The Report 11

Created @June 25, 2025 11:05 AM

Scenario
This challenge is an extension for an existing 'The Report' challenge where you are working in a newly established SOC where there is still a lot of work to do to make it a fully functional one. As part of the SOC improvement process, you were assigned a task to study a report released by MITRE and suggest some useful outcomes for your SOC. Note: Answer the questions with the answers as the way you see in the document to avoid formatting issues.

SCOPE

Report Link: https://www.mitre.org/sites/default/files/publications/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

First PDF file was given to solve this challenge: As a new SOC Analysts make an habit of create notes

Stage 1: Extract the Download zip

Lab Challenge

Question 1) Submit the name of the units/teams (in short form) that are responsible for maintaining network and other IT equipment, incident detection and response, and security compliance and risk measurement (Format: Team1, Team2, Team3)

Ans:

The question is about:

1. team NOC - Network Operating Centre They are responsible for maintaining and IT equipments
2. team SOC - Security Operating Centre: Responsible for incident detection and response
3. team ISCM - Information Security Continious Monitoring of security compliance and risk measurement

Question 2) After investigation, what are the 4 suggested 'Response Options' mentioned in Basic SOC Workflow? (Format: Option1, Option2, Option3, Option4)

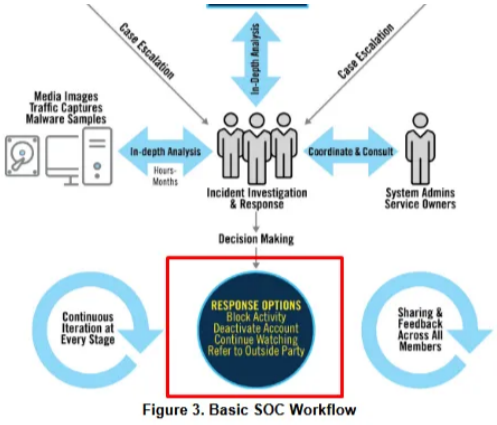
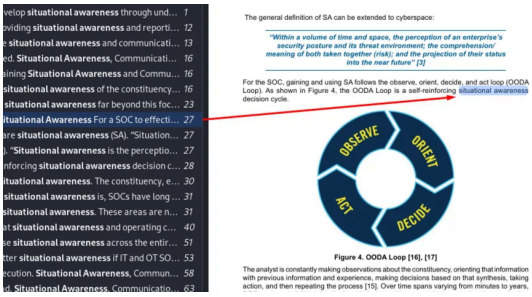


Figure 3. Basic SOC Workflow

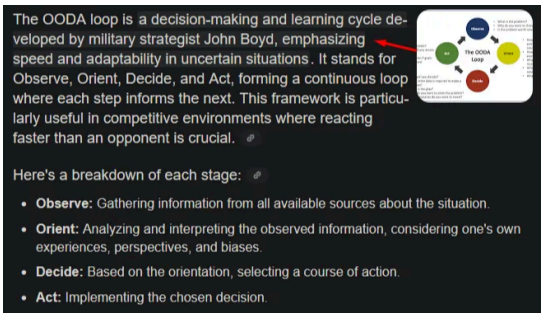
Ans: Block Activity, Deactivate Account,Continue Watching, refer to our party

Question 3) What is the name of a military strategy used in SOCs to achieve a high level of situational awareness? (Format: Strategy Name)

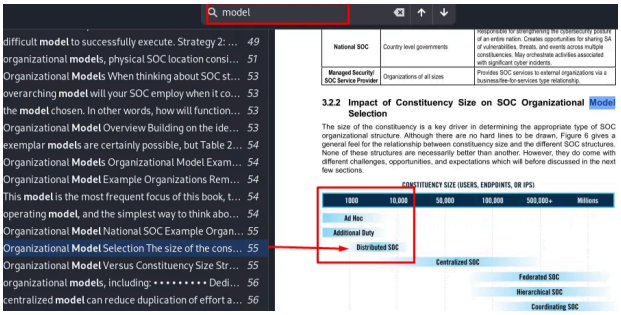
according to Google OODA was develop by military strategist



Explanation: I used situational awareness keyword to find the Answer in pg 28 explain OODA loop used



Question 4) What is the name of the suggested organizational model if the constituency size is between 1000 to 10,000 employees (Format: Organisational Model Name)



Ans Distributed SOC

Question 5) In a Large Centralised SOC, who is responsible for generating SOC metrics, maintaining situational awareness, and conducting internal/external trainings? (Format: Role Name)

On page 62, section 3.3.3 explains what a Large Centralized SOC is about. However, on page 64, there is a hierarchy tree showing what a SOC Operations Lead is responsible for.

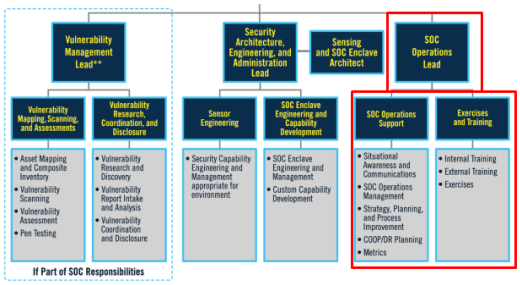


Figure 9. Large SOC

Answer: SOC Operational Lead

Question 6) What are the two virtual console technologies (in short form) mentioned to support Virtual SOC/ Remote Work scenarios during pandemics? (Format: Technology1, Technology

3.7.3 Succeeding with Virtual SOCs and Work from Home

Some SOCs find it necessary to locate elsewhere or virtually for one or more of the following reasons:

- Lack of physical space at/near the headquarters
- Lack of available security talent at/near the headquarters
- A predominate virtual workplace, flexible workplace, or work from home culture
- Widespread health or geopolitical event, such as the COVID19 pandemic

The global phenomenon of COVID19 response forced virtually all SOCs to shift to a partial or total work from home conditions. Regardless of the reasons, the SOC should observe the following tips and tools for making virtual and work from home cultures successful:

- Computing and tool infrastructure that supports remote work.
  - Leverage remote access virtual private network (VPN), virtual console like Integrated Lights-Out (iLO)/Integrated Dell Remote Access Controller (iDRAC), and cloud-based technologies

keyword: virtual console Answer: iLO, iDRAC

Question 7) In Coordinating & National SOCs model what are the 2 functions mentioned as Optional Capability under Expanded SOC Operations Category? (Format: Function1, Function2)

3.4.1 Capability Template

Table 4 illustrates a typical capability offering for several of the SOC organizational models described in Section 3.2.1. It is important to recognize that this table describes the capabilities of each SOC once they have matured into a steady state. In other words, it outlines a target state, not a maturation path; a handful of typical maturation paths are described further in the capability maturation section. Additionally, this table only serves as a starting point—a SOC must always tailor what they take on and how they fulfill organizational needs.

Table 4. Capability Template

	Security As Additional Duty	Distributed SOCs Staffed from Centralized & Federated SOCs	Large/Mature Centralized & Federated SOCs	Hierarchical SOCs	Coordinating & National SOCs
Incident Triage, Analysis, and Response					
Real-Time Alert Monitoring and Triage	b	b	a	a	n
Incident Reporting Acceptance	b	b	a	a	a
Incident Analysis and Investigation	b	b	a	a	a
Containment, Eradication, and Recovery	b	b	a	a	a
Incident Coordination	b	b	a	a	a
Forensic Artifact Analysis	n	o	b	a	a
Malware Analysis	n	o	a	a	a
Fly-Away Incident Response	o	o	b	a	a
Cyber Threat Intelligence, Hunting, and Analytics					
Cyber Threat Intelligence Collection, Processing, and Fusion	o	b	a	a	o
Cyber Threat Intelligence Analysis and Production	n	o	b	a	a
Cyber Threat Intelligence Sharing and Distribution	n	o	b	a	a
Threat Hunting	o	o	a	a	o
Sensor and Analytics Tuning	b	b	a	a	o
Custom Analytics and Detection Creation	o	o	a	a	o
Data Science and Machine Learning	n	o	b	a	o
Expanded SOC Operations					
Attack Simulation and Assessments	n	o	b	a	a
Deception	n	n	o	o	o
Insider Threat	n	n	o	b	o

keyword: capability or SOC operations Answer:Deception, Insider Threat

Question 8) What is the name of the model used to distribute work load of SOC 24/7 across different timezone to eliminate working at night hours? (Format: Model Name)

3.7.8 Follow the Sun

In the "follow the sun" model, the SOC has two or three ops teams, each separated by many time zones. Each ops floor is on the watch during local business hours (e.g., 9 a.m. to 5 p.m.). In a three ops floor arrangement, at roughly 5 p.m. local time, one ops floor roll to the next ops floor, where it is 9 a.m. This pattern continues every eight hours, giving 24x7 coverage but without making people come to work in the middle of the night. A similar pattern ensures for two ops floors working 12 hours each.

This approach is very common for IT help desks that serve wide geographic regions (e.g., with major IT vendors and very large corporations). There are several advantages to follow the sun, including:

- Far fewer analysts, particularly those in triage roles, are routinely required to work at night.
- Analysts on shift are more likely to share the language and culture of those calling during their shift.
- In terms of labor costs, it also may be more affordable than a single ops floor staffed 24x7 because:
  - Paying people during normal business hours may be less expensive than paying them to come in at night.
  - Some of the ops centers may be located in geographic regions with lower median income for security analysts.
- In the case of a high-criticality incident, in contrast to a single site asymmetrically-staffed SOC, it may be easier to keep more staff in the office and working the issue 24x7 until resolution.

keyword: SOC 24×7. Answer: Follow the sun.

Question 9) Submit the priorities(Low, Medium, High) assigned to Phishing, Insider Threat and Pre-incident Port Scanning activities respectively as per the Incident Prioritization mentioned in the document (Format: Priority1, Priority2, Priority3)

On page 128, section 5.2.1 "Prioritizing Incident Categories" identifies the types of attacks the SOC sees in Table 6. The categories show the answer

Table 6. Sample Incident Prioritization Planning [116], [117]

Incident/Event	Priority Level	Response or Action
Most port Scanning activity (pre-incident)	Low	Ignore most of these. Block or incorporate into detection if scans are tied to other reconnaissance, a known bad reputation, or there are multiple events from the source.
Malware infection	Medium	Remediate any malware infections as quickly as possible before they progress. Scan the rest of the constituency or enclave for associated indicators (e.g., SHA256 hashes).
Denial of service	Low-Medium, depending on duration	Configure affected externally facing services/systems e.g., web servers) to protect against DoS requests (e.g., HTTP and/or synchronized (SYN) flood). Coordinate with Internet Service Provider (ISP) to block/reroute the activity.
Unauthorized access	High	Detect, monitor, and investigate all unauthorized access attempts; prioritize mission-critical or sensitive data. Remediate through rebuilding accounts, systems, etc. as determined.
Insider threat	High	Identify associated privileged accounts for all domains, servers, apps, and critical devices. Ensure monitoring is enabled. Shut down access and/or coordinate with authorities where appropriate.
Web attacks (XSS, SQL ingestion, Cross-Site Request Forgery (CSRF), etc.)	High	Follow unauthorized access and/or malware response, depending on circumstance. Check web services, application, and database logs for extent of incident.
Phishing	Medium	Follow malware infection response or action. Check e-mail and other indicators for other recipients and attacks.

keyword prioritizing,priority level.

Question 10) Mention the name of the Open source Operating system mentioned, that can help in mobile incident investigations (Format: OS Name)

Tools and techniques for investigating will vary, depending on the mobile and wireless policies of the constituency. Some of the open source, free, or widely available tools are the following:

- **Santoku:** Open-source tools available and specific for mobile forensics, malware, and security; the toolkit enables investigators to image and analyze devices as well as decompile and disassemble malware and binaries [155].
- **Mobile device management (MDM):** Software installed on clients which support central management and implement security features specific to the type of device. Several commercial providers provide MDM software for clients and can integrate with central management, including Unified Enterprise Management (UEM); for example, Microsoft provides MDM natively, providing ability for clients to be enrolled, and a management server and client MDM protocol [156].
- **Mobile threat defense (MTD):** Software that can actively block enrolled devices from affecting constituency resources when malware and other threats are detected. Several commercial solutions exist and can be integrated into the constituency. For example, Microsoft provides Intune, which can integrate other MTD commercial solutions to actively block mobile devices considered compromised (including with malware) [157].

keyword: open source, mobile. Answer:Sankotu