Fully Managed- versus Co-Managed-Detection & Response Service

What kind of service does IT security need?

Companies often find it difficult to maintain their IT security due to a shortage of specialists - and the threats are growing due to increasingly sophisticated forms of attack. This is where the individual use of IT security services based on the modular principle with flexible, hybrid approaches can help: Co-managed detection and response services close gaps in cyber defense when resources, expertise or specialists are lacking and represent a valuable alternative to complete in-house concepts or fully managed services.

High-performance IT security is fundamentally based on two pillars: on the one hand, the prevention or at least the slowing down of successful cyber attacks through comprehensive security mechanisms, and on the other hand, the rapid detection and defense of cyber attacks that have been able to circumvent the security mechanisms. The more digitization advances, the more challenging it becomes to protect companies from damage caused by cyberattacks: Sophisticated malware, ransomware, malicious scripts and advanced persistent threats (APTs), which mostly find their way into the network via social engineering, threaten the IT security of companies worldwide.

In recent years, a trend has emerged that has now become one of the greatest threats to cyber defense: there is a lack of the necessary manpower; the shortage of skilled workers is also having a full impact on the IT security industry. Small and medium-sized companies in particular are finding it difficult to fill vacant positions. Specialized IT security service providers offer urgently needed support here with Managed Detection & Response (MDR) services. This additional, external manpower relieves in-house IT security teams or offers companies the opportunity to have their "own" IT security team.

What does Detection & Response mean?

The sole use of classic security measures has long since ceased to guarantee effective IT security. Today, fast and comprehensive threat detection and response are more important than ever. To this end, many companies are already using a wide variety of "Threat Detection and Response" tools that aim to detect, report and partially automate attack activities in a timely manner: EDR (Endpoint Detection & Response), NDR (Network Detection & Response) or XDR (Extended Detection & Response) are currently considered relevant security solutions that effectively counter current and future cyber threats.

The three letters EDR, NDR and XDR stand for "detection and response" technologies that detect cyber attacks and manage them in different ways. The solutions are used to detect attacks on corporate networks at an early stage and to stop them as quickly as possible.

The IT security teams responsible - mostly cyber defense analysts and threat hunters - receive immediate reports on identified anomalies and security-relevant data indicating acute threat situations through detection and response solutions. This enables them to react appropriately in the shortest possible time and avert major damage.

Why Managed Detection & Response Services?

According to a large-scale global study, a lack of manpower threatens cybersecurity in 85 percent of all organizations. There is no relief in sight on the labor market; on the contrary, all indicators suggest that the problem will become even more acute in the coming years. Managed Detection & Response Services (MDR) address precisely this glaring vulnerability. The term stands for managed detection and response of attacks. Here, the focus is not on technology or a solution, but on a service provided by specialized IT security service providers such as SECUINFRA.

Companies can thus access services from professional IT security providers that specialize in the detection, analysis and defense against cyber attacks - ideally around the clock. For example, the IT security analyst responsible for a company externally can use an orchestration tool (Security Orchestra-tion Automation and Response, or SOAR) to initiate appropriate defensive measures immediately upon detection and confirmation of a real threat. MDR services can be used as needed and relieve internal IT security teams of routine tasks or the time-consuming handling of false alarms.

Fully Managed or Co-Managed Service?

A Fully Managed Detection & Response Service is to be understood as a complete package in which all IT security tools necessary or deemed useful for a company are provided, managed and operated by a service provider. This can be, for example, a SIEM (Security Information and Event Management), supplemented by a SOAR system for faster, partially automated analysis and defense against cyber attacks. All systems that can initially detect a potential IT security incident, provide further information for assessment or initiate protective measures are connected to SIEM and SOAR. In concrete terms, this may involve the connection of EDR/NDR/XDR solutions. However, other solutions such as phishing detection, threat intelligence or vulnerability management can also be connected.

With the Fully MDR Service, security service providers implement and operate all the necessary IT security tools and monitor the customer's networks and end devices for anomalies around the clock, seven days a week. If necessary, defensive measures are initiated in close consultation with the customer. In addition, the service provider takes care of all administrative tasks, such as evaluating log files, updating the tools used with patches and updates, and creating reports.

A co-managed detection and response service is characterized by individual and flexible utilization: Operation and management of specific security tools are transferred to a service provider. The co-managed approach is based on the fact that many organizations and companies have already invested in IT security tools such as AntiPhishing, SIEM, EDR/NDR/XDR and SOAR, but then found that a complete, efficient operation fails due to a lack of sufficient manpower. Missing expertise or additional tools can be added with Co-Managed Detection & Response Services according to the modular principle - with predictable, transparent and scalable costs.

Knowledge transfer and close cooperation

Co-Managed Detection & Response Services should not be seen as a substitute, but rather as a supplement to the existing IT security architecture, in order to ensure that identified IT security threats can be responded to immediately and appropriately. Thanks to the expertise and manpower of the MDR service provider, this can be achieved so quickly that significant damage to the company can be averted or at least greatly reduced. In addition, co-managed detection and response services offer another advantage that should not be underestimated: customers receive high-quality consulting services and knowledge transfer. This is because close cooperation is an essential part of co-managed service approaches. Experienced, external specialists compensate for the lack of expert knowledge within the company - and the company's internal IT benefits from the professional exchange of their know-how.

Conclusion

Experienced specialists in the field of IT security are hard to come by on the labor market. All too often, small and medium-sized companies in particular find themselves without the urgently needed human expertise, even if technical security solutions are available. Managed Detection & Response (MDR) services fill these gaps in cyber defense. While Fully Managed Detection & Response Services provide all the necessary tools and services as a complete package, modular and flexible Co-Managed Detection & Response Services compensate for the lack of resources and capacities in specific areas.

Authors:

Ramon Weil - Founder & CEO - SECUINFRA GmbH
Norbert Nitsche - Head of Cyber Detection & Response Center - SECUINFRA GmbH

Further Information:

https://www.secuinfra.com/en/techtalk/fully-managed-versus-co-managed-detection-response-what-service-does-your-it-security-need/

Press contact:

SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland
Tel. +49 (0) 160 921 633 44
svenja.koch@secuinfra.com