Security Operations Center Strategies

The purpose of a Security Operations Center (SOC) is to continuously monitor for incidents and respond to them as they occur to prevent loss. They perform intelligence gathering via threat research and analysis of logs. They conduct threat hunting, monitor IDS/IPS systems, and other blue team activities. The SOC is the central hub of cyber security for an organization, and it is crucial that it is able to respond effectively and rapidly to any security incidents.

Due to the higher quality and responsiveness it will provide, my recommendation is to build out our own internal SOC using Splunk as a SIEM.

Benefits and Risks of an In-House SOC VS. Outsourcing

Traditionally a SOC is operated with internal staff. However, it is becoming increasingly popular to outsource SOC operations to a third party who provides better availability and resources than an organization can allocate for an internal SOC. There are benefits and risks associated with each method.

The main benefits of housing an internal SOC have to do with closer relationships with those security engineers staffing it. A SOC which is directly staffed by internal employees will be more closely aligned with the business mission, and have a higher stake in protecting it. Executives also have more flexibility with in-house staff, allowing them to be temporarily focused on critical tasks that would fall outside the scope of a typical SOC. An internal SOC also allows closer monitoring and control if there are procedures that must be done a certain way according to our policies and regulations. Finally, an internal SOC will be able to provide immediate reports when a threat is discovered. The drawbacks of an internal SOC include the cost of all the employees needed to staff a 24/7 responsive SOC, and any software licenses we need to purchase. Additionally, there is a broad scope of tasks an SOC is responsible for, which may draw resources away from our core business tasks.

The foremost benefit of outsourcing a SOC is that it can be cheaper than maintaining one in house. A managed security service provider (MSSP) benefits from economies of scale, as it services many organizations. This also means they can provide more tools, and are generally more efficient. They also provide scalability. We are also better able to focus on our core, mission critical business tasks as they take care of the “grunt work” of security. The cons to outsourcing are the hidden costs, which may negate the savings of not having our own staff. Merely selecting a vendor can cost up to 2% of the deal value. There is also the time cost of transitioning our operations to a third party and training them. Layoffs, if they were to occur, would also be a cost factor. Aside from cost, quality of service could be a concern. For example, there can be communication barriers with an MSSP if they are in a foreign country. We will also have less control over specific procedures they follow, which could be a compliance problem. Finally, we will have less flexibility, as third party contractors cannot be temporarily reassigned if their labor could be better used elsewhere.

Considerations when Choosing a Method

There are several key points to consider when evaluating whether to go with in house or outsourcing. Since our organization is geographically spread out and built from multiple previous companies, we must consider the ability of our SOC to handle multiple operating systems, devices, and regulations from different countries. We will need to calculate the cost of additional employees needed to operate the SOC, or the monetary cost of outsourcing. There is also the cost of software licenses, cloud instances, and storage requirements. Finally, we will consider the time to respond to incidents, efficiency, and our ability to control the SOC.

First we will consider an in-house SOC built with Free/Open Source software, in this case the ELK stack. ELK is a suite that uses lightweight “beats” installed on endpoint devices to send data to a central ElasticSearch server. They support Mac, Windows, and Linux OSes, and send all data in a standardized Elastic Common Schema (ECS) format, making them easier to analyze. We will need to hire more employees to manage the software, especially at the beginning as it will need to be installed and configured on every endpoint in our organization. There are no monetary costs for licenses. ELK offers a cloud version, Elastic Cloud, either through themselves or through AWS, Microsoft Azure, or Google Cloud, which means we could easily incorporate it into existing cloud IT infrastructure at a cost. Storage requirements for logs will be comparable to if we used commercial products, and if we use the Elastic Cloud, they offer up to 540TB of storage through their Multi-Solution plan, or more if we use a custom plan. The time to response will be low once the system is set up and configured. Finally, this setup gives us the most control and flexibility over any of the options, as we are in direct control of both the staff and the application. Since it is open source it can be customized as we see fit.

Many of the considerations for an in house SOC using commercial software (Splunk) are similar to if we used open source software. We will likely have to employ fewer full time employees as a commercial product like Splunk will offer support and be easier to manage. Splunk also offers Splunk SOAR to automate many tasks. However, this comes at the trade off of needing to purchase an enterprise license.

The considerations for outsourcing are different from using in house. Many of the minute concerns are abstracted, as the MSSP will take care of the details for us. Instead of considering the cost of employees, we will need to look at the cost of our contract. The quality of service will impact the cost. The MSSP we select will have to be able to comply with regulations across international borders, which will also likely bring the cost up. We will have much less control over the operations than if we used an in-house SOC. Finally, outsourcing is known to lower staff morale.

Recommendation

Due to the spread-out nature of our company and the state of our IT situation, I recommend building our own SOC using Splunk for our SIEM, and hiring at least one more full time employee. I believe this is the best option for three primary reasons. First, in-house staff will be better able to conform to different regulations for sectors of our company in different countries. Second, internal staff will be more reliable and responsive to incidents as they occur. Third, morale will improve, as staff will be less overworked and better able to focus on core tasks as Splunk SOAR offers opportunities for automation. Although it will be more expensive than outsourcing, the above reasons as well as the greater amount of control we will be able to exercise makes this the best option for our company.