CYBERSECURITY ANALYST / SOC ANALYST L1–L2 INTERVIEW PREPARATION

BY Samiran Das

1. INTRODUCTION

1.1 Overview of SOC Environment

A Security Operations Center (SOC) is the command hub where cybersecurity analysts monitor, detect, analyse and respond to security incidents. SOCs can broadly be divided into two main environments:

1.1.1 In-House SOC

An in-house SOC is a security operations centre that is built and operated within an organisation, typically in large enterprises such as banks, government agencies, healthcare institutions or energy providers. Because it resides inside the company, it provides full visibility into the organisation's infrastructure and allows processes to be tailored closely to internal policies, business risk management and compliance requirements. This alignment means analysts have deeper knowledge of the systems they protect and can collaborate directly with governance and risk teams. The advantages of such a SOC include strong alignment with the company's objectives and a higher level of customisation to the specific threat landscape the organisation faces. However, the challenges are significant: maintaining an in-house SOC requires high costs for infrastructure and skilled staff, constant training to stay current with evolving threats and there may be limited exposure to diverse attack types compared to MSSPs. A clear example is a bank in Malaysia operating its own SOC to comply with Bank Negara Malaysia's Risk Management in Technology (RMiT) guidelines, ensuring continuous monitoring, incident response and regulatory reporting remain under its direct control.

1.1.2 MSSP (Managed Security Service Provider) SOC

An outsourced or external SOC, often called an MSSP SOC, is a security operations centre service offered to multiple clients rather than being built in-house. In this model, analysts monitor security events for many organisations at the same time, usually through shared SIEM or XDR platforms. The processes are standardised across clients, but there is still a need for client-specific runbooks and escalation procedures. The advantages are significant: it is cost-effective for clients compared to building their own SOC, provides access to a pool of skilled analysts and offers broad exposure to different types of attack scenarios since the provider sees threats across industries. However, challenges include limited visibility into each client's internal systems, potential delays in communication and reliance on clients to forward the right logs for monitoring. A common example is a telecommunications provider in Malaysia operating a SOC for over 50 organisations spanning finance, retail and manufacturing, ensuring these clients receive 24/7 monitoring without having to build their own dedicated SOC.

1.2 Roles of L1 vs L2 Analyst

1.2.1 Level 1 (L1) SOC Analyst

- Responsibilities:
  - First line of defence, monitoring SIEM dashboards.
  - Triage incoming alerts (decide if false positive or genuine).
  - Escalate to L2 when deeper analysis is needed.
  - Document findings in tickets.
  - Handle routine tasks (daily health checks, IOC lookups).
- Example tasks:
  - Checking if login failures from an IP are normal or malicious.
  - Looking up a suspicious domain in VirusTotal.
  - Closing false positives (e.g., vulnerability scanner generating noise).

1.2.2 Level 2 (L2) SOC Analyst

- Responsibilities:
  - Perform deeper investigation on escalated cases.
  - Correlate multiple log sources (firewall, proxy, EDR, email).
  - Decide containment steps (isolate host, disable accounts, block IP).
  - Write incident reports for management or client.
  - Guide L1 analysts on detection improvements.
- Example tasks:
  - Investigating why a compromised account is authenticating from two countries within 5 minutes.
  - Confirming malware behaviour using sandbox analysis.
  - Mapping attacker behaviour to MITRE ATT&CK to understand tactics.

1.3 Typical Day-to-Day Workflow

For L1 Analyst

1. Morning Log Health Checks
   - Ensure all security log sources (firewall, EDR, DNS, etc.) are forwarding to SIEM.
   - Check SIEM dashboards for failed/paused log ingestion.
   - Example: Notices that EDR logs from “HR Department laptops” stopped flowing — escalate to engineering.
2. Alert Monitoring & Triage
   - Continuously monitor SIEM alerts.
   - Apply playbooks: Is this alert a false positive or true incident?
   - Example: SIEM triggers alert for “Multiple failed logins” → analyst checks if it’s a user typing wrong password vs brute force attempt.
3. Initial Investigation
   - Gather data: IP reputation, domain lookups, endpoint logs.

    - Example: Suspicious outbound traffic to 185.220.101.2 → VirusTotal shows it's a Tor exit node.
4. Escalation / Documentation
    - Escalate confirmed suspicious alerts to L2.
    - Close benign/false positive alerts with explanation.

For L2 Analyst

1. Deeper Investigation
    - Review escalated tickets from L1.
    - Example: L1 escalates "Suspicious login from Nigeria" → L2 checks AD logs, VPN logs, email access logs.
2. Correlation & Analysis
    - Correlate across sources to confirm incident scope.
    - Example: Finds user "finance_admin" logged in from Nigeria and Malaysia within 10 minutes → possible account compromise.
3. Containment & Response
    - Initiate actions: disable account, isolate machine, block C2 IPs.
    - Example: Disable finance_admin account, notify IT to reset password, block Nigerian IP range on firewall.
4. Reporting & Lessons Learned
    - Document root cause, timeline, affected systems.
    - Suggest rule tuning to reduce false positives.
    - Example: Report shows compromise due to phishing email → recommend awareness training.

1.4 Simulation Example – "Suspicious Login Alert"

Scenario

- SOC SIEM triggers alert: "Multiple failed logins followed by successful login – User: finance_admin"
- Login attempts came from IP: 185.220.101.2 (Tor exit node).
- User is based in Kuala Lumpur, but login success shows location: Lagos, Nigeria.

L1 Analyst Actions

1. Receives alert → validates timestamp and source.
2. Checks if user is on leave (possible abnormal login).
3. Looks up IP on VirusTotal → marked as malicious.
4. Escalates to L2 with details: "Suspicious successful login from Nigeria for finance_admin, IP flagged as malicious, user supposed to be in KL."

L2 Analyst Actions

1. Pulls AD and VPN logs → sees logins from both Nigeria and KL within 10 mins.
2. Checks email logs → finds phishing email with malicious link delivered to finance_admin last week.
3. Confirms account compromise.
4. Takes action: disables user account, forces password reset, checks for lateral movement attempts.
5. Creates incident report and updates SOC playbook: “Add Tor exit nodes to watchlist for login activity.”

2. CORE CYBERSECURITY FUNDAMENTALS

2.1 CIA Triad – Confidentiality, Integrity, Availability

The CIA triad is the backbone of cybersecurity principles. Every security control, detection or response relates to at least one of these three.

- Confidentiality – Protecting sensitive data from unauthorised access.
    - Examples: Encrypting customer data, access controls, data classification.
    - Interview question: How do you ensure confidentiality of user passwords?
    - SOC context: Alerts for unauthorised access attempts directly tie to confidentiality breaches.
- Integrity – Ensuring data is accurate and not tampered with.
    - Examples: Hashing files to verify authenticity, database checksums, digital signatures.
    - Interview question: What would you do if logs are being modified or deleted?
    - SOC context: Detecting log tampering or file modification attempts.
- Availability – Ensuring data/systems are accessible when needed.
    - Examples: DDoS protection, redundancy, backup and recovery.
    - Interview question: What's the risk if a bank's payment system goes offline for 2 hours?
    - SOC context: Alerts for denial-of-service or system outages fall under availability.

2.2 Common Threats & Attacks

SOC analysts constantly face these threat categories:

- Phishing – Fake emails tricking users to click links or give credentials.
    - Example: "Your Microsoft 365 password expired, click here to reset."
    - SOC detection: Email gateway detects suspicious sender domains.
- Malware – Software designed to harm or gain unauthorised access.
    - Example: Keylogger installed via malicious attachment.
    - SOC detection: EDR generates alert when malicious process spawns.
- Ransomware – Encrypts files and demands ransom.
    - Example: WannaCry, LockBit.
    - SOC detection: Multiple file modifications in short time, ransom note dropped.
- DDoS (Distributed Denial of Service) – Overwhelms system with traffic.
    - Example: Flooding e-commerce website during a sale.
    - SOC detection: Firewall logs show traffic spikes from thousands of IPs.
- Insider Threats – Employees abusing access.
    - Example: Finance staff exporting payroll database to USB.

    - SOC detection: UEBA (User & Entity Behaviour Analytics) flags unusual data transfer.

2.3 Security Concepts

Least Privilege

- Users should only have access they need, nothing more.
- Example: HR staff shouldn't access financial systems.
- SOC monitoring: Detect privilege escalations (normal user becoming domain admin).

Zero Trust

- Never trust, always verify — all access requests are authenticated and authorised.
- Example: Even internal employees must authenticate via MFA for VPN.
- SOC monitoring: Track failed MFA attempts.

Defense in Depth

- Multiple layers of defence protect critical assets.
- Example: Firewalls + EDR + Email filters + DLP = overlapping security.
- SOC monitoring: Analysts must check alerts across all layers, not just one.

Cyber Kill Chain

- Stages of an attack, used for detection mapping.
- Phases: Recon → Weaponisation → Delivery → Exploitation → Installation → Command & Control (C2) → Actions on Objectives.
- Example: Detecting attack early in Recon saves impact later.
- SOC use: Helps analysts map alerts to attacker stage.

2.4 Protocols & Networking Basics

SOC Analysts must understand protocols, as most alerts/logs reference them.

- TCP/IP – Foundation of internet communication.
    - Example: SOC may detect port scanning across TCP 22 (SSH).
- DNS (Domain Name System) – Converts domain names to IPs.
    - Example: Malware using DNS tunnelling for C2.
    - SOC detection: Excessive unusual DNS queries from a host.
- HTTP/HTTPS – Web traffic protocols.
    - Example: Malicious JavaScript delivered via HTTP GET.
    - SOC detection: Proxy logs showing suspicious requests.

- SMTP (Simple Mail Transfer Protocol) – Email sending.
    - Example: Compromised account spamming phishing emails.
    - SOC detection: Email gateway logs show hundreds of outbound mails.
- VPN (Virtual Private Network) – Secure connection over public internet.
    - Example: Remote worker connects to office network via VPN.
    - SOC detection: Logins from two VPN endpoints at the same time.
- SSL/TLS – Encryption protocols securing traffic.
    - Example: TLS used for HTTPS.
    - SOC detection: SSL inspection may show expired or self-signed certificates.

2.5 Simulation – Applying Fundamentals

Scenario: Phishing Attack with Credential Theft

1. Event:
    - User in finance receives phishing email: "Reset your Microsoft 365 password."
    - User clicks link, enters credentials on fake login page.
2. Logs Detected:
    - Email gateway log: Email from suspicious sender not in allowlist.
    - Proxy log: User accessed http://microsoft365-login-reset.com.
    - Authentication log: Successful login from IP in Nigeria shortly after.
3. L1 Analyst Actions
    - Sees SIEM alert: "Successful login from unusual geography."
    - Checks user profile — based in Malaysia, not traveling.
    - Uses VirusTotal to confirm domain is malicious.
    - Escalates to L2 with details: "finance_user credentials compromised via phishing."
4. L2 Analyst Actions
    - Confirms with correlation: email + proxy + auth logs align.
    - Checks MITRE ATT&CK mapping:
        - Initial Access → Phishing (T1566)
        - Credential Access → Valid Accounts (T1078)
    - Containment: Reset user's password, force logout from all sessions.
    - Eradication: Block malicious domain in proxy/firewall.
    - Reporting: Incident categorised as Credential Compromise.
5. CIA Triad Impact
    - Confidentiality: Compromised user credentials → data at risk.
    - Integrity: Potential tampering of finance records if not stopped.
    - Availability: No major downtime, but potential impact if used for lateral movement.

3. SOC Basics (Deep Dive + Full Simulation)

3.1 SOC Structure (Tiered & Operating Models)

Tiers

- Tier 1 (L1) — Monitoring & Triage
  - 24×7 eyes-on-glass, acknowledge alerts, perform quick checks, suppress noise and escalate.
- Tier 2 (L2) — Investigation & Containment
  - Deep analysis across data sources, scope the incident, recommend/execute containment (with approvals), create interim IR reports.
- Tier 3 (L3) — DFIR, Threat Hunting, Content Engineering
  - Root-cause, forensics, malware triage, long-hunt missions, build/maintain detections (SIEM rules, EDR policies), purple-team.

Operating Models

- In-house SOC: Dedicated to one org; tight integration with IT/Compliance; highest visibility; higher cost.
- MSSP/MDR: Shared analysts, multi-tenant tooling, wide exposure to threats; needs strong runbooks per client.
- Hybrid/Virtual SOC: Lean internal team + external surge/DFIR; common for mid-size orgs.

Coverage Models

- Follow-the-sun (global handoff), single-region 24×7 (shifts) or business-hours + on-call (smaller orgs).

3.2 Responsibilities by Tier (with RACI-style view)

Activity	L1	L2	L3/DFIR	Sec/Platf. Eng.	IR Manager
Acknowledge alerts (SLA 5–10 min)	R	C	I	I	I
Triage (enrich, decide FP/TP)	R	A	I	I	I
Case investigation (multi-source)	C	R/A	C	I	I
Containment recommendation	C	R	A	C	C
Execute containment (EDR isolate, disable acct, block IOC)*	C	R	A	R (firewall/SIEM)	C
Forensics, malware analysis, timeline	I	C	R/A	I	C
Detection tuning / rule engineering	I	C	R/A	R/A	I
Threat hunting / purple team	I	C	R/A	C	I
Reporting (exec/technical) & PIR	C	R	A	I	A

*Execution rights vary by org policy; some actions require IR Manager/IT approval.

What “good” looks like

- L1: fast, consistent, disciplined documentation; low false escalations.
- L2: strong correlation skills; clear containment plans; high signal/noise.
- L3: closes root causes; turns lessons into new detections/playbooks.

3.3 Key Tools & What Each Tier Uses Them For

- SIEM (Splunk, QRadar, Sentinel, Elastic)
  - L1: alert queue, quick pivots (user/ip/host), dashboards, basic searches.
  - L2: correlation across sources (auth, EDR, DNS, proxy, VPN, cloud), timeline building, mapping to MITRE ATT&CK.
  - L3: content engineering (rules, parsers), performance/tuning, data onboarding.
- EDR/XDR (Cortex XDR, CrowdStrike, Defender, Carbon Black)
  - L1: verify detections (malicious process, quarantine status), quick isolate recommendation.
  - L2: process tree analysis, persistence checks, lateral movement evidence.
  - L3: custom IOC policies, memory dumps, response scripts.
- NDR (Darktrace, Corelight/Zeek, Vectra)
  - L1: suspicious lateral traffic, anomalous SMB/RDP, beaconing hints.
  - L2: confirm C2 patterns, data exfil channels, host-to-host relationships.
  - L3: protocol-level investigations, JA3/JA4 fingerprints.
- SOAR (Cortex XSOAR, Splunk SOAR, Sentinel automation)
  - L1: one-click enrich (VT/WHOIS/GeoIP), case templates, notify channels.
  - L2: semi-automated containment (disable user, EDR isolate, firewall block).
  - L3: playbook authoring, approvals, guardrails, post-incident automations.
- TIP (MISP, OTX, BrightCloud, ThreatMiner)
  - L1: reputation checks.
  - L2: campaign linkage (infrastructure reuse, overlaps).
  - L3: feed curation, false-positive control, long-lived IOCs → behavioral detections.
- Case Mgmt / Ticketing (ServiceNow, Jira, TheHive)
  - Mandatory fields, SLA clocks, handover notes, evidence attachments, linkage to runbooks.

3.4 Alert Lifecycle (end-to-end with SLAs & evidence)

1) Detection

- Sources: SIEM correlation, EDR analytic, NDR anomaly, cloud identity events, UEBA.

- Quality gates: severity (High/Med/Low), confidence, deduplication.
- Output: New case with IOC snapshot & affected asset(s).
- Owner: L1
- SLA: Acknowledge ≤ 5–10 minutes (24×7).

2) Triage

- Actions: Verify trigger, pull last 24–72h context, enrich IP/domain/hash, user/asset criticality, quick false-positive tests.
- Decision: FP → close with reason; TP/suspicious → escalate.
- Owner: L1 (L2 consult if needed)
- SLA: ≤ 15–30 minutes (severity-dependent).
- Evidence: Screenshots, raw log excerpts, enrichment results.

3) Analysis

- Actions: Correlate across SIEM, EDR, DNS, proxy, VPN, email, cloud; build timeline; determine scope & entry vector.
- Owner: L2
- SLA: First analysis note ≤ 60 minutes; material updates hourly on Sev-1.
- Artifacts: host list, user list, IOCs, suspected technique mapping (MITRE).

4) Escalation / Decision

- Actions: Recommend containment steps with rationale & impact; seek approvals per runbook/RACI.
- Owner: L2 (+ IR Manager/IT approver)
- SLA: Immediate for Sev-1; ≤ 2h for Sev-2.

5) Containment / Eradication / Recovery

- Actions: EDR isolate, block IP/domain, disable/force-reset accounts, remove persistence, patch, restore from backup, monitor.
- Owner: L2 executes; L3 guides complex IR; IT ops assists.
- SLA: Containment start ≤ 30–60 minutes after decision on Sev-1.

6) Closure & Lessons Learned

- Actions: Root cause, impact statement, executive & technical reports, detection updates, SOAR playbook tweaks, user awareness actions.
- Owner: L2 report; L3 RCA; IR Manager approves.
- Metrics: MTTD, MTTA, MTTR, % automated triage, recurrence rate.

3.5 Practical Rubrics & Examples

Severity rubric (simplified)

- Sev-1: Confirmed compromise on critical asset, data exfil in progress, ransomware activity.
- Sev-2: Active malicious behavior on non-critical asset, lateral movement indicators.
- Sev-3: Suspicious but unconfirmed, early-stage recon, single failed auth anomaly.

Quick triage questions (L1)

- Is the asset/user critical or privileged?
- Is the IOC reputable (multi-engine malicious)?
- Is behavior new for this entity (UEBA/geo/time)?
- Is there chained behavior (failed→success logins + new process + outbound)?

Enrichment checklist

- IP/domain reputation (VT/OTX), WHOIS age, hosting ASN, GeoIP distance ("impossible travel").
- Hash lookup, known malware family, sandbox report.
- Asset baseline (EDR: new driver, autoruns, scheduled tasks).

3.6 Mini-Library: Useful Detection Examples

Splunk (multiple failed → success)

```
index=auth (EventCode=4625 OR EventCode=4624)
| bin _time span=5m
| stats count(eval(EventCode=4625)) as failed count(eval(EventCode=4624)) as success by user, src_ip, _time
| where failed>=5 AND success>=1
```

Splunk (DNS tunneling – excessive TXT)

```
index=dns query_type=TXT
| stats count by src_ip
| where count>100
```

Microsoft Sentinel (Office spawning PowerShell)

```
DeviceProcessEvents
| where InitiatingProcessFileName in ("WINWORD.EXE","EXCEL.EXE")
| where FileName =~ "powershell.exe"
```

Sentinel (Impossible Travel)

```
SigninLogs
| project UserPrincipalName, IPAddress, TimeGenerated
| extend loc=ipv4_is_private(IPAddress) ? "" :
tostring(parse_json(geo_info_from_ip_address(IPAddress)).country)
| sort by UserPrincipalName, TimeGenerated asc
| extend prevLoc=prev(loc), prevTime=prev(TimeGenerated)
| where prevLoc != "" and loc != "" and prevLoc != loc and datetime_diff('minute',
TimeGenerated, prevTime) < 60
```

3.7 Full Simulation: "Phish → Valid Account → C2 Beacon"

Context

- Organisation: financial services; hybrid SOC (internal L1/L2, external DFIR on retainer).
- Crown jewels: Core banking, payment switch, CFO mailbox.
- Controls: Email gateway, EDR, NDR (Zeek), SIEM, SOAR, MFA on VPN/O365.

T-00:00 — Delivery & Initial Access

- Email Gateway Log
- 2025-09-09T10:12:03Z from="payroll-alerts@micros0ft-support.com"
- to="finance_analyst@corp.local" subject="Payroll Dispute - Action Required"
- verdict=delivered spf=pass dkim=pass url="hxxps://micros0ft-auth[.]io/login"
- User action: Clicks link, enters creds (fake O365).

L1 triage (Detection & Triage)

- SIEM alert: "O365 successful login from unusual location" for finance_analyst.
- Enrich IP: 102.89.22.14 (Geo: Lagos; VT: malicious on 5 engines).
- Check user calendar: not traveling; last usual geo: Kuala Lumpur.
- Decision: Escalate to L2 with enrichment + timeline stub.

T+00:25 — Credential Use & Privilege Attempts

- AzureAD Sign-in Logs
    - Successful login from Nigeria; MFA challenge failed twice (legacy protocol bypass?).
- EDR Telemetry (host: FIN-LAP-022)
- Parent: WINWORD.EXE -> Child: powershell.exe -enc JABsAG8… (Base64)
- File write: %APPDATA%\msedge_update\update.ps1
- Network: 45.77.13.220:443 JA3=72a589da… (rare in org)
- Zeek/JA3: Unseen TLS fingerprint, periodic 60s beacons.

L2 analysis

- Correlate email → proxy → O365 → EDR → NDR.
- MITRE mapping:
  - T1566 Phishing, T1078 Valid Accounts, T1059 PowerShell, T1105 Exfiltration Over C2 Channel.
- Scope: 1 user, 1 workstation, no DC events yet, beacon active.

Containment plan (L2 proposes)

1. Disable finance_analyst account & revoke O365 tokens.
2. EDR isolate FIN-LAP-022.
3. Block IOCs: micros0ft-auth[.]io, IP 45.77.13.220, JA3 fingerprint.
4. Acquire triage artefacts (EDR live response): autoruns, scheduled tasks, suspicious scripts.
5. Search org for same IOCs (proactive sweep).

Approvals

- IR Manager approves immediate actions (Sev-2 elevated to Sev-1 due to beacon + financial data access risk).

T+00:45 — Containment Execution

- SOAR playbook: "Cred Compromise + Beacon"
  - Step 1: Disable user (Graph API) → Success.
  - Step 2: Revoke sessions, force reset → Success.
  - Step 3: EDR isolate host → Success.
  - Step 4: Firewall policy push IOC set → Blocked.
  - Step 5: Notifies IT Helpdesk & Finance Head on isolation impact.

T+01:20 — Eradication & Validation

- L3/DFIR triage on host (remotely)
  - Finds update.ps1 and persistence via HKCU\Software\Microsoft\Windows\CurrentVersion\Run\msedge_update.
  - No evidence of credential dumping or LSASS access.
  - Deletes artefacts, removes autorun, clears scheduled tasks, updates EDR policy to block similar command lines.
- Hunt results (org-wide)
  - No other machines contacting 45.77.13.220.
  - Two users clicked the same phish; one blocked by email sandbox (no credential post).

T+02:30 — Recovery & Monitoring

- Rebuild browser profiles, patch Office, enforce Conditional Access to block legacy auth.
- User re-enabled after password reset and security awareness refresh.
- 48-hour heightened monitoring: no recurrence.

Closure Package

- Executive Summary (1 page)
  - Cause: Phishing → credential reuse; MFA gap via legacy protocol attempt.
  - Impact: 1 workstation isolated; no confirmed data exfiltration.
  - Time to Detect (MTTD): 7 minutes; Time to Contain (MTTC): 45 minutes.
- Technical Appendix
  - Timeline with UTC timestamps, raw log excerpts, IOCs, MITRE table.
  - EDR process tree screenshots; registry artefacts; JA3 hash.
- Lessons Learned
  - Enforce MFA on legacy protocols; Conditional Access by geo + risk.
  - Add SIEM rule: Office app → PowerShell child; block encoded-command by policy.
  - SOAR: auto-disable on confirmed impossible travel + high-risk sign-in.

3.8 What Interviewers Listen For (L1 vs L2)

- L1: fast triage structure, enrichment discipline, when to escalate, documenting false positives cleanly.
- L2: correlation depth, clear containment plans with business impact awareness, mapping to MITRE, crisp comms and updating detections/SOAR.

3.9 Short "Cheat Cards"

L1 Triage 5×5

1. Who/what is impacted?
2. Is it new/rare for this entity?
3. IOC reputation & age?
4. Any chained signals (auth + process + net)?
5. If true, what is the first safe action?

L2 Investigation 6-step
Hypothesis → Collect multi-source logs → Build timeline → Confirm technique(s) → Decide containment → Validate & report.

4. SECURITY LOG SOURCES & MONITORING

4.1 Firewall Logs

- What they capture:
  - Source & destination IP/port, protocol (TCP/UDP/ICMP)
  - Allowed vs denied connections
  - Intrusion prevention (IPS) signatures (if enabled)
  - Volume of connections (possible DDoS indicators)
- Why important in SOC:
  - First line of network defence.
  - Detects port scanning, brute force, malicious outbound traffic (C2 connections).
- Example log:

  2025-09-09T14:12:21Z action=deny src=185.220.101.2 dst=10.1.2.5 s_port=443 d_port=3389 proto=TCP threat="RDP Brute Force Attempt"

  Interpretation: An external IP (Tor exit node) attempted to brute force RDP access.

4.2 Proxy & DNS Logs

- Proxy logs:
  - Track outbound web traffic.
  - Show URL requests, domains, categories (gambling, malware).
  - Detect malicious downloads, phishing, data exfiltration.
- DNS logs:
  - Track domain resolution requests.
  - Catch malware C2 beaconing via domain lookups.
  - Spot anomalies: excessive queries, long/encoded domains.
- Example log (proxy):

  2025-09-09T14:13:45Z user=izzmier src=10.1.3.55 url=http://fakebank-login.com/login
  category=phishing action=allowed

  Interpretation: User izzmier accessed a phishing domain that slipped past filtering.

- Example log (DNS):

  2025-09-09T14:14:05Z client=10.1.3.55 query=asdjkhqwe12345.maliciousc2.com type=A

  Interpretation: Potential DNS tunnelling / malware beacon.

4.3 Endpoint Logs (Sysmon, EDR)

- Sysmon (Windows System Monitor):
    - Detailed process creation logs.
    - File creation, registry changes, network connections.
    - Great for detecting lateral movement and persistence.
- EDR logs (Cortex XDR, CrowdStrike, Defender, Carbon Black):
    - Behavioural detections (e.g., suspicious PowerShell).
    - Host isolation actions.
    - Threat intelligence correlations.
- Example log (Sysmon):
- EventID=1 (Process Create)
- Parent=WINWORD.EXE Child=powershell.exe
- CommandLine="powershell -enc JABzAGM..."

  Interpretation: Word document spawned encoded PowerShell = likely malicious macro.

- Example log (EDR):

  2025-09-09T14:15:33Z alert="Malicious process tree"
  host=FINANCE-PC1 user=izzmier
  process=cmd.exe → powershell.exe → rundll32.exe
  action=isolate_host

  Interpretation: EDR detected malicious process chain and quarantined the host.

4.4 Server / Application Logs

- Windows Event Logs: Authentication (4624, 4625), group membership changes, account lockouts.
- Linux Syslog: SSH attempts, sudo activity, file permission changes.
- Application logs: Database queries, web server access logs, API requests.
- Example log (Windows):

  2025-09-09T14:16:12Z EventID=4625 user=admin
  src=185.220.101.2 logon_type=3 status=failed

  Interpretation: Failed login attempt to admin account from external IP.

  Example log (Linux):

  Sep 09 14:17:03 web01 sshd[2224]: Failed password for root from 185.220.101.2 port 54812 ssh2

Interpretation: Brute force SSH attempt.

4.5 Cloud Logs (AWS, Azure, GCP)

- AWS CloudTrail: Tracks API calls (who did what, from where).
- Azure Activity Logs: Resource changes, identity actions, risky sign-ins.
- GCP Audit Logs: Admin activity, data access, system events.
- Why important: Cloud = shared responsibility. SOC needs to detect:
    - Suspicious API usage (new IAM user created at odd hour).
    - Public exposure (S3 bucket opened).
    - Privilege escalation (role assumption).
- Example log (AWS CloudTrail):

  2025-09-09T14:18:00Z eventName=CreateUser user=unknownIP srcIp=102.89.22.14 userAgent=aws-cli

  Interpretation: Suspicious IAM user creation from Nigeria.

4.6 Email Gateway Logs

- What they capture:
    - Sender, recipient, subject line.
    - Attachment hashes, links clicked.
    - Delivery verdict (allowed, quarantined).
- SOC usage:
    - Detect phishing attempts.
    - Correlate with proxy (did user click?) and auth logs (did attacker log in?).
- Example log:

  2025-09-09T14:19:11Z from="support@microsoft.com.fake" to="finance_analyst@corp.com" subject="Urgent: Password Reset" action=delivered link="hxxp://microsoft365-reset-login.com"

  Interpretation: Phishing attempt bypassed filters.

4.7 Simulation – Multi-Source Log Correlation

Scenario: Phishing → Credential Theft → Lateral Movement Attempt

1. Email Gateway Logs
    - Phishing email delivered to finance_analyst.
    - Subject: “Urgent payroll update”.
    - Contained link: http://payroll-auth365.com/login.
2. Proxy Logs

    - User clicked the link, accessed domain.
    - URL not blocked at time of click.
3. Authentication Logs (O365 / Windows)
    - Successful login from Nigeria minutes later.
    - Event ID 4624 shows login by finance_analyst from external IP.
4. DNS Logs
    - Host started querying suspicious subdomains: asjk12q.maliciousc2.com.
    - Pattern: repeated queries every 60s (possible beacon).
5. EDR Logs (Finance workstation)
    - Word → PowerShell → rundll32 spawned.
    - Suspicious persistence registry key added.
    - Host isolated automatically.
6. Firewall Logs
    - Outbound connection blocked to IP 45.77.13.220.
    - Threat signature: “C2 Traffic.”
7. CloudTrail Logs (AWS)
    - Attempted login to AWS console using compromised credentials.
    - IP matched Nigerian source.

Analyst Workflow

L1 SOC Analyst

- Receives SIEM alert: “Suspicious login from impossible travel.”
- Validates against proxy & email logs.
- Sees correlation: user clicked phishing link earlier.
- Escalates case with enrichment.

L2 SOC Analyst

- Correlates logs: email → proxy → auth → EDR → firewall → cloud.
- Confirms credential theft and active beaconing.
- Actions: disable finance_analyst account, reset password, isolate host, block IOCs.
- Reports: Incident classified as Credential Compromise with Initial Beaconing.

CIA Triad Impact

- Confidentiality: Credentials stolen → sensitive payroll data at risk.
- Integrity: Registry tampering observed on endpoint.
- Availability: Firewall blocked beacon; no outage yet, but high risk.

5. SIEM & ALERT TRIAGE

5.1 Understanding SIEM Rules, Correlation and Dashboards

What is a SIEM?

- Security Information and Event Management (SIEM) collects logs from multiple sources (firewall, EDR, DNS, email, cloud, servers).
- It normalises logs (different formats → one format).
- It applies rules & correlation logic to generate alerts.

SIEM Rules

- Rule types:
  - Threshold rules: e.g., 10 failed logins in 5 minutes.
  - Correlation rules: combine multiple log sources, e.g., failed login → success login from unusual country.
  - Anomaly rules: detect deviations from baseline (UEBA).
  - Watchlist rules: trigger when IOC matches (e.g., known malicious IP).
- Example Splunk Rule:

  ```
  index=auth (EventCode=4625 OR EventCode=4624)
  | stats count(eval(EventCode=4625)) as failed count(eval(EventCode=4624)) as success by user, src_ip
  | where failed>=5 AND success>=1
  ```

  Meaning: Trigger if ≥5 failed logins followed by a success (possible brute force).

Dashboards

- L1 uses dashboards for quick situational awareness:
  - Failed logins by user.
  - Top blocked IPs.
  - Malware alerts by endpoint.
- L2 uses dashboards for trend analysis:
  - Daily increase in phishing attempts.
  - Beacon detection over time.

5.2 Common SIEM Queries

Different SIEM platforms (Splunk, QRadar, ArcSight, Elastic, Sentinel) use different syntax, but the logic is similar.

- Splunk: Search Processing Language (SPL).

- QRadar: AQL (Ariel Query Language).
- ArcSight: ESM correlation rules.
- Elastic: Lucene/KQL.
- Sentinel: KQL (Kusto Query Language).

Examples:

- Detect brute force login (Splunk)

  ```
  index=auth EventCode=4625
  | stats count by user, src_ip
  | where count > 10
  ```

  → 10+ failed logins = brute force attempt.

- Impossible travel (Sentinel)

  ```
  SigninLogs
  | extend location = tostring(parse_json(LocationDetails).countryOrRegion)
  | summarize min(TimeGenerated), max(TimeGenerated) by UserPrincipalName,
  location
  | where count_distinct(location) > 1 and datetime_diff('minute',
  max_TimeGenerated, min_TimeGenerated) < 60
  ```

  → Detects logins from two different countries within <60 mins.

- Suspicious outbound traffic (QRadar)

  ```
  SELECT sourceip, destinationip, COUNT(*) as attempts
  FROM events
  WHERE destinationport=4444
  GROUP BY sourceip, destinationip
  HAVING attempts > 50
  ```

  → 50+ outbound attempts to known C2 port.

5.3 IOC & IOA Correlation

- IOC (Indicator of Compromise): tangible evidence of malicious activity.
  - Examples: malicious IP, hash of malware file, phishing domain.
  - SIEM checks logs against watchlists (e.g., VirusTotal feed).
- IOA (Indicator of Attack): behavioural sign an attack is in progress.
  - Examples: PowerShell spawning from Word, lateral movement patterns, credential dumping.

    - More proactive → used for detection engineering.

SOC Example:

- IOC: Alert triggers when outbound connection goes to 185.220.101.2 (Tor exit node).
- IOA: Alert triggers when process WINWORD.EXE → POWERSHELL.EXE (malicious macro behaviour).

5.4 Alert Severity Categorisation

High Severity

- Confirmed malicious activity targeting critical assets.
- Examples: successful login from known malicious IP, ransomware file encryption detected.
- Response: immediate escalation & containment.

Medium Severity

- Suspicious but not confirmed malicious. Needs further investigation.
- Examples: unusual DNS queries, possible beaconing, multiple failed logins.
- Response: deeper triage by L2.

Low Severity

- Informational alerts, possible policy violations or noisy detections.
- Examples: single port scan, user typing wrong password.
- Response: monitor/close as false positive.

SOC Tip: During interview, always explain severity → "I would categorise this as High because it involves confirmed credential use from a malicious IP, which could lead to privilege escalation."

5.5 Common SIEM Use Cases

Brute Force Login

- Logs: Multiple 4625 (failed logon), followed by 4624 (success).
- Detection: Threshold rule (≥5 fails then success).
- Example attack: SSH brute force on Linux servers.

Multiple Failed Logins

- Logs: Spikes of failed logins for multiple accounts.

- Detection: “Spray & pray” password attacks.

Suspicious Outbound Traffic

- Logs: Firewall shows connections to non-standard ports or blacklisted IPs.
- Detection: Possible C2 beacon or data exfiltration.

File Hash Matches

- Logs: EDR detects file execution with hash matching known malware.
- Detection: Automatic match via threat intel feeds.

5.6 Simulation – SIEM Alert Triage in Action

Scenario: Suspicious Login & Outbound Traffic

1. Alert Triggered (SIEM)
    - Rule: “Multiple failed logins followed by success.”
    - Alert details:
        - User: finance_admin
        - Failed attempts: 8
        - Success login: from IP 185.220.101.2 (flagged in threat intel as Tor node).
2. L1 Analyst Actions
    - Opens ticket, validates alert.
    - Cross-checks IP in VirusTotal → confirmed malicious.
    - Reviews firewall logs → same IP attempting RDP connections to other servers.
    - Categorises severity: High (confirmed successful login from malicious IP).
    - Escalates to L2 with enrichment.
3. L2 Analyst Actions
    - Correlates across logs:
        - Auth logs: login succeeded for finance_admin.
        - EDR logs: suspicious PowerShell spawned.
        - DNS logs: unusual queries to abcd123.maliciousc2.com.
    - MITRE ATT&CK mapping:
        - T1078 (Valid Accounts)
        - T1059 (Command-Line Execution)
        - T1071 (Application Layer Protocol – beaconing)
    - Containment steps:
        - Disable finance_admin account.
        - Isolate affected workstation.
        - Block Tor exit IP on firewall.
        - Sweep environment for same IOC.

4. Closure
    - Incident classified as Credential Compromise + C2 Communication Attempt.
    - Report highlights need for stronger MFA & geo-blocking.
    - New SIEM rule added: “Impossible travel + IOC match = auto-disable account (SOAR integration).”

6. INCIDENT RESPONSE PROCESS

6.1 NIST SP 800-61 Phases (Computer Security Incident Handling Guide)

The NIST SP 800-61 Rev.2 is the gold standard for IR. It defines five phases:

1) Preparation

- Goal: Be ready before an incident happens.
- Activities:
    - Documented playbooks (phishing, malware, ransomware).
    - Tools: SIEM, EDR, SOAR, ticketing system.
    - Access: Ensure SOC has privilege to isolate hosts, reset passwords, block IPs.
    - Training: Regular tabletop exercises and red team simulations.

Example: SOC has a playbook for "Phishing → Credential Compromise" that defines who to notify, how to reset accounts and what logs to pull.

2) Detection & Analysis

- Goal: Identify, verify and understand the incident.
- Activities:
    - Monitor SIEM/EDR alerts.
    - Validate true vs false positives.
    - Collect IOCs (IPs, domains, hashes).
    - Build a timeline of activity.
- SOC Context:
    - L1 = first validation & enrichment.
    - L2 = correlation across multiple logs + root cause.

Example: SIEM alert shows suspicious login from Nigeria; analyst checks if user is traveling → no → confirms anomaly.

3) Containment

- Goal: Stop the attacker without causing unnecessary business disruption.
- Approaches:
    - Short-term: Isolate endpoint, disable user, block IP.
    - Long-term: Apply patch, segmentation, new firewall rule.
- Balance: Contain without tipping off attacker too early (important for stealth APT cases).

Example: Isolate a workstation infected with ransomware before it encrypts shared drives.

4) Eradication & Recovery

- Eradication: Remove the threat (delete malware, close backdoors, remove persistence).
- Recovery: Restore systems to business as usual.
    - Reset passwords, rebuild machines, restore data from backup.
    - Continuous monitoring for recurrence.

Example: Remove malicious registry keys, reinstall OS, re-onboard into domain, validate logs.

5) Lessons Learned

- Goal: Improve security posture for next time.
- Activities:
    - Post-incident review (PIR).
    - Update SIEM rules and playbooks.
    - Awareness training for users.
    - Metrics: MTTD (Mean Time to Detect), MTTR (Mean Time to Respond).

Example: After phishing incident, company enforces MFA and updates SIEM rules for impossible travel.

6.2 SANS Incident Handler's Handbook Steps

SANS defines a 6-step process, similar but more granular:

1. Preparation (same as NIST)
2. Identification (detect abnormal event, verify as incident)
3. Containment (short-term & long-term)
4. Eradication (remove root cause, e.g., malware, accounts)
5. Recovery (bring systems back, monitor carefully)
6. Lessons Learned (PIR, improve defences)

This complements NIST and is often used by SOCs for training.

6.3 Escalation Workflows (L1 → L2 → L3)

L1 SOC Analyst Escalates When:

- IOC matches confirmed threat intel (e.g., ransomware hash).
- Alert involves privileged account or critical system.
- Multiple log sources show related suspicious activity.
- Not enough context/log access for deeper investigation.

L2 SOC Analyst Escalates When:

- Incident shows active lateral movement.
- Malware sample requires reverse engineering.
- Widespread compromise across multiple systems.
- Business impact requires executive awareness (CISO, IR Manager).

Example:

- L1 detects “multiple failed logins + success.” Escalates to L2.
- L2 confirms C2 traffic + persistence registry key. Escalates to L3 for forensic memory dump.

6.4 Practical Actions in IR

- Account Lockout / Password Reset
  - Disable compromised accounts.
  - Force password resets with MFA enforcement.
  - SOC triggers via Active Directory or AzureAD APIs.
- Endpoint Isolation
  - Quarantine infected host using EDR (CrowdStrike “Contain”, Cortex XDR “Isolate”).
  - Ensures malware cannot spread laterally.
- Blocking IP / Domain / URL
  - Firewall rules or SOAR automation.
  - Proxy block for malicious domains.
  - Cloud blocklist for suspicious IPs.
- Malware Analysis Referral
  - If suspicious binary detected, refer to malware analysts (sandbox, reverse engineering).
  - Provides insight for IOC generation & detection updates.

6.5 Simulation – Incident Response End-to-End

Scenario: Ransomware Infection in Finance Department

1) Preparation

- SOC has ransomware playbook.
- EDR agent deployed on all endpoints.
- Backups tested weekly.

2) Detection & Analysis

- Alert (SIEM): EDR detects unusual file modifications + ransom note.
- Firewall logs: Outbound traffic to known ransomware C2 IP 45.77.13.220.
- Sysmon log: explorer.exe spawning powershell.exe -enc ... → file encryption script.
- DNS logs: Host queries ransomc2.malicious.com.

L1 Actions:

- Validates alert (multiple IOC matches).
- Enriches IP in VirusTotal → flagged ransomware C2.
- Escalates to L2 as High Severity – Ransomware Infection.

3) Containment

L2 Actions:

- Confirms encryption in process (file extensions changed to .locked).
- Initiates endpoint isolation via EDR.
- Disables user account finance_user1.
- Blocks 45.77.13.220 and ransomc2.malicious.com in firewall/proxy.
- Communicates with IT Ops to disconnect network shares.

4) Eradication & Recovery

- Eradication:
  - Malware binary removed.
  - Persistence registry keys deleted.
  - IOC sweep confirms no other infections.
- Recovery:
  - Restore encrypted files from backup.
  - Re-image affected machine.
  - Reset user's AD password + enforce MFA.

5) Lessons Learned

- Root Cause: User opened phishing email attachment (invoice.docm).
- MITRE Mapping:
  - T1566 (Phishing),
  - T1059 (Command Execution – PowerShell),
  - T1486 (Data Encrypted for Impact).
- Gaps Identified:
  - Email gateway didn't block .docm attachment.
  - No geo-blocking for outbound to unusual IPs.
- Improvements:
  - Ban Office macros by policy.

    - Update SIEM rules for macro-based PowerShell execution.
    - Conduct phishing awareness training.

6.6 Interviewer "Listen For" Signals

When answering IR questions, show:

- Structured approach → "First, I prepare… then detect… then contain…"
- Clear escalation points → "As L1, I escalate when IOC is confirmed or critical accounts are affected."
- Practical actions → "I would isolate endpoint, disable account and block IPs immediately."
- Business awareness → "Containment should not impact critical services unless absolutely necessary."
- Framework reference → "I follow NIST SP 800-61 and SANS steps."

7. THREAT INTELLIGENCE & HUNTING

7.1 Using Threat Intelligence (TI) Feeds

Threat Intelligence (TI) helps SOC analysts enrich alerts, confirm IOCs and predict attacker moves.

Key TI Sources & Use Cases

- VirusTotal
  - Checks file hashes, URLs and domains against 70+ antivirus engines.
  - Used by L1 during triage: confirm if file hash is known malware.
  - Example: SHA256 hash of suspicious EXE shows as “Emotet Trojan” on 50 engines.
- AbuseIPDB
  - Database of malicious IPs (botnets, brute force sources).
  - SOC uses it to validate login attempts from external IPs.
  - Example: IP flagged in >200 reports for SSH brute force attempts.
- AlienVault OTX (Open Threat Exchange)
  - Community-driven intelligence on campaigns & IOCs.
  - Useful for L2: correlation of domains with known threat actor campaigns.
  - Example: IOC from OTX linked to TA505 phishing campaign.
- BrightCloud / Commercial TI feeds
  - Provide categorisation of domains (malware, phishing, botnet).
  - Often integrated directly into SIEM, firewall or EDR.
  - Example: Proxy log shows connection to “Newly Registered Domain (NRD)” flagged malicious in BrightCloud.

7.2 Understanding TTPs with MITRE ATT&CK

- TTPs = Tactics, Techniques, Procedures
  - Tactics = attacker goals (e.g., Persistence, Exfiltration).
  - Techniques = general methods (e.g., T1059 – Command-Line Execution).
  - Procedures = exact commands/scripts attackers use.
- Why it matters in SOC
  - IOC-based detection = reactive (bad IP/file).
  - TTP-based detection = proactive (behaviour → detect even if IOC changes).

Example

- IOC detection: Alert on malware.exe hash.
- TTP detection: Alert on “Word spawning PowerShell with encoded command” (works even if hash changes).

SOC usage:

- L1 checks if IOC matches TI feeds.
- L2 maps activity to MITRE ATT&CK → builds better hunting queries.
- L3 uses ATT&CK matrix to prioritise coverage and detection engineering.

7.3 Threat Hunting Basics

What is Threat Hunting?

- Proactive search through logs/data to find threats not yet detected by SIEM alerts.
- Complements detection rules.
- Often hypothesis-driven.

Threat Hunting Methodology

1. Form a Hypothesis
    - Based on intel, reports or suspicious trends.
    - Example: "Attackers often use PowerShell with Base64 encoding for persistence."
2. Collect & Query Data
    - Pull logs from SIEM, EDR, DNS, firewall.
    - Build queries based on hypothesis.
3. Identify Anomalies
    - Look for rare behaviours, unusual process chains, strange network connections.
4. Investigate & Validate
    - Enrich anomalies with TI feeds.
    - Escalate if confirmed malicious.
5. Document & Improve
    - Update SIEM rules.
    - Add new IOCs to blocklists.
    - Share findings with wider team.

7.4 Practical Examples of Hunting Queries

- Hunt for PowerShell with Encoded Command (Splunk)

  ```
  index=windows EventCode=4688
  | search NewProcessName="*powershell.exe*" CommandLine="* -enc *"
  ```

  → Finds PowerShell launched with encoded script, common in malware.

- Hunt for DNS Tunnelling (Elastic/KQL)

dns.question.name: /[a-z0-9]{30,}\.com/

→ Finds suspiciously long domain queries (possible tunnelling).

- Hunt for Rare External Connections (Sentinel KQL)

  DeviceNetworkEvents
  | summarize count() by RemoteIP
  | where count_ < 5

  → Finds IPs only contacted by one host = potential beaconing.

7.5 Simulation – Threat Intel & Hunting in Action

Scenario: Beaconing from Compromised Workstation

Step 1 – TI Trigger (IOC)

- EDR alert: powershell.exe -enc JABzAGM… running on user HR-PC01.
- File hash checked in VirusTotal → flagged as "AgentTesla Trojan."
- Proxy logs: Outbound traffic to newdomain123.info.
- BrightCloud categorises as Newly Registered Domain (NRD).

Step 2 – L1 Actions

- Triages alert, confirms IOC match.
- Escalates to L2: "Malicious PowerShell execution, IOC confirmed in VirusTotal, suspicious outbound domain."

Step 3 – L2 Hunting (IOA/TTP Focus)

- Hypothesis: If one host is beaconing to NRD, others may be too.
- Builds hunting query in SIEM:
- index=proxy url_domain=newdomain123.info OR category="Newly Registered Domain"
- | stats count by src_ip, user
- Finds 3 more hosts contacting NRDs with suspicious patterns.
- Uses MITRE ATT&CK mapping:
  - T1059 (Command-Line Execution)
  - T1071 (Application Layer C2)
  - T1568.002 (Dynamic Resolution – DNS for C2)

Step 4 – Containment & Response

- Isolate 4 affected endpoints via EDR.
- Block newdomain123.info at firewall/proxy.
- Reset credentials for compromised users.
- Send malware sample to malware analysis team.

Step 5 – Lessons Learned & Improvement

- Add SIEM rule: “PowerShell with Base64 encoding → High Severity.”
- Subscribe to more TI feeds focusing on Newly Registered Domains.
- Schedule weekly hunts for DNS tunnelling + rare domains.

7.6 Interview “Listen-For” Points

- Show awareness of both IOC (short-term detection) and IOA/TTP (long-term hunting).
- Mention specific TI feeds you’ve used.
- Explain how hunting queries are hypothesis-driven.
- Tie findings back to MITRE ATT&CK.
- Emphasise that hunting results must lead to detection improvements.

8. HANDS-ON TECHNICAL AREAS

8.1 Packet Analysis (Wireshark Basics)

Wireshark is a network protocol analyser. SOC analysts often use it for:

- Verifying suspicious traffic (C2, data exfiltration).
- Identifying malware communication patterns.
- Reconstructing sessions (HTTP, FTP, DNS).

Key Skills

- Filtering traffic
    - ip.addr == 192.168.1.10 → filter traffic from one host.
    - http.request → show only HTTP GET/POST requests.
    - dns.qry.name contains "malicious.com" → filter malicious DNS.
- Spotting anomalies
    - Large outbound connections at odd hours → possible data exfil.
    - DNS queries with long, random subdomains → DNS tunnelling.
    - TLS connections with strange JA3 fingerprints → C2 activity.

Example:

Frame 1542: 1800 bytes on wire
Src: 192.168.1.25 → Dst: 45.77.13.220
Protocol: TCP, Port: 443
Note: JA3 fingerprint “72a589da…” not seen before in environment

Interpretation: Suspicious encrypted traffic (potential beacon).

8.2 Log Parsing & Regex Familiarity

Logs often need parsing and searching quickly. Regex is essential.

Common Regex for SOC Work

- Extract IP: ([0-9]{1,3}\.){3}[0-9]{1,3}
- Extract email: [a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-z]{2,}
- Extract URL: https?:\/\/[^\s]+

Use Cases

- Searching through raw firewall logs for IPs.
- Extracting suspicious email addresses from phishing logs.

- Filtering DNS logs for unusual domains.

Example Log (proxy)

2025-09-09 14:22:01 user=izzmier src=10.1.3.55 url=http://malicious-domain.com/download.exe

- Regex extract domain → malicious-domain.com
- Regex extract file → download.exe

8.3 Query Building in SIEM

Every SIEM has its own query language. Analysts must pull evidence and hunt efficiently.

Splunk Example – Find Multiple Failed Logins

```
index=auth EventCode=4625
| stats count by user, src_ip
| where count > 10
```

Sentinel Example – Detect Office Spawning PowerShell

```
DeviceProcessEvents
| where InitiatingProcessFileName in ("WINWORD.EXE","EXCEL.EXE")
| where FileName == "powershell.exe"
```

QRadar Example – SSH Brute Force

```
SELECT sourceip, destinationip, COUNT(*) as attempts
FROM events
WHERE destinationport=22
GROUP BY sourceip, destinationip
HAVING attempts > 20
```

SOC Tip: Always explain why you query:

- "I'd run this query to see if the same source IP attempted SSH brute force across multiple hosts."

8.4 Malware Sandboxing Overview (Any.Run, Hybrid Analysis)

When suspicious files are detected, sandboxing is used to:

- Run malware safely in an isolated environment.

- Observe behaviour (processes, network traffic, file system changes).
- Generate IOCs (hashes, domains, registry keys).

Tools

- Any.Run (interactive, can watch malware run step-by-step).
- Hybrid Analysis (static + dynamic report, community driven).
- Cuckoo Sandbox (open-source, customisable).

SOC Workflow

- L1 finds suspicious attachment.
- L2 submits hash/file to Any.Run.
- Malware attempts to contact c2.malicious.net.
- IOC added to SIEM & firewall blocklists.

8.5 Hashing & File Analysis (MD5/SHA256)

Hashes = digital fingerprints of files.

- MD5: Fast but weak (collisions possible).
- SHA256: Stronger, standard for malware analysis.

SOC Uses

- Verify if suspicious file is known malware.
- Compare against TI feeds (VirusTotal).
- Detect file tampering (integrity check).

Example

File: invoice.docm
MD5: 5d41402abc4b2a76b9719d911017c592
SHA256: 2c26b46b68ffc68ff99b453c1d30413413422d706483bfa0f98a5e886266e7ae

- Upload hash to VirusTotal → detected as Emotet malware.

8.6 Full Simulation – Hands-On Investigation

Scenario: Suspicious Email Attachment Leads to Malware Execution

Step 1 – Email Gateway Log

2025-09-09T14:30:21Z from="support@banking-help.com"

to="finance_user@corp.com" subject="Invoice Attached"
attachment="invoice.docm"

Step 2 – Proxy Log

2025-09-09T14:31:02Z user=finance_user url=http://malicious-bank.com/payload.exe

Step 3 – EDR Alert

WINWORD.EXE → POWERSHELL.EXE -enc JABzAGM...
Child process created rundll32.exe

Step 4 – Sandbox Analysis (Any.Run)

- File invoice.docm drops payload.exe.
- Connects to domain: c2.malicious.net.
- Writes registry key for persistence.

Step 5 – Wireshark Capture

- Outbound TCP 443 to 45.77.13.220.
- JA3 fingerprint = uncommon in org.
- Traffic every 60 seconds (beaconing).

Step 6 – Hash Check

- SHA256 hash of payload.exe matches ransomware in VirusTotal.

Analyst Workflow

L1 Actions

- Validates SIEM alert: “Suspicious process spawn.”
- Enriches hash in VirusTotal (confirmed ransomware).
- Escalates to L2 with IOC package.

L2 Actions

- Runs packet capture in Wireshark → confirms beaconing.
- Uploads malware to Any.Run → confirms persistence behaviour.
- Correlates logs: email → proxy → EDR → network.
- Containment: isolate endpoint, disable finance_user account, block C2 domain & IP.

Result

- Incident classified as Ransomware Delivery Attempt via Phishing Email.
- MITRE ATT&CK mapping:
    - T1566 (Phishing),
    - T1059 (Command Execution – PowerShell),
    - T1105 (Exfiltration Over C2 Channel).
- Lessons Learned: block .docm attachments, enhance SIEM rule for Word spawning PowerShell.

8.7 Interviewer "Listen-For" Cues

- Do you know how to read packet captures and spot anomalies?
- Can you parse logs with regex and build queries in SIEM?
- Do you understand how to sandbox malware and extract IOCs?
- Do you know the difference between MD5 and SHA256 and when to use them?
- Can you walk through a simulation end-to-end instead of stopping at "alert seen"?

9. COMPLIANCE & GOVERNANCE KNOWLEDGE

9.1 General Security Frameworks

ISO 27001 (Information Security Management System – ISMS)

- Purpose: Provides a framework for managing information security risks.
- SOC Relevance:
  - Log monitoring & retention are part of ISO 27001 Annex A.
  - SOC must generate audit trails for access to critical systems.
- Example: SOC ensures failed login attempts are logged & reviewed, supporting ISO 27001 control A.12.4 – Logging and monitoring.

NIST Cybersecurity Framework (CSF)

- Five Functions: Identify, Protect, Detect, Respond, Recover.
- SOC Relevance:
  - Detect → SIEM monitoring, anomaly detection.
  - Respond → SOC incident handling aligns with IR processes.
- Example: During a ransomware incident, SOC follows NIST CSF phases (Detect → Respond → Recover).

CIS Controls (formerly SANS Top 20 Critical Security Controls)

- Purpose: Prioritised security controls (basic hygiene to advanced defence).
- SOC Relevance:
  - Control 8: Audit Log Management → SOC responsibility.
  - Control 13: Network Monitoring → SOC correlation rules.
- Example: SOC ensures logs from EDR and firewalls are centralised, satisfying CIS Control 8.

9.2 Malaysia-Specific Regulations

PDPA (Personal Data Protection Act 2010)

- Governs how organisations in Malaysia collect, store and process personal data.
- SOC Relevance:
  - Alerts involving unauthorised access to personal data must be flagged.
  - Log monitoring must support forensic review in case of data breach.
- Example: If a compromised account exfiltrates customer IC numbers, SOC triggers incident classification as PDPA breach.

BNM RMiT (Bank Negara Malaysia – Risk Management in Technology, 2020)

- Applies to: Financial institutions in Malaysia.
- SOC Relevance:
    - Section 10.9: Continuous security monitoring.
    - Section 10.11: Real-time detection and response capability.
    - SOC must demonstrate 24×7 monitoring with reporting to BNM on major incidents.
- Example: SOC escalates confirmed malware activity to the Incident Response Manager, who then reports within regulatory timelines to BNM.

NACSA (National Cyber Security Agency) Guidelines

- Purpose: Strengthen Malaysia's cyber resilience.
- SOC Relevance:
    - Guidelines for log retention, incident reporting, cyber drill participation.
    - SOC must align incident reporting with NACSA's Critical National Information Infrastructure (CNII) requirements.
- Example: SOC detecting APT activity on a government system must notify NACSA within required timeframes.

GPIS (Guideline on Payment Instruments & Systems – Bank Negara Malaysia)

- Applies to: Payment providers, e-wallets, financial systems.
- SOC Relevance:
    - Ensures payment systems are monitored for fraud & cyberattacks.
    - Requires secure authentication and continuous monitoring of access logs.
- Example: SOC detects multiple failed transactions from unusual IPs → flagged as suspicious under GPIS monitoring.

9.3 GDPR (General Data Protection Regulation – EU)

- Applies to: Any organisation processing EU citizens' data.
- SOC Relevance:
    - Breach notification required within 72 hours to regulators.
    - SOC must have evidence from logs to support reporting.
- Example: If a Malaysian bank handles EU customer accounts, a SOC-detected breach involving data exfiltration requires GDPR-compliant reporting.

9.4 Simulation – SOC in a Compliance Context

Scenario: Data Exfiltration Attempt in a Malaysian Bank

Step 1 – SIEM Alert

- Alert: “Unusual outbound traffic from DB server (10.10.5.22) to unknown IP 185.45.13.77.”
- Firewall logs: 500MB transferred in 10 minutes.
- Proxy logs: IP categorised as “Malicious / Unknown.”

Step 2 – L1 Actions

- Validates alert with VirusTotal (IP flagged).
- Checks database server criticality (contains customer PII).
- Escalates to L2 with High Severity – Possible Data Exfiltration.

Step 3 – L2 Actions

- Correlates logs:
  - DB logs show SELECT * FROM customer_data query executed by user admin01.
  - Authentication logs: admin01 logged in from unusual VPN endpoint.
- MITRE Mapping:
  - T1078 (Valid Accounts)
  - T1041 (Exfiltration over C2 Channel).
- Containment: disables admin01 account, isolates DB server from external network, blocks outbound IP.

Step 4 – Compliance Triggers

- Incident involves personal data → triggers PDPA requirements.
- Because bank is under BNM RMiT, incident must be reported within regulatory timeframe.
- If EU customers were affected, GDPR breach notification within 72 hours applies.

Step 5 – Eradication & Recovery

- Forensics confirms compromised admin account used.
- Malware sample submitted to NACSA for analysis (as per CNII reporting requirement).
- Restore DB from clean backup.
- Strengthen access controls (MFA for DB admins).

Step 6 – Lessons Learned

- Root Cause: Phishing email led to credential theft of admin01.
- Compliance Outcomes:
  - SOC report shared with BNM as part of monthly RMiT compliance audit.
  - Breach recorded in PDPA compliance log.

    - EU regulator notified (GDPR).
- Improvements:
    - SIEM rule for “large outbound transfer from DB server.”
    - Awareness campaign for admins.

9.5 Interview “Listen-For” Signals

- You know which frameworks apply where (e.g., ISO 27001 global vs PDPA Malaysia-specific).
- You can link SOC work (log monitoring, IR, escalation) to compliance requirements.
- You can demonstrate how compliance affects reporting timelines (BNM RMiT, GDPR 72h).
- You balance technical & regulatory language — showing you can brief both IT and compliance teams.

10. COMMON INTERVIEW QUESTIONS

10.1 General Knowledge

Q1: Explain the CIA Triad with examples.

Answer Framework

- Confidentiality: Preventing unauthorised access to sensitive data.
    - Example: Encrypting customer credit card details in a database.
- Integrity: Ensuring data is accurate and unchanged.
    - Example: File hashing to verify logs weren't tampered with.
- Availability: Ensuring systems are accessible when needed.
    - Example: Using redundant firewalls and DDoS protection.

Mini-Simulation

- SIEM alert shows unauthorised DB query exporting customer IC numbers.
- CIA Impact:
    - Confidentiality = breached (PII accessed).
    - Integrity = logs intact, no tampering.
    - Availability = DB still online.
- Escalation: Report as Confidentiality Incident under PDPA Malaysia.

Q2: What is the difference between IDS and IPS?

Answer Framework

- IDS (Intrusion Detection System) = detects and alerts (passive).
- IPS (Intrusion Prevention System) = detects and blocks (active).
- IDS is like a CCTV camera (records activity), IPS is like a security guard (stops intruder at the door).

Mini-Simulation

- IDS: Detects port scanning activity from IP 185.220.101.2 → SOC analyst receives alert.
- IPS: Actively blocks that IP after multiple failed RDP attempts.

Q3: How does DNS work?

Answer Framework

- DNS = "phonebook of the internet." Converts domain names → IP addresses.

- Process:
    1. User types www.bank.com.
    2. Request goes to local DNS resolver.
    3. Resolver queries root, TLD, authoritative DNS servers.
    4. Returns IP (e.g., 192.168.10.25).
- SOC Importance: DNS often abused for phishing (fake domains) and C2 (beaconing, DNS tunneling).

Mini-Simulation

- DNS log shows host HR-PC1 querying x9adfh28sh.maliciousc2.com every 60 seconds.
- Analyst conclusion: Likely malware beaconing via DNS.

10.2 Technical

Q4: Analyse a brute force login alert. What steps do you take?

Answer Framework

1. Validate alert: Is it multiple failed logins from one IP?
2. Check logs: Windows EventID 4625 (failed) and 4624 (success).
3. Enrich IP: Threat intel lookup (AbuseIPDB, VirusTotal).
4. Check user impact: Is it admin or privileged account?
5. Action: Block IP if malicious, force password reset if compromise confirmed.

Mini-Simulation

- SIEM shows 50 failed SSH logins from 102.89.22.14 in 10 mins, then success for root.
- AbuseIPDB: IP flagged for brute force.
- Containment: Block IP at firewall, reset root password, check for lateral movement.

Q5: You see unusual outbound traffic to an unknown IP. What's your workflow?

Answer Framework

1. Identify the host making the connection.
2. Check logs: firewall, proxy, EDR.
3. Enrich IP in TI feeds.
4. Check process tree (was it PowerShell? Browser?).
5. Decide severity: Beaconing? Exfiltration?
6. Contain if confirmed malicious (isolate host, block IP).

Mini-Simulation

- Firewall log: Finance-PC1 → 45.77.13.220:443 every 60s.
- EDR log: powershell.exe -enc … executed from Word.
- VirusTotal: IP flagged as C2.
- Action: Isolate Finance-PC1, disable user, block IP.

Q6: SIEM shows repeated failed logins followed by a success. What do you do?

Answer Framework

1. Check user context: normal or privileged account?
2. Check login geo/time: impossible travel? abnormal hour?
3. Correlate with threat intel: IP malicious?
4. Containment: reset password, force MFA re-enrollment, monitor other accounts.

Mini-Simulation

- User finance_admin: 12 failed logins, then success from Nigeria.
- Geo-IP: normal logins always from Kuala Lumpur.
- VirusTotal: IP flagged as Tor exit node.
- Containment: Disable account, reset password, block Tor IPs.

10.3 Scenario-Based

Q7: A user reports a phishing email. Walk through your response.

Answer Framework

1. Collect evidence: email headers, links, attachments.
2. Analyse indicators: domain reputation, hash attachments.
3. Check SIEM: did anyone else receive/click?
4. Contain: quarantine emails, block domain.
5. Eradication: reset creds if user clicked.
6. Report: Document incident, update phishing playbook.

Mini-Simulation

- Email: “Reset Microsoft 365 password now” → link http://ms365-reset.com.
- DNS log: HR-PC2 queried domain.
- Auth log: login success from Nigeria.
- SOC Action: Reset HR-PC2 user’s password, block domain, notify users, update awareness training.

Q8: You detect malware beaconing to a C2 server. What actions will you take?

Answer Framework

1. Validate beacon: frequency, destination.
2. Correlate with host logs: which process initiated connection?
3. Enrich IOC: IP/domain reputation.
4. Contain: isolate endpoint, block IP/domain.
5. Investigate spread: search SIEM for same IOC across environment.
6. Report: Document attack chain (MITRE mapping).

Mini-Simulation

- NDR: Host IT-PC1 connecting every 60s to c2.evilhost.net.
- EDR: Process = powershell.exe spawned from Word.
- VirusTotal: Domain linked to AgentTesla C2.
- SOC Action: Isolate IT-PC1, block domain, scan for persistence, sweep logs for other infected hosts.

10.4 Soft Skills / Behavioural

Q9: How do you prioritise multiple alerts?

Answer Framework

- Use severity + impact + likelihood.
- Prioritise:
    1. Confirmed malicious on critical system (High).
    2. Suspicious but needs investigation (Medium).
    3. Noise/false positives (Low).

Mini-Simulation

- Alert A: Malware hash detected on CEO's laptop. (High Priority)
- Alert B: 20 failed logins on test server. (Medium Priority)
- Alert C: Port scan on unused subnet. (Low Priority)
- Analyst: Focus on Alert A first, escalate immediately.

Q10: How do you handle shift handover?

Answer Framework

- Clear documentation of open incidents.
- Update ticketing system with evidence collected.

- Verbal/virtual briefing with incoming analyst.
- Highlight pending actions and severity.

Mini-Simulation

- Outgoing L1: “Currently investigating phishing emails targeting Finance. 2 users clicked, creds reset. Still checking logs for lateral movement. Please continue search for related domains.”

Q11: Tell me about a time you worked under pressure.

Answer Framework

- Use STAR method (Situation, Task, Action, Result).
- Example:
    - Situation: During shift, SOC received ransomware alert.
    - Task: I had to confirm and escalate within minutes.
    - Action: Validated IOC, isolated endpoint, escalated to L2.
    - Result: Attack contained before spreading to shared drives.

10.5 Key Interview Tip

When answering:

- Always structure (step-by-step thinking).
- Map to frameworks (MITRE, NIST, SANS).
- Give practical examples (logs, actions).
- Show communication skills (explain to non-technical audience if asked).

11. TOOLS TO REVISE & PRACTISE

11.1 SIEM Platforms

Splunk

- Strengths: Flexible search language (SPL), strong dashboards, widely used in enterprises.
- Interview Tip: Expect to write or interpret SPL queries.
- Example Query – Brute Force Login:
- index=auth EventCode=4625
- | stats count by user, src_ip
- | where count > 10

  → Finds users with 10+ failed logins.

IBM QRadar

- Strengths: Prebuilt correlation rules, strong compliance focus.
- Query Language: AQL (Ariel Query Language).
- Example – Detect RDP Brute Force:
- SELECT sourceip, destinationip, COUNT(*) as attempts
- FROM events
- WHERE destinationport=3389
- GROUP BY sourceip, destinationip
- HAVING attempts > 20

Elastic (ELK)

- Strengths: Open-source, fast searching, widely used in startups.
- Query Language: Lucene/KQL.
- Example Query – DNS Tunneling Detection:
- dns.question.name: /[a-z0-9]{25,}\.com/

  → Finds suspiciously long DNS queries.

Microsoft Sentinel

- Strengths: Cloud-native, integrates with Azure AD, Office 365, Defender.
- Query Language: KQL (Kusto).
- Example Query – Impossible Travel:
- SigninLogs
- | summarize min(TimeGenerated), max(TimeGenerated) by UserPrincipalName, Location

- | where datetime_diff('minute', max_TimeGenerated, min_TimeGenerated) < 60

  → Detects logins from two countries within 60 minutes.

11.2 Endpoint Detection & Response (EDR)

CrowdStrike Falcon

- Detects malware, suspicious processes, lateral movement.
- Can isolate host remotely.
- Example: Alert – "WINWORD.EXE → POWERSHELL.EXE → rundll32.exe" = malicious macro.

VMware Carbon Black

- Strong behavioural detection.
- Focuses on endpoint visibility and process lineage.

Palo Alto Cortex XDR

- Combines EDR + NDR + cloud telemetry.
- Integrates well with Palo Alto firewalls & SOAR.

SOC Usage:

- L1 confirms if detection is malicious.
- L2 analyses process trees, checks persistence.
- Actions: Isolate host, kill process, block hash.

11.3 Threat Intelligence Tools

VirusTotal

- Submit hash, domain or IP → get multi-engine verdict.
- Example: Hash of suspicious EXE = flagged by 45/70 engines.

AlienVault OTX

- Community-based TI platform.
- Provides "pulses" (IOCs linked to campaigns).

ThreatMiner

- Search malware families, domains, relationships.

- Used by L2 to connect an IOC to a broader campaign.

11.4 Packet / Log Analysis Tools

Wireshark

- Analyse PCAPs for anomalies.
- SOC use: confirm beaconing, data exfil, malware C2.
- Example Filter:
- dns.qry.name contains "malicious.com"

  → Detects DNS queries to malicious domain.

Sysmon

- Windows logging tool.
- Captures process creation, network connections, registry changes.
- Example:
- EventID=1 Process Create
- Parent=WINWORD.EXE
- Child=POWERSHELL.EXE

  → Suspicious macro behaviour.

Zeek (formerly Bro)

- Network traffic analysis.
- Produces logs (conn.log, dns.log, http.log).
- Example:
- 09/09/25 14:22:11 192.168.10.25 → 185.45.13.77
- protocol=SSL JA3=72a589da… (rare fingerprint)

  → Possible C2 traffic.

11.5 Labs & Practice Platforms

TryHackMe

- Offers Blue Team labs: SOC investigations, Splunk basics, Wireshark PCAPs.
- Example: “Threat Hunting with Splunk” room.

HackTheBox (Blue Team)

- Provides SOC-oriented challenges (“Detection Labs,” “Attack/Defend”).

CyberDefenders

- Platform with real-world blue team challenges.
- Example: “PCAP Analysis” challenge where you detect beaconing.

SOC Interview Tip: Always mention you practise on these platforms — it shows passion + initiative.

11.6 Simulation – SOC Tools in Action

Scenario: Suspicious Phishing Email Leads to Malware Beacon

Step 1 – SIEM (Splunk)

- Alert: “Multiple failed logins followed by success – User: finance_admin.”
- SPL Query run:
- index=auth (EventCode=4625 OR EventCode=4624) user="finance_admin"
- | stats count by src_ip, EventCode
- Finding: Success login from IP 185.220.101.2 (Tor exit node).

Step 2 – Threat Intel (VirusTotal & OTX)

- Check IP in VirusTotal → flagged in 30 reports.
- OTX: IOC linked to “TA505” phishing campaign.

Step 3 – EDR (CrowdStrike Falcon)

- Alert: Host FIN-PC01 shows WINWORD.EXE → POWERSHELL.EXE -enc ….
- Process tree reveals dropped file payload.exe.
- Analyst isolates endpoint.

Step 4 – Packet Analysis (Wireshark)

- PCAP review: traffic from FIN-PC01 → 45.77.13.220 every 60s.
- TLS JA3 fingerprint matches known C2 profile.

Step 5 – Sandbox (Any.Run)

- Upload payload.exe.
- Behaviour: connects to c2.malicious.net, creates persistence registry key.

Step 6 – Hunting (SIEM Query)

- Analyst runs hunt for same IOC:

- index=proxy url_domain="c2.malicious.net"
- Finds 2 other hosts contacted domain.

Step 7 – Containment

- Isolate 3 affected endpoints.
- Block domain & IP on firewall/proxy.
- Force reset of affected user accounts.

Step 8 – Lessons Learned

- Root cause: Phishing email bypassed email filter.
- Improvement: Update gateway policy to block .docm attachments.
- Add SIEM rule: “Word spawning PowerShell = High Severity.”

11.7 Interview “Listen-For” Signals

- Can you name tools across categories (SIEM, EDR, TI, packet/log, labs)?
- Do you understand how to use them (queries, enrichment, isolation)?
- Can you describe how you practise in labs (TryHackMe, CyberDefenders)?
- Do you connect tools to real incidents (simulation walk-through)?

12. PRACTICAL EXERCISES

12.1 Build Mock SIEM Queries

Why?

- Interviewers often ask: “Can you write a query to detect brute force?”
- Being comfortable with queries (Splunk, Sentinel, Elastic, QRadar) sets you apart.

Exercise A – Brute Force Detection (Splunk)

```
index=auth EventCode=4625
| stats count by user, src_ip
| where count > 10
```

- Output: Shows accounts with >10 failed logins.
- Simulation:
    - Logs:
    - 2025-09-09T08:12:01 user=finance_admin src_ip=185.220.101.2 EventCode=4625
    - 2025-09-09T08:12:05 user=finance_admin src_ip=185.220.101.2 EventCode=4625
    - ... (10 more failed attempts) ...
    - 2025-09-09T08:14:01 user=finance_admin src_ip=185.220.101.2 EventCode=4624
    - Analyst conclusion: Successful brute force → escalate.

Exercise B – Unusual IP Traffic (Sentinel KQL)

```
DeviceNetworkEvents
| summarize count() by RemoteIP
| where count < 5
```

- Purpose: Find IPs rarely contacted → possible beacon.
- Simulation: Host HR-PC01 connects every 60s to 45.77.13.220.

12.2 Analyse Sample Logs

Firewall Logs

2025-09-09T09:02:11 action=deny src=185.220.101.2 dst=10.1.2.5 d_port=3389 proto=TCP threat="RDP Brute Force Attempt"

- Interpretation: External Tor IP attempted RDP brute force.

DNS Logs

2025-09-09T09:03:45 client=10.1.3.55 query=ajd92h3qwe.maliciousc2.com type=A

- Interpretation: Possible beaconing via DNS.

EDR Logs

2025-09-09T09:04:33 host=FIN-PC01 user=izzmier
Parent=WINWORD.EXE Child=POWERSHELL.EXE -enc JABzAGM...

- Interpretation: Macro-enabled Word doc launched PowerShell.

Exercise: Correlate → Brute force (firewall) + beacon (DNS) + malicious macro (EDR).

12.3 Create an Incident Workflow (Detection → Closure)

Step 1 – Detection

- SIEM alerts: multiple failed logins, suspicious PowerShell.

Step 2 – Triage (L1)

- Validate alerts.
- Enrich IP/domain with VirusTotal.
- Escalate if confirmed malicious.

Step 3 – Analysis (L2)

- Correlate across firewall, DNS, EDR logs.
- Confirm: user finance_admin compromised, beaconing to C2.

Step 4 – Containment

- Disable account finance_admin.
- Isolate host FIN-PC01.
- Block maliciousc2.com domain.

Step 5 – Eradication & Recovery

- Remove malware from host.
- Reset password with MFA.
- Monitor for recurrence.

Step 6 – Closure

- Incident Report delivered.
- SOC playbook updated: add SIEM rule for Word → PowerShell chain.

12.4 IOC Enrichment with VirusTotal / OTX

Exercise – Enrich IP 45.77.13.220

- VirusTotal: Flagged in 25/70 engines as C2.
- OTX: Part of "AgentTesla Campaign – Sept 2025."
- SOC Use:
    - Confirm IOC is malicious.
    - Sweep SIEM for other hosts contacting same IP.
    - Block IOC in firewall.

12.5 Practise Writing Incident Reports

Why?

- SOC analysts must write clear, concise executive summaries.
- Interviewers may ask: "Write a short incident report."

Template (Executive Summary Style)

Title: Credential Compromise – Finance_Admin Account

Date/Time: 09 Sept 2025, 08:12 UTC

Summary:
SOC detected multiple failed login attempts followed by a successful login for privileged account finance_admin. The login originated from IP 185.220.101.2 (Tor exit node). Subsequent activity included execution of malicious PowerShell on workstation FIN-PC01 and beaconing to C2 domain maliciousc2.com.

Actions Taken:

- Disabled finance_admin account.
- Isolated affected workstation.
- Blocked C2 IP/domain across firewall/proxy.
- Reset account credentials with MFA enforcement.

Impact:
No confirmed data exfiltration. Early containment prevented lateral movement.

Recommendations:

- Enhance SIEM rules for failed logins + success pattern.
- Block Tor exit nodes by default.
- Conduct user awareness training for phishing risks.

12.6 Full Simulation – Practical Exercise End-to-End

Scenario: A user downloads a malicious attachment from phishing email.

Logs Collected

- Email Gateway: Delivered mail with subject “Invoice Attached”, file invoice.docm.
- Proxy: User clicked URL http://malicious-bank.com/payload.exe.
- EDR: Process chain WINWORD.EXE → POWERSHELL.EXE → rundll32.exe.
- DNS: Queries to x9afh23.maliciousc2.com.
- Firewall: Outbound traffic blocked to 45.77.13.220.

Analyst Workflow

L1 Actions

- SIEM triggered alert for “suspicious process chain.”
- Enrich hash in VirusTotal → flagged ransomware.
- Escalates to L2 with evidence.

L2 Actions

- Correlates logs (email + proxy + EDR + DNS).
- Runs IOC sweep: finds 2 more users with same phishing email.
- Containment: isolates all affected endpoints, disables accounts, blocks domains.
- Eradication: removes persistence registry keys, reimages hosts.
- Recovery: restores files from backup.

Executive Summary Report

Title: Phishing Campaign Leading to Malware Execution (Blocked)
Date: 09 Sept 2025
Summary: Three users received phishing emails. One executed malicious macro which attempted to download ransomware payload. SOC responded quickly, isolating endpoints and blocking domains before encryption or exfiltration occurred.
Impact: No data loss; limited to three endpoints.
Lessons Learned: Block .docm files at email gateway, improve SIEM rules for Word spawning PowerShell.

12.7 Interview “Listen-For” Signals

- Can you write SIEM queries?
- Do you know how to read logs across firewall, DNS, EDR?
- Can you map incident workflows clearly?
- Do you use TI enrichment (VirusTotal, OTX) effectively?
- Can you write short, clear incident reports?

13. TIPS FOR SUCCESS (L1–L2 SOC INTERVIEWS)

13.1 Focus on fundamentals (esp. for L1)

Know these cold:

- Networking basics: TCP/UDP, common ports (22/25/53/80/443/445/3389), three-way handshake, NAT, VPN.
- Windows auth events: 4624 (success), 4625 (fail), 4672 (special privileges), 4720/4728 (user/group changes).
- Linux auth: /var/log/auth.log, sshd successes/fails, sudo.
- DNS & web: How DNS resolves; HTTP verbs; HTTPS/TLS at a high level.
- Core logs: Firewall allow/deny, proxy URL/category, EDR process tree, DNS queries, cloud sign-ins.
- IR actions: Disable/lock account, reset password, EDR isolate, block IP/domain, collect evidence, escalate.

60-minute "night-before" cram:

1. Review a MITRE ATT&CK matrix; memorise 8–10 common techniques (T1566 Phishing, T1059 PowerShell, T1078 Valid Accounts, T1041 Exfiltration, T1021 Remote Services, T1055 Process Injection, T1053 Scheduled Task, T1547 Persistence Registry).
2. Rehearse 3 SIEM queries (failed→success logins, rare outbound IPs, Word→PowerShell).
3. Practise 60-second incident summary (see §13.5).

13.2 Show structured thinking in scenarios (step-by-step)

Interviewers care how you think more than tool trivia. Use a crisp, repeatable template.

The 6-step Triage & Response Pattern (say it out loud):

1. Validate the signal (time, scope, dedupe).
2. Enrich (user/asset criticality, VT/OTX on IOCs).
3. Correlate (auth + EDR + DNS + proxy + firewall + cloud).
4. Assess severity & impact (business context).
5. Contain safely (account/host/network), with approvals if needed.
6. Document & handoff (facts, evidence, next actions).

Example answer skeleton (you can reuse across scenarios):
"First I validate the alert and time window, then enrich the IP/domain/hash. Next I correlate across auth, endpoint, DNS/proxy and any cloud sign-ins to confirm scope. If it's a

privileged account or critical host, I escalate severity. For containment I'd [specific action] and I'll document evidence/screenshots in the ticket and brief the next tier."

13.3 Use MITRE ATT&CK (esp. for L2)

Don't drown the panel in codes—bridge behaviour → technique → why it matters.

How to phrase it:

- "The pattern looks like Initial Access: Phishing (T1566) → Credential Use: Valid Accounts (T1078) → Execution: PowerShell (T1059) → C2 over HTTPS (T1071). That implies we should search for lateral movement (e.g., T1021 RDP/SMB) and persistence (T1547). I'll hunt those next."

Why this helps: shows you think in behaviours, so your detections survive when IOCs rotate.

13.4 Be clear on escalation boundaries

L1—Do:

- Acknowledge/triage within SLA, enrich, close obvious false positives with rationale, escalate suspected TPs, keep tidy notes.

L1—Don't (without runbook approval):

- Reset privileged accounts, change firewall rules org-wide, wipe evidence.

L2—Do:

- Deep correlation, decide & execute containment within runbook (EDR isolate, disable non-critical accounts), propose firewall/proxy blocks, brief stakeholders, produce incident timeline and recommendations.

L2—Escalate to L3/IR Manager when:

- Possible domain compromise, lateral movement, ransomware encryption or regulated data at risk (triggering PDPA/BNM/GDPR).
- Memory forensics/reverse engineering needed.
- Containment may disrupt critical services—need senior approval.

13.5 Communicate confidently (thinking under pressure)

Use the 60-second "S.A.F.E.R." update:

- Summary: one-line what's happening.
- Assert impact: what's at risk (user/system/data).
- Facts: 3 concrete evidence points (logs/IOCs).
- Execute plan: 2–3 actions now + owner.
- Risks/Requests: approvals or support you need.

Example (spoken):
"Summary: We have a confirmed account compromise on finance_admin. Impact: privileged access and possible data exposure. Facts: 12 failed then successful sign-in from a Tor IP; Word→PowerShell on FIN-PC01; DNS queries to a known C2. Execute: I'm disabling the account and isolating FIN-PC01 now; requesting approval to block the C2 at the edge. Risks: business impact minimal; I'll provide timeline updates every 30 minutes."

Handover note template (3 bullets max):

- Status: What's true now (incident type/severity, systems affected).
- Evidence: Links to SIEM searches, key screenshots/IOCs.
- Next: 2–3 actions pending + owners/ETAs.

13.6 Simulations (ready-to-practise scripts)

Simulation A — L1 vs L2 on "Failed→Success Login"

Prompt: "SIEM shows 10 failed logins followed by a success for finance_admin."

Strong L1 answer (≤60s):

- Validate alert window; confirm user not travelling.
- Enrich source IP (VT/AbuseIPDB).
- Quick checks: any MFA failures? new device?
- Severity: High if privileged + malicious IP.
- Escalate with evidence: auth logs, geo, TI verdict, user/host criticality.

Strong L2 answer (≤90s):

- Correlate with proxy/DNS/EDR for macro→PowerShell or new services.
- Map to MITRE (T1566 → T1078 → T1059/T1071).
- Containment: disable account, revoke sessions, EDR isolate host, block IOC.
- Hunt blast radius (same IP/domain across fleet).
- Plan: post-incident actions (Conditional Access, legacy protocol blocks).

Simulation B — "Four alerts at once" (prioritisation)

- A: Ransomware note dropped on CFO laptop (EDR).

- B: 30 failed logins on a test VM.
- C: Port scan on a printer subnet.
- D: Beacon to rare IP from a non-critical kiosk.

Answer:
Priority A (confirmed impact on critical user) → D (possible active C2) → B (likely spray) → C (noise). Give the SAFER update for A, place holds on D, queue quick queries for B/C and document all.

Simulation C — 90-second Sev-1 briefing (ransomware start)

- "We have early-stage ransomware on FIN-PC03. Impact is local only—no share encryption. Facts: EDR flagged rapid file renames; PowerShell -enc spawned from Word; outbound to 45.77.13.220. Actions: host isolated; user disabled; IOC blocked; we're sweeping for the hash and C2. Risks: if another host detonates, potential file server impact. Need: approval to push a temporary block to all egress for the C2 subnet."

13.7 Common pitfalls & how to avoid them

- Jumping to containment without evidence. Fix: show the 3 facts you validated before acting.
- Tool-only answers. Fix: describe process and reasoning, then tool clicks.
- Forgetting business context. Fix: state asset criticality and likely impact in every answer.
- Weak documentation. Fix: keep a running timeline + attach raw log snippets and screenshots.
- No closure. Fix: always end with "hunt/blast radius, lessons learned, detection updates."

13.8 Pocket cheat-sheet (use in mock interviews)

- Triage 5: Validate → Enrich → Correlate → Assess → Contain.
- Containment menu: Disable account • Revoke tokens • EDR isolate • Block IP/domain/URL • Kill process • Remove persistence • Patch.
- Evidence pack: Auth events (4624/4625) • EDR process tree • DNS/proxy line • Firewall hit • VT/OTX verdicts • Timeline.
- Close-out: Root cause • Impact • MITRE mapping • What changed (rules/playbooks/controls) • User awareness item • Metrics (MTTD/MTTR).

L1 SOC ANALYST INTERVIEW SIMULATION

1. Introduction

Interviewer: Welcome. Can you briefly introduce yourself and explain why you're interested in a SOC Analyst role?

Candidate: Thank you. My name is [Your Name]. I come from a background in IT support where I developed strong log troubleshooting and user support skills. Over the past year, I've trained myself in cybersecurity fundamentals through platforms like TryHackMe and CyberDefenders, with a focus on SIEM queries, phishing analysis and incident response. I'm drawn to the SOC role because I enjoy investigating suspicious activity and contributing to protecting organisations against real threats. I see the L1 analyst role as the perfect foundation to grow into an advanced cybersecurity professional.

2. General Cybersecurity Knowledge

Interviewer: Can you explain the CIA triad with examples relevant to a SOC environment?

Candidate: The CIA triad stands for Confidentiality, Integrity and Availability.

- Confidentiality means protecting sensitive information from unauthorised access. In a SOC, that could mean ensuring attackers can't access customer data in databases.
- Integrity means making sure data isn't altered maliciously. For example, ensuring log files aren't tampered with.
- Availability means systems must remain accessible. An example would be protecting online banking from downtime caused by DDoS attacks.

Interviewer: What's the difference between IDS and IPS?

Candidate: An IDS (Intrusion Detection System) detects suspicious traffic and raises alerts, while an IPS (Intrusion Prevention System) actively blocks malicious traffic in real time. For instance, IDS might log a port scan from an attacker, while IPS would automatically block the attacker's IP after repeated malicious attempts.

Interviewer: How does DNS work and why is it important in SOC investigations?

Candidate: DNS is the internet's phonebook — it resolves human-readable domains into IP addresses. In SOC, DNS logs are critical because attackers often use domains for phishing or C2 servers. If we see a host making repeated DNS queries to random subdomains of a suspicious domain, it could be malware beaconing.

3. Technical Knowledge

Interviewer: A SIEM shows 15 failed logins followed by a success for a user account. What would you do?

Candidate:

1. Validate: Confirm timestamps and IPs.
2. Enrich: Look up the source IP in VirusTotal/AbuseIPDB.
3. Context: Check if user is privileged or traveling.
4. If malicious: Disable the account and reset password.
5. Escalate to L2 if confirmed compromise.
6. Document all actions.

Interviewer: How would you investigate unusual outbound traffic to an unknown IP?

Candidate:

- First, identify the internal host making the connection.
- Check proxy/firewall logs for frequency, ports and data size.
- Enrich IP in TI feeds.
- Check host logs via EDR for processes behind the traffic.
- If confirmed malicious, isolate host, block IP, reset accounts.
- If uncertain, escalate with evidence for deeper L2 analysis.

Interviewer: What common Windows Event IDs should you know in log analysis?

Candidate:

- 4624 = Successful login
- 4625 = Failed login
- 4672 = Special privileges assigned
- 4720 = User account created
- 4728 = User added to security-enabled group

These are critical for detecting brute force, privilege escalation and persistence attempts.

4. Scenario-Based

Interviewer: A user reports receiving a phishing email. Walk me through your response as an L1 analyst.

Candidate:

- Step 1: Collect the email, headers and any links or attachments.
- Step 2: Check if other users received similar emails.

- Step 3: Run enrichment on links (VirusTotal, OTX).
- Step 4: If user clicked, check proxy/EDR logs for connections or malicious processes.
- Step 5: Escalate with evidence to L2 for containment.
- Step 6: Document everything and notify awareness team if needed.

Interviewer: Suppose our EDR detects malware beaconing to a C2 server. What would you do?

Candidate:

- Validate: Confirm the beacon pattern (e.g., every 60s outbound traffic).
- Enrich IP/domain in TI feeds.
- Identify the host and isolate via EDR.
- Disable any compromised accounts.
- Escalate with logs and timeline.
- Sweep SIEM for same IOC to check other affected hosts.

Interviewer: Here's a simulation. Firewall logs show:

2025-09-09T09:02:11 action=allow src=10.1.3.55 dst=45.77.13.220 d_port=443
2025-09-09T09:03:11 action=allow src=10.1.3.55 dst=45.77.13.220 d_port=443
2025-09-09T09:04:11 action=allow src=10.1.3.55 dst=45.77.13.220 d_port=443

What do you see here?

Candidate:

- This is beaconing behaviour — the host 10.1.3.55 connects every 60 seconds to the same external IP.
- As L1, I would enrich the IP, check EDR logs for the initiating process, escalate if malicious.
- Possible C2 traffic. Immediate recommendation: escalate to L2 for isolation.

Interviewer: Another scenario. Logs show multiple failed logins:

EventID=4625 user=admin src_ip=185.220.101.2
EventID=4625 user=admin src_ip=185.220.101.2
EventID=4625 user=admin src_ip=185.220.101.2
EventID=4624 user=admin src_ip=185.220.101.2

What's happening?

Candidate:

- This is a brute force login attempt that succeeded.
- Actions: Enrich IP (likely malicious), disable admin account, reset password, check for lateral movement, escalate as High Severity.

5. Soft Skills / Behavioural

Interviewer: You're monitoring SIEM and suddenly 5 alerts come in at once. How do you prioritise?

Candidate:

- I prioritise based on severity and business impact:
    - Confirmed ransomware on CEO laptop = highest.
    - Privileged account compromise = high.
    - Suspicious port scan on test subnet = low.
- I handle the highest impact incident first, while flagging others for investigation.

Interviewer: How do you handle shift handover?

Candidate:

- Ensure tickets are updated with evidence and actions.
- Document pending investigations and next steps.
- Verbally or via chat brief incoming shift.
- Example: "Phishing campaign targeting Finance, 2 users clicked, creds reset, still checking logs for lateral movement. Please continue hunt for related domains."

Interviewer: Tell me about a time you worked under pressure.

Candidate:

- Situation: During a blue team exercise on TryHackMe, I simulated a SOC role where multiple alerts triggered simultaneously.
- Task: I had to prioritise incidents and respond quickly.
- Action: Focused on confirmed credential compromise first, while documenting evidence for other alerts.
- Result: Contained the main incident in time, learned to keep calm and structured under pressure.

L2 SOC ANALYST INTERVIEW SIMULATION

1. Introduction (5 mins)

Interviewer: Welcome. Could you introduce yourself and explain why you're ready for an L2 SOC Analyst role?

Candidate: Thank you. I started in SOC operations as an L1 analyst, where I built strong experience triaging alerts, working with SIEM platforms and escalating confirmed incidents. Over time, I've developed deeper skills in log correlation, MITRE ATT&CK mapping and incident response workflows, including containment and eradication. I've also practised threat hunting, malware sandboxing and creating detection use cases. I believe I'm ready for L2 because I can not only triage but also investigate across multiple sources, identify root cause and recommend containment actions, which are the hallmarks of an L2 analyst.

2. Cybersecurity Knowledge

Interviewer: How does the MITRE ATT&CK framework help SOC analysts in daily work?

Candidate: MITRE ATT&CK maps attacker behaviour to tactics and techniques. As an L2, it helps me categorise suspicious activity beyond IOCs. For example:

- Phishing email → T1566 (Initial Access).
- Compromised credentials → T1078 (Valid Accounts).
- Word spawning PowerShell → T1059 (Command Execution).
  By mapping incidents, I can both understand the attack stage and recommend proactive hunts for related activity.

Interviewer: Explain the difference between IOC-based and TTP-based detection.

Candidate:

- IOC detection relies on indicators like IPs, domains, file hashes — but attackers can change these easily.
- TTP detection relies on attacker behaviours (e.g., encoded PowerShell, DNS tunneling). This is harder for attackers to avoid.
  In SOC, L1 may confirm IOC matches, but as L2 I try to identify behavioural patterns for stronger detection coverage.

Interviewer: Why is log correlation across multiple sources important?

Candidate: Because no single log tells the full story. For example, an authentication success alone isn't suspicious. But if correlated with DNS queries to malicious domains

and EDR logs showing PowerShell execution, it indicates compromise. Correlation helps reduce false positives and identify true scope of incidents.

3. Technical Deep Dive

Interviewer: How would you investigate suspicious DNS traffic?

Candidate:

1. Identify the host generating queries.
2. Review frequency, length and domain type.
3. Check if it's a Newly Registered Domain or algorithm-generated domain (DGA).
4. Enrich with TI feeds.
5. Check EDR process that initiated queries.
6. If malicious, isolate host and block domain.

Interviewer: Write or describe a query to detect brute force followed by success in Splunk.

Candidate:

```
index=auth (EventCode=4625 OR EventCode=4624)
| bin _time span=5m
| stats count(eval(EventCode=4625)) as fails, count(eval(EventCode=4624)) as success by user, src_ip
| where fails >= 5 AND success >= 1
```

This shows accounts with 5+ failed logins followed by success in 5 minutes.

Interviewer: You see multiple EDR alerts: "WINWORD.EXE → POWERSHELL.EXE -enc ...". How do you respond?

Candidate: That's a common malicious macro pattern. Steps:

- Correlate: check proxy logs for outbound traffic after PowerShell.
- Enrich domains contacted.
- Hunt: check if other hosts triggered same chain.
- Containment: isolate affected hosts.
- Update detection: tune SIEM/EDR rules to auto-flag Word spawning PowerShell.

4. Scenario-Based

Interviewer: A phishing email delivers malware. Logs show:

- Email gateway: message delivered with invoice.docm.

- Proxy: user downloaded payload.exe.
- EDR: Word → PowerShell → rundll32.
- Firewall: outbound traffic to 45.77.13.220:443 every 60s.

Walk me through your investigation as L2.

Candidate:

- Step 1: Validate with SIEM (correlation of email + proxy + EDR + firewall).
- Step 2: Enrich IP/domain → flagged as C2.
- Step 3: Identify affected host (FIN-PC01) and isolate.
- Step 4: Disable user account, force password reset.
- Step 5: Sweep SIEM for same IOC across environment.
- Step 6: Recommend malware sample to sandbox.
- Step 7: Document incident, map to MITRE (T1566 → T1059 → T1071).

Interviewer: Another scenario. SIEM shows:

- Multiple failed logins for admin01.
- Success login from Nigeria.
- CloudTrail log: IAM user created from same IP.

What do you do?

Candidate:

- Correlate: confirm login success → malicious activity in AWS.
- Immediate containment: disable admin01, revoke sessions.
- Block IP at firewall.
- Check if IAM user created has privileges — disable/remove.
- Sweep for lateral movement in cloud logs.
- Escalate as High Severity (Cloud Account Compromise).
- Lessons learned: enforce MFA, apply geo-blocking, add SIEM rules for impossible travel.

Interviewer: Let's simulate lateral movement. EDR shows psexec.exe used from HR-PC02 to DB-SERVER01. What's happening?

Candidate: That indicates lateral movement attempt via PsExec. As L2:

- Confirm if HR-PC02 was compromised.
- Check if account used was privileged.
- Review DB-SERVER01 logs for process execution.
- Containment: isolate HR-PC02, disable associated account.

- Map to MITRE T1021 (Remote Services).
- Escalate to L3 for deeper forensic capture on DB server.

5. Behavioural / Soft Skills

Interviewer: You're handling 3 incidents at once: phishing, brute force and ransomware note detected on a laptop. How do you prioritise?

Candidate: I'd prioritise based on impact and severity:

1. Ransomware (active impact, encryption risk) → contain immediately.
2. Brute force with success (privileged account) → handle next.
3. Phishing email with no clicks yet → lower priority, but still investigate.
   I'd also delegate or escalate to ensure all incidents are covered.

Interviewer: How do you handle escalation boundaries between L1, L2 and L3?

Candidate:

- L1 triages alerts, enriches IOCs, escalates confirmed suspicious activity.
- As L2, I do deep correlation, propose/execute containment and handle scope analysis.
- I escalate to L3 when forensic expertise, malware reverse engineering or high business impact (APT, ransomware spreading, critical system compromise) is involved.

Interviewer: Tell me about a time you had to communicate technical findings to a non-technical audience.

Candidate: In training, I simulated reporting on a phishing incident. For the technical team, I explained the attack chain: malicious doc → PowerShell → C2. For management, I simplified: "Attackers tried to steal employee credentials via fake invoices. We contained it before data was stolen. Users must avoid opening attachments from unknown senders." That balance kept both audiences informed without overwhelming them.