**SOC Strategy Presentation**

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.

Organisations 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.

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.

* Building an internal SOC or hiring a security-as-a-service company that provides a SOC solution are the two basic ways to install a SOC. Employing and educating a security staff is necessary to create an internal SOC building out the infrastructure, purchasing the required hardware and software, and hiring analysts to support the SOC's activities. On the other hand, outsourcing to a security-as-a-service provider requires negotiating a deal with a third-party provider who provides a SOC solution; this option may be more affordable for smaller enterprises or those with limited resources. A SOC is an essential part of a company's cybersecurity strategy since it offers capabilities for continuous monitoring, threat detection, and incident response to guard against potential cyber threats and attacks.

The decision of which solutions to use will depend on a number of variables, including money, personnel knowledge, and special security requirements. Building an internal SOC (Security Operations Center) requires much planning and consideration.  
The

following are the steps to build an internal SOC using FOSS:

* Define your security goals and requirements.
* Examine the FOSS options and choose the ones that best fit your needs. FOSSproducts include, for instance, ELK Stack, OSSEC, and Kiwi Syslog Server. On your network, install and configure the FOSS solutions you've chosen.
* To identify potential security threats and incidents, develop monitoring and alerting procedures.
* Educate your personnel on how to use the tools correctly and react to security incidents.
* Create communication guidelines for coordinating incident response and exchanging security-related information.
* To ensure the SOC's efficiency, constantly review and tweak it.

Benefits

* Since FOSS solutions are open source and cost nothing to use, this strategy is economical.
* FOSS solutions are very flexible, permitting the business to fit them to its own requirements.
* There is a sizable user base for FOSS solutions, giving access to a wealth of knowledge and experience

Disadvantages

* Technical experience is require, the company's IT security staff may encounter difficulties setting up and managing FOSS solutions because they demand technical know-how.
* Compared to commercial solutions, FOSS solutions may only receive a limited amount of support, forcing the company to rely more largely on community help.
* It may be difficult to integrate FOSS solutions with the business's current systems, which will require more technical know-how to fix.

more expenses:

* To set up and run the SOC, the organisation would need to engage more staff with expertise in FOSS solutions.
* To support the FOSS solutions, the company might need to buy more cloud instances.
* To support the SOC, the company might need to buy more storage.

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

* Describe your security goals and requirements.
* Evaluate the commercially available options and pick the ones that best fit your needs. The commercial products IBM QRadar, Splunk, and McAfee SIEM are a few examples.
* Invest in and implement the chosen commercial solutions on your network.
* Configure the solutions to your unique security requirements and incorporate them with your current security tools.
* Create rules for alerting and monitoring to find potential security threats and occurrences.
* Provide staff training on how to use the tools efficiently and handle security incidents.
* Develop communication guidelines for exchanging security-related details and planning incident responses.
* Keep an eye on and improve the SOC constantly to ensure its performance.

Benefits:

* Commercial solutions frequently include technical support, reducing some of the workload for the IT security staff.
* Commercial solutions are frequently made to be simple to use, making them available to a wider range of employees.
* To reduce the need for additional technical know-how, commercial solutions are made to integrate with a variety of existing systems.

Disadvantages:

* Commercial solutions are often more expensive than FOSS solutions since they

typically demand licence fees.

* provider lock-in: Commercial solutions might lock the company down to a single

vendor, restricting future flexibility.

* Compared to FOSS alternatives, commercial solutions could be less adaptable, which restricts a company's ability to customise the SOC to meet its particular requirements.

Additional expenses

* To handle the commercial SOC, the organisation may need to hire more employees.
* In order to use the commercial solutions, the company would need to obtain software licences.
* To support the commercial SOC, the company might need to buy more cloud instances.
* To support the commercial SOC, the company might need to buy more storage

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 licences, 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.

Benefits:

* By outsourcing SOC services, a corporation is able to change the service level as needed.
* Third-party providers often have a high level of technical skills that minimises the workload on the IT Security team.
* Third-party vendors can offer 24/7 coverage  
    
  Disadvantages

* When outsourcing, a company's ability to ensure the security of its systems and data

may be compromised. There could be security vulnerabilities if the third-party

provider doesn't always have a thorough understanding of the company's security

requirements, rules, and culture.

* In order to manage and monitor its security activities, the organisation becomes

dependent on the third-party provider. This may add another level of complexity

and dependency, especially if the provider's availability or level of knowledge

is restricted.

* Outsourcing has the potential to lighten the load on the internal IT security staff, but it

can also be pricey. The amount that third-party suppliers charge for their

services depends on a number of things, including the degree of service needed

for the size