



SOC ANALYST CHEAT SHEET

A Quick Reference Guide

**Covers Key Concepts, Tools,
and Techniques used in Threat
Hunting, Incident Response,
and Security Monitoring.**

www.cyveer.com



CYVEER



Threat Hunting

- **Techniques:**
 - Log Analysis
 - Vulnerability Scanning
 - Threat Intelligence
 - Endpoint Detection and Response (EDR)
 - Network Traffic Analysis
 - Hunting Queries

www.cyveer.com



CYVEER



Tools

- SIEM (Security Information and Event Management)
- EDR (Endpoint Detection and Response)
- Vulnerability Scanners
- Threat Intelligence Platforms
- Network Traffic Analysis Tools

www.cyveer.com



CYVEER



Incident Response

- **Phases:**
 - Preparation
 - Detection
 - Investigation
 - Containment
 - Eradication
 - Recovery
 - Lessons Learned

www.cyveer.com



CYVEER



Key Considerations

- **Chain of Custody:** Maintain proper chain of custody for all evidence.
- **Communication:** Maintain clear and concise communication with stakeholders.
- **Documentation:** Document all actions and findings throughout the incident response process.

www.cyveer.com



CYVEER



Daily Security Monitoring

- **Key Activities:**
 - Log Monitoring
 - Alert Review
 - Vulnerability Management
 - Threat Intelligence Monitoring
 - Security Posture Assessment

www.cyveer.com



CYVEER



Technical Skills

- **Strong understanding of:**
 - Networking and System Administration.
 - Scripting and automation (e.g., Python, PowerShell).
 - Security Protocols and Technologies (e.g., firewalls, IDS/IPS, VPNs).
 - Experience with SIEM, EDR, and other security tools.
 - Ability to analyze log files and network traffic.

www.cyveer.com



Soft Skills

- Problem-solving and critical thinking.
- Communication and interpersonal skills.
- Attention to detail.
- Ability to work independently and as part of a team.
- Strong work ethic and ability to handle pressure.

www.cyveer.com



Resources

- MITRE ATT&CK Framework
- OWASP (Open Web Application Security Project)
- CERT/CC (Computer Emergency Response Team Coordination Center)
- Security blogs and forums

www.cyveer.com



Think you've got
what it takes to be
an SOC analyst?

LIKE & SHARE

FOLLOW FOR MORE
INSIGHTS!

www.cyveer.com