport Layer Summary	
				DHCP	
				DNS	
				NAT	
				File Transfer and Sharing Services	
				Email	
				HTTP	
				Network Services Summary	
				Network Devices	
				Wireless Communications	
				Network Communication Devices Summary	
6	**Network and NIST framework**	How devices and services are used to enhance network security and NIST functions	7 Videos	Network Topologies	Quiz - 6
				Security Devices	
				Security Services	
				Network Security Infrastructure Summary	
				Soc and its framework-introduction	
				NIST-part a Identity	
				NIST-part b protect	
7	**NIST framework**	NIST functions	5 videos	NIST-part c detect & respond	Quiz - 7
				NIST-part d recover	
				part e - MITRE ATT&CK-1	
				part f ISO 27001	
				CIS benchmark and GDPR	
8	**Risk & Network attacks**	How networks are attacked	8 videos	CyberOps Associate - Phase 02 Introduction	Quiz 8 Lab - 2
				Threat, Vulnerability, and Risk	
				Risk Management	
				Cyber Security Tasks, IoC, and IoA	
				Threat Actor Tools & Attackers and their Tool Summary	
				Malwere	
				Common Network Attack - Reconnaissance, Access, and social engineering	
				Network Attack - Denial of Service, Buffer Overflow, and Evasion	
9	**Network Monitoring Tools & Attacking the Foundation**	Explanation on network traffic monitoring & Explain how TCP/IP vulnerabilities enable network attacks.	10 Videos	Introduction to Network Monitoring	Lab - 3
				Introduction to Network Monitoring Tools	
				Network Monitoring Tools -	
				Summary	
				Attacking the Foundation -	
				Introduction	
				IP PDU Detail	
				IP Vulnerabilities	
				TCP and UDP Vulnerabilities	
				Attacking the Foundation - Summary	

10	**Access control**	network security defense approaches Explanation on how access control protect a network	13 Videos	IP Services	Quiz - 9
				Enterprise Services	
				Attacking What We Do - Summary	
				Defense-in-Depth	
				Security Policies, Regulations, and Standards	
				Understanding Defense - Summary	
				Access Control Concepts & Communication Security: CIA	
				Zero Trust Security	
				Access Control Models	
				AAA Operation	
				AAA Authentication	
				AAA Accounting Logs	
				Access Control - Summary	
11	**Threat intelligence & cryptography**	Use various intelligence sources to locate current security threats.And how public key infrastructure supports network security	12 Videos	Threat Intelligence & Network Intelligence Communities	Lab 4
				Cisco Cybersecurity Reports & Security Blogs and Podcasts	
				Cisco Talos & FireEye	
				Automated Indicator Sharing & Common Vulnerabilities and Exposure Database & Threat Intelligence Communication Standards & Threat	
				Securing Communication & Cryptographic Hash Function	
				Cryptographic Hash Operations & MD5 and SHA &Origin Authentication	
				Confidentiality	
				Asymmetric Encryption - Authentication, Integrity & Diffie-Hellman	
				Publick Key Cryptography	
				Encryption - Integrity & Diffie- Hellman	
				Authorities and PKI Trust Systems	
				Applications and Impacts of Cryptography & Cryptography - Summary	
12	**Endpoint protection & security technologies**	Generating a malware analysis report & how security technologies affect security monitoring	13 Videos	End Point Protection	Quiz - 10
				Antimalware Protection	
				Host-Based Intrusion Prevention	
				Application Security	
				Endpoint Protection - Summary	
				Network and Server Profiling	
				Common Vulnerability Scoring System(CVSS)	
				Secure Device Management	
				Information Security Management Systems	
				Endpoint Vulnerability Assessment System - Summary	
				Monitoring Common Protocols	
				Security Technologies	
				Technologies and Protocols - Summary	

13	**Network Security Data**	The types of network security data used in security monitoring.	6 Videos	Types of Security Data	
				End Device Logs	
				Network Logs	
				Network Security Data - Summary	
				Sources of Alerts	
				Overview of Alert Evaluation & Evaluating Alert - Summary	
14	**Working with Network Security Data**	Interpret data to determine the source of an alert.	12 Videos	Working with Network Security Data	
				A Common Data Platform	
				Investigating Network Data	
				Enhancing the Work of the Cybersecurity Analyst & Working with Network Security	
				Data - Summary	
				Digital Forensic and Incident Analysis and	
				Response	
				Evidence Handling and Attack Attribution	
				The Cyber Kill Chain	
				The Diamond Model of Intrusion Analysis	
				Incident Response	
				Digital Forensics and Incident Analysis and Response Summary	

Evaluation Policy

Internal	Quiz 20%	30%	100 %
	Lab Assignments 10%		
	10 quizzes and 4 labs are considered for internal marks		
External	End semester Exam – 70Marks MCQs -30marks Descriptive & practicals-40 marks	70%	

Faculty Information

Mr. Cherukupalli Veda Vyasa Aditya
Senior security consultant,
Audius India Private Limited, Pune.

Rajeswari R
Teaching Assistant
Cyber security
Amrita Ahead
r_rajeswari @ahead.amrita.edu