Buying Security Tools vs. Hiring a SOC

Explore the differences between acquiring cybersecurity products vs. hiring a full-service security operations center.

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP NETWORK SECURITY

Introduction

The desire to build an internal cybersecurity capability is understandable. You know your organization, and your IT, better than anyone else. You have a good sense of the risks you're defending against. You have the budget to buy or build the tools you need. So, you do it yourself. You procure the right products and train your people. Yet, you still get hacked. What went wrong?

Part of the problem is just today's threat environment. No in-house security operations center (SOC), no matter how well equipped, can defend everywhere all at once at the same level of strength. But, you could probably do better. The reality is that in-house security teams are often working at a disadvantage. The resources, know-how and personnel can simply be out of reach for all the most well-funded organizations. And, even with ample money, security deficiencies can still abound, especially in system and threat monitoring. It is generally a better idea to have 24/7 monitoring done by a team of dedicated external security experts.

The Basic Essentials for any Cybersecurity Team

A security team that wants to run its own cybersecurity operation must set up a few essential functions. These vary from company to company, but in general, the bare minimum setup includes:

Access Control

Penetration Testing Tools

Endpoint Detection and Response (EDR)

Email Security

Security Information & Event Management (SIEM)

Back Up Solution

A threat detection capability is a "must have," coupled with threat and intrusion monitoring. Log management is required especially for compliance regulated organizations. Most security teams run threat mitigation tools, as well, which help quarantine and block threats to stop their spread, or remove them altogether. The team also needs to develop and enforce security policies. Incident response processes put policies into action when there is an actual attack.

SECNAP NETWORK SECURITY

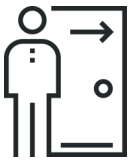
Challenges Inherent in Cybersecurity Tools

Even with the essentials in place, it can still be challenging to run an effective cybersecurity operation. Here are just a few of the most common challenges IT teams face when running cybersecurity operations in-house:

Monitoring & Misconfigurations Without tuning and near real-time monitoring, your efforts will not pay in terms of a sound security posture. For example, a misconfiguration in a threat detection system can increase your vulnerability to a breach.

Budget Cost and resources are challenges to implementing security operations. Procuring the tools is just the start. There can be significant costs for their implementation and ongoing maintenance.

Staffing Difficulty recruiting experienced cybersecurity personnel is a known issue in the industry, and salaries are trending up. Scheduling people to monitor systems on a 24/7 basis, which is usually required, can be prohibitively expensive—if you can even find people.



Leadership Buy-in Security operations carry overhead. Costs can add up once you include items like training and certifications. Senior business leadership will want to understand the costs of staffing and tools. It can be hard to justify.

Alert Fatigue The work itself is not easy, either. Staff burnout is common, with false positives causing alert fatigue. When tools are segregated, staff may miss serious incidents that take the form of separate low-severity alerts. If analyzed together, these alerts would accurately be seen as a posing a real threat.

Vulnerability Management Patch management is a further burden on staff and resources. It can be nearly impossible to keep a patch management program up to date given the exponential increase in vulnerabilities in recent years. These include “Zero Day” attacks and open-source vulnerabilities like the notorious Log4J.

SECNAP NETWORK SECURITY

Making the Decision to Work a SOC Provider

Considering these challenges, it's not surprising that a growing number of businesses are electing to work with external SOCs, also sometimes called security-as-a-service (SECaaS). This approach offers a range of advantages over doing security in-house.

Security-as-a-Service

A security-as-a-service provider allows for a layered approach, wherein the client can select the security modules it wants for its specific security and compliance requirements.

Ongoing Service options typically include:

- ✓ **Intrusion Detection System (IDS) Management and Monitoring**
- ✓ **Intrusion Prevention System (IPS) Management and Monitoring**
- ✓ **Security Information and Event Management (SIEM) Management and Monitoring**
- ✓ **Internal and Lateral Threat Detection**
- ✓ **Endpoint Detection and Response (EDR)**
- ✓ **Vulnerability Management**
- ✓ **Data Loss Prevention (DLP)**
- ✓ **Security Assessments**
- ✓ **Dark Web Monitoring**

Benefits of a Managed Cybersecurity Platform

If a managed security services provider can take care of these security workloads, that alleviates a great deal of stress on your in-house team. Your people can handle day-to-day issues and enhancements that will improve business processes and profitability. However, they no longer have to worry about staffing 24/7 and overseeing complex security products. The false positives no longer burn people out, because someone else is handling them.

Further benefits of a managed cybersecurity platform include continuous proactive monitoring, which offers a fast reaction to incipient incidents. The results are improved Mean Time to Detection (MTTD) and Mean Time to Resolution (MTTR). This should make sense, given that a highly trained external team, working with a well-tuned toolset, can move more quickly than the average internal team.

A cybersecurity partner can perform security refinement and optimization, informed by cross client intelligence. You gain the advantage of learning from experiences that other companies are having, even outside your industry. This might be coupled with root cause investigation and forensic analysis.

Key Metrics

Mean Time to Detection (MTTD): A common key performance indicator (KPI) which refers to the average time passed between the onset of an IT incident and its discovery.

Mean Time to Resolution (MTTR): A common KPI for which calculates the average amount of time it takes to neutralize an identified threat or failure within their network environment.

Security Assessments and Threat Mitigation

Regular Security Assessments are a highly recommended practice. There are many products that can help scan your network and compile data on your network. However, properly interpreting these reports requires a level of expertise.

Depending on the relationship with a cybersecurity partner , they may be able to empower your team by performing regular security assessments. The information provided in this process allows your team to close the gaps and improve your security posture.

The external team may do a better job of prioritizing investigations and completing them on a timely basis. This occurs partly because of better automation and orchestration capabilities for threat investigations and incident response workflows. The same is generally true for remediation assistance and threat mitigation. The external team will have a strong incident response and recovery plan it can put into action.

Managed Cybersecurity & Regulatory Compliance

Working with a managed cybersecurity platform can help with compliance reporting, another important but time-consuming chore that tends to overstretch an in-house team. The managed provider has the ability to flag non-compliant controls and systems, while also aiding in audits and attestations, if needed. On a related front, the external provider is able to help you obtain the right kind of cyber insurance–working with you to implement controls and policies that keep the cost of insurance down, e.g., by adopting strong password rules and encrypting data at rest.

Conclusion

Doing cybersecurity yourself makes sense, until it doesn't. While you understand your organization better than an outsider ever could, the realities of today's threat environment and staff shortages make it difficult—if not impossible—to build a truly effective security operation in-house. Monitoring, in particular, can be a serious challenge. A managed cybersecurity platform offers a solution, with 24/7 proactive monitoring and a range of support services, such as incident response and forensic data. MTTD and MTTR both accelerate, while your overall security posture improves. The provider relationship further builds the basis for future growth and the ability to adapt to inevitable changes in your organization, as well as those in the threat landscape.

Not ready to decide?

Start with a Security Assessment to get a clear view of your organization's security posture. Reducing your attack surface and closing gaps is always a good first step.

SECNAP NETWORK SECURITY

Get a complimentary and customized consultation regarding your organization's cybersecurity strategy.

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP's proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

AICPA SOC aicpa.org/soc4so

GSA Advantage!®