**The Fundamentals of SOC**

The Fundamentals of Security Operations Centre training is a high-level introduction to the general concepts of SOC and SecOps. This lesson provides an overview of the Security Operations framework.

The Fundamentals of Security Operations Centre training is a high-level introduction to the general concepts of SOC and SecOps. It will introduce the Security Operations framework, people, processes, and technology aspects required to support the business, the visibility that is required to defend the business, and the interfaces needed with other organizations outside of the SOC.

The training consists of nine lessons and will take approximately 3 hrs to complete. This training is intended for learners who want to enter the field of cybersecurity - whether a student entering the workforce or an established professional transitioning from another field - and will help them demonstrate knowledge about SOC. It is recommended that the lessons be taken in order, but the menu below can be used to access any lesson, should you wish to determine your own learning path.

**Lesson 1** - Day in the Life of a SOC Analyst

This lesson provides an overview of the Security Operations framework.

Duration 20 minutes

**Lesson 2** - Business

The Business pillar defines the purpose of the Security Operations team to the business.

Duration 20 minutes

**Lesson 3** - People

The People pillar defines the humans that will be accomplishing the goals of the Security Operations team.

Duration 20 minutes

**Lesson 4** - Processes

The Processes pillar defines the processes and procedures executed by the Security Operations organization.

Duration 20 minutes

**Lesson 5** - Interfaces

The Interfaces pillar defines what functions need to be involved to achieve the stated goals.

Duration 20 minutes

**Lesson 6** - Visibility

The Visibility pillar defines what information the SecOps function needs.

Duration 20 minutes

**Lesson 7** - Technology

The Technology pillar increases the capabilities for Security Operations to complete its core mission.

Duration 20 minutes

**Lesson 8** - SOAR

SOAR is the automation of the orchestration of all the elements of Security Operations.

Duration 20 minutes

**Lesson 9** - SOAR Solution

Cortex XSOAR is a Security Orchestration, Automation, and Response (SOAR) platform.

Duration 20 minutes

***Lesson 1: Day in the Life of a SOC Analyst***

a SOC analyst on the Security Operations team and it is his job to triage alerts to determine if there is a security threat. Before Erik starts his job, he will need to understand the general concepts of SOC and SecOps, and the business goals. Erik will need training and support from the people he interacts with on a daily basis. While mitigating threats, Erik will need to know the processes to follow, the teams he will be interacting with, and the technology he will be using to gain visibility into the network.

***Lesson 2: Business***

Both Erik and the SOC team are responsible for protecting the business. The reason for Security Operations, for all of the equipment, for everything SOC does is ultimately to service one main goal, protect the business. Without the Business pillar, there would be no need for Erik or the SOC team.

The Business pillar defines the purpose of the Security Operations team to the business and how it will be managed. The Business pillar helps to provide Erik and the rest of the SOC team with answers to questions such as "Who do we need to help protect the business?"; "How will we protect the business?"; "Where are we going to do this from?"; and "How do we know if what we have in place is working effectively?"

***Lesson 3: People***

The People pillar defines who will be accomplishing the goals of the Security Operations team and how they will be managed. As a part of the People pillar, Erik received training necessary for him to be able to triage the alerts in addition to the other processes and functions within the SOC.

This training provides Erik with the skills necessary to become efficient at detecting and prioritizing alerts. As Erik’s knowledge increases, he will have opportunities to grow on the SOC team. He will also have the skills to advance in his career to other areas.

***Employee Utilization***

Methods should be developed to maximize the efficiency of a Security Operations team specific to the existing staff. Security Operations staff are prone to burnout due to console burn out and extreme workloads. To avoid this, team members should be assigned different tasks throughout the day. These tasks should be structured and may include:

• Shift turnover stand-up meeting (beginning of shift)

• Event triage

• Incident response

• Project work

• Training

• Reporting

• Shift turnover stand-up meeting (end of shift)

Another tactic to avoid burnout is to schedule shifts to avoid high-traffic commute times. Depending on the area, 8am-5pm may line up with peak (vehicle) traffic patterns. Shifting the schedule by two hours could reduce stress on the staff.

***Training***

Proper training of staff will create consistency within an organization. Consistency drives effectiveness and reduces risk. Use of a formal training program will also enable the organization to bring on new staff quickly. Some organizations resort to on-the-job or shadow training for new hires, which is not recommended on its own. While shadowing other analysts during initial employment in the SOC is important, it should not be the only means of training.

***Lesson 4: Processes***

While monitoring the ticketing queue, Erik notices a new set of alerts that has been sent to the SOC team by one of the network devices. Based on the alert messages, Erik needs to determine whether the alert message is a security incident, so he opens an incident ticket. Erik starts by doing his initial research in the log files on the network device to determine if the threat is real. After reviewing the log files, Erik determines that the alert is a real threat. Based on the Severity Triangle, Erik has determined that the severity level for this alert is currently High.

The Processes pillar defines the step-by-step instructions and functions that are to be carried out by the SOC team for the necessary security policies to be followed. Processes are a series of actions or steps taken to achieve an end goal. As part of the Processes pillar, Erik will need to determine the other teams that should be involved, the scope of the work for each team, and what each team will be responsible for.

***Lesson 5: Interfaces***

The alert generated by the network device; he partners with the Threat Intelligence Team to identify the potential risks this threat may pose to the organization. Erik also interfaces with the Help Desk, Network Security Team, and Endpoint Security Teams to determine the extent the threat has infiltrated the network.

Security operations is not a silo and needs to work with many other functions or teams. Each interaction with another team is described as an interface. The Interfaces pillar defines which functions need to take place to help achieve the stated goals, and how the SOC will interface with other teams within the organization by identifying the scope of each team’s responsibilities and the separation of each team’s duties.

***Lesson 6: Visibility***

A detailed analysis of the threat, he will need to gather all of the necessary information to make a well-informed decision. Network visibility is needed for Erik to gather information about the network’s status, the traffic passing through the network, and the conditions on which traffic is allowed to pass through. Without network visibility, Erik may miss important data that could lead to a real threat being treated as a false positive or missed altogether. The better visibility Erik has into every aspect of the company’s network, the better he and the SOC team can make an informed decision.

The Visibility pillar enables the SOC team to use tools and technology to capture network traffic, limit access to certain URL’s determine which applications are being used by end users, and to detect and prevent the accidental or malicious release of proprietary or sensitive information.

***Lesson 7: Technology***

The beginning of our scenario has been mitigated. Erik now needs to work with SOC team members and other teams to determine if the current network technology can be used to automate a process or response to automatically remediate this issue, or similar issues that may arise.

The Technology pillar includes tools and technology to increase our capabilities to prevent or greatly minimize attempts to infiltrate your network. In the context of IT Security Operations, technology increases our capabilities to securely handle, transport, present, and process information beyond what we can do manually. By using technology, you amplify and extend your abilities to work with Information in a secure manner.

***Lesson 8: SOAR***

Scale is one of the biggest challenges for SOCs. We stepped through each pillar to mitigate a threat, but while Erik was working on one threat, alerts and incidents continued to pour in. The number of incidents that each member of the SOC team must respond to is greater than what can be managed through human intervention.

The only reasonable long-term solution is to empower existing resources with a combination of innovative orchestration, artificial intelligence, and machine learning technologies to automate many of the manual processes that a SOC team faces each day. By automating processes, the SOC team can focus its attention on what is truly critical: identifying, investigating, and mitigating emerging cyberthreats.

***Lesson 9: SOAR Solution***

Cortex by Palo Alto Networks offers solutions that improve SOC efficiency. Cortex XDR and Cortex XSOAR in particular allow SOC analysts like Erik to do in minutes what would take them hours to resolve otherwise. It is tools such as these that will allow SOCs to scale into the future.