Journal of Information Warfare

A cybersecurity architecture that supports effective incident response

Mutemwa, Muyowa; Mtsweni, Jabu S

Abstract
A Cybersecurity Operation Centre (SOC) is a centralized hub within an organisation that houses people, processes, and technologies aimed at continuous monitoring of the organization's assets to prevent, detect, analyse, and respond to cybersecurity incidents against that organisation. SOCs are critical to the collection, analysis, and response to cybersecurity events and incidents faced by an organisation. This article discusses the architecture of an SOC that enables quick and timely responses to events and incidents. Firstly, the article describes an architecture of the SOC, the SOC's processes, personnel, and technologies. Secondly, the article discusses what type of information and logs should be collected, analysed, and interpreted. Lastly the article discusses how to handle an incident through the six stages of incident response.