CRITICALSTART™

Build vs. Buy

How MDR boosts the value provided by a traditional Security Operations Center (SOC)

CRITICALSTART

Executive Summary

In this paper, you will learn how to uncover the hidden costs involved in deploying and staffing a SOC. We'll take a realistic look at the effort, expertise and infrastructure necessary and break down the best option for a cost-effective yet strong approach to information security.

Topics Include:

- How to calculate human capital costs, including analyst hiring versus alert volumes, certifications and continuing education
- Technology requirements including IDS/IPS, EDR, SIEM and more
- Real estate costs and other support expenses
- A comparison of "do-it-yourself" SOC vs. working with a Managed Detection and Response (MDR) provider
- The ramifications of both internal and third-party options to security

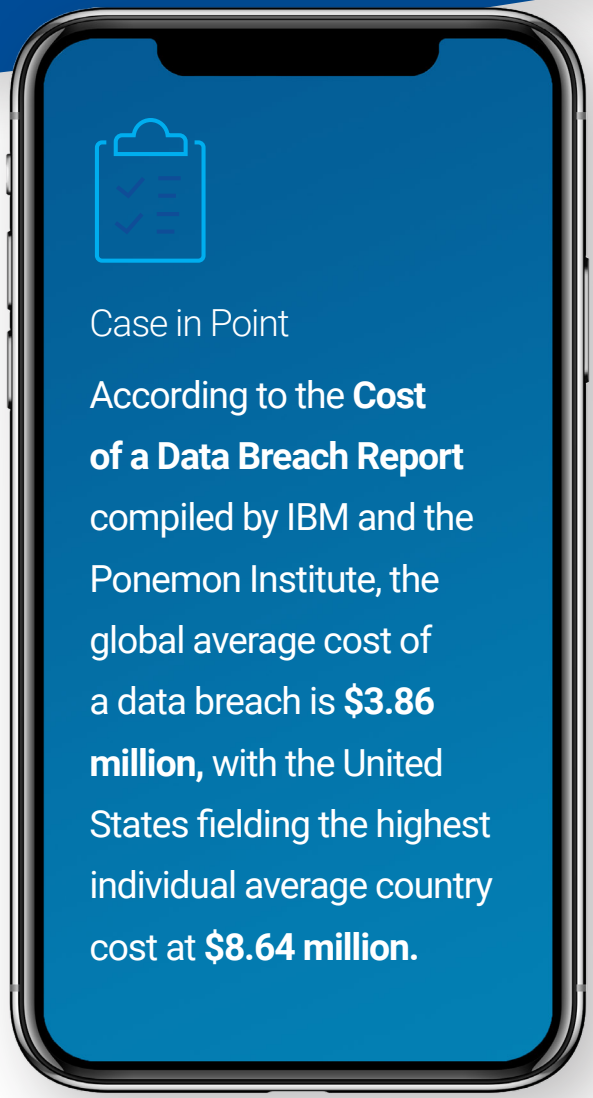
CRITICALSTART

No One Doubts the Cost of a Cyberattack

> When calculating the cost of security, it's good to remember what's at stake.

These numbers don't include the operational impacts, the negative customer experience or the reputational damage that a business can experience as the result of an attack. The hard truth is that **an attacker only needs to be successful one time** to steal data or severely disrupt your business. **As the defender, you must be successful every time**—time after time—to make sure that your organization is secure.

This is why all companies need a dedicated Security Operations Center (SOC). Building a SOC costs time and money—expenses that can be alleviated by using a services provider such as Managed Detection and Response (MDR) to reduce both human and operational costs. But which option, an internally developed SOC or working with an MDR partner, will make the most sense for your specific operational environment? Let's break down some of the costs to see if we can offer a clear answer to that crucial question.



CRITICALSTART

Building a SOC Internally, Cost by Cost

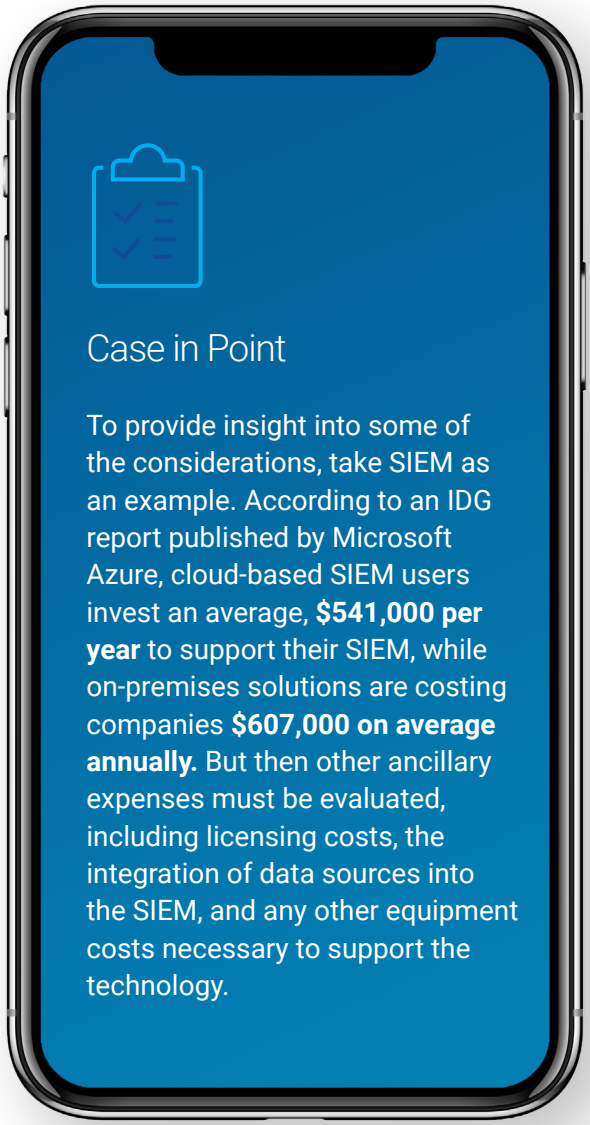
There are a variety of expenses incurred when a company tries to deploy a SOC internally, including staffing and expertise, equipment and software, facility expenses for the SOC and recurring costs. Let's take a look at the first of these expenses, physical costs, and break down the scope of investment needed for an internal deployment.

Building a SOC Internally

Physical Costs

Non-human expenses will also consume a large part of a SOC capital investment. Depending on the make-up of your SOC, you may be deploying Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), Vulnerability Scanners, Security Information and Event Management (SIEM) systems, Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR), threat intelligence, and forensic tools.

Beyond technology investment, there are also facility considerations to include such as the square footage cost where the analysts will be located and the utilities necessary to support their mission. With square footage costs ranging anywhere from $20 per square foot all the way to **$85 per square foot,** space costs for internal staff need to be taken into account.



Case in Point

To provide insight into some of the considerations, take SIEM as an example. According to an IDG report published by Microsoft Azure, cloud-based SIEM users invest an average, **$541,000 per year** to support their SIEM, while on-premises solutions are costing companies **$607,000 on average annually.** But then other ancillary expenses must be evaluated, including licensing costs, the integration of data sources into the SIEM, and any other equipment costs necessary to support the technology.

CRITICALSTART

Building a SOC Internally

Human Costs

On average, a single endpoint will generate **5,000** alerts annually. If a hypothetical business has **2,000** endpoints, it will translate into **10,000,000** alerts per year that security analysts will need to investigate.

Here's what that looks like :

Critical-Priority Alerts

.1% of total events

2-3 analysts

$175,000/year

High-Priority Alerts

.9% of total events

21-22 analysts

$1,575,000/year

Medium-Priority Alerts

29% of total events

697-698 analysts

$50,750,000/year

Low-Priority Alerts

70% of total events

1682-1683 analysts

$122,500,000/year

There's One More Thing To Consider

This example is based on an assumption of 8-hr shifts. But an attack rarely comes when it's convenient. To provide 24x7 protection will require a minimum of 10 individuals, regardless of the size of the organization or the number of alerts generated. With an average annual cost of $75,000 per analyst, that's a minimum of **$750,000 per year.**

Many companies may attempt to control costs by only investigating critical- or high-priority alerts. But this can be an expensive mistake as many of today's ransomware attacks are only detected through medium- or low-priority alerts.

CRITICALSTART

Building a SOC Internally

Putting It All Together

Once you've calculated the costs to hire analysts in your area, and you've determined the ongoing educational and certification expenses, and you've defined the real estate costs where your SOC will be located, the formulas for Total Cost of Ownership look something like this:

Annual Salary
+ Training
+ License
+ Space Costs
=

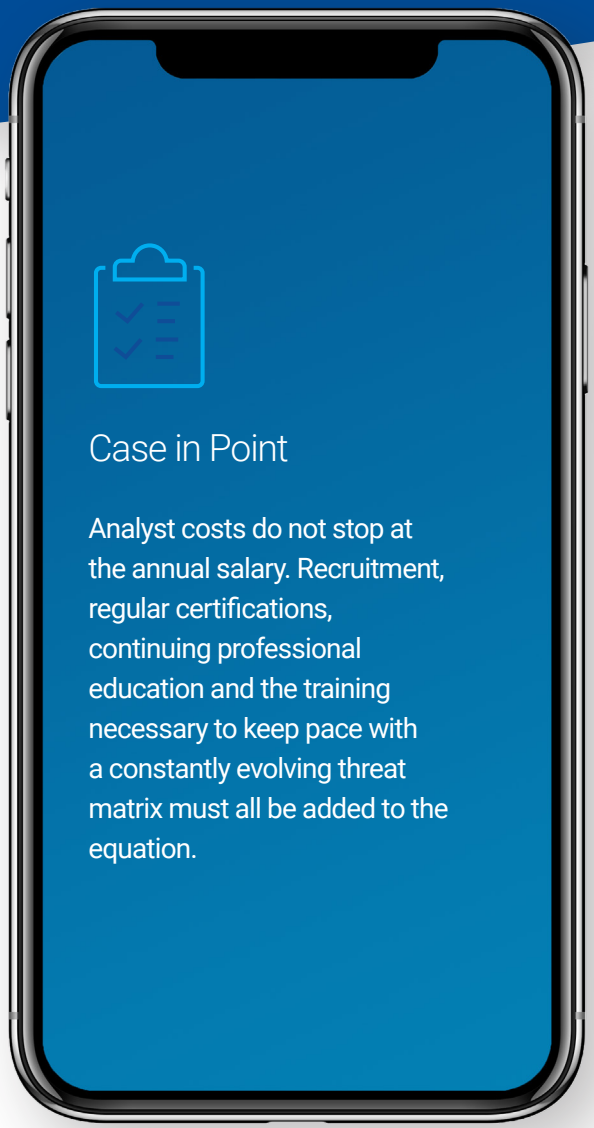
Per Analyst Annual Cost

Alerts Per Year
/ 2 Alerts Per Hour
=

Number of Analysts Required

Number of Analysts
x Per Analyst Annual Cost
=

Yearly Total Cost of Ownership



Case in Point

Analyst costs do not stop at the annual salary. Recruitment, regular certifications, continuing professional education and the training necessary to keep pace with a constantly evolving threat matrix must all be added to the equation.

CRITICALSTART

Sounds Expensive. Is There Another Option?

After running through the previous calculations, you may come to the conclusion that deploying a 24x7x365 SOC internally is an expensive proposition. And you're right. But there are options that can cut this expense dramatically, such as working through a service provider to obtain the human and technical resources to protect your business without the prohibitive expense.

Providers that offer services like Managed Detection and Response (MDR) can help you take advantage of economies of scale to shrink TCO while increasing the expertise and resources you have at your disposal. The analysts provided by an MDR provider work across a variety of industries, enabling you to capitalize on their expertise while taking advantage of the cost efficiencies of not shouldering the entire burden of bringing these individuals on as full-time employees. The MDR provider will already have the real estate, technology, and expertise to integrate efficiently with your current environment. Software license costs can be significantly reduced, since the MDR provider can purchase licenses at scale, distributed across their entire client base.

Capability That's Hard to Put a Price On

Beyond the cost savings, there's an even more important consideration. What kind of capabilities can you leverage through MDR that might not even be possible if your company were to deploy their own SOC? When working with a limited budget, corners are inevitably cut. But what if they didn't have to be?

Consider the example of alerts. Investigating all alerts is usually cost prohibitive for an internal SOC. But an MDR can work with a client to build a trusted registry of alerts that are normal. The result is less alerts that need to be investigated, which translates into the capability for alerts of all priorities that fall outside of the registry to be treated equally. This approach eliminates "risk acceptance" and can auto resolve 98% of events, while enabling SOC analysts to focus on the remaining 2% that can indicate a real threat. Confirmed threats and corrective actions can then be escalated and reported to the client.

CRITICALSTART

Putting it All Together

If we take all of these variables and put them together to build a comparison of SOC deployment options, it looks something like this:

Total Cost of SOC Ownership	Internal	MDR
SOC Analysts	$750k to $100,000,000+ based on number of alerts processed	Included
Alerts processed	Typically critical/high only	All alerts resolved
Technology cost	$500k-$1,000,000	Included
Real-estate cost	$25-$85 per square foot	Included
Level of expertise	Varies	Very high, spanning multiple industries, security environments and threat scenarios
Level of protection	Varies	Extremely high

The Bottom Line

If you follow the process we've outlined here, you should gain a clear picture of the total cost of your security options. In doing so, also keep in mind the intangibles — such as strategic advantages gained from security posture improvements, like using an MDR provider to focus on the daily challenges of alert resolution while your in-house team takes on the issues that can drive future opportunities for your business.

If you need support in calculating a real-life Total Cost of Ownership for your own enterprise, CRITICAL**START** security experts can survey your security landscape and help put together options to increase threat identification, shrink response time, and meet the unique security and compliance goals of your organization.

To request an evaluation or learn more, contact an MDR specialist at:
info@criticalstart.com
877-684-2077
or www.criticalstart.com

CRITICALSTART