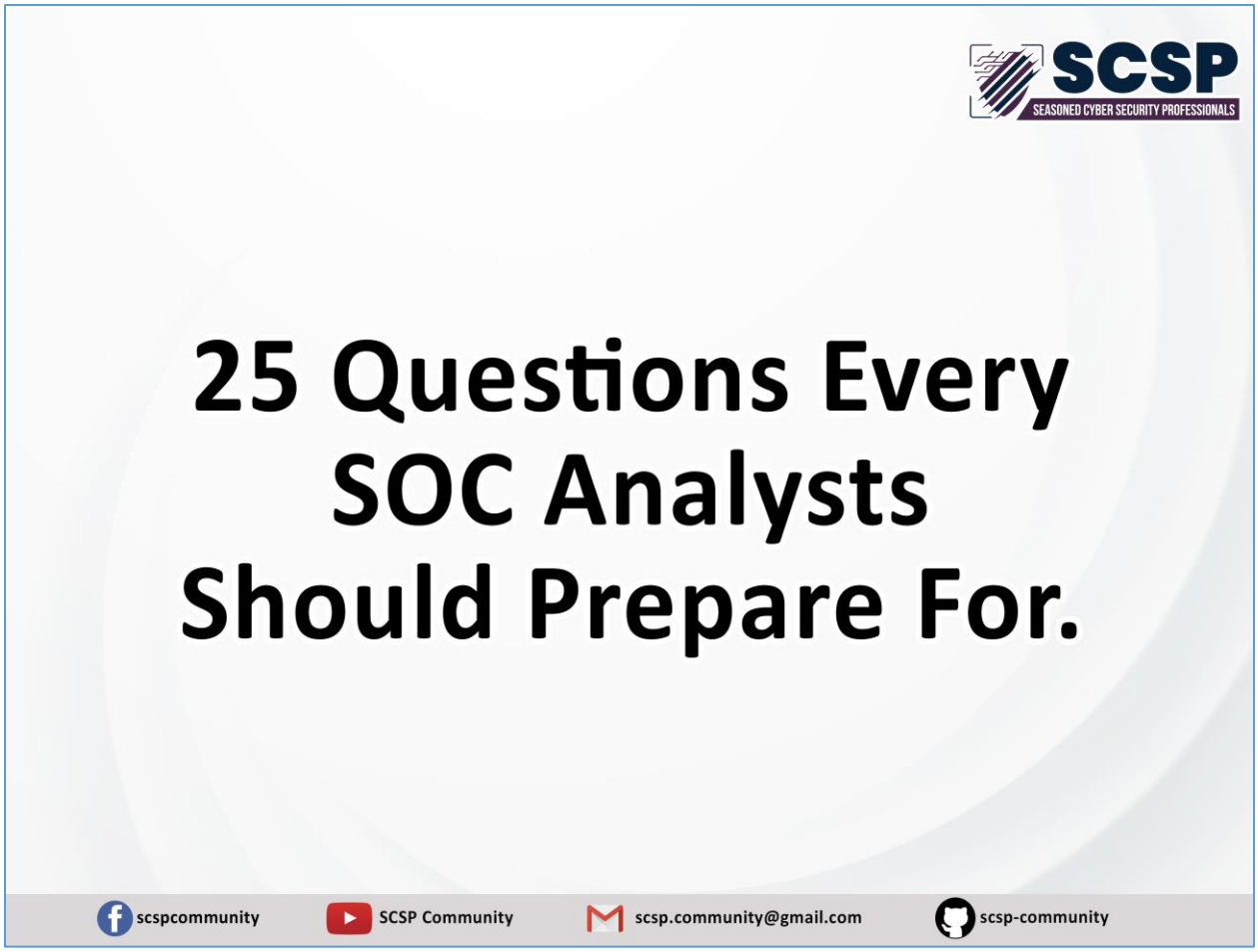
SCSP
SEASONED CYBER SECURITY PROFESSIONALS
25 Questions Every SOC Analysts Should Prepare For.
scspcommunity
SCSP Community
scsp.community@gmail.com
scsp-community

SCSP
SEASONED CYBER SECURITY PROFESSIONALS

Q1. What are the basic components in a Security Operation Center?

Q2. What are the fundamentals of a Security Operation Center?

Q3. What is a SIEM solution and how does it work?

Q4. Describe an efficient and effective method which can be used to prevent violations of computer security procedures?

Q5. SOC analysts need to gather information from multiple sources. How can you determine which information is relevant and differentiate between false positives and false negatives logs?

SCSP
SEASONED CYBER SECURITY PROFESSIONALS

Q6. Explain a plan of action which will safeguard computer files against modification, destruction, or disclosure.

Q7. In your firewall, do you prefer filtered ports or closed ports?

Q8. Which Incident Response methodology do you prefer? Explain why you use it.

Q9. Consider you are looking at the incoming traffic, but it is encrypted, how would you figure out if the payloads are malicious or benign?

Q10. If a company wants to implement a new security event manager. Describe your approach for the implementation.

SCSP
SEASONED CYBER SECURITY PROFESSIONALS

Q11. What are the multiple sources from which a SOC receives log and data?

Q12. What is the difference between traditional and next generation SOC?

Q13. How would you define a cyber threat or cyber-attacks?

Q14. What is the difference between an IOC and an IOA?

Q15. How would you define local logging and central logging? What is the difference between them?

Q16. What are the concepts of handling alerts, triaging them and analyzing the alerts?

Q17. In your opinion, why do you think there is a need for a threat intelligence driven SOC?

Q18. What are the phases of incident handling?

Q19. Define insider incidents and how would you respond to such events?

Q20. Does only setting up a SIEM solution complete a SOC?

SCSP
SEASONED CYBER SECURITY PROFESSIONALS

Q21. Consider that a device is not sharing any logs, being a SOC analyst how would you identify and detect that particular device?

Q22. Consider an in-house application or any other custom built application which does not have the capability to share its logs, how would you handle and monitor such applications?

Q23. At times certain applications send raw logs, being a SOC analyst how would you parse such logs?

Q24. How can you evaluate how Mature is your SOC?

Q25. Being an analyst how important is a SOC playbook or Workflow?