

BitLyft

Cybersecurity



BUILDING A SECURITY OPERATIONS CENTER

COMPARISON GUIDE

IN-HOUSE vs VENDOR

OVERVIEW

An organization with data to protect needs to have cybersecurity. There are two main ways that organizations go about building a cybersecurity team, or security operations center. The first method is hiring a complete internal team and buying the software and hardware for them to perform their daily operations. The second method is to hire a cybersecurity vendor to handle your security operations, or simply augment your existing team. There are pros and cons associated with each method of building a security operations center based on your organization size, budget, and goals. The following guide will compare and contrast the important components to consider.

TABLE OF CONTENTS

Cost Per Employee	3
Uptime and Coverage	4
Communication	5
Turn Over Resilience	5
Contractual Obligation	6
Focus on Security	7
Tool Mastery	7
Company Culture	8
Hidden Costs	9
Here to Help	10

COST PER EMPLOYEE

IN-HOUSE

VENDOR



Your organization is on the hook for everything. Salary, benefits, bonuses, and paid time off for all security operations center employees. Salary will be the largest expense to your organization. Below are the national averages for the common positions to fill depending on the size of your organization.

Your security operations center will come fully staffed by the organization that you choose. You will not need to worry about sick time, benefits, or vacation time. The company you hire is required to manage personnel and staffing ensuring that you are covered 24/7/365.

JOB TITLE	STAFF	SALARY
Analyst	4	\$53K - \$116K
Engineer	2-4	\$73K - \$130K
Director	1	\$105K - \$198K
CISO	1	\$176K - \$263K
CIO	1	\$100K - \$263K

AVERAGE COST: \$739,000 - \$1,708,000

UPTIME AND COVERAGE

IN-HOUSE

VENDOR



Hiring a single security analyst can be anywhere from \$53,000 to \$116,000. This only guarantees coverage eight hours a day, five days a week and doesn't include PTO. Cybersecurity requires full time coverage (24/7/365) and the ability to respond quickly and remediate in real time.

A vendor allows you to no longer worry about your analysts getting sick or taking a vacation. The responsibility always falls onto the vendor to ensure that you have 24/7 coverage and your network is protected 100% of the time.

IN-HOUSE UP TIME



STANDARD 9-5 EMPLOYEES ARE ONLY WATCHING YOUR NETWORK 23.8% OF THE TIME. THIS LEAVES YOUR NETWORK EXPOSED FOR 76.2% OF EVERY WEEK.

*Based on a 40 hour work week.

COMMUNICATION

IN-HOUSE

VENDOR



One of the biggest advantage to having an in-house security team is control and communication. You remain in control of the day to day operations of your security team and the tasks they are assigned. They are focused solely on your environment 24/7/365. There are no additional clients that your SOC team is required to monitor. Typically, communication is the fastest with an in-house team as compared to a vendor.

Not all vendors will have communications comparable to an in-house SOC team. However, the quality of the communication can be significantly higher. For example, you may only receive notifications of high level alerts and not the less critical issues. A vendor may also have insights that your internal team might not. This is because they have their eyes on multiple environments throughout the day.

TURN OVER RESILIENCE

IN-HOUSE

VENDOR



Turnover for small in-house teams can be a nightmare. In many cases a team member leaving work can cause major headaches in the SOC. It's important to consider the vulnerabilities that each member of your team could present if they were to suddenly leave.

Using a vendor for your security operations center insulates you from hearing the the words "I quit" or "match my other offer." Vendors carries the responsibility to hire, train, and retain analysts. If employees stay with the vendor, it's a good sign they treat their staff well and they're happy while protecting your environment.

CONTRACTUAL OBLIGATION

IN-HOUSE

VENDOR



Depending on the region, the United States "at will employment laws" allow you to hire and fire employees when you see fit. There are no contractual obligations to keep employees that you feel are not performing to your organization's standards. You retain the ability make staffing decisions to ensure you're getting the performance your organization needs.

In most cases you are contractually tied to your vendor's cybersecurity team. You may not be able to remove members from your team at will. If there is a bad relationship or you are shifting budgets, you could be on the hook for the duration of your contract. Ensure you review the termination clauses in the SOW and MSA to understand your commitment, even on monthly subscription models.

ALWAYS REVIEW YOUR VENDOR'S MSA & SOW FOR CLAUSES PERTAINING TO PERFORMANCE AND TERMINATION IN ORDER TO ASSESS YOUR LONG TERM CONTRACTUAL OBLIGATIONS.



FOCUS ON SECURITY

IN-HOUSE

VENDOR



Oftentimes we find that internal security staff get called in as IT personnel. This takes their focus away from just protecting your organization. Larger organizations can afford to hire individual specialists to segment skillsets, but small to medium size businesses typically lack the budgets to get specialized people.

When using a vendor you should count on your team being laser focused on cybersecurity. Having a fully staffed security operations center will ensure that there are eyes on your environment at all times if anything should go wrong. It's also important to assess whether the vendor you're hiring is focused on security, or just adding it on to a wide range of other services.

TOOL MASTERY

IN-HOUSE

VENDOR



Having a powerful tool is only part of the battle. Having highly trained users that knows how to utilize the tool to its full potential will give you the greatest ROI. Every time you add a new tool to your team's cybersecurity stack there is a learning curve. Your in-house staff may not be operating at full capacity for quite some time as they learn the new tool.

Your vendor should come with a full stack of cybersecurity tools to which they are highly trained to use. You can also leverage partnerships with SaaS offerings through your vendor to get better pricing. SIEM tools are a great example of a robust software that needs certified experts to install and manage to get the most ROI.

COMPANY CULTURE

IN-HOUSE

VENDOR



Your in-house team should live and breathe your company culture. They should be trained to do things exactly the way you want them to be done, every single time. They are trained in your organizational team norms and expectations, and are the first line of fulfilling your company vision and mission.

A SOC vendor has their own company culture and set of team norms. Before you sign a contract, get to know your vendor's internal culture and preferred method of communication. It's important to understand the type of people who will be protecting your environment and how they will interact with your staff.



ENSURE YOUR VENDORS ALIGN WITH YOUR ORGANIZATIONAL VISION, MISSION, AND VALUES.

IN-HOUSE HIDDEN COSTS

We know it's difficult to navigate whether to build a security team internally or to outsource to a vendor. So here are a few additional hidden costs to consider when building an in-house security team.

-  You may be paying full retail price for security tools when a vendor can oftentimes arrange discounted pricing.
-  Some of the products that you will need to purchase for an in-house team could already be licensed by your vendor.
-  You will need to purchase the hardware to allow your internal SOC team members to do their job.
-  Consider the time it takes to train team members and implement new security tools.
-  There is often downtime for training new employees or continued education courses that could incur additional costs.

HERE TO HELP

Building an effective in-house security operations center is a big commitment in both time and resources. If you're looking to get the best security ROI and leverage the benefits of a vendor, contact BitLyft and let's start the conversation.

Schedule a meeting with your BitLyft Success Team today.



"In over a decade of helping businesses decide to build their own SOC or outsource to a SOCaaS provider, I have seen time and time again a much better ROI to subscribe to the right vendor than to build internally. Everyone's environment is different and the use cases can vary. However, there's never a bad reason to take a moment to review your current state and future needs with experts like those at BitLyft."

securonix

MIKE JOHNSON
CHANNEL SALES DIRECTOR
SECURONIX, INC.