Resumen

La gestión de eventos de ciberseguridad puede presentar demoras y dificultades en el momento en que las herramientas de detección, análisis y respuesta funcionan de forma independiente y necesitan actividades manuales. Frente a esta problemática, la presente investigación tiene como propósito diseñar e implementar un entorno de orquestación y automatización para la respuesta ante incidentes en el laboratorio de Ciberseguridad, como referencia en las capacidades funcionales de XSOAR junto con las herramientas Wazuh, TheHive, Cortex y MISP. La investigación adoptó un enfoque tecnológico aplicado, con alcance exploratorio, descriptivo y cuasiexperimental. La arquitectura fue aplicada sobre una máquina virtual Ubuntu Server y utilizó Docker y Docker Compose para el despliegue de los servicios en contenedores. Se trabajó con escenarios controlados de archivos sospechosos, fuerza bruta SSH y movimiento no autorizado de un archivo protegido. Durante las cinco ejecuciones del escenario de archivo sospechoso el tiempo medio de detección obtenido es de 0,007 segundos, 15,734 segundos de tiempo medio de respuesta y 16,407 segundos de tiempo promedio de extremo a extremo. Para la prueba de fuerza bruta SSH el tiempo de respuesta registrado fue de 15,844 segundos. A su vez, se obtuvieron cinco verdaderos positivos en las pruebas de efectividad, por último, las actividades consideradas en los flujos evaluados fueron ejecutadas de manera automática. Durante las pruebas de carga, los 35 eventos fueron gestionados de manera correcta, sin que se evidencien interrupciones por tiempo de espera, Así mismo, las pruebas de persistencia corroboran con la recuperación de los nueve servicios contenerizados y recuperación del flujo luego de los reinicios. Los resultados indican que el entorno planteado funciona de manera correcta para realizar prácticas controladas. No obstante, los resultados obtenidos se encuentran limitados a los escenarios y necesidades evaluadas.

***Palabras clave**:* SOAR, MTTD, MTTR, XSOAR

Abstract

When detection, analysis, and response tools begin to function independently and necessitate manual tasks, managing cybersecurity events can cause delays and challenges. Using the functional capabilities of XSOAR and the tools Wazuh, TheHive, Cortex, and MISP as references, the current study attempts to address this problem by designing and implementing an orchestration and automation environment for incident response in the cybersecurity laboratory. A technologically applied strategy with an experimental and descriptive scope was created for the study. The architecture was implemented on a virtual machine running Ubuntu Server, and services were deployed in containers using Docker and Docker Compose. Unauthorized movement of a secured file, SSH brute force, and controlled scenarios of suspicious files were investigated. The suspicious file scenario was executed five times, with an average detection time of 0.007 seconds, an average reaction time of 15.734 seconds, and an average end-to-end time of 16.407 seconds. The recorded response time for the SSH brute force test was 15.844 seconds. At the same time, the efficacy tests yielded five true positives, and ultimately, the actions taken into account in the assessed flows were carried out automatically. The 35 events were handled properly during the load tests, and there was no indication that waiting time caused any disruptions. Similarly, the flow recovery following restarts and the recovery of the nine containerized services are verified by the persistence tests. The findings show that the suggested setting is operating as intended for carrying out regulated procedures. Nevertheless, the outcomes are restricted to the demands and circumstances that were assessed.

***Keywords**:* SOAR, MTTD, MTTR, XSOAR