Security Operations
Threat Detection and Response

A Buy vs. Build Solution Brief

Where Technology Means More®

Introduction

Cyber attacks continue to threaten our companies, and organizations today are under nearly constant assault. This year, ransomware will attack a victim every eleven seconds.[1]

Fending off the sheer volume of threats, however, is only one of the challenges. Criminals have evolved their methods and techniques, too. And the result has been both successful and costly. Overall cyber crime damages, in fact, are expected to cost the world $6 trillion next year—twice as much as it did just six years ago.[2]

Threat detection and response—the security operations process of detecting threats and taking mitigating action before a breach can occur—is key to addressing these challenges. But not all security operations teams have the software tools and capability they need to perform the function successfully.

As you evaluate your needs in this area, you must answer the one question every IT leader asks when a new business requirement emerges for which they need to implement a solution: Buy or build? Should you invest the time and energy and resources needed to build your own solution or buy one already on the market?

Finding the Option That Works Best for You

Every organization is different, yet most are very much alike when it comes to the need for cyber security. Although some may be more vulnerable than others, companies large and small are targets of cyber attack and in need of protection, especially threat detection and response capability.

But how do you choose between building that capability yourself in-house or buying it? This paper will explore some of the key factors you should consider as you are evaluating your options.

But First, A Word About Data

Data lies at the heart of all security operations. Like other networking operations, security relies on the ability to trust the data. Data pools that are outdated, duplicated, or overwhelming can impact your security operations team's ability to perform analysis and develop policies. Intrusions can go undetected. Malware can spread. Assets may be compromised and infections may go without remediation. To address this, security operations must leverage systems to view this data accurately and in a timely fashion, in order to create and enforce policies to protect the organization. This often leads to the debate to develop these systems or to purchase them.

Building effective security operations includes deploying in-house expertise to develop and maintain solutions that ensure data trust. In contrast, buying is leveraging a qualified vendor to provide these solutions and associated services. There are several key factors in deciding

which approach is right for your organization, which we will cover later in this paper. But the goals regarding data are the same for both. They are:

+ Data in full: Is all the data available for analysis or only a portion?
+ Data accuracy: Are the systems producing accurate data?
+ Data consistency: Can the data provided by multiple systems be accessed?
+ Data de-duplication: Are the same data points being provided multiple times?
+ Data relevance: How stale is the data?

Trusted data is the starting point for effective security operations. Do you trust your data? As you evaluate potential solutions, consider the effect each option may have on your data. Where is there opportunity for human error, either in data input or analysis? Where is there potential for system faults and failures that could lead to data corruption? Are there opportunities for data integration failure? Are there complexities in the systems that can slow or even prevent access? Can issues like multiple language support, data formatting, or conflicting weights of criticality lead to improper reporting and alerts? Answering these questions can help uncover potential problems and steer you toward the best option for your organization.

The Build Option – Creating Your Own Security Operations Center

When you decide to build your own solution, you are in a way creating your own in-house security operations center. One that is responsible for designing, implementing, and administering the systems and tools you will need to carry out your security mission and protect your company against threats. But developing your own threat detection and response capability in-house has both benefits and challenges.

Benefits

One benefit of building your own solution is control. When you keep all aspects of your security operations in-house, you are in complete control of your data, your hardware, your staff, and your operations. You determine who has access to your equipment and your data, and what they can do. And you don't have to worry about a third-party doing something that may compromise your data or negatively affect your security posture.

Another advantage to keeping the solution in-house is process customization. You decide how your processes should work for your operation to be successful, and you don't have to adapt in order to accommodate the processes of a third party.

A third benefit is the ability to leverage your existing systems architecture. If you have a security platform already in place, you can leverage your investment and build on it. Depending on your configuration, you can upgrade hardware, add components, or do both to build out an automated threat detection and response capability that your security operations team can manage.

Challenges

To build your own capability, you will need a talented team of security professionals. You will need security analysts, SIEM (security information and event management) experts, threat researchers, and others. But finding these people, and retaining them, is a difficult, because these skills are in high demand. In fact, by the end of 2021, there will be an estimated 3.5 million unfilled cyber security jobs in the industry.[3]

Implementation time is another drawback. Developing your own internal security capability takes time and effort—it's costly, and it requires ongoing attention to be effective.[4] It involves developing processes and internal metrics for data integrity, data retention, and service levels for reporting and response.

A third challenge is overcoming barriers to success. Organizations that have developed their own security operations centers cite lack of skilled staff (58%) and the absence of effective orchestration and automation (50%) as the most frequent barriers to excellence.[5]

The Buy Option – Outsourcing and Hybrid Alternatives

The buy option has a range of possibilities, from a fully outsourced security solution to a hybrid model that provides managed detection and response (MDR) capabilities. Each has advantages and disadvantages, and you'll need to evaluate the details carefully. But generally, the buy option, in whatever form you choose, will have some common benefits and challenges.

Benefits

If you choose to purchase a solution, you will need fewer security resources. Instead of hiring and training a large staff of security experts yourself—and struggling to keep them from leaving your organization for higher-paying opportunities—you can leverage an outside team of experts. The onus for acquiring and maintaining top security talent rests on your provider.

Packaged solutions typically leverage an integrated security platform to deliver threat detection and response capability. You don't have to architect and design the components of a security platform that will enable you to detect anomalies, analyze them, and automatically respond.

Another benefit is that threat research is usually included. Most packaged solutions leverage threat data and playbooks that are continually updated with intelligence on the most current known threats.

Implementation time is shorter. Buying a solution reduces the time and resource effort it takes to deploy a threat detection and response capability in your environment. Much of the work has already been done by the provider.

Challenges

The most significant drawback to outsourcing is loss of control. When you engage a provider, you turn over much of the responsibility for security operations to them. The amount varies, depending on the extent of your arrangement, but you do lose some control. And you create a dependency on a third party that you previously did not have.

You also lose the ability to customize processes as much as you may wish. Now that you are working with a provider, you have to adapt to the provider's processes and procedures. That may require little effort on your part, or it could be a lot of work. Regardless, loss of context is a risk, because a provider will not understand your business the way you do—for example, what is really important and what is not—and that will require you to translate the risk for them.

When you outsource, communication and coordination become very important. You no longer have complete control in-house for security issues and concerns. You now have a third party to interface with. Delays may occur, which can impact time to resolution for issues, because the service is not fully integrated into your organization, and you can't just talk over the cubicle to a colleague and get things done. Success requires good communication and coordination between your staff and your provider.

Conclusion

Threat detection and response is a foundational capability of an effective security operation, and there are many factors to consider when deciding if you should build the capability yourself or buy a managed detection and response (MDR) solution. Weigh and evaluate each factor carefully in light of your security needs, your existing security posture, and your organization's goals. The effort will prove invaluable as you develop your business case and perform your cost analysis.

Additional Resources

Visit our **Managed Detection and Response Solutions Resource Center** where you can access additional information and schedule a meeting with one of our MDR experts.

About ePlus

With expertise in Security, Collaboration, Data Center, AI, Emerging Technologies, Digital Infrastructures, Hybrid Cloud Networks and Financing to a range of managed, professional and other services, we help organizations navigate their technology options – and then design, orchestrate and seamlessly implement solutions. Backed by a staff of experts, more than 650 of whom are certified on the latest technologies from industry-leading IT companies, ePlus provides unparalleled guidance and expertise that allows customers to maximize the return on their technology investments. For more information, visit **www.eplus.com**.

References

1 Cybersecurity Ventures "Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021." May 29, 2020, Steve Morgan.

2 Ibid.

3 Ibid.

4 "**Security Operations Centers and Their Role in Cybersecurity**." Gartner Press Release. October 12, 2017.

5 Chris Crowley and John Pescatore. "**Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey**." SANS Institute. July 2019.