MDR Showdown: Developers vs. Reseller/Integrators

Devolutions

THE ECOSYSTEM OF COMPANIES OFFERING SAFETY OVERSIGHT SERVICES IS DIVERSE

The ecosystem of companies offering safety oversight services is diverse. There are IT outsourcers that provide security services as an add-on to other IT services (networking, etc.). There are firms that specialize solely in cybersecurity services. And there are cybersecurity software developers that offer managed services. Each type of provider has its own strengths and weaknesses, and the security services they offer are often very different. Some provide basic security services called Security Operation Center (SOC), while others offer more advanced services, such as Managed Detection and Response (MDR).

But what's your best option? SOC or MDR? And if you choose MDR, do you go with a provider who has developed its own the technology or a reseller/integrator?

Origins: The External SOC

The first and oldest type of supervision service on the market is the external SOC. An external SOC relies primarily on a security log and event management tool (SIEM) to monitor the security of its customers' networks. Using the SIEM, analysts create scenarios (use cases) and monitor them to identify threats.

Examples of use cases that are actively monitored include:

- Creation of new admin accounts
- Multiple failed connection attempts from a single source
- Logging in via an administrator account outside working hours

However, given the evolution of security threats, passive monitoring via SIEM isn't a particularly effective strategy anymore. Every day new attacks appear, and it's not realistic for a SOC team to identify and add new use cases daily. Given these limitations, the industry has been turning away from the external SOC model and looking for solutions that have the capacity and flexibility to deal with today's threat environment.

Managed Detection and Response to the Rescue

One of the most effective answers to the fluid and high-volume nature of today's cyber threats is MDR services. MDRs provide organizations with threat detection, analysis, and remediation. They combine technology and human expertise to secure client networks. For example, the MDR team's analysts take any suspicious movement identified in the network and analyze it in depth to prevent it from turning into a problem. With an MDR service, you have true cyber threat hunters working in combination with advanced technology to manage your security proactively.

Two Types of Companies Offer MDR Services

There are **two typical profiles for MDR providers**: resellers/integrators and developers that use their own proprietary technologies. **Let's compare**.

MDR Resellers/Integrators

This MDR service is offered by IT outsourcing companies or cybersecurity firms, whose core business is not developing security products.

Though these companies can develop substantial expertise in MDR, they are hampered by the fact that they have no control over the evolution and effectiveness of the security technologies they use. They have to focus on making the best out of the platform they use, which can impact effectiveness.

Case in point: an MDR service provider identifies a malicious tool not detected by the solution it uses. They report the threat to the solution provider. It takes almost a month for the solution provider to respond. In the meantime, the client's network is at risk.

Even with best efforts and good intentions, these vendors may not be able to provide you with optimal security.

IT outsourcing companies that offer MDR or SOC services often face the dilemma of passing on vulnerabilities and security flaws that exist in their own networks. This can put them in an uncomfortable position. To avoid any conflict of interest, best practice is to separate your security outsourcing from your IT infrastructure outsourcing.

MDR Providers with Proprietary Technologies

Another model is MDR services offered by companies whose core business is the development of security products (e.g., developers of intrusion detection or antivirus systems). These providers are more flexible and can quickly create signatures or detection profiles when an unknown attack or malicious tool is identified in your network.

Because they have the expertise required to develop security technologies, they typically have a better understanding of hacker behavior and are always on the lookout for new hacking techniques. For example, the MDR analysts at these companies can analyze a new virus, create its signature, and inject it into their technology, which is not the case for companies that offer an MDR service without having their own technology.

Choosing the Right MDR Provider

The traditional SOC service simply isn't up to dealing with the current generation of cyber threats. MDRs represent the best current option to protect your network against fast-changing threats. And among MDR providers, your best option is to go with an MDR service provider that has developed its own technology because its analysts have much more advanced expertise than resellers and integrators.