عنوان مقاله:

.Provide architecture for response to computer incident in framework NIST sp۸۰۰-۶۱ and ITIL

محل انتشار:

یازدهمین کنفرانس بین المللی فناوری اطلاعات،کامپیوتر و مخابرات (سال: 1399)

تعداد صفحات اصل مقاله: 7

نویسندگان:

Mahdi Sadeghi Ghahareh - *Master engineer computer, Department of computer, Faculty of Electrical and Computer Engineering, Islamic Azad University, Tehran north Branch, Tehran, Iran*

Nasser Modiri - *Assistant Professor, Department of Computer, Faculty of Electrical and Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran*

خلاصه مقاله:

In this paper provided response architecture for incident. This architecture is made for computer emergency response team (CERT) to incident response. This helps to team just for response. In this architecture used parameters NIST sp۸۰۰-۶۱ and also this is in framework NIST standard and ITIL framework. This architecture activated after discover incident and gain information about incident. This is response incident after pass a process. This architecture in this process makes documentary, report and etc. for incident response. In addition, defensive center can certain some incident (now can say these are threat) if necessary and when happens these are, CERT impact defensive or offensive to the threat. In the end this architecture can response incident in the form of documentary, limiting system that have response, reports to the defensive center and manager system or organ, defensive or offensive against .incident(or threat) and etc

کلمات کلیدی:

incident, response, defensive, offensive, ITIL, NIST, incident response

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1197105