Mini Project 27: SOC Strategy Presentation

Mini-Project Overview

Time Estimate: 2 Hours

Read through this explanation of a SOC from Alert Logic before proceeding to **Project Submission Steps:**

> As you know, a SOC is a dedicated team of security analysts that monitor your IT environment, assess threats, provide threat intelligence against potential breaches or system weaknesses, and conducts deep incident analyses. It maintains a unified and efficient front against malicious attacks, detects unauthorized activity and provides 24×7 monitoring for your environment.
>
> Organizations find themselves stuck between two choices: building their own internal SOC or outsourcing to a security-as-a-service company that offers a SOC solution. Each of these options has its own benefits and drawbacks, but since each company is different, there is no “standard” answer.

(Yoo, M. (2016, September 29). In-House or Outsourced: What a Security Operations Center (SOC) Means to Your Organization. Alert Logic. https://www.alertlogic.com/blog/in-house-or-outsourced-what-a-security-operations-center-means-to-your-organization-d54/.)

Project Submission Steps

You are a cybersecurity analyst for a global energy services firm. The company has 600 sites across over sixty countries, and employees over 24,000 people. The IT environment is mostly Windows-based and uses Active Directory for authentication, but there are some systems running Red Hat Enterprise Linux and Solaris. These systems primarily run the financial reporting software, both at the corporate headquarters and in two other key locations: Dubai and Kuala Lumpur.

In addition, the company has industrial control systems at most of its sites that perform various functions such as monitoring pipelines and wind turbines. These systems are part of the Operational Technology (OT) environment and are separated from the corporate IT network for security reasons.

The company has grown quickly over the last few years, mainly as a result of mergers and acquisitions (M&A). As a result, it has become increasingly difficult to manage its security operations. Some sites are managed better and more effectively than others. Currently, the IT Security team is made up of a manager and three analysts, of which you are one. You and the other analysts use a variety of tools to manage and monitor both the IT and OT environments, but it's clear that the staff is overwhelmed, resulting in lower morale.

Management wants to address this situation as quickly as possible before people start leaving, and they need to know what their options are. They have asked your manager to deliver a presentation that lays out the options along with the pros and cons of each. However, he's busy fighting fires so he doesn't really have time to work on it. Since you are the only team member that has had formal cybersecurity training, he has tapped you to put something together for him.

*** Your task to is write a report (5-6 pages) comparing the following three strategies:**

1. Create an in-house SOC using FOSS (Free and Open Source Software) solutions. Examples include ELK Stack, OSSEC, and Kiwi Syslog Server.

2. Create an in-house SOC using commercial solutions.

3. Outsource the SOC to a third party MDR or SOCaaS. Assume that no members of the IT Security team will need to be eliminated if this option is selected since the vendor would simply end up being an extension of the existing team.

Be sure to include important data points such as additional FTEs (Full Time Employees), software licenses, cloud instances, and storage requirements. The average salary for a SOC/cybersecurity analyst is about $90,000/yr so use that for calculating FTE costs.