CYBERSECURITY SOC ANALYST

AI PROMPT

SkillWeed

CONTENTS

I. THREAT DETECTION AND MONITORING

1

Prompt: "Explain the purpose of a SIEM tool in threat detection."

Expected Outcome: A description of how SIEM tools collect, analyze, and correlate security logs to detect threats.

2

Prompt: "List five common types of alerts a SOC analyst might encounter."

Expected Outcome: Alerts like unauthorized access attempts, malware infections, port scans, phishing attempts, and anomalous traffic patterns.

3

Prompt: "How do you investigate a brute-force attack alert on a server?"

Expected Outcome: Steps such as reviewing logs, identifying affected accounts, and implementing IP blocking.

4

Prompt: "Write a step-by-step guide to creating custom detection rules in a SIEM."

Expected Outcome: Instructions for defining event triggers, correlating logs, and testing rules.

5

Prompt: "Explain the difference between signature-based and anomaly-based detection."

Expected Outcome: A comparison of detecting known threats via signatures versus spotting deviations from normal behavior.

II. INCIDENT RESPONSE

6

Prompt: "What are the phases of an incident response process?"

Expected Outcome: Phases like preparation, detection, containment, eradication, recovery, and lessons learned.

7

Prompt: "Draft an incident report for a malware outbreak in an organization."

Expected Outcome: A sample report including incident summary, impact, root cause, and mitigation steps.

8

Prompt: "How do you prioritize incidents in a SOC environment?"

Expected Outcome: Guidelines using risk severity, asset criticality, and business impact.

9

Prompt: "Write a playbook for responding to a phishing email attack."

Expected Outcome: A detailed playbook with steps for identifying, isolating, and mitigating phishing attempts.

10

Prompt: "What are the key differences between an incident and a security event?"

Expected Outcome: An explanation showing incidents involve harm or impact, while events may not.

III. MALWARE ANALYSIS

11

Prompt: "What are the steps to analyze a suspicious file in a sandbox environment?"

Expected Outcome: Steps like uploading the file, monitoring behavior, and reviewing indicators of compromise (IOCs).

12

Prompt: "List five tools commonly used for malware analysis."

Expected Outcome: Tools like VirusTotal, Cuckoo Sandbox, IDA Pro, Ghidra, and Wireshark.

13

Prompt: "Explain how to identify ransomware activity in network traffic."

Expected Outcome: Patterns such as unusual encryption processes or communication with known malicious IPs.

14

Prompt: "Draft a report template for documenting malware analysis findings."

Expected Outcome: Sections for malware type, behavior, IOCs, and mitigation steps.

15

Prompt: "What is the role of hash values in identifying malware?"

Expected Outcome: An explanation of using MD5/SHA hashes to compare suspicious files with known malware signatures.

IV. LOG ANALYSIS

16

Prompt: "Explain how to analyze firewall logs for suspicious activity."

Expected Outcome: Guidelines for spotting anomalies like repeated failed access attempts or unusual IP traffic.

17

Prompt: "List three common log sources monitored by SOC analysts."

Expected Outcome: Examples like firewall logs, endpoint logs, and DNS logs.

18

Prompt: "What are the key fields to check in a Windows Event Log?"

Expected Outcome: Fields such as event ID, timestamp, user account, and source.

19

Prompt: "How can you identify lateral movement using log analysis?"

Expected Outcome: Insights into tracking account logins across multiple hosts or unusual SMB activity.

20

Prompt: "Write a step-by-step guide for investigating failed login attempts in Active Directory logs."

Expected Outcome: Steps including filtering event IDs and cross-referencing affected accounts.

V. NETWORK SECURITY

21

Prompt: "How do you use Wireshark to detect malicious network activity?"

Expected Outcome: Steps for setting filters, analyzing packet headers, and identifying suspicious payloads.

22

Prompt: "Explain the significance of TCP flags in network analysis."

Expected Outcome: A breakdown of flags like SYN, ACK, and FIN in understanding connection states.

23

Prompt: "What are the common signs of a DDoS attack in network traffic?"

Expected Outcome: Indicators like high traffic volume, SYN floods, and source IP spoofing.

24

Prompt: "Write a guide to creating firewall rules to block specific traffic."

Expected Outcome: Steps for defining source/destination IPs, ports, and protocols.

25

Prompt: "How do you investigate DNS exfiltration in a network?"

Expected Outcome: Steps to detect unusual DNS queries, excessive traffic, or encoded data in DNS requests.

VI. VULNERABILITY MANAGEMENT

26

Prompt: "What are the steps to conduct a vulnerability scan?"

Expected Outcome: Steps including tool configuration, scanning, analyzing results, and remediation.

27

Prompt: "Explain how to prioritize vulnerabilities after a scan."

Expected Outcome: Guidelines using CVSS scores, exploit availability, and asset criticality.

28

Prompt: "What are some common tools used for vulnerability scanning?"

Expected Outcome: Tools like Nessus, Qualys, OpenVAS, and Rapid7.

29

Prompt: "How do you handle false positives in vulnerability scanning?"

Expected Outcome: Methods for verifying issues and excluding legitimate findings from future scans.

30

Prompt: "Write a report summarizing vulnerability management findings."

Expected Outcome: A summary including vulnerabilities, affected assets, and mitigation timelines.

VII. ENDPOINT SECURITY

33

Prompt: "What are common signs of a compromised endpoint?"

Expected Outcome: Signs like high CPU usage, unexpected processes, or unauthorized access.

32

Prompt: "Explain how EDR tools enhance endpoint security."

Expected Outcome: Features like real-time monitoring, threat detection, and automated response.

33

Prompt: "How can you use Windows Defender logs to investigate malware?"

Expected Outcome: Steps for accessing logs, filtering threats, and reviewing detections.

34

Prompt: "Draft a playbook for responding to endpoint ransomware."

Expected Outcome: Steps for isolating systems, restoring backups, and improving defenses.

35

Prompt: "What are the key differences between EPP and EDR solutions?"

Expected Outcome: A comparison of endpoint protection platforms and endpoint detection and response.

VIII. THREAT INTELLIGENCE

36

Prompt: "Explain how to use threat intelligence feeds in a SOC."

Expected Outcome: Guidelines for integrating feeds to enrich alerts and improve detection.

37

Prompt: "List five popular threat intelligence platforms."

Expected Outcome: Platforms like AlienVault, Recorded Future, and IBM X-Force.

38

Prompt: "How do you identify new IOCs from a recent attack report?"

Expected Outcome: Steps for extracting IPs, hashes, and domains from reports.

39

Prompt: "Write a threat intelligence summary for a new malware campaign."

Expected Outcome: A report including malware name, behavior, and mitigation steps.

40

Prompt: "Explain how open-source intelligence (OSINT) can aid a SOC."

Expected Outcome: Examples of using publicly available data for threat investigations.

IX. SECURITY AUTOMATION

41

Prompt: "What are the benefits of using SOAR platforms in a SOC?"

Expected Outcome: Insights into automation of workflows, incident response, and threat enrichment.

42

Prompt: "Write an automation workflow to handle phishing emails in a SOAR platform."

Expected Outcome: A workflow involving email parsing, IOC analysis, and user notifications.

43

Prompt: "How can playbooks be used to automate incident response?"

Expected Outcome: Examples of predefined steps for common incidents.

44

Prompt: "List five use cases for automation in a SOC."

Expected Outcome: Use cases like log analysis, alert triage, and IOC enrichment.

45

Prompt: "Explain the difference between manual and automated incident response."

Expected Outcome: A comparison of speed, scalability, and error reduction.

X. CAREER DEVELOPMENT FOR SOC ANALYSTS

46

Prompt: "What are the key skills needed to succeed as a SOC analyst?"

Expected Outcome: Skills like log analysis, scripting, and threat detection.

47

Prompt: "List five certifications beneficial for SOC analysts."

Expected Outcome: Certifications like CompTIA Security+, CEH, and Splunk Core Certified User.

48

Prompt: "How can a SOC analyst detect and respond to privilege escalation attempts?"

Expected Outcome: Steps for identifying unusual account activity, analyzing logs for patterns like sudo or whoami commands, and implementing immediate measures such as access revocation and forensic investigation.

49

Prompt: "What should be included in a phishing response playbook for a SOC analyst?"

Expected Outcome: A detailed playbook outlining email header analysis, sandboxing suspicious links/attachments, notifying affected users, and implementing preventative measures like SPF/DKIM/DMARC.

50

Prompt: "Explain how to use Splunk to identify and analyze suspicious activity."

Expected Outcome: A guide covering setting up search queries, filtering key fields like source IP and event ID, and identifying anomalous patterns through dashboards and alerts.

SkillWeed