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.

In our global energy services firm with 600 sites spanning across sixty countries, the monitoring and managing of both the IT and Operational Technology (OT) environments needs to be addressed. 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 make up the IT environment and primarily run the financial reporting software. The industrial control systems that are part of OT monitor the pipelines and wind turbines. The firm is expanding rapidly and the security staff cannot handle the workload of monitoring both IT and OT. The recommendation is to make some changes to the Security Operations Center (SOC). One of the three options needs to be chosen and each option has it's advantages and disadvantages. There are a few issues that need to be looked at for each option before the final decision is made and they are as follows:

- Each Full Time Employee (FTE) in the SOC earns an average of $90,000/year
- Software licenses will need to be purchased for any commercial products
- Cloud instances need to be configured for the expansion of the in-house SOC
- Storage requirements need to be expanded as the in-house SOC expands

ELK Stack, an open source software solution, is one of the options for monitoring and monitoring the global energy services firm. Elastic Stack is the newer version of ELK Stack with more flexibility. "ELK" is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a JSON-based search engine that performs analytics. Kibana was developed to be the visual interface of the data stored in elastic search. For example, a dashboard would display charts and graphs of the data. A common scenario in Elastic stack is a plot of the total number of clients visiting a website and showing the traffic in real time. It also allows you to filter the website traffic based on location and the specific browser in use. Logstash is a data processing pipeline. The data that logstash receives is handled as events ranging from operating system log file data to e-commerce orders. For example, after logstash processes the log entries it sends the results to elasticsearch. A feature known as X-Pack can perform abnormality detection and forecasting. For example, if forecasting indicates that there is heavy Linux and Solaris CPU usage then EC2 server instances can be started on AWS to handle the extra workload in the IT environment. Elastic stack can perform the following as a SOC solution:

- Monitor infrastructure and application performance and usage
- Use for threat and business intelligence
- Use for storage and analysis of geospatial data

Elastic stack has the following advantages if chosen as a SOC solution:

- As long as the software is not integrated with the firm’s own modifications, Elastic stack remains open source.
- Elastic stack integrates well with the Industrial Internet of Things (IIOT) that is necessary to monitor the devices in the firm’s OT environment. The firm’s OT environment consists of different kinds of devices such as pipeline and wind turbine sensors. These use different technologies to communicate with the internet. Using sensor data is very effective for analyzing the health of IoT devices. With Elastic you can collect, enhance, and analyze IIoT data and create alerts in case of a failure.
- Amazon ElasticSearch Service is a fully managed service that makes it easy for the firm to deploy, secure and operate 19 versions of open source Elasticsearch. In addition this Amazon service integrates with Amazon IoT that gives the firm the flexibility to select the data ingestion tools necessary for the gas and electric industrial control systems. In addition, the OT environment consisting of the industrial control systems used Supervisory Control and Data Acquisition (SCADA) systems which is a system architecture for managing complex processes and controlling functions over a large geographical area. AWS IoT integrates AWS services to SCADA systems by deploying simple sensors to monitor processes without replacing existing hardware. Therefore, with AWS IoT the firm can scale IoT applications to millions of devices.
- Since Elastic stack is open source, there is no cost in licensing. The only cost will be to hire two or three Full Time Employees (FTE’s) which get paid $90,000 annually. The total cost will then be roughly $200,000 to $300,000 annually.

The disadvantages of using an in-house SOC solution such as Elastic stack are as following:

- If the SOC is in-house, the energy services firm will not be able to focus on it’s core business which is to provide energy. This will result in the extra cost of hiring skilled people to do the job and the extra cost of training current or new employees.
- The Elastic stack has changed it’s licensing and there is a higher security risk for the firm in keeping it’s operations confidential. With the previous license, Elastic stack could be freely incorporated into the firm’s software.Under the new license, there is a risk of being forced to release all of the firm’s code.

The firm might want to consider using Splunk as an in-house commercial SOC solution. Splunk can be used to manage and monitor the firm's IT and OT environment. There is a great amount of functionality in Splunk and it is easy to use. It helps resolve problems in the following areas:

Network security where it generates alerts for any security threats

Systems where it reports on any failure condition in the IT and OT infrastructure

CPU, memory and networks where it analyzes the data from bottlenecks in order to make decisions about the ways to improve machine functionality.

Data comes from many sources such as servers, cloud services, IoT, mobile devices and websites. These sources produce machine data which is complex and unstructured however, Splunk can leverage this data and generate dashboards and reports. The most important usages of Splunk are:

- Analyze system performance
- Search and investigate an outcome
- Troubleshoot any failure condition
- Create dashboards to visualize and analyze results
- Monitor business metrics
- Store and retrieve data for later use

Industrial Control Systems (ICS) also known as SCADA are responsible for keeping the critical infrastructure such as electric and oil & gas refineries that the firm services all running safely and continually. The three areas customers are concerned with involving ICS that the firm needs to address are:

- Keeping the systems running and reducing downtime
- Protecting ICS from cybersecurity threats
- Optimizing the ICS processes to reduce waste of time and maintenance

The Splunk Essentials for ICS Monitoring and Diagnostics primary focus is the monitoring of ICS systems in order to reduce downtime. When the customer proactively identifies concerning areas, diagnoses problems and responds productively to them, downtime can be kept to a minimum. Most importantly as a SOC solution for the firm, the Splunk Enterprise Security software is responsible for security monitoring, advanced threat detection, and rapid threat investigation and response.

AWS and Splunk, an AWS Partner Network (APN) Security Competency Partner and help the firm implement better cloud security. Since the firm is expanding at a rapid pace, the cloud will serve as a way to get on-demand resources to meet the demand. For example, the firm will spin up EC2 Linux and Solaris instances. It will also use the AWS Storage Gateway which is a hybrid cloud storage solution that provides on-premises access to basically unlimited cloud storage. Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help protect the firm's workloads. Using Splunk in AWS, the firm can use GuardDuty events and perform correlation searches with diverse data sources and various AWS services such as AWS CloudTrail data. These data sources can then be used to confirm a threat, investigate root cause and determine remediation steps. Splunk strengthens the security of the firm's data on AWS with end-to-end visibility. Splunk integrates with many AWS services such as GuardDuty, CloudWatch and Kinesis to collect and index machine-generated data to deliver security in real-time, detect threats and operate effectively. For the purchase of the Splunk license, it is recommended that the firm use ingest pricing. Ingest pricing offers volume-based pricing to the firm based on GB/day data ingestion into Splunk products. Since the firm is growing at a fast pace, the license will reflect the data generated by the firm and it will pay only for what it needs. With this kind of license, term licenses are available for on-premises and annual subscriptions are available for cloud solutions.

The third option the firm has is to outsource the SOC to Rapid7 which is a third party MDR. Rapid7 is a cloud-based security platform that transforms data into observations and reports. The Rapid7 platform consists of the following core security solutions:

- Allow the firm to monitor the OT and IT environments for malicious activity
- Manage vulnerabilities
- Investigate and block threats
- Automate operations
- Application security
- Cloud security

The firm can choose any combination of solutions it requires to monitor and manage the IT and OT environments. Pricing varies according to the solutions that are chosen by the firm. Incident detection and response is core to Rapid7 and therefore makes it a reliable SOC solution. It has the ability to shutdown intrusions. Before attackers reach critical assets, Rapid7 combines behavior analytics, activity monitoring, endpoint protection and automated threats to hunt down threats and block attackers. Once malicious activity is observed through anomaly detection, an alert is triggered and the investigation begins. The Incident Response dashboard displays an entire view of what is happening across the entire network including the time and location of the malicious activity. This visibility will allow the SOC to prioritize threats and take remediatiary actions. This will prevent future data breaches. Another core element of Rapid7 is vulnerability management. The Top Vulnerabilities Threat Feed is entered into this solution which is then used to collect information on new risks displaying the threats that put the most risk to the firm's infrastructure and which assets would be compromised. The SOC will then generate tickets to address the vulnerabilities that would need to be resolved and the steps needed for the fix. The advantages of Rapid7 are that it is easy to use and that it is cloud based. The firm also pays for what they need. The disadvantages are that there has been an increase of false positives and negatives and irregular long scan times.

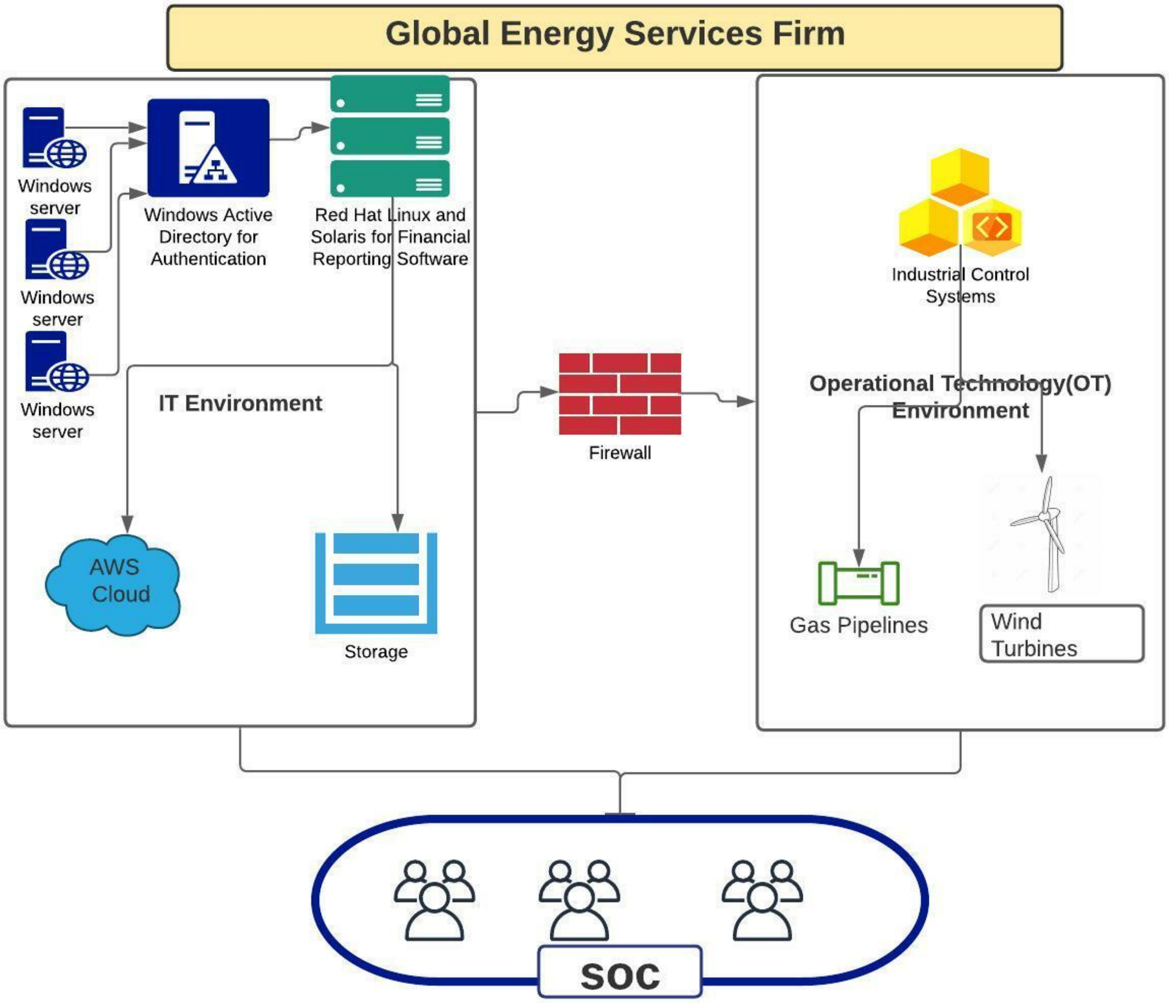
According to Rapid7, doing routine and ongoing assessments for vulnerability is not necessary, however, the firm needs to understand the assets in the OT environment and how they communicate with each other for a more effective approach to control system monitoring. Security monitoring is static in the ICS environment. This is different from the IT environment which consists of a diverse amount of protocols and devices. For example, there are no patches available for the ICS. For ICS the firm only sees machine to machine behavior. Looking at patterns of data moving from one device to another and being able to pick out vulnerabilities is key to finding any malicious activity. For the ICSs, the devices cannot be taken down. It is crucial that there is no downtime and the maintenance window usually occurs once annually.

There are benefits and disadvantages for outsourcing. Some benefits are:

- Overall decreased cost for the firm's security operations
- Increased security expertise of the employees in the SOC
- The firm can focus on it's core business which is to provide gas and electricity
- There is more scalability in a SOC if it is out-sourced if there is an increase in the amount of work.

The risks of outsourcing the SOC are:

- The out-sourcing vendor might have strict policies in place resulting in less flexibility.
- There might be a misalignment of goals between the firm and the vendor.
- There could be hidden costs such as regulatory fines.


Global Energy Services Firm
Windows server
Windows server
Windows server
Windows Active Directory for Authentication
Red Hat Linux and Solaris for Financial Reporting Software
IT Environment
AWS Cloud
Storage
Firewall
Industrial Control Systems
Operational Technology(OT) Environment
Gas Pipelines
Wind Turbines
SOC