What is MDR?

Managed Detection and Response (MDR) is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response. The main benefit of MDR is that it helps to quickly identify and limit the impact of threats without the need for additional personnel.

MDR remotely monitors, detects and responds to threats detected within your organization. For this, the service provider uses an endpoint detection and response (EDR) tool, which provides the necessary visibility into security events at the endpoint. After providing the necessary visibility, the telemetry data obtained from the endpoints are collected in the central console, where rapid suspicious event detection and response is carried out with the help of threat intelligence data and advanced analytics.

What are the Main Characteristics of the Services Offered by MDR?

The most basic characteristic of the services offered by MDR is to detect in detail the cyber attacks that cannot be caught and prevented by classical protection solutions and to response these attacks at their source as much as possible. Special capability software called EDR is used to operate advanced detection and response processes to be provided by MDR at endpoints.

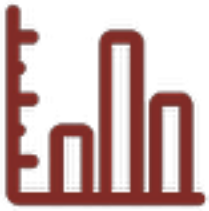
Within the scope of the MDR service, cyber threat intelligence related to cyber attacks against the relevant institution itself or other domestic and foreign institutions in the same sector is broadly defined to be used in all processes. This step utilizes many sources of cyber threat intelligence, both commercial and non-commercial.

Regardless of the SOC processes operated by the institution, the above-mentioned technologies that increase visibility at both the endpoint and the network layer are monitored and operated on a 7x24 basis by the special team that provides the MDR service.

If the institution already has an outsourced SOC service, the MDR provider and the SOC service provider can work in coordination and feed each other as data flow. In addition, MDR plays the most critical role in detecting cyber incidents and responding to these incidents quickly and accurately, and the processes defined in the institution are reviewed and organized specifically for this issue.

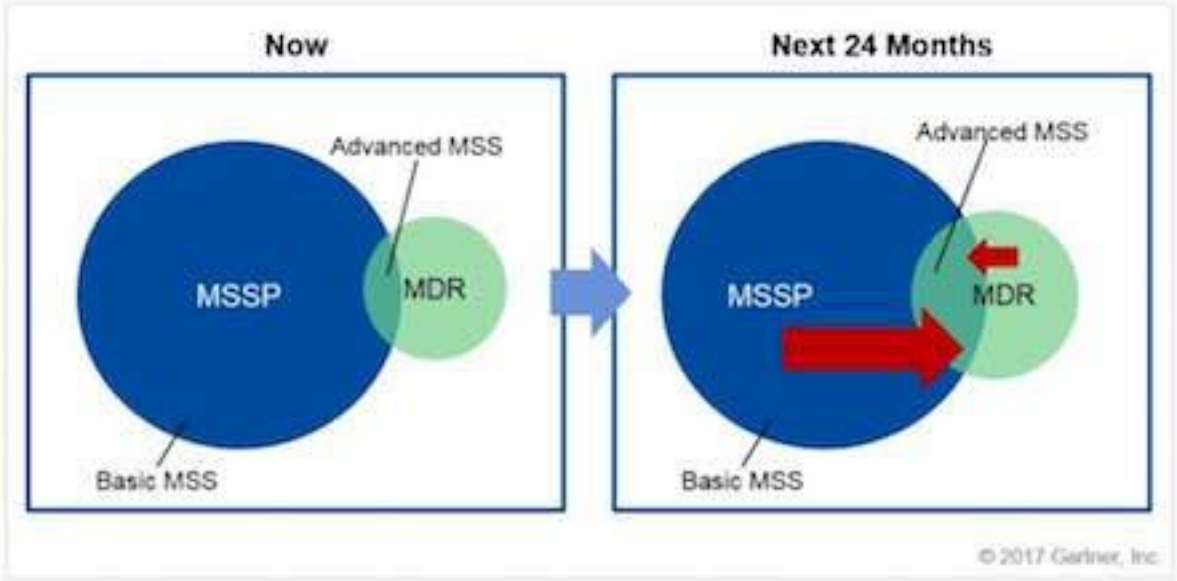
Due to the unwieldiness of traditional security monitoring approaches and their inadequacy in incident response, MDR service is of critical importance in order to detect and respond to a cyber attack on the corporate network in the fastest and most accurate way, and it has been used by more and more companies and businesses day by day.

What does MDR do?

 Reduces the probability or impact of successful attacks.	 It provides 24/7 visibility and covers all assets in the organization.	 It provides continuity by researching new threats and vulnerabilities.
 It balances human experience and technology at its core to provide accuracy and value.	 Offers tailored response approaches that reflect the business and attack context and cause	 It provides reliable, accessible and useful results and reports.

SOC vs MDR

MDR service is sometimes confused with services offered by SOCs. The figure below, prepared by Gartner, clarifies the issue.



Cyber security monitoring and management services offered under SOC aim to detect and prevent a cyber attack using traditional security tools and using known cyber attack signatures (at the endpoint, gateway level or log collection center). SOCs that monitor and manage organizations' cybersecurity infrastructures are particularly critical in preventing known cyberattacks. In addition, many relevant organizations recognize that today's cyber attacks are too advanced and the technology and processes used in the classical SOC approach are insufficient to detect and respond to these advanced cyber attacks. It is the point where the technologies and services used by the MDR service center increase the resistance of the organizations against advanced cyber attacks. Below are comparisons of SOC and MDR, taking into account the main steps of the incident response process.

Detection	
SOC	**MDR**
Classical SOCs use existing security products, which often results in low visibility into organizations at both the endpoint and network layer. This, in particular, causes alarms received by the SOC to require a great deal of verification, to have a disjointed content from and other related events, and to be indecisive in determining what to do next.	All details of a cyber incident can be obtained with the help of technologies that are deployed in-house by MDRs and increase visibility both at the endpoint and at the network layer. This allows the cyber attacks detected by MDRs to have a very high accuracy rate, to see in detail what happened before and after the relevant cyber incident, and to prepare the environment for what can be done to quickly prevent this attack

	immediately after the cyber attack. In this way, institutions gain a serious resistance against both known and unknown cyber attacks.

Verification	
SOC	**MDR**
The biggest problem faced by SOC analysts is the necessity of detailed verification of all events that are marked as a cyber attack by the technologies used by the relevant SOC and that generate a warning in this context. It is known that all SOCs deal with high amounts of false-positive alarms and even incorporate many technologies into their security infrastructures in order to minimize these alarm numbers. Even then, a SOC analyst's biggest problem is determining whether an incoming alarm is true. One of the most fundamental problems for SOCs is not knowing whether the relevant warning message belongs to a real cyber attack, and if it is a real cyber attack, what happened before and after this incident, especially since the records of the events before and after the alarms detected far from the center of the action taken by the attackers in cyber attacks are kept.	One of the most fundamental features that distinguishes MDR analysts from SOC analysts is the technologies they use. Thanks to the fact that they have access to trace records on the components where a cyber-attack took place in the internal network, in detail that can confirm this attack, and the attack alerts produced based on the behavior models for similar attacks, MDR analysts can detect real-time cyber incidents and take very fast action regarding these detected cyber attacks. Considering that especially advanced cyber attackers aim to reach their targets in a very short time, it can be seen how vital the ability to verify and take action is.

Detailed Analysis	
SOC	**MDR**
All processes operated by SOCs depend on the collection of records collected from many sources in a central record server (SIEM) and the detection and verification of these records. In particular, the centralization of a large amount of records from many different systems requires the correlation of these records. The first condition for a successful correlation is the collection of accurate records from the relevant technologies. In	Through to the detailed records provided by the technologies used by MDRs and the processes operated, the root cause of a cyber attack can be determined very quickly. Revealing the root cause quickly plays a key role in both preventing the encountered cyber-attack quickly and revealing the actions to be taken to prevent similar cyber-attacks from occurring in the future.

most cases, many SOC processes are incomplete and a successful case investigation cannot be carried out, due to the fact that the relevant technologies do not keep sufficient details in the records and that these technologies require the operation of some extra processes in order to detail the records.	

Prevention	
SOC	**MDR**
The processes operated to prevent cyber attacks detected by SOCs often depend on actions to be taken by third parties. This allows for a rapid response that needs to be carried out to slow down and therefore the cyber attack to continue within this period.	The biggest feature of the technologies used by MDRs is that they have advanced response capabilities in order to prevent detected cyber attacks as quickly as possible. In this way, MDRs can intervene in a cyber attack without the need for the support of any third party, and isolate the cyber-attacked component from the network when necessary, collect digital traces of the relevant cyber attack, and quickly detect similar attack traces on all other system components monitored by MDRs can reveal where the cyber attack has spread.

Proactive Cyber Hunting and Threat Hunting	
SOC	**MDR**
Many technologies used in SOC infrastructures are signature-based, and the success of preventing a cyber attack depends on whether the signatures of the relevant attack exist in the technologies used. In particular, the fact that the signatures of almost all of the advanced cyber attacks encountered today are not known in any way or that the attackers use their own tools of the operating systems without bringing any outside tools while carrying out the cyber	All of the toolkits used by MDRs aim to provide full visibility into systems. In this way, all of the tools and methods used by the attackers are recorded in detail on the systems. Detailed examination of these records is also carried out by MDR analysts, and threat hunting processes are carried out for the detection of cyber attacks that could not be detected in any way by the technologies used.

attack makes it impossible to detect these attacks using signature-based systems.	

EDR Platforms

Through to this technology to be used within the scope of the MDR service, records of all transactions on the basis of the operating system are collected and sent to the central server via **an agent to be installed on all servers and clients**. In this way, **these records of all activities on the computer, such as running applications, opened files, network addresses, are kept on a central server and cyber incident detection can be made very quickly thanks to the cyber threat intelligence sources activated on this server.**

Particularly, very good results are obtained in the detection of **cyber attacks indicated by certain behavior patterns** and in revealing the root causes of cyber attacks. Another feature of these platforms is their ability to respond to a cyber attack. In this way, computers or servers that have been hacked **can be completely isolated from the network**, **applications can be run** on these systems using the EDR platform, **or the necessary files can be collected from endpoints** for the detailed analysis of the cyber attack.

Microsoft Defender for Endpoint	Microsoft Defender for Endpoint