Write-up: "the Report II " Challenge – Blue Team Labs Online

Objective: Extract actionable insights from MITRE's *11 Strategies of a World-Class Cybersecurity Operations Center* to improve the maturity of a newly established SOC.

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

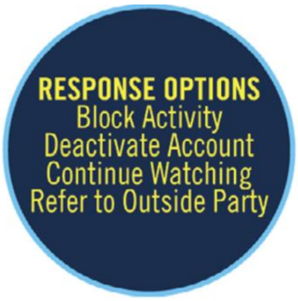
1. Summary

In *The Report II*, the analyst is placed in the role of a security professional supporting the development of a newly created SOC. As part of the SOC maturity process, the analyst is tasked with reviewing the MITRE publication *11 Strategies of a World-Class Cybersecurity Operations Center*. The goal is to extract organizational best practices, workflow methodologies, and technical recommendations relevant to incident detection, response, risk measurement, and long-term SOC sustainability. This report summarizes the key concepts identified during the challenge, aligned with the questions presented, and highlights their relevance to real-world SOC operations.

2. Questions and Answers

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.
Answer: NOC, SOC, ISCM

- NOC (Network Operations Center): manages infrastructure and connectivity.
- SOC (Security Operations Center): handles security monitoring and incident response.
- ISCM (Information Security Continuous Monitoring): focuses on compliance and risk posture.



RESPONSE OPTIONS
Block Activity
Deactivate Account
Continue Watching
Refer to Outside Party

Question 2
After investigation, what are the 4 suggested 'Response Options' mentioned in Basic SOC Workflow?
Answer: Block activity, deactivate account, continuous watching, refer to outside party
These represent the four basic response paths available in a SOC after triaging an alert, depending on severity and context.

Question 3
What is the name of a military strategy used in SOCs to achieve a high level of situational awareness?
Answer: OODA Loop
For the SOC, gaining and using SA follows the observe, orient, decide, and act loop (OODA Loop). As shown in Figure 4, the OODA Loop is a self-reinforcing situational awareness decision cycle.

Question 4

What is the name of the suggested organisational model if the constituency size is between 1000 to 10,000 employees?

Answer: Distributed SOC

This model provides central coordination with distributed presence across business units or regions, suitable for mid-sized organizations.

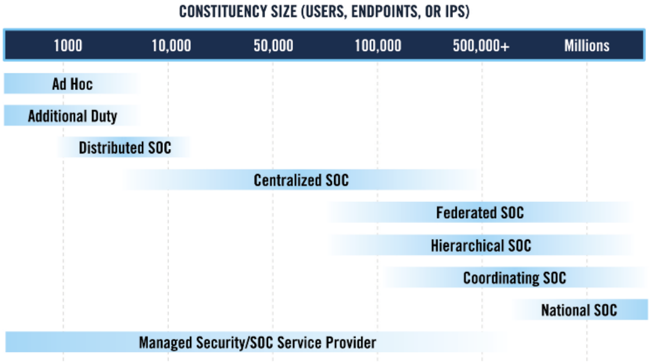


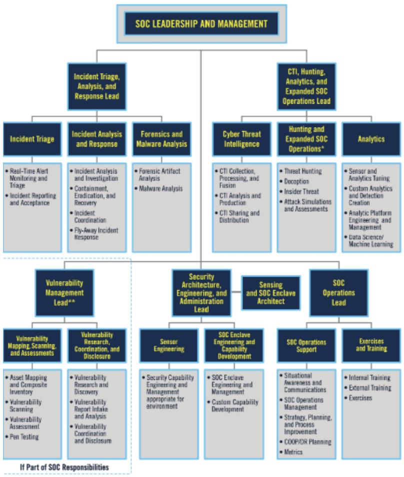
Figure 6. SOC Organizational Model Versus Constituency Size

Question 5

In a Large Centralised SOC, who is responsible for generating SOC metrics, maintaining situational awareness, and conducting internal/external trainings?

Answer: SOC Operations Leader

The SOC Operations Leader ensures operational oversight, drives reporting, and leads training initiatives to maintain readiness and accountability.

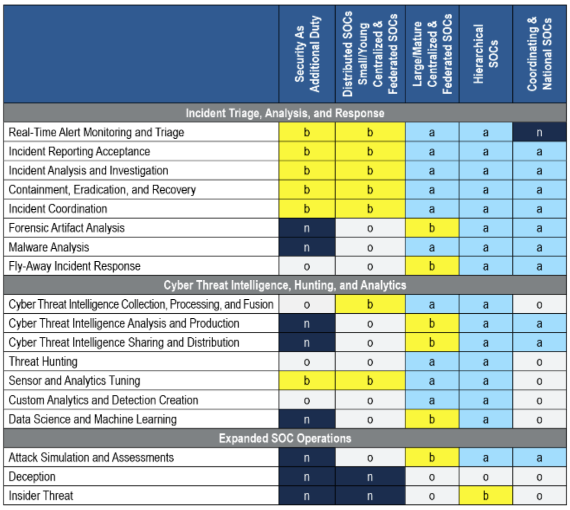


SOC LEADERSHIP AND MANAGEMENT
Incident Triage, Analysis, and Response Lead
CTI, Hunting, Analytics, and Expanded SOC Operations Lead
Incident Triage
• Real-Time Alert Monitoring and Triage
• Incident Reporting and Acceptance
Incident Analysis and Response
• Incident Analysis and Investigation
• Containment, Eradication, and Recovery
• Incident Coordination
• Fly-Away Incident Response
Forensics and Malware Analysis
• Forensic Artifact Analysis
• Malware Analysis
Cyber Threat Intelligence
• CTI Collection, Processing, and Fusion
• CTI Analysis and Production
• CTI Sharing and Distribution
Hunting and Expanded SOC Operations*
• Threat Hunting
• Deception
• Insider Threat
• Attack Simulations and Assessments
Analytics
• Sensor and Analytics Tuning
• Custom Analytics and Detection Creation
• Analytic Platform Engineering and Management
• Data Science/ Machine Learning
Vulnerability Management Lead**
Vulnerability Mapping, Scanning, and Assessments
• Asset Mapping and Composite Inventory
• Vulnerability Scanning
• Vulnerability Assessment
• Pen Testing
Vulnerability Research, Coordination, and Disclosure
• Vulnerability Research and Discovery
• Vulnerability Report Intake and Analysis
• Vulnerability Coordination and Disclosure
If Part of SOC Responsibilities
Security Architecture, Engineering, and Administration Lead
Sensing and SOC Enclave Architect
Sensor Engineering
• Security Capability Engineering and Management appropriate for environment
SOC Enclave Engineering and Capability Development
• SOC Enclave Engineering and Management
• Custom Capability Development
SOC Operations Lead
SOC Operations Support
• Situational Awareness and Communications
• SOC Operations Management
• Strategy, Planning, and Process Improvement
• COOP/DR Planning
• Metrics
Exercises and Training
• Internal Training
• External Training
• Exercises

Question 6

In Coordinating & National SOCs model, what are the 2 functions mentioned as Optional Capability under Expanded SOC Operations Category?

Answer: Deception, Insider Threat



	Security As Additional Duty	Distributed SOCs Small/Young 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

For each SOC organizational model(s), and each potential SOC service, a recommendation is given:

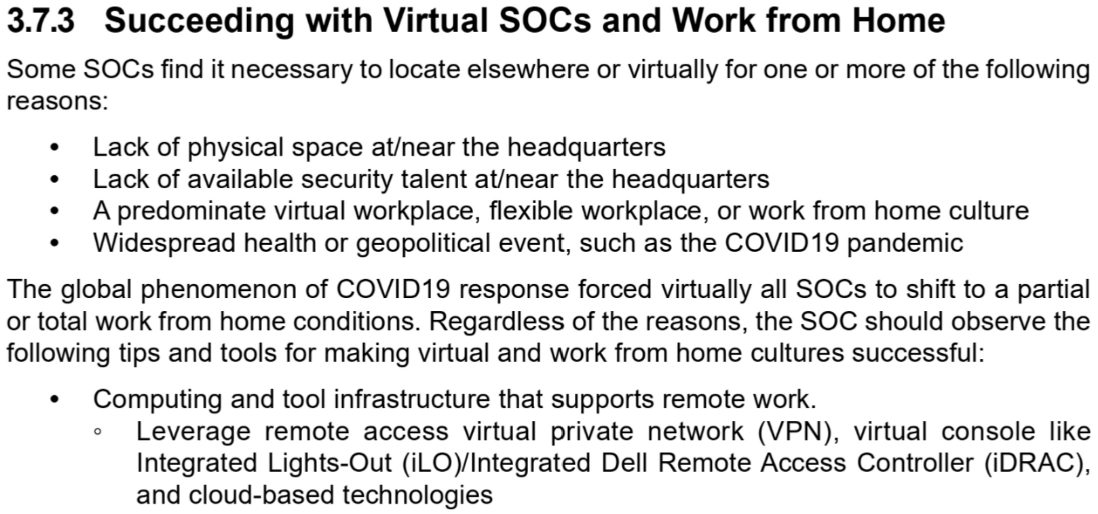
- **Basic (b):** SOCs in this category typically offer this capability/service at a basic level of performance inside the SOC.
- **Advanced (a):** SOCs in this category offer this capability/service at a more advanced, mature level of performance inside the SOC.
- **Optional (o):** SOCs in this category may or may not offer this capability or function. Their choice to do so usually has more to do with their maturity, resourcing, focus, and external requirements than necessarily their organizational model.
- **Not recommended (n):** SOCs in this category are unlikely to offer this capability or function in house. This is usually due to foundational capability and competency not being present, resources being limited, or scoping the focus to what is most appropriate for the organizational model type.

Question 7

What are the two virtual console technologies (in short form) mentioned to support Virtual SOC/ Remote Work scenarios during pandemics?

Answer: VNC, RDP

Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP) enable remote access to SOC systems during distributed operations.



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:

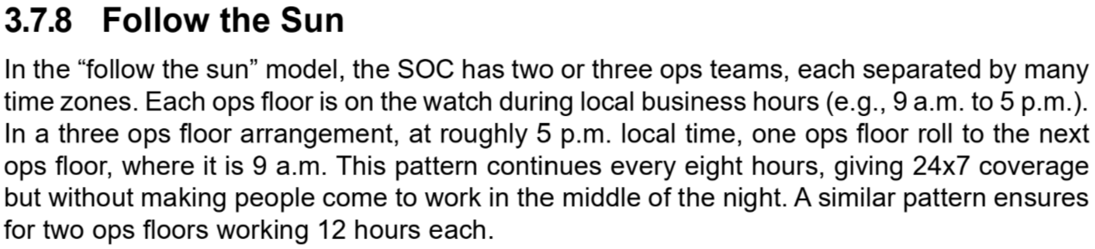
- Computing and tool infrastructure that supports remote work.
  - Leverage remote access virtual private network (VPN), virtual console like Integrated Lights-Out (iLO)/Integrated Dell Remote Access Controller (iDRAC), and cloud-based technologies

Question 8

What is the name of the model used to distribute workload of SOC 24/7 across different timezones to eliminate working at night hours?

Answer: Follow the Sun

This model rotates responsibilities between geographically distributed teams, allowing 24/7 coverage without overnight shifts.



3.7.8 Follow the Sun

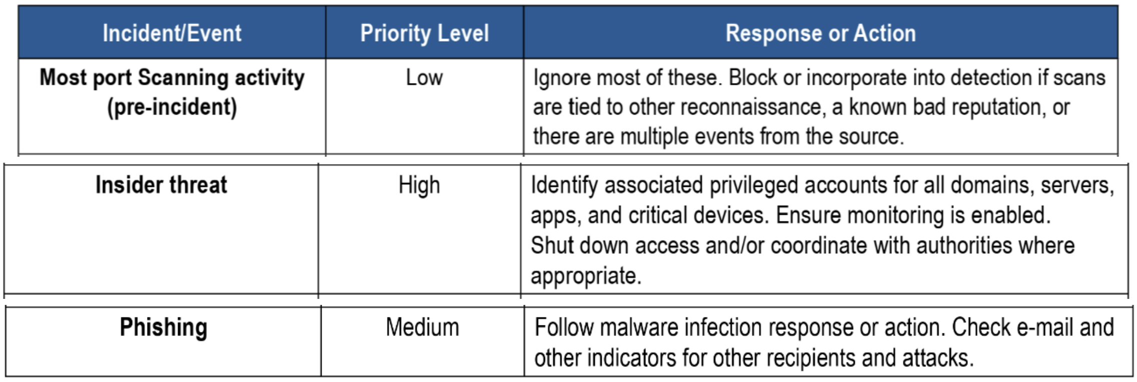
In the “follow the sun” model, the SOC has two or three ops teams, each separated by many time zones. Each ops floor is on the watch during local business hours (e.g., 9 a.m. to 5 p.m.). In a three ops floor arrangement, at roughly 5 p.m. local time, one ops floor roll to the next ops floor, where it 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.

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.

Answer: Low, High, Medium

Insider Threat poses the highest risk, phishing is more manageable, and port scanning indicates early-stage reconnaissance.

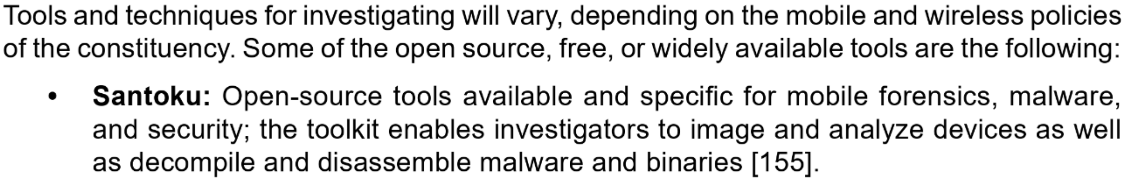


Incident/Event	Priority Level	Response or Action
Most port Scanning activity (pre-incident)	Low	Ignore most of these. Block or incorporate into detection if scans are tied to other reconnaissance, a known bad reputation, or there are multiple events from the source.
Insider threat	High	Identify associated privileged accounts for all domains, servers, apps, and critical devices. Ensure monitoring is enabled. Shut down access and/or coordinate with authorities where appropriate.
Phishing	Medium	Follow malware infection response or action. Check e-mail and other indicators for other recipients and attacks.

Question 10

Mention the name of the Open source Operating system mentioned, that can help in mobile incident investigations.

Answer: Santoku



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:

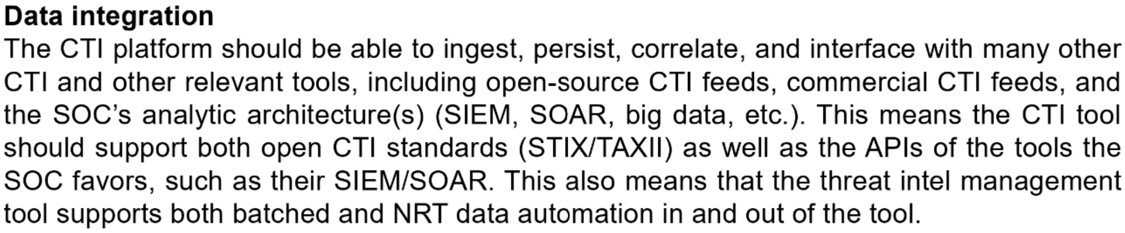
- **Santoku:** Open-source tools available and specific for mobile forensics, malware, and security; the toolkit enables investigators to image and analyze devices as well as decompile and disassemble malware and binaries [155].

Question 11

Before choosing a CTI tool, the document suggests tool support for 2 open threat intelligence standards (short forms), what are they?

Answer: STIX, TAXII

Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) are standards for sharing threat intelligence in machine-readable formats.



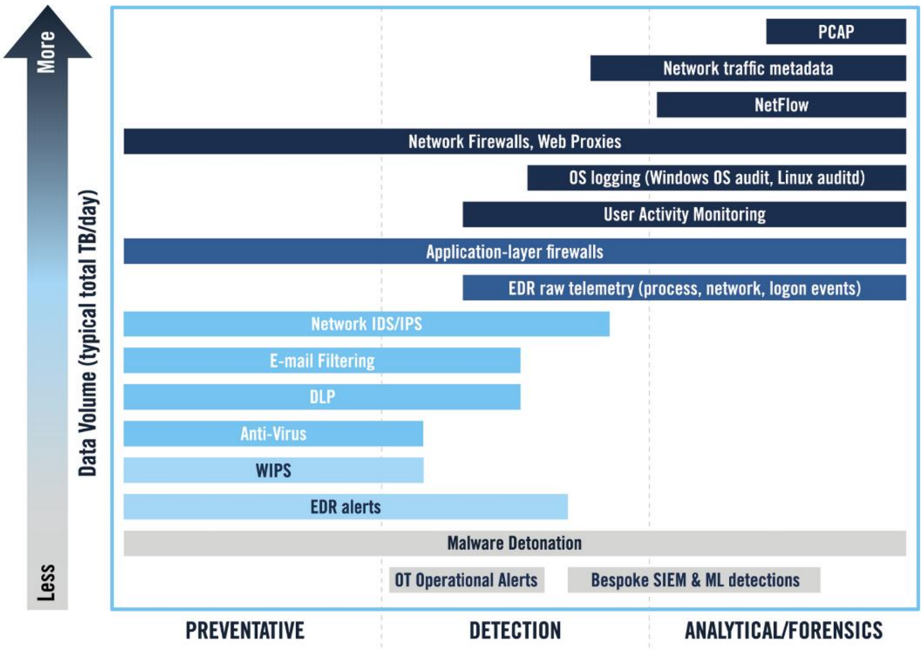
Data integration

The CTI platform should be able to ingest, persist, correlate, and interface with many other CTI and other relevant tools, including open-source CTI feeds, commercial CTI feeds, and the SOC's analytic architecture(s) (SIEM, SOAR, big data, etc.). This means the CTI tool should support both open CTI standards (STIX/TAXII) as well as the APIs of the tools the SOC favors, such as their SIEM/SOAR. This also means that the threat intel management tool supports both batched and NRT data automation in and out of the tool.

Question 12

Name the Data Source which consumes the highest volume (typically TB's/day)?

Answer: PCAP

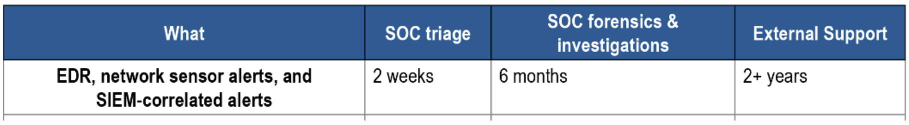


Question 13

In order to support forensics, what is the recommended data retention period (in months) to store logged EDR data?

Answer: 6

Table 15. Suggested Minimum Data Retention Time Frames



What	SOC triage	SOC forensics & investigations	External Support
EDR, network sensor alerts, and SIEM-correlated alerts	2 weeks	6 months	2+ years

Question 14

According to the threat intelligence concept the 'Pyramid of Pain', what indicators are Trivial, Easy, Challenging, Tough for adversaries to change?

Answer: Hash values, IP Addresses, Tools, TTPs

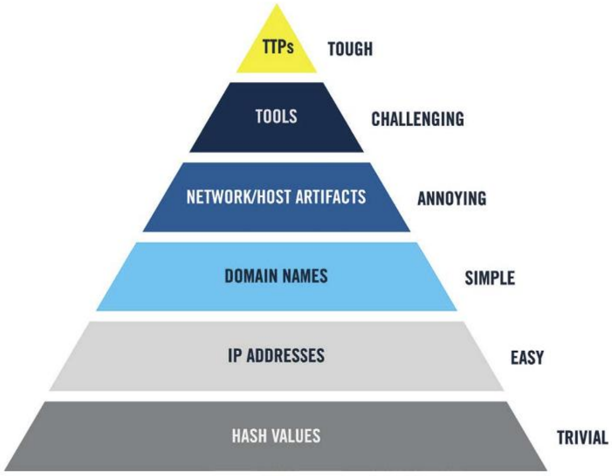
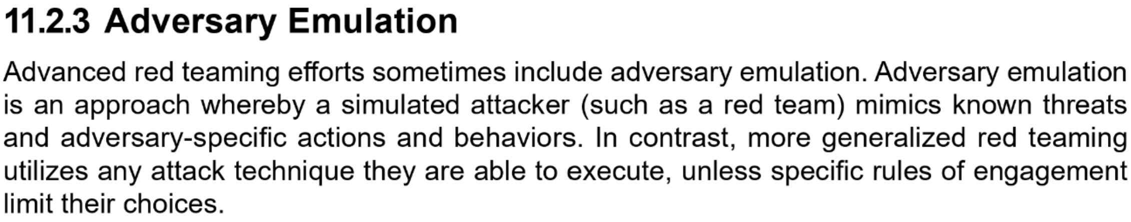


Figure 40. Pyramid of Pain [431]

Question 15

Name of the Red Teaming approach to mimic the TTPs of an adversary?

Answer: Adversary Emulation



11.2.3 Adversary Emulation

Advanced red teaming efforts sometimes include adversary emulation. Adversary emulation is an approach whereby a simulated attacker (such as a red team) mimics known threats and adversary-specific actions and behaviors. In contrast, more generalized red teaming utilizes any attack technique they are able to execute, unless specific rules of engagement limit their choices.

3. Conclusion

The *Report II* challenge reinforces the need to align a SOC’s strategy with globally recognized frameworks. Through an in-depth analysis of the MITRE guidance, the analyst identified critical recommendations across organizational design, response options, and tooling standards. These insights are essential for any team striving to build a resilient, scalable, and intelligence-driven Security Operations Center.