EDR, XDR, MDR & Co.

What do companies need now for their IT security?

Today, active, fast and comprehensive threat detection and defense against cyber attacks is more important than ever. Companies are already using many different threat detection and response tools. The goal is to detect and report attack activities in a timely manner and thus significantly increase the level of security. EDR, XDR or MDR are currently considered relevant security responses to current and future threats: The times when the use of antivirus solutions was sufficient for solid protection of corporate networks are long gone.

According to the German Federal Office for Information Security (BSI), dealing with vulnerabilities is and remains one of the greatest challenges in information security. In addition to sophisticated malware, IT security teams must also keep an eye on social engineering attacks, ad-vanced persistent threats and malicious scripts. Behind the three letters EDR, XDR or MDR and hide "Detection and Response" models that detect, i.e. recognize, cyber threats and respond to them. The solutions and services are considered particularly relevant for securing a company network against cyber attacks, where classic security measures are no longer effective.

What is Endpoint Detection & Response (EDR)?

Endpoints, i.e. all devices connected to a network, are potential entry points for cyber threats: EDR stands for endpoint detection and response. The focus is thus on increasing the visibility of anomalies on the endpoint. In this way, EDR systems differ from other technical security solutions such as firewalls: protection takes place directly on the end devices and not at the network boundary. In the age of the Internet of Things and a sharp increase in the proportion of employees working from the home office, the number of endpoints in the company has also risen sharply in small and medium-sized enterprises. Endpoint Detection & Response captures, logs and analyzes endpoint activity in real time to detect potential attacks early. The ability to centrally provide artifacts and traces left by attackers provides analysts with a comprehensive view of the overall security posture. EDR systems also significantly speed up responses. Rapid response is supported by extensive automation capabilities and the use of APIs.

Identified anomalies are reported by EDR solutions to the IT security teams, which can then react promptly. EDR is primarily used by IT security analysts and the so-called "threat hunters", specially trained IT security experts who use threat information to protect IT systems against attacks. EDR thus marks the first steps toward automated threat defense controlled by IT specialists.

What is Extended Detection & Response (XDR)?

Extended Detection & Response is an extended solution approach that takes the principles of EDR and adds automation approaches and the use of Artificial Intelli-gence (AI). XDR not only focuses on endpoints in the enterprise, but also holistically monitors all traffic and applications within a network - including email, servers, endpoints, network, and cloud workloads. By incorporating activity data from all levels of IT risk, XDR enables a multi-layered defense strategy through just one consolidated management console. The upfront: An XDR Security Platform captures all data from the IT infrastructure and stores it in a database. The data is automatically analyzed, sorted and prioritized and made available to IT security experts via a central dashboard. Analysts thus work with detailed and correlated threat information. In addition, an XDR solution provides them with automated response recommendations.

The analysis of detected attack activities is hardly possible with a purely manual evaluation due to the diverse parameters - this is where AI approaches come into play, among other things. With their support, an XDR system detects IT security threats comprehensively, reliably and, above all, quickly.

What can XDR do more compared to EDR?

XDR systems master threat detection and defense across a company's entire IT infrastructure. A holistic picture of the threat situation is created - unlike EDR systems, which view IT security solely from the perspective of the endpoints. Accordingly, an EDR system can be a good starting point for increasing visibility on endpoints.

With XDR, this approach is extended to the network, email, app, cloud, container and user layers. Thus, correlations and machine learning can be used to trace attacks back to their source. For a reliable deployment of XDR solutions, an orchestrated system from a vendor's portfolio of components is usually required.

What is managed detection and response (MDR) needed for?

MDR stands for managed detection and response of attacks. The focus here is not on technology, but on a service provided by specialized IT security service providers. As a managed service, MDR provides companies with round-the-clock, 365-day-a-year security services from IT security teams specializing in IT infrastructure monitoring, IT security incident analysis and

appropriate response. An external security analyst can take immediate defensive action upon detection and confirmation of a real threat.

MDR services, which are usually modular, can be called upon as a company needs them and relieve internal IT security teams of the time-consuming task of handling alerts. Another major advantage of Managed Detection & Response is that customers receive high-quality consulting services and a valuable transfer of knowledge.

When does MDR make sense for a company?

Hardly any company has the appropriate tools internally, as well as the necessary manpower and expertise to manage a current security posture and proactively protect against new cybersecurity threats: Savvy IT security experts are scarce in the job market. The more data is generated, the more complex threat detection becomes.

This is why a service provider is needed to detect, identify and respond to IT security threats in whole or in part as required - and to do so quickly enough to avert or at least reduce significant damage. The use of MDR service providers who can do exactly this will therefore play an increasingly important role in the IT security industry. Professional and state-of-the-art analysis tools coupled with the cyber defense expertise of the MDR service provider ensure that events are correctly interpreted and evaluated and that the appropriate response is made to actual threats. For this purpose, MDR experts usually rely on a combination of different host and network security layers. Ideally, MDR service providers should ensure 24/7 availability of their services.

When selecting an MDR provider, aspects such as the size of the company, existing IT security solutions, manpower, expertise and experience of the company's own IT security team, and corporate guidelines should be included in the decision-making process.

Conclusion

Complex threat situations require efficient measures: Companies around the world are currently being targeted by cyber criminals and have to deal with espionage, extortion attempts or social engineering attacks. Accordingly, companies are building their cyber defenses in multiple layers - often with several tools deployed in parallel, each covering a specific threat scenario. Vast amounts of data are generated that need to be analyzed and overburden IT security team capacities.

As a managed service, MDR provides companies with security services from professional IT security teams around the clock, 365 days a year. Specialized in monitoring and analyzing IT

security incidents, they can respond quickly. Similar to authorities and organizations with security tasks (BOS), IT security teams are used to extreme situations. Critical situations that are perceived as stressful by the company are handled routinely.

Authors:

Klaus Wunder - Senior Cyber Defense Consultant SECUINFRA
Ramon Weil - Founder & CEO - SECUINFRA GmbH

Further Information: https://www.secuinfra.com/en/techtalk/edr-xdr-mdr-co-what-do-i-need-now-for-my-it-security/

Press contact:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0) 160 921 633 44

svenja.koch@secuinfra.com