Diseño e implementación de un Centro de Operaciones de Seguridad (SOC) basado en cómputo en la nube

Design and implementation of a Security Operations Center (SOC) based on cloud computing

Ing. Fredy Fernando Álvarez Sánchez[a]*, Dr. Víctor Manuel Morales Rocha[a]
[a]Maestría en Cómputo Aplicado, Departamento de Ingeniería Eléctrica y Computación, Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez, México.
*Autor de correspondencia. Correo electrónico: al228230@alumnos.uacj.mx

N.° de resumen
7CP24-5

Formato
Ponencia

Tema
Cómputo Aplicado

Presentador
Fredy Fernando Álvarez Sánchez

Fecha de la presentación
Mayo 28, 2024

Estatus
Estudio en curso

Resumen

Esta investigación tiene como objetivo la creación de una herramienta de Software como Servicio (SaaS) enfocada en el análisis inteligente de amenazas. Esta herramienta integrará sistemas de recopilación de datos y herramientas de análisis para establecer las bases de un Centro de Operaciones de Seguridad (SOC). Al desarrollar el software, se utiliza la metodología para realizar un modelo de prototipo por desarrollo evolutivo para poder ofrecer a los usuarios una vista previa del programa o sistema en el contexto de un SOC. También es necesario considerar diferentes metodologías no solo relacionadas con el software, sino también la interacción con sistemas de información y elementos físicos, así como las evaluaciones de los resultados. La principal herramienta por considerar será la información proporcionada por los sistemas informáticos de acceso a la red, para posteriormente realizar un análisis de la información que brindan estos, utilizando algoritmos de IA como herramientas secundarias. La presente etapa se enfoca en la investigación del estado del arte, así como del análisis de amenazas para conocer las necesidades del caso de uso y aplicación. Se enuncian también las limitaciones que se consideran para el desarrollo del proyecto. Por otra parte, se describen algunos términos importantes sobre el tema como es la inteligencia de amenazas y los principales proveedores comerciales. Por último, se describe también un modelo teórico de arquitectura de un SOC, así como los roles del personal involucrado en el funcionamiento de este.

Palabras clave: SOC; SaaS; nube; logs; IA.

Abstract

This research aims to create a Software as a Service (SaaS) tool focused on intelligent threat analysis. This tool will integrate data collection systems and analysis tools to establish the foundations of a Security Operations Center (SOC). When developing the software, the methodology is used to perform a prototyping model by evolutionary development to provide users with a preview of the program or system in the context of a SOC. It is also necessary to consider different methodologies not only related to the software, but also the interaction with information systems and physical elements, as well as the evaluations of the results. The main tool to be considered will be the information provided by the network access computer systems, to subsequently perform an analysis of the information provided by these, using AI algorithms as secondary tools. The present stage focuses on the investigation of the state of the art, as well as the threat analysis to know the needs of the use case and application. The limitations considered for the development of the project are also stated. On the other hand, some important terms on the subject such as threat intelligence and the main commercial providers are

described. Finally, a theoretical model of SOC architecture is also described, as well as the roles of the personnel involved in its operation.

Keywords: SOC; SaaS; cloud; logs; TI.

Entidad legal responsable del estudio

Universidad Autónoma de Ciudad Juárez

Financiamiento

Fredy Fernando Álvarez Sánchez, becario CONAHCYT (Beca Nacional Tradicional 2022 -2024).

Conflictos de interés

Los autores declaran que no existe conflicto de intereses.