**Azure Sentinel**

Azure Security Centre provides us with basic visibility and Analytics but Azure Sentinel goes beyond this and provides complete cybersecurity whereby it is able to provide visibility/analytics and Hunting/ Incidents and finally responding to the incidents with automation.

Initiating Sentinel

* To initiate the Sentinel service, we need to create or connect Log Analytic Workspaces. Once done, you will see the Sentinel Panel.

Here are the phases of Azure Sentinel:

1. Collect data

1. a. Azure Sentinel can collect data at cloud scale across the enterprise, both on-premises and in multiple clouds.
2. b. There are 98 data connectors available as of today like Azure/ AWS etc and we can connect to these sources and receive the data. Examples of Azure data are azure sign-in activity from Azure AD.

2. Create Alerts

a. Once the data is collected, we can run queries against the data. We focus on what is important using the analytics and create suitable alerts.

b. There are prebuilt workbooks available which can be selected and used to get insights.

Workbooks selection

We need to select the template and save it and we will be able to get the details.

3. Automate and Orchestrate

a. We build automation rules which will automate incident configuration. We could trigger playbooks to handle security alerts.

b. We create rules which will trigger the playbooks to be run automatically based on the conditions

Hunting Feature

Azure Sentinel has the hunting feature where we could go further and search for various activities like listing of storage keys or high DNS queries etc.,

This will help us identify attacks targeted and we could go and proactively block the malicious activity.

Sentinel Community

There is a sentinel community where we can get different types of resources like Workbooks,

Analytics rules, Hunting queries, and Playbooks.

Azure Sentinel pricing

* Billing is based on the volume of data ingested for analysis. Azure Sentinel offers a flexible and predictable pricing model and we could pay either with Capacity Reservations or Pay-as-you-Go.
* With Capacity Reservations, we can get as much as 60% less as compared to Pay-as-you-Go.

**Advanced Threat Protection**

Azure has a product called Azure defender for SQL which is a unified package for advanced SQL security capabilities. This is designed for the database offerings viz., Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics.

Some of the functionality of the tools include

● Discovering and Classification of sensitive data

● Identifying and mitigating potential database vulnerabilities

● Detection of anomalous activities that could be a potential threat

The tool does 2 major activities. One is Vulnerability assessment and the other is Advanced

Threat Protection.

Under ATP, the following features are available:

● Detect anomalous activities

o Unusual/potentially harmful attempts to access or exploit your database.

● Continuous monitoring of database for suspicious activities

● Immediate security alerts on

o Potential vulnerabilities

o SQL injection attacks

o Anomalous database access patterns.

● Recommend action on how to investigate and mitigate the threat.

How to Enable ATP:

● We can enable/disable different type of alerts under ATP

Under Security settings of the SQL server, we can enable ATP.

● We can see the ATP alerts in the Security Center as it is integrated with it.

● The MYSQL Database server can be configured under Security Option.

**Azure Information Protection**

AIP helps us classify and protect our documents based on the sensitivity of the data. AIP is based on Azure Rights Management (RMS) which is a cloud based protection technology.

We can look at the lifecycle of data below:

Lifecycle of data

1) Identify/Classify/Tag

a. In this phase, we identify the data that needs to be protected. There are two types of data in an organization. Structured and unstructured.

b. Data that resides in a database can be classified as structured. Data that resides on the servers and user systems can be classified as unstructured.

We identify the unstructured data

c. Then we classify the data. Simple classification could be Public data which is non-personal and non-confidential. Likewise we could have confidential data.

d. Then we need to tag the data

2) Share and Protect

a. Once the data is classified and tagged, we encrypt the data. We could either use cloud key or we could use our own keys

b. Then we grant or revoke access to the data. We could grant viewing/editing permissions to different groups as needed

3) Usage tracking

a. With RMS, we could track the usage of data

b. We can see who accessed the data from which location and when

c. We can grant or deny access

4) Revoke access

a. Once we revoke the access to the data, the users who had access before cannot access the same data going forward.

● The Labels are available as default as seen below. We can create custom labels if needed to suit our needs.

AIP lifecycle:

Here are the practical steps to the same

1) Subscribe AIP – We need to have suitable licenses like AD Premium P1/P2. There are other enterprise licenses also like E5.

2) Azure AD – We need to integrate with our AD

3) AIP Label and Policy – We need to create labels and then add them to our Policies.

There is a global policy available by default. We can further customize or add our own Policy.

4) Install AIP client – We need to install AIP client on all servers that we want to manage

5) Create custom label – We create custom labels if needed

6) Revoke Access – We review and revoke access ending the life of the data managed

AIP Scanner

For On-premises setup, we need to install AIP Scanner which does the following:

1)

2)

3)

4)

Discover

Protect

Classify

On-prem repository – Any folder/drive like c: etc is considered as a repository

Requirements for AIP Scanner – Windows Server and SQL server

Steps for setting up AIP scanner

1) Create Profile

● Settings like manual / automatic scan

● Policy enforcement

● Add Repositories like c:/, f:/docs

2) Install SQL server

3) Run Powershell command and setup AIP Scanner

● Install-AIPScanner -Sqlinstance “instance name”

-Profile “profile-name”

4) Setup Access token

**Azure DDoS Protection**

What are DoS and DDoS?

DoS stands for denial of service and DDoS stands for distributed denial of service.

Scenario:

Let’s say that you have a web server serving web traffic and you are a medium enterprise handling 1000 requests per second. If any malicious entity sends 100,000 requests per second, your server will be busy trying to respond to the 100K requests and unable to serve the regular customers. This is called Flooding.

Often the load will be so heavy that it will cause the server/machine to crash. This is called denial of service where customers are denied service by rendering the server unusable. Imagine the same 100K requests coming from multiple servers where malicious entities do a coordinated attack with multiple servers. This is called distributed denial of service where multiple servers hit a given target to bring it down. We have seen attacks feeding as much as 800 Gbps which can bring the biggest servers down.

Azure DDoS

It provides protection against DoS attacks with always-on monitoring and automatic network mitigation.

😊

There are two levels of Service – One is BASIC and the other is STANDARD. Basic plan is free

and enabled by default. After all, Azure needs to protects its resources

Basic plan, like the name says, provides only basic services (always-on monitoring and

automatic network mitigation).

Standard protection provides multiple features. This could cost you as much as 3000$ to

protect about 100 resources like

● Azure firewall, App Gateway/WAF

● VMs, AKS

● SQL, CosmosDB, Storage, App Services etc.

● Vnet

● So, let’s say that a DoS/DDoS attack occurs. The Cloud is resilient usually due to the

elasticity and if you have good autoscaling, then the cloud resources will keep scaling

up like VM spinning up, App Service scaling up etc.

● As a result, you will have a lot of traffic and you must be aware that while ingress

traffic is not charged, consumers pay for egress traffic.

● So you will land with a huge compute bill and egress data charges.

● If we had the DDoS standard protection plan, we would be issued credit for the

excessive charges if the plan failed to protect us.

Some of the features of DDoS Standard protection are:

● DDoS Rapid response – We can engage the DDRT (DDoS Rapid Response

Team) for attack investigation and analysis

● Cost Guarantee – As discussed, we will be issued a service credit for the

application scale out and excess data transfer

● Attack alerting/Metrics - Alerts can be configured to be notified at the

start/stop and logging will be done and metrics provided.

● Extensive Mitigation Scale – This works at a global scale and is highly scalable

and can mitigate over 60 types of attacks.

● Multi-layered protection – It can protect at different layers (layer 3/4/7)

● Adaptive tuning –Let's say there is unusual traffic from an IP and it is

determined as anomalous by the DDoS cognitive services, ddos protection

will automatically deny traffic from the IP and block it.

In addition, we can have our own monitoring to alert when a DDoS attack occurs.

We can set up this rule in Azure Monitor to notify us that ddos mitigation has started. We

can set up an action group and take actions like notifications, isolating the resource for

forensics etc.,