Comparison of Strategies for Improving SOC Operations for [Utility Provider]

Nathan Tendido

Cybersecurity Career Track, Springboard

May 20, 2023

[Utility Provider] is a global energy services firm which currently has 600 sites, across 60 countries, with well over 24,000 employees. As a result of recent M&A, [Utility Provider] has expanded quickly and is now facing increasing difficulties in managing its security operations. Current staff members are notably overwhelmed by the rapid increase in security operations and this has led to a visible decrease in employee morale. The result of which will inevitably lead to staff members leaving [Utility Provider], if not addressed soon. This report compares three strategies for improving security operations .

The three strategies to compare as as follows:

1. Create an in-house Security Operations Center (SOC) using FOSS (Free and Open Source Software) solutions.
2. Create an in-house SOC using commercial solutions.
3. Outsource the SOC to a third-party Managed Detection and Response (MDR) or SOC-as-a-Service (SOCaaS) provider.

1. Create an In-house SOC using FOSS Solutions:

This strategy involves building an in-house SOC using Free and Open Source Software (FOSS) solutions. Examples of FOSS solutions that can be utilized include the ELK Stack, OSSEC, and Kiwi Syslog Server.

Pro considerations for this strategy are:

- Cost-effective: FOSS solutions eliminate the need to manage commercial software licenses. These licenses can often be expensive, especially for a large organization like [Utility Provider].

- Customizability: FOSS solutions can be customized to fulfill company-specific requirements. FOSS solutions often offer a plethora of customizability from large community support as well as a large number of use cases to reference when considering builds.
- Community support: FOSS solutions benefit from the open source community that contributes to ongoing development and support.

Con considerations for this strategy are:

- Expertise and training: Building and maintaining an in-house SOC using FOSS solutions requires specialized knowledge and training. Depending on customizability goals, each FOSS may require in-depth expertise to build and maintain. In any cases with higher turnover, training may be expected to take longer periods of time.
- Scalability: FOSS solutions may have limitations in scaling up to handle the growing needs of a rapidly expanding and international organization.
- Support and accountability: FOSS solutions rely on community support, which may not offer the same level of availability and reliability as commercial vendors, especially in cases where highly customized builds are used. This would be dangerous in cases where critical-level vulnerabilities are found.

2. Create an In-house SOC using Commercial Solutions:

This strategy involves implementing a commercial SOC solution provided by established vendors in the cybersecurity market. Some examples of commercial solutions include SIEM

(Security Information and Event Management) platforms, threat intelligence platforms, and endpoint detection and response (EDR) systems.

Pro considerations for this strategy includes:

- Robust features: Commercial solutions often offer comprehensive features and advanced capabilities already in-place without the need for extensive customizability
- Vendor support: Commercial vendors provide dedicated support and maintenance, ensuring timely updates and patches. Vendors can also act as solutions experts, taking away the need for dedicated in-house experts
- Scalability: Commercial solutions are designed to scale with organizational growth and evolving security need

Con considerations for this strategy includes:

- Cost: Commercial solutions typically involve upfront costs, including software licenses, maintenance fees, and potential hardware requirements. Hardware requirements across international sites may be difficult to address.
- Vendor lock-in: As an extremely large organization, changing vendors at a later stage of growth may become incredibly difficult. Thorough vendor research would be required in order to ensure that the vendor has potential and is expected to grow and scale indefinitely with [Utility Provider].
- Customization limitations: Commercial solutions may have limitations when it comes to customization and integration with existing systems.

3. Outsource the SOC to a Third-party MDR or SOCaaS:

This strategy involves outsourcing the SOC functions to a third-party Managed Detection and Response (MDR) or SOC-as-a-Service (SOCaaS) provider.

Pro considerations for this strategy includes:

- Expertise and round-the-clock coverage: Outsourcing to a specialized provider ensures access to a team of experienced security analysts and continuous monitoring.
- Scalability and flexibility: Third-party providers can quickly scale their services to meet the organization's evolving needs.
- Cost savings: Outsourcing eliminates the need for hiring additional FTEs, reducing costs associated with training, salaries, and benefits.

Con considerations for this strategy includes:

- Dependency: Organizations must rely on the third-party provider for critical security operations, potentially raising concerns about control and trust. Explicitly designating scope of work by the third-party would be required. The option to keep high-level evaluative decisions to in-house staff is available.
- Data privacy and confidentiality: Sensitive data may be passed through the third party, and would require thorough addressing in a contractual statement.
- Onboarding period: Onboarding third-party staff can take a long period of time, depending on knowledge, network, location, and staffing requirements. Some additional considerations which could affect onboarding times include communication across culture and language.