Table of Contents

[Defender XDR 2](#_Toc162976787)

[EDR, MDR, XDR and SIEM and SOAR. 2](#_Toc162976788)

[EDR 2](#_Toc162976789)

[NDR 3](#_Toc162976790)

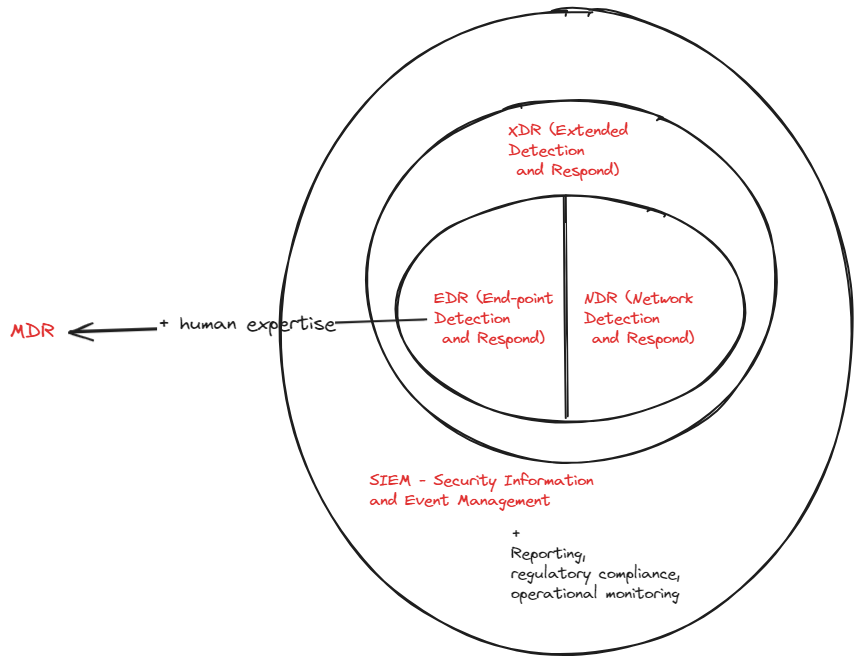
[XDR 3](#_Toc162976791)

[XDR Vs SIEM and SOAR 3](#_Toc162976792)

[MDR and MXDR 4](#_Toc162976793)

# Defender XDR

## EDR, MDR, XDR and SIEM and SOAR.

****

### EDR

*EDR stands for endpoint detection and response, and its primary goal is to identify malicious activity occurring at the endpoint.*

* EDR technology provides a great view of threats occurring at the endpoint.
* If a user browses to a malicious website and some sort of malware is downloaded, EDR can stop that threat before it turns into something like a ransomware attack.
* Focus is on malicious behaviour.
* It monitors activities and events on devices, looks for patterns that may indicate malicious action.
* This provides data for future investigation and this data is vital when the breach is detected.
* The EDR provides details on how the breach occurred and what the attackers actually did.
* This is the part of *Detection* part
* *Response*: can proactively take action to mitigate attacks before they have a chance to cause damage.
* If events are recorded that indicate a system has been breached, EDR can automatically isolate the system from the network in order to cut off the network.
* ! The challenge with EDR is the amount of information it produces.
* EDR provides way more alerts for investigation than a traditional AV. It is a bit hard to detect a definitely good or definitely bad information.

### NDR

*Network detection and response (NDR), identifies malicious activity traversing hosts; for example, detecting lateral movement across the network.*

* This primarily focused across the network.
* ! It tells you what is occurring on your network, who is coming across it, and what anomalies are happening across your network.
* NDR also gives you the ability to respond to a threat.
* *Microsoft 365 Defender*, specifically the XDR (*Extended Detection and Response*) component, offers NDR capabilities.

### XDR

* XDR gives you a combination of EDR and NDR.
* It merges these two technologies and looks at what is happening at the endpoint and then checks the movement of attackers or malware across a network.

*It combines EDR and NDR functionality with some elements of #UEBA User and Entity Behavior Analytics (UEBA)*

* EDR focuses on endpoints. XDR solutions integrate data from other systems as well.
* It is an EDR solution while pull in the logs from other sources like firewalls.

### XDR Vs SIEM and SOAR

*It’s like comparing a speedboat to a warship. Both go in the water and do similar things, but one takes a lot more feeding and watering and provides a lot more protection. One’s very easy to drive, but you can’t do as much with it. So you get there quicker, but you won’t be able to see as much*

* SIEM is used for threat detection, compliance, operational risk, and many other things. SIEM collects information from many different sources and as a result, it is a broad and shallow approach.
* It consumes information from solutions such as NDR, UEBA, and EDR.
* EDR + additional capabilities, like **reporting**, **compliance**, and **operational monitoring**.
* Provides actionable response, but doesn't provide any kind of automated remediation.
* SOAR can orchestrate and automate the common tasks and remediations.
* XDR does the same sort of things as both SIEM and SOAR.
* XDR is not so comprehensive compared either of these two tools.
* XDR is more focused on endpoints and data ingestion and analytics of XDR is not as powerful as SIEM tool.
* The orchestration capabilities are limited compared to SOAR.
* The XDR tools are cheap than SEAM and SOAR tools.

## MDR and MXDR

* The provider uses tools like *EDR and XDR* along with *human expertise*, to monitor your security environment.

## Defender for Identity

Microsoft defender for identity is a core element of ITDR (Microsoft Identity Threat Detection and Response). Defender for identity focuses on identity-based threats across your organization. Previously Defender for identity was called as Azure Advanced Threat Protection to safeguard against identity-based attacks in legacy Active Directory. This solution captures signals from both Windows Active Directory and deployed on-premises and Entra Id in cloud.

An example of how an attack happens and compromises an entire organization.

A diagram of a cloud computing system

Description automatically generated