



SOC Analyst

Cheat Sheet

A Comprehensive Guide





1. Incident Response Phases:

- **Preparation:** Establish incident response policies and procedures.
- **Identification:** Detect potential security incidents.
- **Containment:** Limit the scope and magnitude of an incident.
- **Eradication:** Remove the root cause and any traces of the incident.
- **Recovery:** Restore and validate system functionality.
- **Lessons Learned:** Document the incident and improve future response efforts.

2. Common Tools and Commands:

Wireshark: Packet analysis tool.

Command:

```
~$ wireshark
```

tcpdump: Command-line packet analyzer.

Command:

```
~$ tcpdump -i eth0
```

nmap: Network mapping tool.

Command:

```
~$ nmap -sV -p 1-65535 <IP>
```

Netcat: Networking utility for reading/writing network connections.

Command:

```
~$ nc -nvlp <port>
```

Splunk: Log analysis tool.

Command in Splunk Search:

```
source=/var/log/messages | top limit=10 host
```



3. Log Monitoring:

Monitor authentication logs, system logs, application logs, and network traffic logs.

Key log files in Linux:

[/var/log/auth.log](#)

[/var/log/syslog](#)

[/var/log/apache2/access.log](#)

etc.

4. Indicator of Compromise (IoC) Identification:

- IP addresses, URLs, domain names, and file hashes.
- Unexpected system or network behavior, unusual outbound traffic, and alerts from security tools.

5. Phishing Analysis:

- Verify the sender's address and domain.
- Look for urgency, grammatical errors, and suspicious attachments or links.
- Use tools like VirusTotal or URLScan.io to analyze URLs and files.

6. SIEM Utilization:

- Familiarize yourself with your organization's Security Information and Event Management (SIEM) tool.
- Develop and refine correlation rules to detect anomalies and potential threats.
- Regularly review and investigate alerts generated by the SIEM.

7. Threat Intelligence:

- Utilize threat intelligence feeds to stay updated on the latest threat actors, malware, and vulnerabilities.
- Integrate threat intelligence into security monitoring and incident response processes.



8. Communication:

- Document all findings and actions taken during incident investigation and response.
- Communicate effectively with relevant stakeholders during and after an incident.

9. Continuous Learning:

- Stay updated with the latest cybersecurity trends, threat intelligence, and best practices.
- Participate in training, webinars, and conferences.

10. Daily Checks:

- Check for critical alerts and review dashboards in your SIEM.
- Monitor news feeds for the latest vulnerabilities and threats relevant to your organization.

Keep this cheat sheet handy to quickly reference key concepts, tools, and procedures that are vital to your role as a SOC analyst.

Explore our CyberSecurity Courses

**Ethical
Hacking
Training**

INR 15,000/-

**Diploma in
Cyber
Security**

INR 63,300/-

**Cyber
Security
Training**

INR 23,599/-

Call Us 1800-123-500014

Registered Office
Kolkata, India

DN-36, Primarc Tower, Unit
no-1103, College More, Salt
Lake, Sec-5, Kolkata-700091

Corporate Office
Bangalore, India

Nomads Horizon, Building No.
2287, 14th A Main Road, HAL
2nd Stage, Indiranagar,
Bangalore - 560008, Land
Mark: Beside New Horizon
School

Corporate Office
Hyderabad, India

Awfis Oyster Complex, 3rd
Floor, Oyster Complex,
Greenlands Road Somajiguda,
Begumpet, Hyderabad,
Telangana 500016



www.indiancybersecuritysolutions.com



info@indiancybersecuritysolutions.com