Many businesses are moving towards cloud technology. With the global energy services firm merging with new acquisitions has given a rise to a new set of challenges and risks. Cyber attacks are more prevalent now than they have ever been as the company is more exposed to attacks due to growth from merging businesses. One great way to mitigate exposure to attacks is by implementing in-house SOC or outsourcing solutions to a SOC service provider that fits the business’s size and comfort level. In this topic, we will be discussing the three main highly contented strategies that the company can undergo to compare and contract.

Docking as the first is SOC using FOSS. perfect for businesses that prioritize the confidentiality and integrity of their data. You get complete control over how your data is managed and who has access to which file. This minimizes the risk of a costly leak of sensitive information like trade secrets or unreleased innovations. Though the cons can be shortages of trained specialists in the industry. The cost of hiring, training, and retaining staff specialists continue to increase due to shortage. The time span it takes for an in-house team to be fully functional is anywhere between 18-24 months. With in-house, you have daily control over your staff." Including work schedules and visibility into their work. With outsourcing, there is a lot more distance between you and the work. You can choose how to measure stall performance. Focus on attendance, deadlines, or other indicators. When you outsource, you measure the deliverables. “As cyber threats continue to evolve, they pose new and difficult challenges. How can organizations effectively defend against them? The answer lies within internal and external Security Operation Centers. Choosing between an internal and outsourced SOC is an essential first step for an organization designing its security program. Both options have pros and cons; the right choice can depend on an organization’s unique situation and conditions.”

Inhouse SOC using commercial solutions is another great way to fortify security protection against attacks. MSSP(managed security service provider) Intrusion detection system monitoring, 24/7 security operations center, and vulnerability testing are examples of highly effective key elements incorporated in the SOC model log. By partnering with MSSP, the company can derive great benefits such as filling vacant holes in the company’s security team. Which can reduce the cost and expenses. Alongside surveillance on the walls of the company 24/7 because attacks can occur outside of business hours. “regulatory landscape is growing more complex as new data protection regulations (such as the GDPR and the CCPA) join existing laws (like HIPAA and PCI DSS). An MSSP can help with collecting data and generating reports for demonstrating compliance during audits or after a potential incident.” “When deciding between an in-house SOC versus an MSSP, it’s important to be realistic about the considerations, challenges, and expenses of each and how these factors weigh in importance to your organization. For instance, if keeping down costs and avoiding hassle are your highest priorities, outsourcing to an MSSP is probably the better choice. If retaining complete control of the tools, processes, and personnel employed in your operations is paramount, an in-house solution is better.”

Lastly is outsourcing SOC to outside vendors. Organizations also outsource to lower taxes, avoid government regulation, and reduce direct business expenses. Another reason was to encourage organizational effectiveness. Doing things that are central, core, to your organizational identity. Increase your effectiveness. Which allows you to work from your strengths. Outsourcing offers one way to transfer the difficulty of staff acquisition and retention to an organization that specializes in it. Decreasing operating costs can decrease capital expenditure. Delegating security functions to an outside vendor can increase the quality of your decision-making. Another perk to delegating outside vendors will help the cyber security team concentrate more fully on its core functions. The highest tasks must be done from within the business context(policy setting, architecture design, and risk management) With the ability to scale up or down as needed. Increasing the amount of work that can be done without a lot of delays. Though there are risks to outsourcing. Misalignment of goals can result in failure to achieve some of your other top goals while pursuing outsourcing. You also need to protect company assets. But granting the MSSP access to your sensitive data or systems can be risky and difficult to manage. What if they allow a data breach involving your assets? Or what if the MSSP is the source of a cyber attack against you? Another, having ongoing compliance obligations to meet. But due to strict and unfamiliar laws and regulations, outsourcing across international borders can be risky and expensive, especially if sensitive data types are involved. Hidden costs can destroy your outsourcing business case, and bust your budget. These include the costs of layoffs, implementation delays, inefficiencies of working with people from other cultures who speak other languages, and regulatory fines. It's also possible the outsources will fail to perform or go out of business. Using MDR as an outsource security service that provides advanced protection on endpoints. Providing advanced and deeper protection, plus the ability to stop malware in its track. Typically, MDR uses AI and machine learning for deeper security analysis. The software is important, but the most vital part of the MDR service I recommend is having a team analysis that watches over your network 24/7.

Chkadmin. (2022, August 4). *MSSP - what is a managed security service provider?* Check Point Software. Retrieved February 21, 2023, from https://www.checkpoint.com/cyber-hub/network-security/what-is-a-managed-security-service-provider/

Cozens, B., & ABOUT THE AUTHOR Bill Cozens . (n.d.). *Is an outsourced soc worth it? looking at the roi of MDR*. Malwarebytes. Retrieved February 21, 2023, from https://www.malwarebytes.com/blog/business/2022/12/are-outsourced-soc-services-worth-it-looking-at-the-roi-of-mdr

*In-house SOC vs. MSSP (how to select the right option)*. Avertium. (n.d.). Retrieved February 21, 2023, from https://www.avertium.com/blog/in-house-soc-mssp

Security Magazine. (2020, April 28). *4 trends for building and operating a Security Operations Center*. Security Magazine RSS. Retrieved February 21, 2023, from https://www.securitymagazine.com/articles/92248-trends-for-building-and-operating-a-security-operation-center

Volico. (2022, August 25). *Should you build your own in-house SOC: Volico Data Centers*. Miami and Broward Colocation | Volico Data Centers. Retrieved February 21, 2023, from https://www.volico.com/should-you-build-your-own-in-house-soc/