

**EC-Council**



**Certified SOC Analyst (CSA)**  
Exam Blueprint v1



# Certified SOC Analyst (CSA)

## Exam Blueprint

Sr. No.	Domain	Sub Domains	Weightage
1.	Security Operations and Management	Understand the SOC Fundamentals	5%
		Discuss the Components of SOC: People, Processes and Technology	
		Understand the Implementation of SOC	
2.	Understanding Cyber Threats, IoCs, and Attack Methodology	Describe the term Cyber Threats and Attacks	11%
		Understand the Network Level Attacks	
		Understand the Host Level Attacks	
		Understand the Application-Level Attacks	
		Understand the Indicators of Compromise (IoCs)	
		Discuss the Attacker's Hacking Methodology	
3.	Incidents, Events, and Logging	Understand the Fundamentals of Incidents, Events, and Logging	21%
		Explain the Concepts of Local Logging	
		Explain the Concepts of Centralized Logging	
4.	Incident Detection with Security Information and Event Management (SIEM)	Understand the Basic Concepts of Security Information and Event Management (SIEM)	26%
		Discuss the Different SIEM Solutions	
		Understand the SIEM Deployment	
		Learn Different Use Case Examples for Application-Level Incident Detection	
		Learn Different Use Case Examples for Insider Incident Detection	

		Learn Different Use Case Examples for Network Level Incident Detection	
		Learn Different Use Case Examples for Host Level Incident Detection	
		Learn Different Use Case Examples for Compliance	
		Understand the Concept of Handling Alert Triaging and Analysis	
5.	<b>Enhanced Incident Detection with Threat Intelligence</b>	Learn Fundamental Concepts on Threat Intelligence	<b>8%</b>
		Learn Different Types of Threat Intelligence	
		Understand How Threat Intelligence Strategy is Developed	
		Learn Different Threat Intelligence Sources from which Intelligence can be Obtained	
		Learn Different Threat Intelligence Platform (TIP)	
		Understand the Need of Threat Intelligence-driven SOC	
6.	<b>Incident Response</b>	Understand the Fundamental Concepts of Incident Response	<b>29%</b>
		Learn Various Phases in Incident Response Process	
		Learn How to Respond to Network Security Incidents	
		Learn How to Respond to Application Security Incidents	
		Learn How to Respond to Email Security Incidents	
		Learn How to Respond to Insider Incidents	
		Learn How to Respond to Malware Incidents	