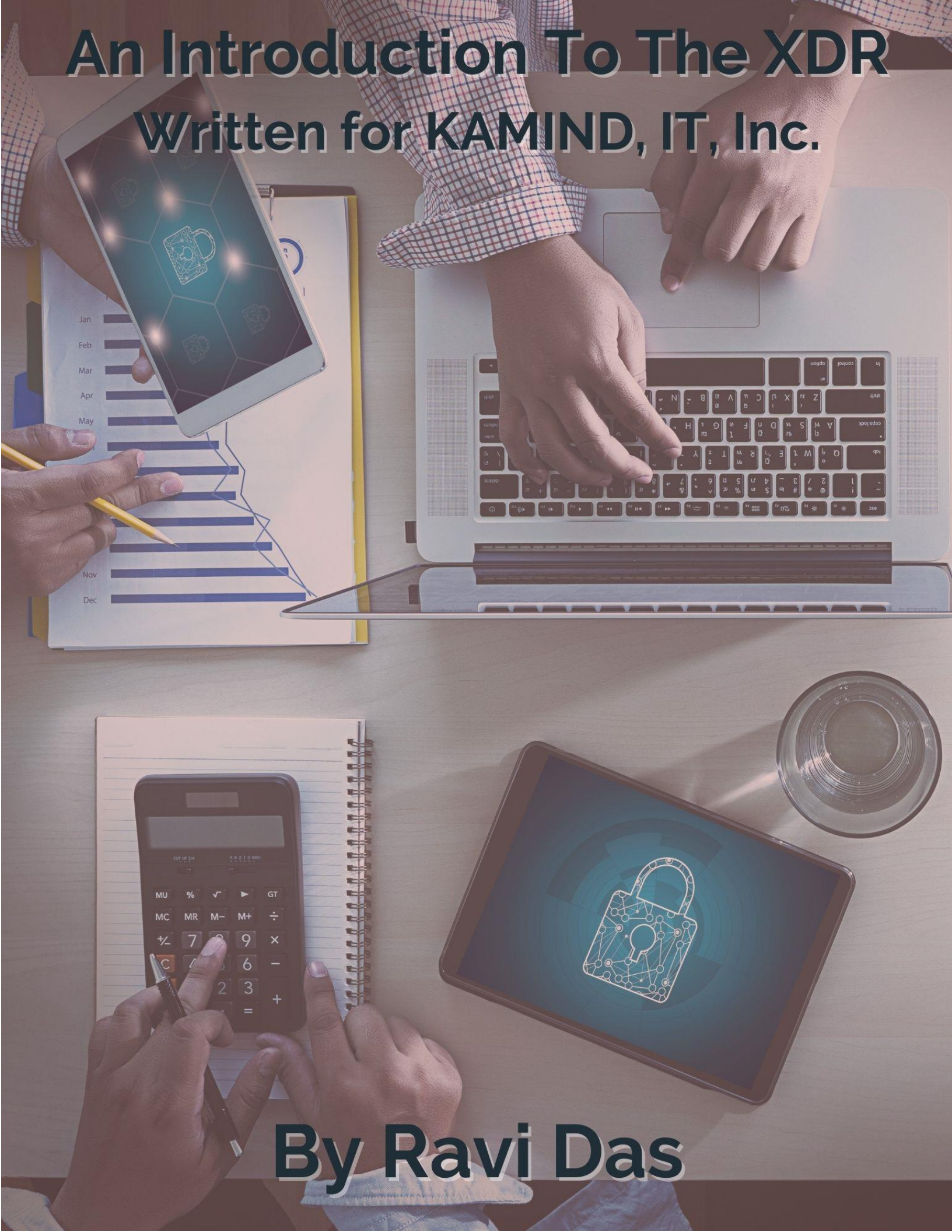
An Introduction To The XDR

Written for KAMIND, IT, Inc.



By Ravi Das

Introduction

One of the common denominators today in Cybersecurity is that of information overload. Despite all of the recent advancements in the technologies, IT Security teams are still simply overburdened with all of the information that is coming their way, even despite the availability of both Artificial Intelligence (AI) and Machine Learning (ML) tools.

What is needed most right now is a tool which can synthesize and crystallize of this information and data into one cohesive console and view. But not only this, it must have the ability to a deeper dive in the IT and Network Infrastructure than what is presently available right now.

There is something that can do this – it is known as Extended Detection and Response, or simply known as "EDR" for short.

What Is The XDR?

Many organizations across Corporate America today are implementing what are known as Endpoint and Detection Response (EDR) systems. These are software agents that are typically deployed at the point of origination (such as the server) to the point of destination (such as the device of the end user). This is used to bridge the line of network communications between the two, in order to provide a stronger layer of defense.

But the main problem with this is that only one EDR solution can only be deployed between a single flow of communications. If your organization is much smaller in terms of employee size, then this is not so much of an issue. But if your company is much larger, say in the range of thousands of employees, then this can be a nightmare for your IT Security team to manage all of warnings and alerts that are coming in, because there are different layers that have to be filtered and examined.

But with an XDR solution, especially one from Microsoft, it goes far beyond the traditional EDR approach, with the following characteristics:

- It goes much deeper into the different layers of security that you have deployed. For example, it can collect the information and data from On Premises solutions, applications that you have deployed into Microsoft Azure, and even Email and Network based servers.
- XDR does not depend upon the signatures of known threat variants in order to build up its repository to predict what future attack vectors could look like. Rather, it makes use of a subset of Artificial Intelligence which is known as "Behavioral Analysis". It contains Machine Learning based algorithms to not only filter through the false positives and the real warnings and alerts, but it also learns on a real time basis once its first deployed in order to predict what the future Cyber Threat Landscape could look like into the future.
- Unlike the EDR, it can gather the information and data that is collected across all of the layers of security that have been implemented, and present that in a holistic fashion to the IT Security team.
- It can even detect those legitimate software applications that Cyberattackers are currently using to hide their tracks as they try to move laterally across your IT and Network Infrastructure.
- The XDR examines everything that is sent to it and has the ability to extrapolate that information. For example, it can take that information/data that is collected from one endpoint and determine what kind of impact (if any) there will be onto a totally different endpoint, such

as your Email server. This can lead to a much more targeted response by your IT Security team as the need arises.

- Although an EDR based solution can provide recommendations as to how to mitigate an impending threat, these tend to be much more general in nature, and with a decent possibility that it may not even work in the end. But with the XDR, given its very sophisticated nature, can also provide recommendations that have a greater probability of working. But even more importantly, they are targeted specifically to that threat, so that there is no extra guesswork involved. The end result of this is that there is a far lesser downtime that will be experienced in case your company is impacted by a security breach.
- The XDR can examine the network traffic that is both incoming and outgoing, in a simultaneous fashion. The primary benefit of this is that any malicious data packets can be captured and isolated in a much quicker fashion.

The Questions That Are Being Answered

Fundamentally, an EDR solution will try to answer these questions after a security breach has occurred. But with the Microsoft XDR, attempts are made to provide your IT Security with these answers ***before a security breach will occur***. For example:

1) What are the statistical odds that a particular system will be infected, say with malware?
2) What are the potential entry points for the Cyberattacker? In other words, the XDR solution will try to comb through on its own any unknown weaknesses or vulnerabilities that could be present but have gone undetected so far.
3) What are possible origins for a possible threat variant to be launched from? This will be determined for the most part by the modeling component of the XDR solution.
4) What are the other parts of the IT and Network Infrastructure that could be impacted? While an EDR solution can provide an answer to this question to some degree, it will only address it from the standpoint of the systems that could be directly affected by an impact to the endpoint that it is protecting. But with XDR, not only can it address this, but it can also provide insight as well as to those other subsystems that are indirectly related to an endpoint, and how they will be impacted.
5) By making use of its sophisticated Graphical User Interface (GUI), the XDR solution will even paint a holistic scenario as to how a potential threat variant could spread itself throughout your organization.
6) With an EDR solution, it can be difficult to determine who the impacted victims will be in your company. But given the sophisticated nature of the XDR, there are far greater chances that you will get a much better idea about this, but even who the impacted parties will be that are external to your organization (namely, your third-party suppliers, or any other contractors that you may be using).

The Components Of An XDR System

Typically, most XDR systems will consist of the following core functionalities:

1) Telemetry/Data Analysis:

With the Machine Learning algorithms that it possesses, an XDR system can collect even the most granular pieces of information and data across each and every layer of security that your company has. It goes all the way from what you have On Premises to all the way what you have deployed in Microsoft Azure. This is all distilled down to the most prevalent alerts and warnings, based upon the context and rankings that they have been given. This makes it far easier for your IT Security team to analyze and escalate further.

2) Threat Detection:

   Since the XDR can determine if a legitimate software is being used maliciously as a point of entry, your IT Security will now more ammunition at its disposal in order to find those Cyberattackers that are attempting to engage in Advanced Persistent Threats (APTs) against your business.

3) Threat Response:

   In this regard, a very powerful feature of the XDR system is that it can automatically update your security rules and baselines of what constitutes a baseline of normal network behavior. Further even the Playbooks that you have created for Microsoft Sentinel can also be updated on a real time basis as well.

The Differences Between The XDR & The SIEM

Although the SIEM and XDR share a great number of similarities, they also have some key differences, such as:

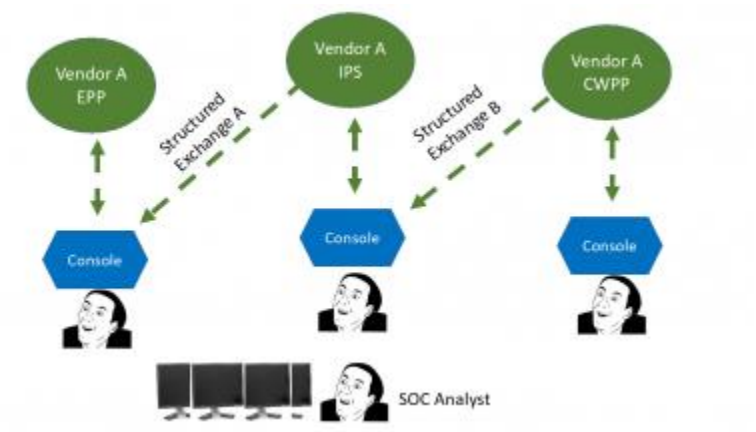
1) The XDR takes a ***proactive approach*** when sifting through alerts and warnings to provide strategies to the IT Security team to mitigate any threats ***before they happen***. The EDR does a ***reactive approach*** and does these actions ***only after a security breach has occurred***.

2) An XDR system is used primarily for fending off looming threat variants, it is not designed for compliance purposes. The SIEM has been designed more specifically for the latter, in that it archives log records, for both retainment and reporting for auditing purposes.

3) The XDR does not need to contain any type of log records. All it needs is the information and data that is gathered from the IT and Network Infrastructure. And if log records are required, the XDR system actually requires far fewer of them than the EDR system.

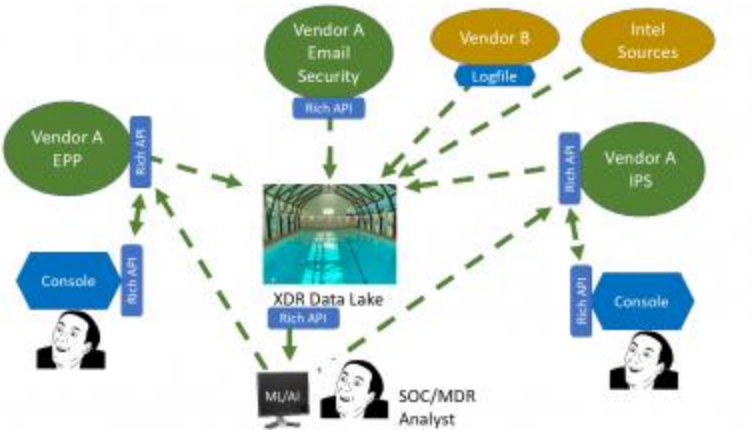
4) Because of the compliance functionality that the possess, an EDR system tends to be far more expensive to procure and deploy than an XDR system.

5) The information and data that is collected from an EDR system tends to be stacked in a siloed fashion, as the diagram below illustrates:



(SOURCE: 1).

The XDR does away with this siloed approach and takes all of the information/data that not only resides in the silos, but also what exists in between them. Further, the XDR system is also not only role specific, but it is also ***attack centric***, by storing everything it collects into a central repository. This unique approach by the XDR is also illustrated below:



(SOURCE: 1).

6) The SIEM only gives you a holistic view of what is happening with your IT/Network Infrastructure, but it is up to your IT Security team to formulate a course of action. The XDR not only does this, but it also, as mentioned before, provides for a possible course of action as well.

7) The XDR system speaks a "language of unification" with all of your digital assets, whereas a SIEM takes a "language of separation" with its siloed approach.

8) Finally, the matrix below depicts the other key differences between the XDR and the SIEM:

The XDR	*The SIEM*
The real time collection of endpoint data across all layers	Wider integration with other security tools and technologies
The analysis and triaging of alerts on a real time basis	The examination of different pieces of information and data (from within the same silo)
The automatic detection of suspicious activity	Alerts and warnings are generated, but not filtered
Data extrapolation and threat hunting functionalities	It can be integrated with workflow management tools, like that of Microsoft Sentinel
Both manual and automated tools can be integrated easily	

(SOURCE: 2).

The Components Of The Microsoft XDR

There are two main components to the Microsoft XDR, and they are as follows:

- The Azure Defender;
- M365 Defender.

<u>The Azure Defender</u>

Azure Defender is primarily used for all of the Microsoft Cloud Platforms that can be created, which include Software as a Service (SaaS); Platform as a Service (PaaS), and the Infrastructure as a Service (Iaas). It is used to help aid in the workloads that have been established in these three platforms and is primarily used to track down and isolate any threat variants which are trying to make their way into any of them.

It can be used for the following Aure based services as well, which include:

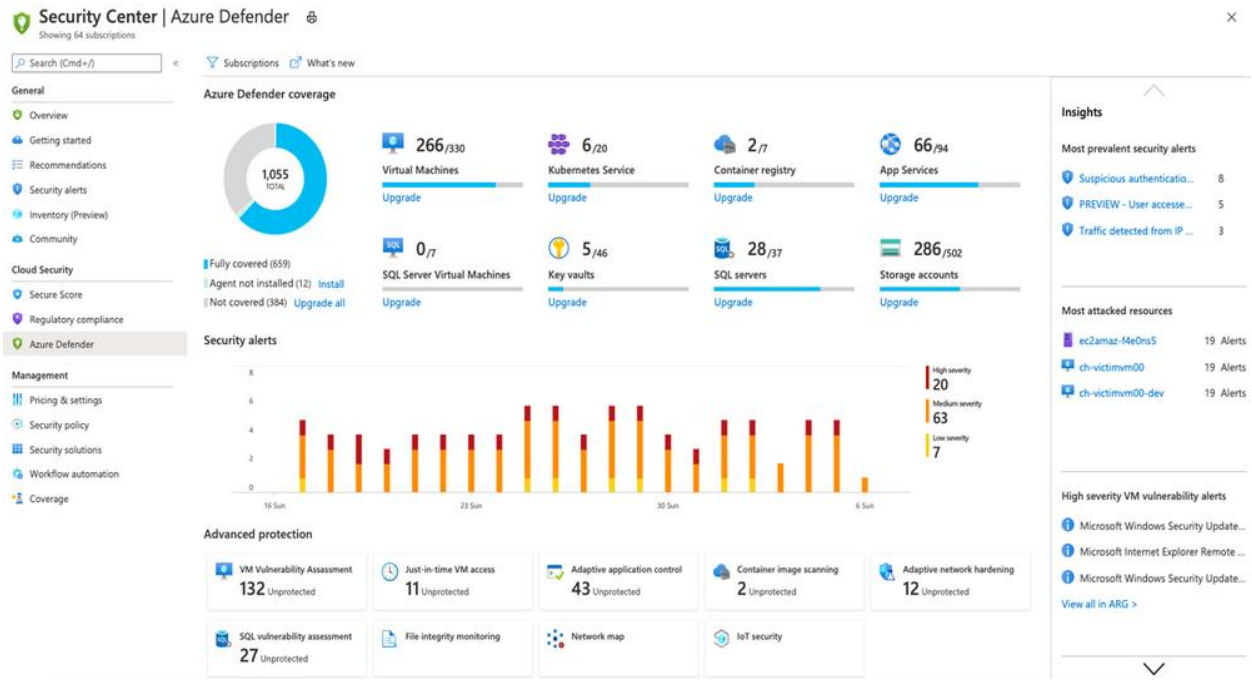
- Azure Defender for Storage (more information can be seen here);
- Azure Defender for Key Vault (more information can be seen here);
- Azure Defender for Azure Kubernetes (more information can be seen here);
- Azure Defender for Azure App Service (more information can be seen here);
- Azure Defender for Azure SQL (more information can be seen here).

The Azure Defender can be easily accessed from within the Azure Security Center, and it is comprised of the four major components:

- The various workload statistics;
- All of the security related warnings and alerts, and these are ranked by the degree of severity, in an effort to streamline the triaging process;
- All of the statistics that are related to any protective mechanisms that are deployed and used from within the Microsoft Azure Platform;

- Other security views, one of the main ones being the likelihood of any of the Virtual Machines (VMs) that you have created in being breached by a Cyberattack.

These components can be seen in the diagram below:



(SOURCE: 3).

It is important to note that Azure Defender can be used to protect a Hybrid Cloud Platform (which is a combination of any of the IaaS, PaaS, or the IaaS), and even conduct Vulnerability Assessment exercises to find any remediate any weaknesses and gaps in your IT and Network Infrastructure.

The M365 Defender

This can be considered as the second component of the Microsoft XDR, and it is made up of the following components:

1) The Microsoft Defender for Endpoint:

   As its name implies, this is the main security arsenal that can be used to protect the various endpoints in your Cloud or Hybrid Cloud environment. It can even be used for On Premises solutions as well. More information about this can be seen here.

2) The Microsoft Defender for Office 365:

   This is suite is primarily used to protect all of the applications that you utilize in your Office 365 environment, such as Word, Excel, PowerPoint, etc. Also, it is great for quarantining suspicious Email messages, malicious links, and any other messages that are deemed to be questionable in nature when Microsoft Teams is used for collaborative purposes. More information about this can be seen here.

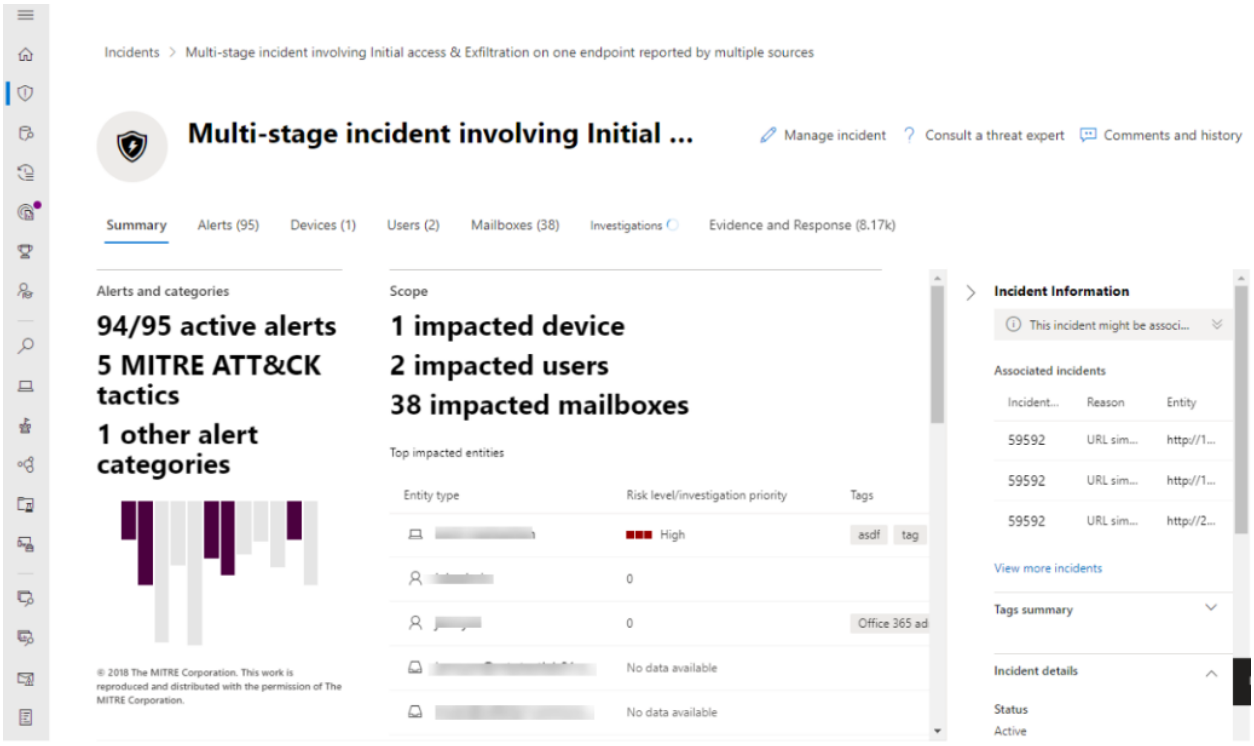
3) The Microsoft Defender for Identity and Azure AD Identity Protection:

The tools that are found in this suite are most notable used to protect the Active Directory Infrastructure. Also included in this are the user groups that you have created, and all of the rights, permissions and privileges that you have created for all of the employees in your company. For example, it is quite useful in sniffing out for login credentials that have been compromised and taking corrective actions that are needed. More information about this can be seen here.

4) The Microsoft Cloud App Security:

This toolset is exclusively designed to protect those software applications you have created and/or deployed into the SaaS infrastructure of Microsoft Azure, focusing especially upon the intentional or unintentional causes of data leakage. More information about this can be seen here.

The M365 Defender platform can even be used to create "stories" with detailed narratives about the origin of a Cyberattack, to where it ended up (either it was mitigated or had some sort of negative impact somewhere in your IT and Network Infrastructure). Also, your IT Security team can even conduct deep dive Threat Hunting exercises with M365 Defender, and this is illustrated below:



(SOURCE: 4).

The Benefits Of The Microsoft XDR

As you go through this whitepaper, you will notice the breadth and scope that the Microsoft XDR offers to your business. It is unlike any other XDR currently in place because it makes heavy use of both AI and ML tools so that your IT Security team can stay one step ahead of the Cyberattacker. With it, you protect just about any digital asset that you have in Microsoft Azure, and even those that are stored and used On Premises.

But to summarize, here some of the other key benefits:

1) It can further reduce the gaps in noticing security incidents:

   Many businesses today still make use of a lot of differing types and kinds of security tools. This can have two very negative effects:

   - It only increases the surface for the Cyberattacker;
   - Your IT Security team will quickly suffer from the phenomenon which is known as "Alert Fatigue", with the many alerts and warnings that they are receiving by the minute.

   But with the Microsoft XDR, you don't need to any invest in so many technologies. Everything that you need is available from just one account.

2) It can greatly speed up the time to detect and respond:

   Many security threats go unnoticed for long periods of time. But with the Microsoft XDR, you can pick up on all of this in real time, in just a matter of a few minutes, given the ultra-sophisticated functionalities that it possesses. The result of this is less downtime in case you are impacted. This will also mean that your IT Security team will start to develop a much more proactive mindset, because less time will have to be spent on analyzing each threat vector, given the automation features of the Microsoft XDR.

3) Simpler investigations:

   Whenever a Cyberattack does occur, usually an investigation is required to determine what actually happened. This can be a rather time-consuming process, but with the Microsoft XDR, the total length investigation can actually be reduced, because it can automatically piece together and correlate all of the events that transpired into one single view.

Sources

1) https://www.trendmicro.com/en_us/research/19/h/why-xdr-is-a-big-deal-and-is-different-from-siem-and-platforms.html
2) https://www.cynet.com/endpoint-protection-and-edr/edr-vs-siem-how-to-choose/
3) https://techcommunity.microsoft.com/t5/itops-talk-blog/what-is-azure-defender/ba-p/1843528
4) https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide
5) https://www.vmware.com/topics/glossary/content/xdr-extended-detection-and-response.html
6) https://heimdalsecurity.com/blog/what-is-extended-detection-and-response-xdr/

7) https://www.netwitness.com/en-us/blog/2021-03/xdr-versus-evolved-siem-whats-the-difference
8) https://afrait.com/blog/xdr-versus-siem/
9) https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction?WT.mc_id=modinfra-9866-socuff
10) https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-introduction?WT.mc_id=modinfra-9866-socuff
11) https://docs.microsoft.com/en-us/azure/security-center/defender-for-kubernetes-introduction?WT.mc_id=modinfra-9866-socuff
12) https://docs.microsoft.com/en-us/azure/security-center/defender-for-app-service-introduction?WT.mc_id=modinfra-9866-socuff
13) https://docs.microsoft.com/en-us/azure/security-center/azure-defender
14) https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
15) https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/overview?view=o365-worldwide
16) https://docs.microsoft.com/en-us/defender-for-identity/
17) https://docs.microsoft.com/en-us/cloud-app-security/
18) https://technologyadvice.com/blog/information-technology/using-xdr-with-edr/