World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:03, 2019

Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems

Authors : M. Mutemwa

Abstract : A Cybersecurity Operation Centre (SOC) is a centralized hub for network event monitoring and incident response. SOCs are critical when determining an organization's cybersecurity posture because they can be used to detect, analyze and report on various malicious activities. For most organizations, a SOC is not part of the initial design and implementation of the Information Technology (IT) environment but rather an afterthought. As a result, it is not natively a plug and play component; therefore, there are integration challenges when a SOC is introduced into an organization. A SOC is an independent hub that needs to be integrated with existing procedures, policies and IT systems of an organization such as the service desk, ticket logging system, reporting, etc. This paper discussed the challenges of integrating a newly developed SOC to an organization's existing IT environment. Firstly, the paper begins by looking at what data sources should be incorporated into the Security Information and Event Management (SIEM) such as which host machines, servers, network end points, software, applications, web servers, etc. for security posture monitoring. That is which systems need to be monitored first and the order by which the rest of the systems follow. Secondly, the paper also describes how to integrate the organization's ticket logging system with the SOC SIEM. That is how the cybersecurity related incidents should be logged by both analysts and non-technical employees of an organization. Also the priority matrix for incident types and notifications of incidents. Thirdly, the paper looks at how to communicate awareness campaigns from the SOC and also how to report on incidents that are found inside the SOC. Lastly, the paper looks at how to show value for the large investments that are poured into designing, building and running a SOC.

Keywords : cybersecurity operation centre, incident response, priority matrix, procedures and policies
Conference Title : ICDWDMTCSA 2019 : International Conference on Data Warehousing and Data Mining Techniques for Cyber Security Applications
Conference Location : Madrid, Spain
Conference Dates : March 26-27, 2019