Certified SOC Analyst v2

EXAM BLUEPRINT

EC-Council

Official Curricula

EC-Council CSA Certified SOC Analyst

Certified SOC Analyst (CSA)v2

Exam Blueprint

Sr. No.	Domain	Sub Domains	Weightage
1.	Security Operations and Management	Understand the principles of security management and identify the role of security operations in effective security management	5%
		Discuss Security Operations Center (SOC) and analyze its importance, capabilities, and functions	
		Describe the SOC workflow flow and identify the People, Process and Technology involved in SOC	
		Compare different SOC models and their respective advantages and disadvantages	
		Explain the concept of SOC maturity models and evolution of SOC	
		Identify KPI's, challenges and implement best practices for effective SOC operations and management	
2.	Understanding Cyber Threats, IoCs, and Attack Methodology	Understand Cyber threats and its impact on Cyber Security	8%
		Understand Network Attack Tactics, Techniques, and Procedures (TTPs)	

		Understand Host Attack Tactics, Techniques, and Procedures (TTPs)	
		Understand Application Attack Tactics, techniques, and Procedures (TTPs)	
		Understand Social Engineering Attack Tactics, Techniques, and Procedures (TTPs)	
		Understand Email Attack Tactics, Techniques, and Procedures (TTPs)	
		Understand Insider Attack Tactics, Techniques, and Procedures (TTPs)	
		Understand and Recognize the Indicators of Compromise (IoCs) of Various Attacks	
		Understanding Attack Methodology and Frameworks	
3.	Log Management	Understand Log Management its importance and approaches	15%
		Understand and Analyze Local Logging Practices: Windows, Linux and Mac Logs	
		Understand and Analyze Local Logging Practices: Firewall and Router Logs	
		Understand and Analyze Local Logging Practices: Web Server, Database, Email	
		Understand and Implement Centralized Logging	
4.	Incident Detection and Triage	Understand the Importance and Architecture of Security Information and Event Management (SIEM)	25%
		Understand Types of SIEM Solutions and their advantages and Disadvantages	

		Understand Deploying a SIEM solution	
		Understand SIEM Use case Management	
		Learn Incident Detection with SIEM	
		Understand the use of AI for generating SIEM rule	
		Understand Handling Alert Triaging and Analysis	
		Understand Visualization and Dashboard Management in SOC	
		Understand SOC Reports	
5.	Proactive Threat Detection	Learn Fundamental Concepts of Threat Intelligence	12%
		Understand Types and Strategies of Threat Intelligence	
		Understand the Various Threat Intelligence Sources	
		Understand Threat Intelligence Platforms (TIP)	
		Understanding Threat Intelligence-Driven SOC and Its Benefits to SOC Team	
		Demonstrate the Use of Threat Intelligence Use Cases to Enhance Incident Response	
		Understand Threat Hunting and its Significance	
		Understand Threat Hunting Frameworks	
		Demonstrate Threat Hunting using PowerShell, Yara, and Threat Hunting Tools	
6.	Incident Response	Understand about Incident Response	25%

		Learn Various Phases in Incident Response Process	
		Learn to Respond to Network Security Incidents	
		Learn to Respond to Application Security Incidents	
		Learn to Respond to Email Security Incidents	
		Learn to Respond to Insider Incident	
		Learn to Respond to Malware Incidents	
		Understanding the Role of SOC Playbooks in Incident Response	
		Understand Enhanced Incident Response using Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR)	
7.	Forensics Investigation and Malware Analysis	Understand about Forensic Investigation	5%
		Investigating Network Security Incidents	
		Learn to Investigate Application Security Incidents	
		Learn to Investigate Email Security Incidents	
		Learn to Investigate Insider Incidents	
		Understand Malware Analysis	
		Learn to Perform Static Malware Analysis	
		Learn to Perform Dynamic Malware Analysis	
8.		Introduction to Cloud SOC	

	SOC for Cloud Environments	Understand Azure SOC Architecture, Microsoft Sentinel and Security Tools	5%
		Understand AWS SOC Architecture, AWS Security Hub and security tools	
		Understand Google Cloud Platform (GCP) SOC Architecture, Security Command Center, Chronicle and security tools	