anand guru

SOC EXPERTS

Interview Questions on
SOC Processes

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

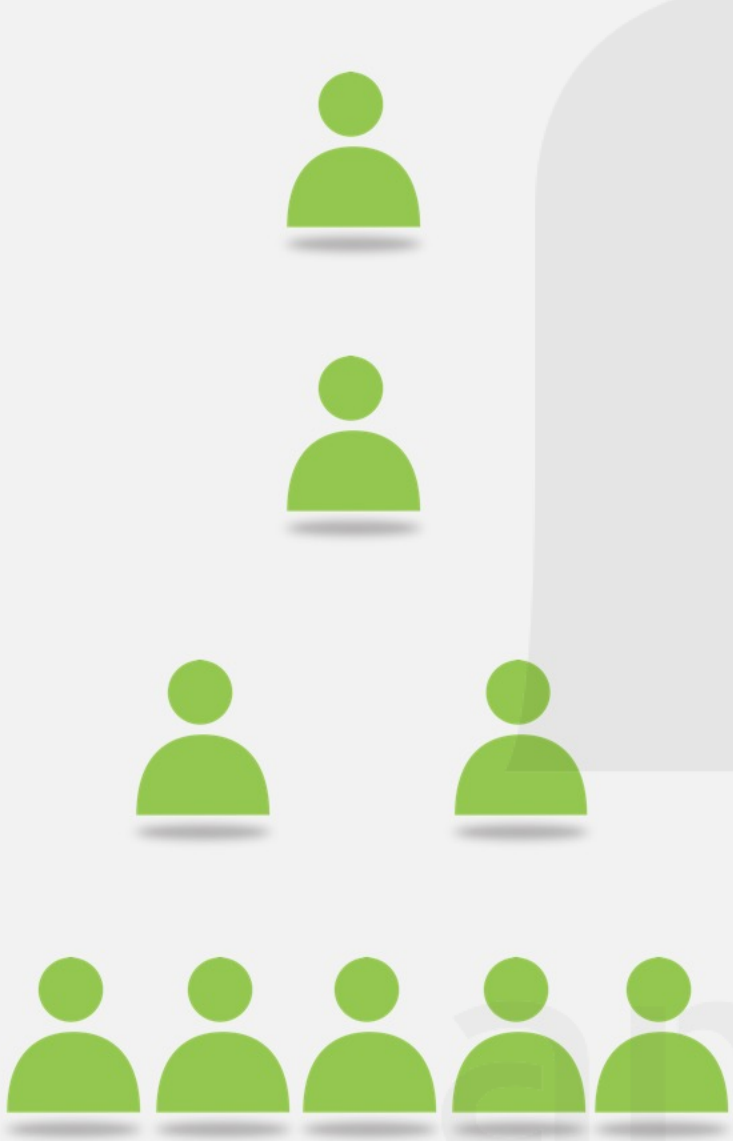
SOC Experts

https://socexperts.com

DISCLAIMER

- **Most of the questions and their answers discussed in this section are subjective.**
- **Different companies follow different processes.**
- **I believe there are no correct or wrong answers for these questions. However there might be better answers than the ones discussed here.**

Explain the SOC Team Architecture/Hierarchy

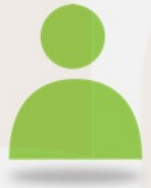


SOC Manager

L3/SOC Lead

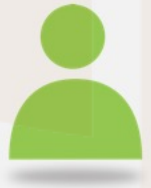
L2 Security Analyst

L1 Security Analyst



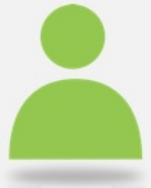
Threat Intelligence

Threat Hunter



Incident Handler

Forensic Investigator



IR Automation Engineer

Red Team Specialist

Roles and Responsibilities of L1/L2 Security Analyst in SOC.

Security Analyst L1

- 24/7 Eyes-on-Glass monitoring
- Analysis of triggered alerts (usually following a Runbook)
- Raising tickets for validated incidents
- Follow-up with incident response team for remediation
- Drafting shift hand-overs
- Assist L2/L3 in reporting

Security Analyst L2

- Deep dive analysis of escalated alerts
- Assist in Incident Remediation
- Assist L1 in alert analysis
- Maintaining and improving SOPs and processes
- Troubleshoot basic SIEM issues

As SOC Lead/SIEM Admin what are your responsibilities?

1. Installing, updating, upgrading SIEM solution.
2. On-boarding log sources and working on log source issues.
3. Create and fine-tune content in SIEM – Correlation Rules, Dashboards, Reports, Lists etc.
4. Interact with SIEM vendor TAC (support) to fix any issues with SIEM.
5. Install, Manage and build content in SIEM.
6. Mentor L1 and L2 security analyst.
7. Assist in analysis that requires involvement of multiple teams.
8. Evaluate new solutions for SOC team.
9. Create Run books for all alerts.
10. Schedule shift rooster.

What are the different SOC Models?

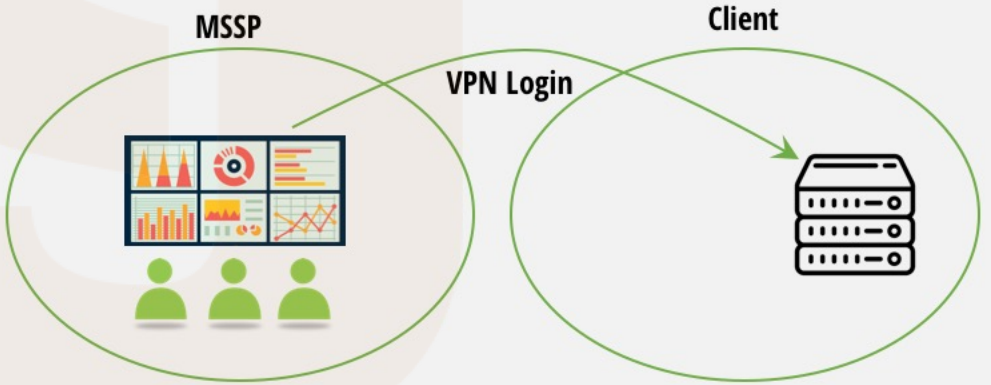
- **In-house SOC**

  An organization runs its own SOC. People, processes and technology are all managed by people with-in the organization.

- **MSSP** (Managed Security Service Provider)/ MSP (Manager Security Provider)

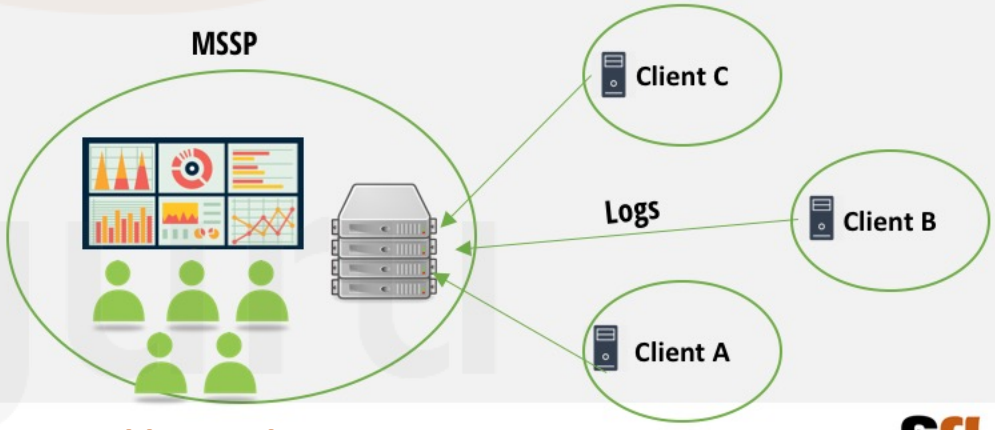
  Dedicated – A team of people with the service provider work for a client. Here the client typically have their own technology i.e. SIEM and other tools will be hosted in clients datacenter.

  Shared – A team of people with the service provider monitor and analyze logs coming from various clients. In this model the technology is hosted on service providers datacenter



- **Hybrid SOC**

  It is a mix of both In-house SOC and MSSP. Typically this is done by out-sourcing the L1 monitoring to a MSSP and the organization runs L2 and Incident Response team in-house



Which model is better MSSP or In-house?

Both the models have their advantages and short comings

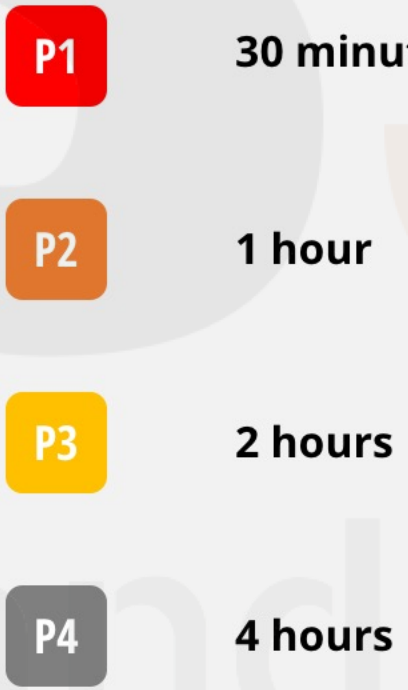
In-house SOC is more effective as the organizations can customize everything as per business requirements. Since the number of technologies in an organization is limited, the focus will be on getting best value out of each solution. However, in-house SOC is very expensive to implement

MSSP model will reduce the cost of ownership and operational expenses; however, the output of SOC (like reports, alerts, recommendation etc.) will be generic.

Hybrid SOC gives a better result, but it is still expensive to implement.

What is SLA?

- SLA stands for Service Level Agreement
- In SOC it is mostly the time taken for a SOC team to identify and report a suspicious activity.
- SLAs are associated with priorities:



Why does a organization need SOC team?

- One of the main benefits of having a Security Operations Center is that it improves security incident detection through constant monitoring and analysis.
- It shifts to proactive approach, rather than being reactive.
- Monitoring 24/7, a SOC is able to provide organizations with an advantage to defend against intrusions regardless of the type of attack at any time.
- SOC also helps to meet the regulatory compliances

When we have Endpoint Security and Network Security, why do we need SOC team?

- Traditionally all the preventive technologies (like AV, firewall, IPS) work separately and needs dedicated skills to manage them. A SOC team helps in **correlating** activities happening at different parts of the network.

What do you document in an Incident?

1. Incident Name
2. Incident Description
3. Priority
4. Occurred Time
5. Detected Time
6. Reported By
7. Assigned To
8. Affected Host/IP/User/Business Unit
9. Information Gathered
10. Analysis
11. Evidence
12. Recommendations

What ticketing tool have you worked on?

Most widely used ticketing tools are

- Service Now (SNOW)
- BMC Remedy
- JIRA
- RSA Archer

Apart from SIEM what other tools have you worked on?

Preventive Technologies

- Endpoint Security – McAfee ePO or SEPM
- Firewall – PaloAlto or Fortinet
- IPS – SNORT
- Vulnerability Assessment - Nessus
- Proxy – Websense
- Email Gateway – Proofpoint
- WAF – Imperva Incapsula

Analysis Tools

- IPVOID
- VirusTotal
- Wireshark
- MXToolBox
- CVEDETAILS
- US-CERT
- IBM X-Force/Threat Crowd

Utility Tools

- Ticketing tool – Service NOW
- Process Explorer
- Process Monitor

What is False Positive?

- A **true positive** is an outcome where the model *correctly* predicts the *positive* case.
  - Downloaded file is a malware, AV detected it as malware
- A **true negative** is an outcome where the model *correctly* predicts the *negative* case.
  - Downloaded file is NOT malware, AV did NOT detect it as malware
- A **false positive** is an outcome where the model *incorrectly* predicts the *positive* case.
  - Downloaded file is a NOT a malware, AV detected it as malware
- A **false negative** is an outcome where the model *incorrectly* predicts the *negative* case.
  - Downloaded file is a malware, AV did NOT detect it as malware

- True Positive and Ture Negative are ideal cases; i.e. when solutions are working correctly
- False Positive – Increases work and lead to alert-fatigue
- False Negative – Is very dangerous; malicious activity has happened, solution did not detect it.

Explain your team in numbers and Hierarchy

- We have 10 people in our team with
  - 6 Level 1 Analyst
  - 2 Level 2 Analyst
  - 1 Lead &
  - 1 SOC manager
- Our team reports to CISO in our company (or client's CISO)
- L1 analysts monitors network 24/7 and do analysis based on the Playbooks
- L2 analysts helps in deep dive analysis and also assist L1s in analysis.
- Threat Intelligence and Threat Hunting responsibilities are shared between L1 and L2 analyst

What are the numbers in your SOC?

No. of Log Source - Around 2800

No. of Logs/day - 25,000,000

No. of Alerts/day - 100 – 130

No. of Incidents/day - 2 – 5

What are the different report/dashboard you generate?

3 major types of reports - Technology Report | SIEM Performance Reports | SOC Performance Report

Technology Reports

1. Malware Summary
   - No. of Infections, Hosts Infected, Users, Malware Type, Malware Name, Action by AV, File Name and File Path
2. Firewall Summary
   - Inbound Allow – Source Country, Source IP, Destination IP, Destination Port (services)
   - Inbound Deny – Source Country, Source IP, Destination IP, Destination Port (services)
   - Outbound Allow – Source IP, Destination IP, Destination Country, Destination Port (services)
   - Outbound Deny – Source IP, Destination IP, Destination Country, Destination Port (services)
3. Account Management Summary
   - Accounts Created, Deleted, Enable, Disabled, Locked-out
   - Privilege Changes
4. Authentication Summary
   - Successful logons, Failed Logons, Admin Logons etc.
5. Proxy Summary
   - Top 10 Users, Top 10 Websites, Top 10 Website Categories, Malicious Website Access and Action, Malicious file downloads and Action
6. Email Summary
   - Top 10 Sender, Top 10 Recipients, Top 10 Sender Domain, Top 10 Mail blocking Reasons, Malicious Attachment and Action
7. Threat Intelligence Summary
   - Inbound – Source country, Source IP, Destination IP, Destination Port, Action
   - Outbound – Source IP, Destination IP, Destination Country, Destination Port, Action

Reports contd...

SIEM Reports

- EPS
- New log sources
- Silent log sources
- New Correlation Rules

SOC Performance Reports

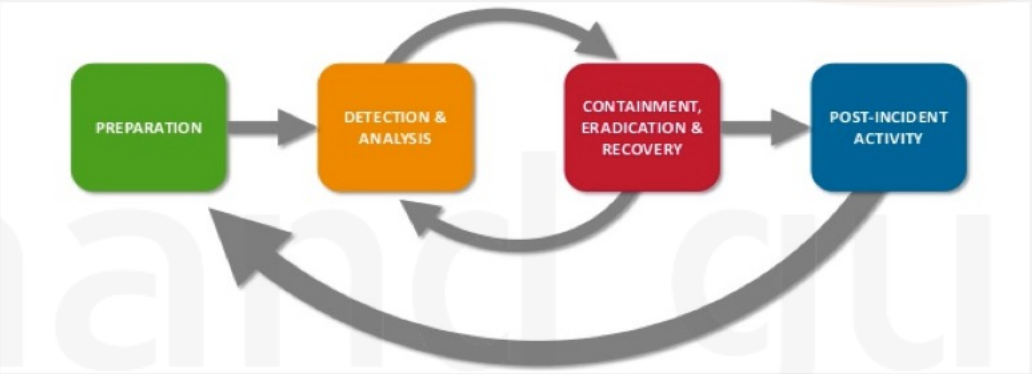
- Number of Alerts
- Number of Incidents by Severity
- SLA adherence
- Number of Escalation

Explain the Incident Response Process/Lifecycle

SANS (SysAdmin, Audit, Network and System) Incident Response Process has 6 stages

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

NIST (National Institute of Standards and Technology) defines the Incident Response in the **Special Publication 800-61**



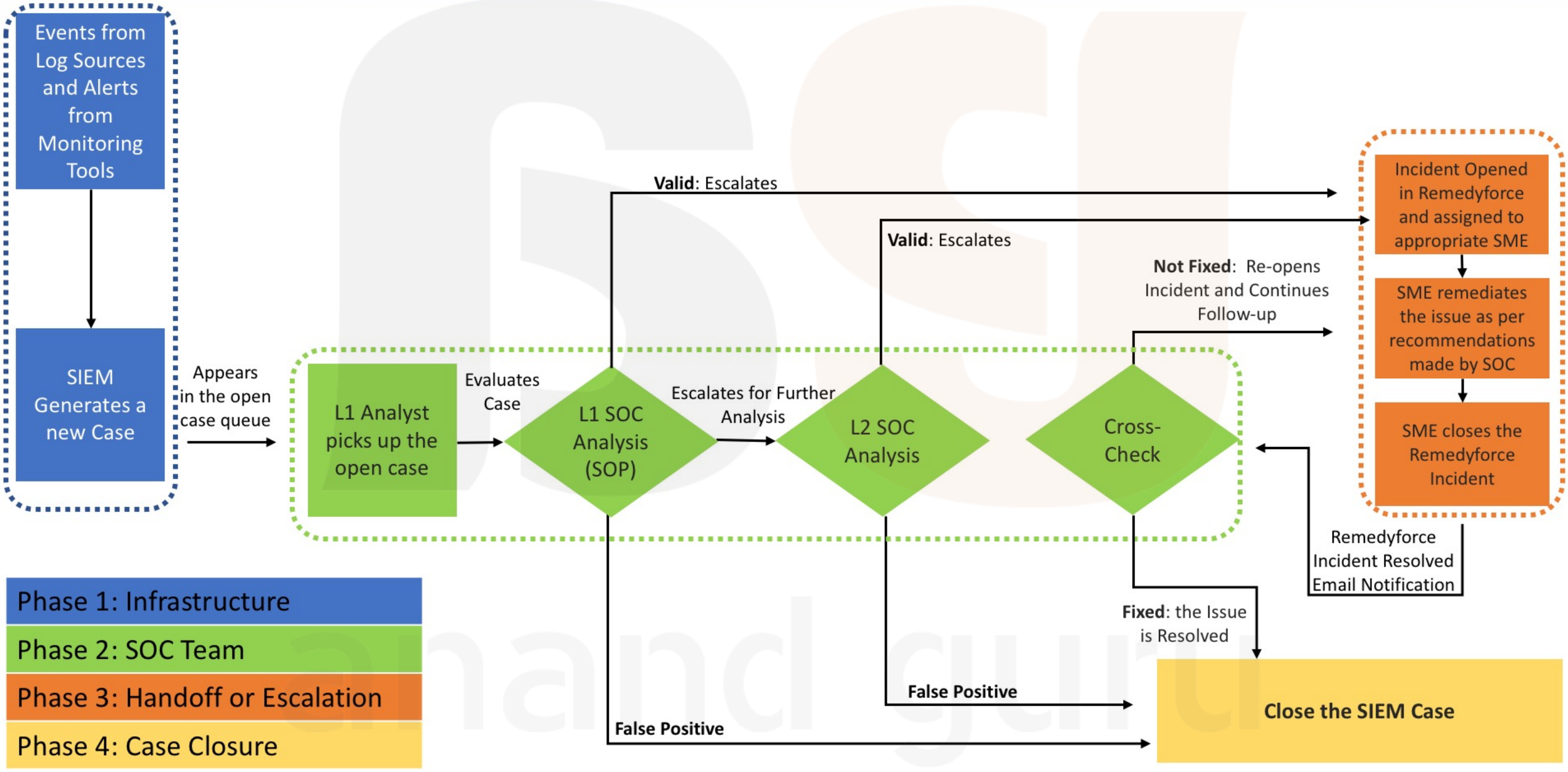
Explain SIEM implementation Phases.

1. Asset Management (List of all the assets)
2. Define the Scope for SOC Monitoring and Analysis
3. Log Source On-boarding preparation
4. Implement SIEM
5. On-board Log sources
6. Use OOB content – DB, Reports, Rules etc.
7. Announce Go Live
8. Analysts start getting comfortable with the tools.
9. Create Custom content as per requirement

Explain SOC Implementation Phases.

1. Define Scope
2. Implement Technologies
3. Hire and Build Team
4. Develop Policies, Processes and Procedures
5. CMM Level 3 (Initial – Managed -- Defined State)
6. Develop KPIs – (Quantitatively Managed)
7. Automate – (Optimized)

Explain SOC Workflow.



What metrics do you use in SOC?

KPI	Why Do We Care?	Possible Measurements	Assessment of...
Number of devices being monitored	· How many devices are being monitoring? · Is the number increasing or decreasing? Why?	· Number of devices · Number of devices / analyst	· Workload
Total number of events	· How many events are being handled? · Is the number increasing or decreasing? Why? · Are the current staffing levels adequate?	· Number of events / hour (/ analyst) · Number of events / day (/ analyst) · Number of events / month (/ analyst) · Number of events / year (/ analyst) · Number of events / event type	· Cost to value · Key risks · Workload
Number of events per device or host	· How many events are received for each device or host? · Are there certain devices or hosts which are more prone to security issues, causing increased risk? Why? · Are there certain devices or hosts which are more prone to false positive events? Why?	· Number of events per device or host/day · Number of events per device or host/month · Number of events per device or host/year · Number of events / device or host type · Number of events / operating system type	· Detection success · Key risks
Number of events per location	· How many events are received per geographic location, office, etc.? · Are certain locations more prone to security events? Why?	· Number of events / department · Number of events / office · Number of events / region	· Key risks
Number of false positive alerts	· How many false positive events are received? Is this acceptable? · Can the number of false positive events be reduced? How?	· Number of false positives / hour · Number of false positives / day · Number of false positives / month · Number of false positives / year · Percentage of events that are false positives	· Detection success
Time to detection	· How long is it taking your organization to detect a security event? Is this acceptable? · Are there ways this time to detection can be reduced? How?	· Measured in minutes, hours or days... · Average time to detection · Average time to detection / technology · Average time to detection / event type · Outliers	· Detection success · Process success
Time to resolution	· How long is it taking our organization to resolve an actual security event? Is this acceptable? · Are there process or technology improvements that can be made to reduce this time? What are they? · Are additional staff or training required? How many staff or what additional training is required?	· Measured in minutes, hours or days... · Average time to identify · Average time to identify / technology · Average time to identify / event type Outliers	·Analyst skills ·Process success
Escalation level	· How many events are being escalated and to what level? · Are events being escalated too quickly or not soon enough? Why? · Are there improvements to the escalation process that can make event handling more efficient? What are they? · Is the training for each level sufficient to produce the desired skill level? If not, what additional training is required?	· Average number of events / level · Average number of events / level / (time period) · Escalation level / event type · Escalation level / technology · Average time (min or hours) to escalate	· Analyst skills · Cost to value · Process success

What do you document in Shift Handover?

Items	Comments
Shift Start Time	18 Feb 2020 | 6:00 AM
Shift End Time	18 Feb 2020 | 15:00 PM
Any on-going issues?	Any alert analysis pending? Any teams waiting for update from SOC team?
Incident Details	Incident raised during the shift • Incident Number • Incident Name & Description • Severity • Assigned to (Team) • Status
Task Handover	Reports to pull

Difference between Blueteam vs Redteam.

Red team is a responsible for offensive security. Typically they do penetration testing, exploiting vulnerabilities, social engineering and various recon activities

Blue team is a responsible for monitoring, detection and responding to a possible threat.

A team that does both Red team and Blue team activities is called a Purple Team

What documents do you create in SOC?

Log Source On-boarding

Log Source Decommissioning

Threat Intel gathering procedure

Threat Hunting methodologies

New Use case development procedure

Staff on-boarding procedure

Play-book/Run-book (Investigation Procedures)

Data/Config backup Procedure

What is SOP/ RunBooks/ PlayBooks?

A step-by-step guide to handle an alert in Security Operation Center

Usually followed by L1 Security Analyst

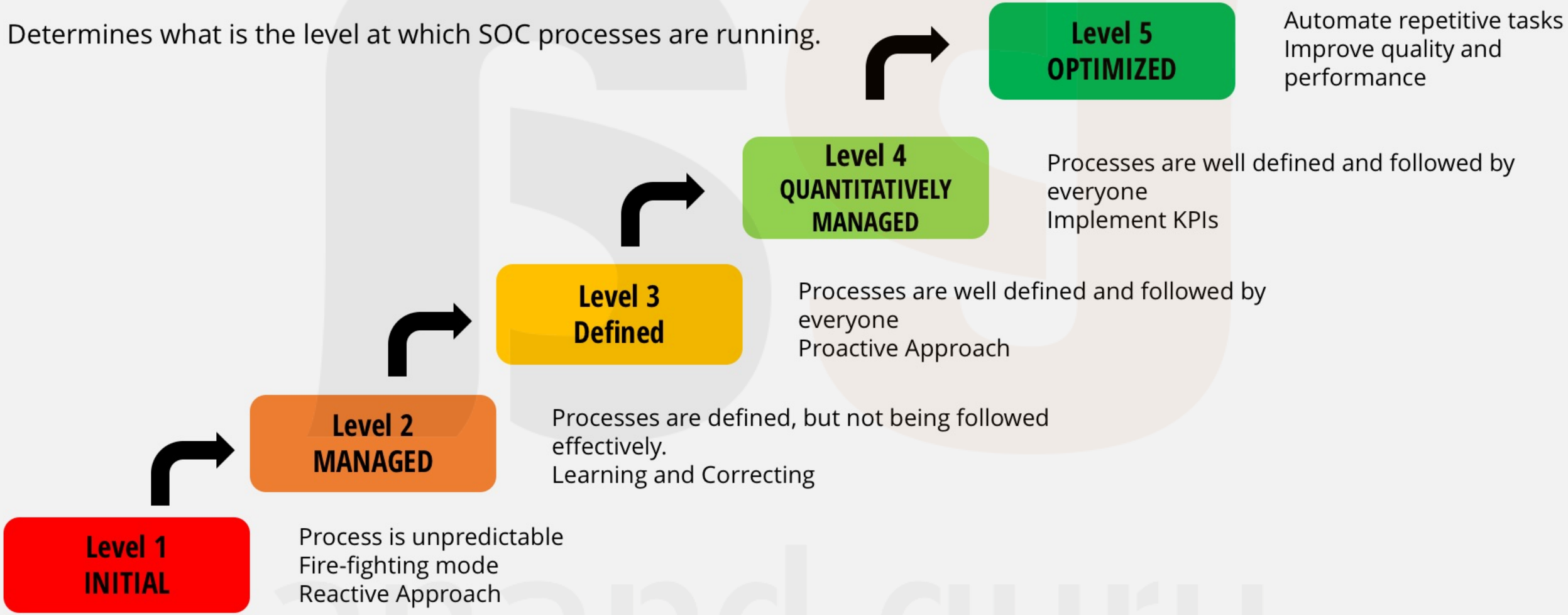
This helps in maintaining the quality of analysis and incident documentation

SOPs also reduce the time to respond

Explain CMM level as applied to SOC.

CMM stands for Capability Maturity Model

Determines what is the level at which SOC processes are running.



How do you handle a P1 incident in your SOC?

- In our organization, the SLA for P1 incident is 30 minutes.
- We have an internal process of involving SOC Lead within first 10 minutes of a P1 alert.
- Lead will take a call of which other teams assistance could be required.
- Open a bridge call and all the stake holders will be notified about the incident.
- I continue to provide the assistance to the lead by pulling reports or checking the status of affected services etc.

What will you do if there are 200 alerts triggered at once?

- If there are so many alerts, it is most likely possible that the same alert has triggered several times.
- So I will isolate the duplicate alerts.
- If there are different alerts, I will sort them by priority and pick the one with high priority and impact.
- If the triggered alerts are for a new correlation rule, it is possible that it is configured incorrectly. I will pass this information to the SIEM Engineer for fine-tuning.

What do you discuss in client calls?

- We have weekly call with the customer
- We discuss things like
  - Incident Trends
  - Threat Indicators Summary
  - SLA Report and KPIs
  - SIEM Health Report
    - EPS
    - New log sources
    - Silent log sources
    - New Correlation Rules