Implementing a Security Operations Center at a Midwest University: A Case Study

TREO Talk Paper

Kenneth Shemroske
University of Southern Indiana
k.shemroske@usi.edu

Abstract

Cyber Security is an area that has become one of the top concerns amongst those in the field of information systems. It is a path along which areas of concentration, majors, minors, certificates, and many other approaches to curriculum development have been based. This study seeks to chronicle the design, implementation, and operation of a Security Operations Center (SOC) at one midwest university.

The process of designing the SOC has been started and several potential stakeholders have been identified. As this design has progressed, as expected, the detail of the conversations has increased. An interesting by product, which was not expected, is that the group of potential stakeholders has also grown. The purpose behind the SOC was originally created out of a need to provide curriculum support for the Cyber Security focus at this university. With the growing stakeholder group and increased levels of detail entering the discussions, it is now evident that this SOC may play multiple roles for the local and extended regions:

- The original intention of curriculum support (as an environment for 'hands-on' experience) will be served
- The CIO of the university has become interested in leveraging the resources of this center to support the cyber security profile of the campus
- Regional businesses have expressed an interest in utilizing the centers services to supplement their own short comings in resources
- The city where this university lives has expressed an interest in both the potential to utilize resources and for sharing information regarding cyber security threats
- The state to which this university belongs is interested in working with the center as part of a state wide initiative to create a unified cyber security grid

The intended SOC will be operated by students in the IS/CS undergraduate programs. Upon graduation, students may have an option to take on full time roles in the center as they become available. One intended goal of this center is to serve as a 'holding place' for talent in the cyber security domain until regional business organizations recognize the need to hire full time security analysts.

Several topics of interest will play a role in the development of research that may come out of this project. The extent to which businesses in the region (especially small to mid-sized) has education/awareness about their own cyber security profiles is currently affecting the employment rate of security analysts. The impact of this SOC on job availability will be monitored. The role of trust between employees of the SOC and external entities will be an important area of interest. Finally, details about the design process, implementation, and operation of the center could provide valuable direction to other universities that may be looking for ways to support their own cyber security curriculums and/or involvement in the community.