Resumen

Con el creciente avance tecnológico que existe en la actualidad, las organizaciones tienen que afrontar múltiples retos. Uno de los retos que ha llamado más la atención de los expertos durante los últimos años, ha sido la ciberseguridad. Con el uso cada vez más frecuente de la tecnología, encontrarse con ciberdelincuentes ya no es algo tan extraño como lo era hace varios años. De hecho, se ha visto una mayor actividad en estos tiempos, tanto que su aumento es preocupante. Es por ello que se han implementado dispositivos de seguridad perimetral para salvaguardar la información de las personas y las organizaciones. Sin embargo, el inconveniente surge cuando cada dispositivo genera su propio *log,* alerta o alarma y no se tiene una plataforma centralizada en donde se pueda recopilar y visualizar esta información en conjunto. El área del ESPE-CERT presenta esta necesidad, por lo cual, en el presente trabajo de titulación, se planteó la instalación de un servicio de monitoreo mediante un correlacionador de eventos (SIEM), que permita satisfacer las necesidades del negocio, que no interrumpa el funcionamiento de los demás servicios y que sirva como una herramienta de apoyo para los mismos. Para conseguir esto, en primer lugar, se realizó una revisión sistemática de literatura, donde se expusieron trabajos similares; en segundo lugar, se aplicó el proceso marcado por la *Information Technology Infrastructure Library* (por sus siglas en inglés, ITIL) para gestionar de manera eficiente un servicio de tecnologías de la información (por sus siglas, TI), este desarrollo tiene las actividades: plan, diseño y transición, entrega y soporte, operación y mejora. Al pasar por cada una de ellas y llegar a la entrega y soporte, se pudo observar que el funcionamiento de SIEM Wazuh (herramienta seleccionada) cumplía con los requisitos, recopilaba la información en un nodo central y no afectaba al funcionamiento de los demás servicios del nodo. Finalmente, se desarrollaron las conclusiones y recomendaciones, teniendo en cuenta los resultados observados durante la operación y las mejoras sugeridas por el evaluador.

Palabras clave: SIEM, ITIL, correlación de eventos, eventos de seguridad, incidentes de seguridad.

Abstract

With the growing technological advance that exists today, organizations have to face multiple challenges. One of these challenges, that has attracted the most attention from experts in recently years, has been cybersecurity. With frequent use of technology, encountering cybercriminals is not strange as it was several years ago. In fact, there has been a greater activity in these times, so much so that its increase is worrying. That is why perimeter security devices have been implemented to safeguard the information of people and organizations. However, the drawback arises when each device generates its own log, alert or alarm and there is no centralized platform where this information can be recollected and viewed as a whole. The ESPE-CERT area presents this need, for which reason in this titling work, the installation of a monitoring service through an event correlator (SIEM) was proposed, which allows satisfying the needs of the business, which does not interrupt the operation of the other services and that serves as a support tool for them. To achieve this, firstly, a systematic review of the literature was carried out, in this stage, we presented similar works; Secondly, the process marked by the Information Technology Infrastructure Library (ITIL) was applied to efficiently manage an information technology (IT) service. This development has the activities: plan, design and transition, delivery and support, operation and improvement. When going through each one of these phases and arriving at the delivery and support, it was possible to observe that the operation of SIEM Wazuh (selected tool) fulfilled the requirements, collected the information in a central node and did not affect the operation of the other node services. Finally, the conclusions and recommendations were developed, taking into account the results observed during the operation stage and the improvements stage suggested by the evaluator.

Keywords: SIEM, ITIL, event correlation, security events, security incidents.