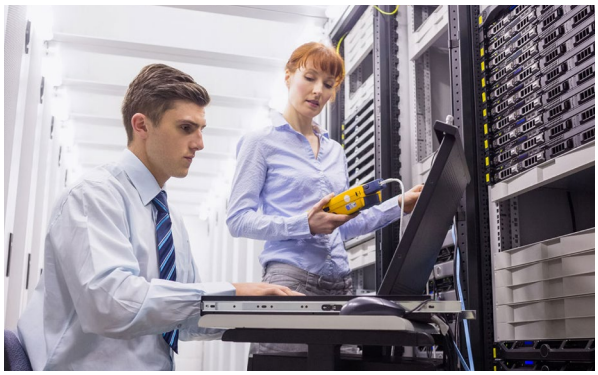
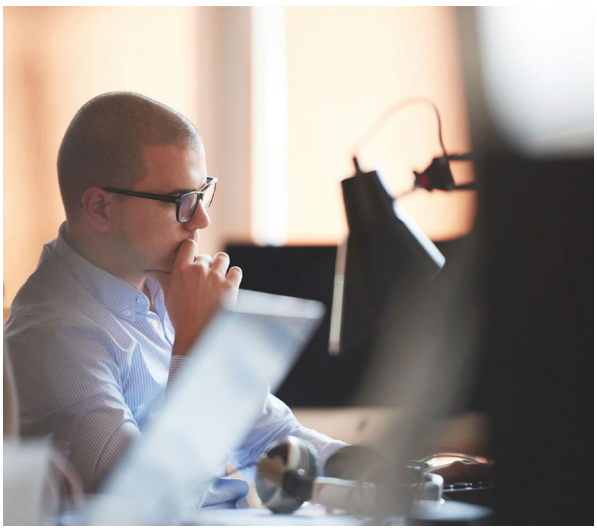
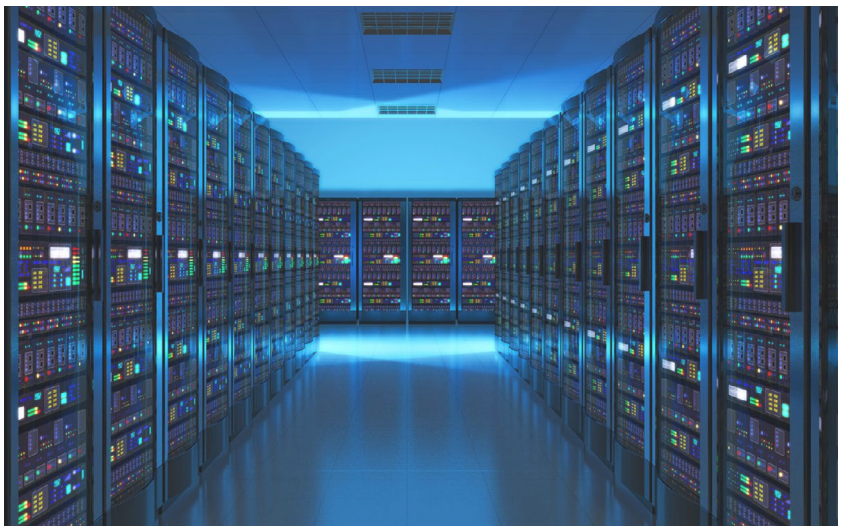
A guide to build vs. buy service models for threat detection and response







In today's cyber-risk environment, organizations need a way to balance prevention with detection and response capabilities. Protective layers that block common attacks are crucial, but they're not foolproof. Strong cybersecurity programs also need a backstop of security monitoring and response functionality for the threats that bypass other layers.

To quickly identify malicious and anomalous activities, prioritize the most severe risks and swiftly take action to disrupt or contain a threat, organizations need appropriate infrastructure, threat intelligence, and staff support. Many paths can lead to an effective detection and response program. The biggest question many decision-makers have as they start to chart their organization's path is whether to build and manage detection and response capabilities or engage a managed security service provider (MSSP) to help bring all the right pieces together.

Many important considerations and factors go into choosing DIY vs. managed. One thing to keep in mind is that the choice is actually not binary. It's more of a spectrum of how far you want to go with certain functions and responsibilities you own versus those you offload. Where you land on the spectrum depends on your needs, as a range of services can be woven onto the threat detection and response technical stack.

Each has pros and cons, plus tradeoffs from both a risk and cost perspective. Let's take a look at what will influence the route an organization takes.

The DIY-to-managed spectrum

Build your own detection and response

The fully DIY option for cyberthreat detection and response has an organization building out its entire cybersecurity technological stack from start to finish. This means procuring a range of different point products—including vulnerability scanners, intrusion detection systems, asset inventory, and SIEM systems—and fueling that environment with handpicked threat intelligence feeds. The organization must then glue everything together through in-house integrations, and it is responsible for tuning and troubleshooting detection mechanisms and rules accordingly.

Monitoring, detection, and response capabilities are staffed completely internally in this model. The organization also must field a team responsible for deployment, maintenance, and system administration of all the underlying infrastructure that supports this bespoke threat detection and response system.

Where it may make sense

A full DIY approach may make sense in highly complex or non-standard environments, such as those running supervisory control and data acquisition (SCADA) or industrial control systems or those with a lot of custom or legacy applications. A custom-built technology stack may appeal to organizations with very specific risk-reduction needs and security clearances or an extremely low-risk appetite.

Pros

- Can be completely tailor-fit to the organization's needs
- Offers a high level of control over what gets monitored and how

Cons

- Needs lots of fine-tuning and integration to get every piece of technology to work together
- Can slow down the window between deployment to first-threat insights
- Requires intensive analysis, data cleansing, and normalization to offer actionable insight
- Requires significant manual work and puts high resource demands on security engineering, security analysts, and security researchers
- Necessitates IT resources for deployment, system admin, and maintenance
- May be slow or expensive to keep up with changes in the business and IT environment, the cyberthreat landscape, and regulatory requirements

Threat detection and response platform

Most organizations have come to realize that a security information and event management (SIEM) system, on its own, is not a silver bullet for threat detection and response. SIEM systems are valuable hubs for aggregating and organizing disparate security data across an organization, but they still require a lot of fine-tuning by organizations that seek to use them as a platform for threat detection and response. This means organizations must still put in a lot of DIY work to get the most out of their SIEM data. They also run into the challenge of effectively feeding threat intelligence into SIEM, which adds additional overhead to the process.

This is where platform-based threat detection and response comes in. The platform-powered DIY approach has organizations tapping into a ready-made platform that brings together essential security capabilities like asset discovery, vulnerability assessment, intrusion detection, SIEM capabilities, security orchestration, automation, and response (SOAR), and automation. These capabilities are all fueled by continuous threat intelligence created by the threat detection and response platform's research team.

For teams that want to manage their own threat detection and response programs, the platform-powered DIY approach has become the new normal. You can see this by surveying the market, where an increasing number of vendors have expanded on SIEM offerings with additional built-in capabilities to support threat detection and response in one platform.

Where it may make sense

When organizations prefer to manage threat detection and responsibilities with in-house staff but don't have the development resources to create custom functionality and broad integrations, the draw to platform-powered DIY can be strong. Similarly, these organizations are also attracted to platforms to help lighten the burden of processing raw threat intelligence feeds for analysis and weeding out false positives.

Pros

- Provides pre-built integration across different security technology elements
- Offers greater threat context through a single pane of glass, saving time in investigation and response
- Centralizes the threat view for security operators
- Offers control over how security operators do work

Cons

- Requires maintenance of the on-premises environment the platform exists on
- Requires internal resources to respond to threats once they're identified and to do the remediation work after
- SIEM systems that boast "newer features," including threat hunting and SOAR, may define themselves as threat detection and response platforms but require teams to either define or tune response playbooks

Threat detection and response as a service

Some organizations may want to choose to go the software as a service (SaaS) route for their threat detection and response, where the platform vendor hosts the environment and maintains it while the organization still manages all of the security work stemming from its output. This is simply a different deployment mode of the platform-powered DIY approach, gaining the benefits of essentially spinning up SIEM or a security operations center (SOC) as a service.

Where it may make sense

Organizations that prefer to self-manage but want to take advantage of the flexibility and scalability of a SaaS model tend to choose this route. It offers the same value proposition as platform-powered DIY without requiring anyone to manage anything in the data center.

Pros

- Offers better scalability and deployment flexibility
- Maintains control over SOC operations and response procedures, as long as you have the resources to monitor your environment and investigate security incidents in a timely manner

Cons

- Requires internal resources to respond to threats once they are identified and to do the remediation work

DIY: hidden costs and misperceptions

As organizations choose between various deployment and management models, they may sometimes choose a DIY approach due to some misperceptions around costs and control. For example, some organizations go to DIY because they've been burned by a black box MSSP in the past, which may have been inflexible, slow to respond to incidents, or non-transparent with dashboards and data available to internal staff. This kind of negative history with less-than-stellar MSSPs drives a lot of DIY threat detection and response activity, but it's important to choose the route for the right reasons. Organizations should be mindful that not every managed service provider is created equally.

Another common misperception is that DIY is cheaper than a managed approach. Before making the decision based on financials, organizations should be sure to dig far enough into what DIY entails to uncover costs that may lurk under the covers. For example, many organizations may not realize that staffing a 24/7 SOC actually requires at least 5 full-time employees to equal one set of eyes on the dashboard at all times. Given the well-documented shortage of skilled cybersecurity workers, these kind of operational costs stack up and may change the financial equations for companies.

Managed detection and response

Organizations that have a low risk tolerance and limited resources to detect and respond to advanced threats are increasingly turning to managed detection and response service providers to handle the bulk of the work for them. This approach layers tier-1 and tier-2 support on top of a threat detection and response technology stack to outsource the intensive work it takes to stay on top of the dynamic threat landscape.

Where it may make sense

The managed detection and response approach makes sense for larger organizations seeking to expand their detection coverage without lengthy hiring processes in the face of the cybersecurity skills shortage. They can quickly supplement their existing team and leave it to building out other areas of the security program. It's also a good choice for organizations that have limited security head count or internal resources to maintain high service levels for incident response.

Pros

- Augments security teams in providing first stages of response and allows experienced in-house staff to focus on more strategic activities
- Provides consistent response processes and high-level of security expertise when internal resources are low
- Fits into a broader security program run internally
- Can also integrate into a more fully managed approach to overall security operations

Cons

- Costs that at first may be tough to justify if the organization doesn't fully consider DIY hidden costs

Hidden pitfalls of managed approach

As organizations seek to layer services into their detection and response capabilities, they should watch out for a few hidden pitfalls of the managed approach. First of all, avoid MSSP mishaps by seeing to it that your provider of choice offers full transparency into its capabilities and daily operations. Truly effective managed detection and response requires close cooperation between the customer and service provider, and when the managed option an organization chooses operates in a black box, it will likely run into problems. This means providing everyone is running on the same dashboard with the same information and access to logs, whether they are internal or external analysts.

On the flip side, if an organization knows it will depend on MSSP services in other areas of its security program, it should be mindful of how well the managed detection and response capability dovetails into that. Some managed detection and response providers don't offer any other traditional MSSP services, which means the organization will need to work with multiple providers to achieve a fully managed SOC experience.

As you choose your place on the spectrum

As decision-makers figure out where on the DIY-to-managed spectrum they would like their organization to land for threat detection and response, they should keep in mind that the factors for the choice operate almost like an audio mixing board with several interdependent sliders. These sliders include factors such as:

- Customizability of features
- Control over processes
- Resources
- Response speeds
- Risk appetite

So the more customizable an organization wants its detection and response features to be and the more control over the processes it wants to hold on to internally, the more resources it will take to maintain fast response speeds and effective mitigation of risk. If internal resources are fixed, then the organization will need to think about the tradeoff between customizability and control versus response speed. It's a delicate balance that requires close consideration of what's right for the organization.

Whether you are looking for a managed solution or to manage one yourself, AT&T Cybersecurity has you covered.

AT&T Managed Threat Detection and Response is a sophisticated managed detection and response (MDR) service that helps you to detect and respond to advanced threats before they impact your business.

It builds on our decades of expertise in managed security services, our award-winning Unified Security Management® (USM) platform for threat detection and response, and AT&T Alien Labs™ threat intelligence.

With advanced features like 24 x 7 proactive security monitoring, security orchestration, and automation in one turnkey solution, you can quickly establish or scale your security program without the cost and complexity of building it yourself.

Get a quote for AT&T Managed Threat Detection and Response

USM Anywhere™ delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines the essential security capabilities needed for highly effective security monitoring across your cloud and on-premises environments, including continuous threat intelligence updates.

Built for today's resource-limited IT security teams, USM Anywhere is affordable, fast to deploy, and easy to use. It eliminates the need to deploy, integrate, and maintain multiple point solutions in your data center. A cloud-hosted platform delivered as a service, USM Anywhere offers a low total cost of ownership (TCO) and flexible, scalable deployment options.

Get a quote for USM Anywhere

AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

This content was commissioned by AT&T and produced by TechTarget Inc.

© 2020 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.