Soc Level 1 Interview Questions

SECTION 1: General Cybersecurity Basics

1. **What is the role of a SOC Analyst Tier 1?**

A Tier 1 SOC Analyst is the **first line of defence**. Their responsibilities include:

- Monitoring alerts from the SIEM
- Performing initial triage
- Escalating verified incidents to Tier 2
- Creating incident tickets
- Documenting daily activity

2. **What is a cybersecurity incident?**

Any event that:

- Compromises the **confidentiality**, **integrity**, or **availability** of an information system
- Indicates that **security controls have failed**

3. **What is the difference between an event and an alert?**

- **Event**: Any log or activity recorded (normal or abnormal)
- **Alert**: A **flagged event** that matches suspicious or malicious behaviour patterns

4. **What is a false positive?**

An alert triggered by normal activity that is **not** an actual threat. It's the SOC's job to identify and reduce false positives through tuning.

5. **Define the CIA Triad.**

- **Confidentiality**: Preventing unauthorised access to data
- **Integrity**: Ensuring data is not altered

- **Availability**: Ensuring data/services are accessible when needed

SECTION 2: Log Sources & SIEM Awareness

6. **What is SIEM?**

SIEM (Security Information and Event Management) is a platform used to:

- Collect and normalise logs from multiple sources
- Detect and correlate events
- Generate alerts based on rules

Examples: Wazuh, Splunk, QRadar, Elastic SIEM

7. **What type of logs does a SIEM collect?**

- Windows Event Logs
- Linux Syslogs
- Firewall logs
- IDS/IPS alerts (e.g., Suricata, Snort)
- Antivirus logs
- VPN and proxy logs
- Authentication logs (e.g., SSH, RDP)

8. **What is a use case in SIEM?**

A defined scenario that describes how a particular threat or malicious behaviour is detected using correlation rules.

Example: Detecting multiple failed login attempts from the same IP.

SECTION 3: Triage & Monitoring

9. **How do you investigate an alert?**

1. Identify the rule and its source
2. Check the associated log data (user, IP, file, etc.)
3. Look for context (is it normal behaviour?)
4. Correlate with other logs if needed

5. Escalate or close the alert based on findings

10. **What do you do if you see a malware alert?**

- Identify host and user
- Check if file was quarantined
- Review endpoint activity
- Check if similar alerts exist across the network
- Escalate to Tier 2 for forensic review

11. **How do you handle a phishing alert?**

- Analyse sender address and headers
- Check if users clicked on the link
- Review web traffic logs
- Quarantine the email if needed
- Escalate with full evidence to Tier 2

12. **What is the difference between IDS and IPS?**

- **IDS (Intrusion Detection System)**: Detects but does **not block** traffic
- **IPS (Intrusion Prevention System)**: Detects and **actively blocks** malicious traffic

13. **What are common security alert categories?**

- **Brute-force attempts**
- **Malware detection**
- **Data exfiltration**
- **Suspicious login activity**
- **Internal reconnaissance**

SECTION 4: Basic Networking & OS Concepts

14. **What are common ports used in networking?**

- SSH: `22`

- HTTP: `80`
- HTTPS: `443`
- DNS: `53`
- RDP: `3389`
- SMB: `445`

15. What is the difference between TCP and UDP?

- **TCP**: Connection-oriented, reliable
- **UDP**: Connectionless, faster but less reliable

16. What is DNS and how can it be abused?

DNS (Domain Name System) resolves domain names to IPs. It can be abused for:

- **DNS tunnelling**
- **Command and Control (C2) communication**
- **Exfiltration**

Abuse Type	Description	Real-world Risk	Why it's dangerous
DNS Tunnelling	Encodes data inside DNS queries	Bypasses firewalls to sneak out data	It looks like normal DNS traffic, so it often goes unnoticed by security systems.
C2 over DNS	Malware gets commands via DNS	Allows remote control over infected systems	It allows hackers to operate even when normal web traffic is blocked by firewalls.
DNS Exfiltration	Sends stolen data via DNS queries	Exposes sensitive data without detection	Firewalls usually don’t inspect DNS content deeply, allowing sensitive information to leak out.

17. How do you identify a suspicious IP address?

- Reverse lookup or Whois
- Use threat intelligence feeds like VirusTotal, AbuseIPDB
- Check geo-location

- Check known blocklists

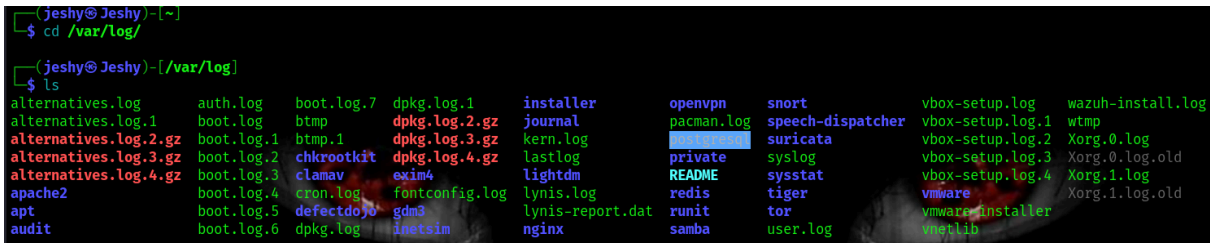
Quick Checklist to Flag a Suspicious IP

Check	Action/Tool
Whois Lookup	DomainTools / ARIN / RIPE NCC
Reverse DNS	`nslookup` / `dig -x`
VirusTotal Reputation	virustotal.com
Abuse Reports	abuseipdb.com
Geo-IP Check	`ipinfo.io` / `iplocation.net`
Blocklist Status	Spamhaus / Cisco Talos / FireHOL
Traffic Behaviour (SIEM)	Check logs for port scanning, brute-force

SECTION 5: OS & Log Familiarity

18. **Where are logs stored in Linux?**

In Linux, **logs are typically stored in the `/var/log/` directory**, which serves as the central repository for system, service, and application logs.




```
/var/log/auth.log
/var/log/syslog
/var/log/messages
```

- All major logs are under `/var/log/`.
- Authentication, kernel, daemon, and system messages have dedicated files.
- Web servers and databases have subdirectories.
- Use tools like `less`, `tail`, or `grep` to read and search logs efficiently.

19. **Where are logs stored in Windows?**

Windows logs system, security, and application events in the **Event Viewer**, which reads from a set of binary `.evtx` log files stored in the system directory.

Event Viewer:

- **Security**
- **System**
- **Application**

Accessing Logs via Event Viewer

Steps:

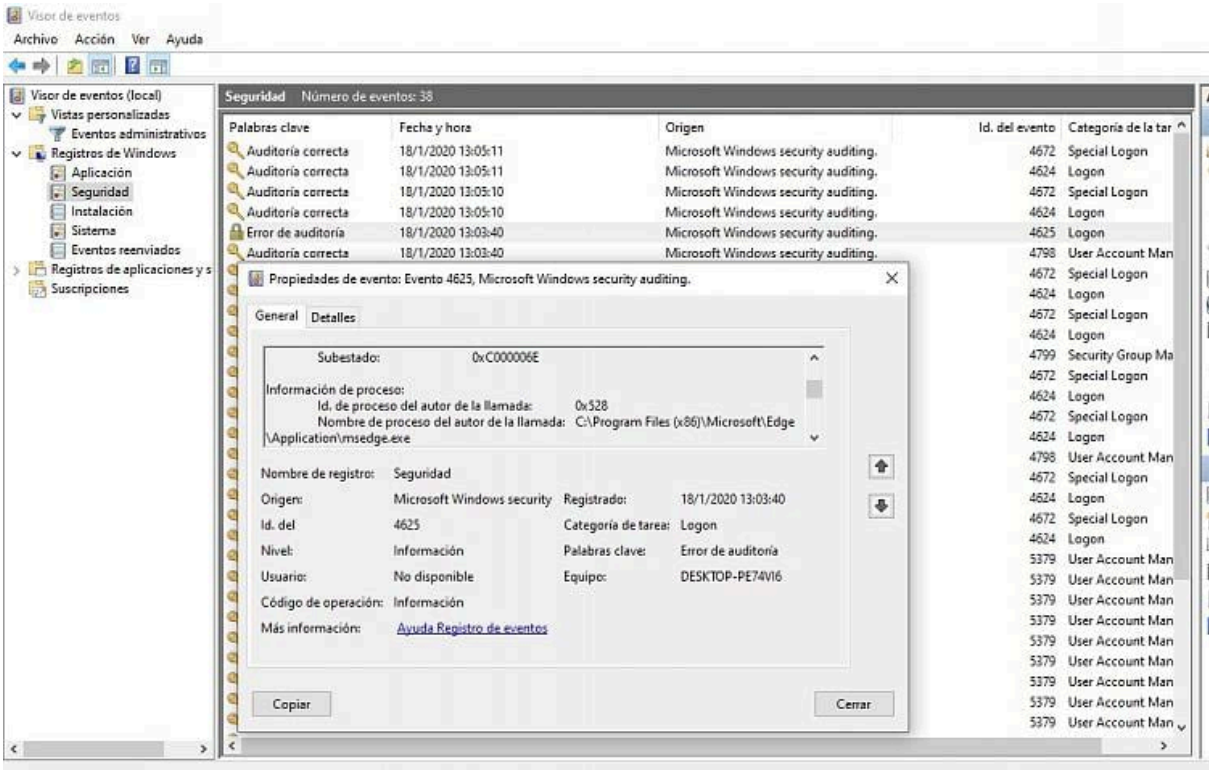
1. Press `Windows Key + R` → Type `eventvwr.msc` → Press **Enter**
2. Expand **Windows Logs** on the left panel

You will see the following main categories:

Log Category	Description
Application	Logs from installed programs and applications (e.g. errors from MS Office)
System	Logs from Windows system components (e.g. driver failures, shutdowns)
Security	Audit logs, logon attempts, privilege use, account lockouts, etc.
Setup	Logs related to OS setup and Windows updates
Forwarded Events	Logs from other systems (if event forwarding is configured)

20. **What is Event ID 4625?**

Windows Security Log ID for **failed login attempt**.



SECTION 6: Threat Intelligence Basics

21. **What is an IOC?**

An **Indicator of Compromise,** evidence of a breach such as:

- Malicious IP address
- File hash
- Domain name
- Registry key

Or, An **IOC (Indicator of Compromise)** is **a piece of forensic evidence** that suggests a system or network may have been breached or is under attack. It helps security teams **detect, identify, and respond** to malicious activity.

Think of IOCs as the **digital fingerprints** left behind by attackers.

Common Types of IOCs (With Examples)

IOC Type	Description	Example
IP Address	Malicious source/destination address	`185.220.101.4` used in C2 communications

IOC Type	Description	Example
File Hash	Unique identifier of a malicious file	`e99a18c428cb38d5f260853678922e03` (MD5)
Domain Name	Malicious domain used for phishing or C2	`evil-login[.]com`
URL	Malicious URL used in spam or exploit	`http://malicious[.]site/download.exe`
Email Address	Used in phishing or spoofing	`fakeadmin@spoofed-company.com`
Registry Key	Modified/added key by malware	`HKCU\Software\Microsoft\Windows\Run\bad.exe`
Process Name	Suspicious or unexpected process	`svhost.exe` (misspelt version of `svchost.exe`)
Mutex/String	Malware-specific strings or mutexes	`Global\MyMalwareMutex`

22. **What is a hash?**

A **unique value** representing file content. Useful to verify file integrity or detect known malware.

23. **Name a few free threat intelligence sources.**

- VirusTotal
- AbuseIPDB
- AlienVault OTX
- IBM X-Force Exchange
- MalwareBazaar

🎯 SECTION 7: Ticketing & Soft Skills

24. **What do you write in an incident ticket?**

- Alert ID and rule
- Timestamps
- Source and destination IPs
- User involved

- Summary of investigation
- Verdict (false positive, true positive, escalated)

25. **How do you prioritise alerts in a busy SOC?**

- Based on **criticality of asset**
- Alert severity level
- Threat type (e.g., known malware vs misconfig)
- Past patterns or repeated alerts

📋 BONUS: Soft Skills / HR Questions

26. **Why do you want to be a SOC analyst?**

Sample:

> I'm passionate about cybersecurity and want to contribute to frontline defence. A SOC analyst role gives me the opportunity to learn real-world threats and play a key role in protecting systems and data.

27. **How do you handle pressure during alert surges?**

> I stay calm, prioritise based on severity, document everything clearly, and focus on the alerts with the highest business impact first.