# An Introduction To The XDR

## *Introduction*

Many SMBs have often been thought of to have a siloed approach to Cybersecurity. This simply means that your IT/Network Infrastructure is broken up into different segments, with no real purpose in mind.

While the thinking is that threat variants will be isolated and that they can be tracked easier, this is not the reality anymore. The bottom line is that these attack vectors can move from one silo to the next, often going undetected for months at a time.

How does one then detect them? Through the use of an Extended Detection Response system, also known as an XDR.

## *What Exactly Is The XDR?*

Although the solution can be quite complex, essentially an XDR can literally break these silos down into one entire infrastructure. That way, your IT Security team gets a complete, holistic view of what is happening out there. The XDR can do a deep dive, and do an exhaustive examination of any threats that may be lingering around. Examples of digital assets that are routinely probed include the following:

- It collects log information/data from each and every network security tool you have out there;
- It examines all of your servers, whether they are virtual or actual hardware based. These can range anywhere from your Web app servers; testing/production servers; Email servers, and even the database servers;
- It closely examines all of your endpoints – these are the points of origination and termination of all network communications that are established in your company. Typically endpoints have been a forgotten about topic, thus leaving them a prime target for the Cyberattacker;
- If you have deployed your entire IT/Network Infrastructure into the Cloud (such as that of AWS or Microsoft Azure), the XDR solution can provide the same amount of protection, if not greater;
- It can even filter out for malicious or malformed data packets, and discard them before they break through your lines of defense.

## *The Advantages of An XDR*

The following are typical advantages, especially for the SMB:

1) Alert Fatigue:

   The Cyber Threat Landscape is constantly changing, in fact even on a minute basis. Because of this, many IT Security teams are simply becoming too overloaded with all of the warnings and messages that are coming through. Many of them turn out to be false positives, which makes it even more difficult to determine what is real and what is not. This is where the XDR can come into play. Through the use of Artificial Intelligence (AI), the process of filtering out for them can be completely automated, depending primarily upon the rules that you established. The end result of this is that the IT Security team is only presented with the real alerts and warning, which then makes triaging far more efficient, for quicker remediation. Another very nice feature of the XDR in this regard is that it can also interface with any type of Security Information and

Event Management (SIEM) system. Essentially, this allows the team to see these alerts from just a single dashboard, rather than having to toggle through different ones.

2) Everything is looked at:

Many SMBs in Corporate America today are using different kinds of security tools and technologies in order to fortify their lines of defenses. One of the major problems of this is that each vendor often provides their own dashboard, which of course is configured differently and even has a different GUI interface, which can take some to get used to, especially if there are multiple numbers of them. A key advantage of the XDR in scenario is that it collects all of this information and data from all these different tools (and even the alerts and warnings), and parses through them in just a matter of a few minutes. This is then presented in the SIEM. This quick turnaround in analysis is also made possible by AI, as it has learned what to look for based upon the previous information/data that has been fed into it.

3) Conducting the investigation:

After you have been impacted by a security breach, one of the things that crosses your mind is how to start the investigative process in order to determine what exactly happened. True, this can take same time especially if you are undertaking a detailed forensics investigation. But the XDR can actually cut this time down. By making use of the processes from AI, any manual steps can now be automated. For example, through the SIEM, the IT Security team can create a virtual map which shows the trajectory of the attack vector form when it first entered to where it is going now. Given that you can access this kind of information in just a matter of seconds, you now mitigate that threat from going any further by literally stopping it its projected path.

4) It cuts down the detection time:

It is known that it can be months before a threat is detected in your systems. There are many reasons for this, perhaps it was covert in nature, or your team simply could not detect in time because of the other tasks it had in hand. But whatever the cause, the XDR can greatly trim down what is known as the Mean Time To Detect (MTTD) and the Mean Time To Respond (MTTR). These key metrics simply reflect how long it takes you to detect that there something lurking in your system and how long it takes to you act on it, respectively. Rather than taking months to detect them, the XDR can this time down into just minutes, by making use of the rapid information/data collection processes in the AI system. This serves a number of key benefits, which include the following:

- You can prove to your customers that you are proactively protecting their PII datasets;
- This is in turn will lead to a much stronger brand reputation that will quickly separate you from your competition. Remember, while providing great customer service is one thing, many people now look at how well your Cyber defenses are before they make a purchasing decision.

***Conclusions***

If you have not deployed an XDR solution yet, now is the time to do so. It is expected that 2022 is only going to get worse in terms of the Cyber threats, so the time to act is now. The XDR is not expensive, it

is actually very affordable for the SMB, especially if you have your IT/Network Infrastructure based in the Cloud.

***Sources***

1) https://www.trendmicro.com/en_us/what-is/xdr.html