CHAPTER 7

Automated Security Monitoring

Security monitoring is the automated process of collecting and analyzing potential security threats and taking appropriate actions to create secure applications. Nowadays, more and more companies are entering the market with cloud adoptions. Monitoring this cloud workload is a must in order to create secure and safe applications.

The previous chapter took a quick tour of threat modelling and securing infrastructure deployment, including security testing, key management, and disaster recovery.

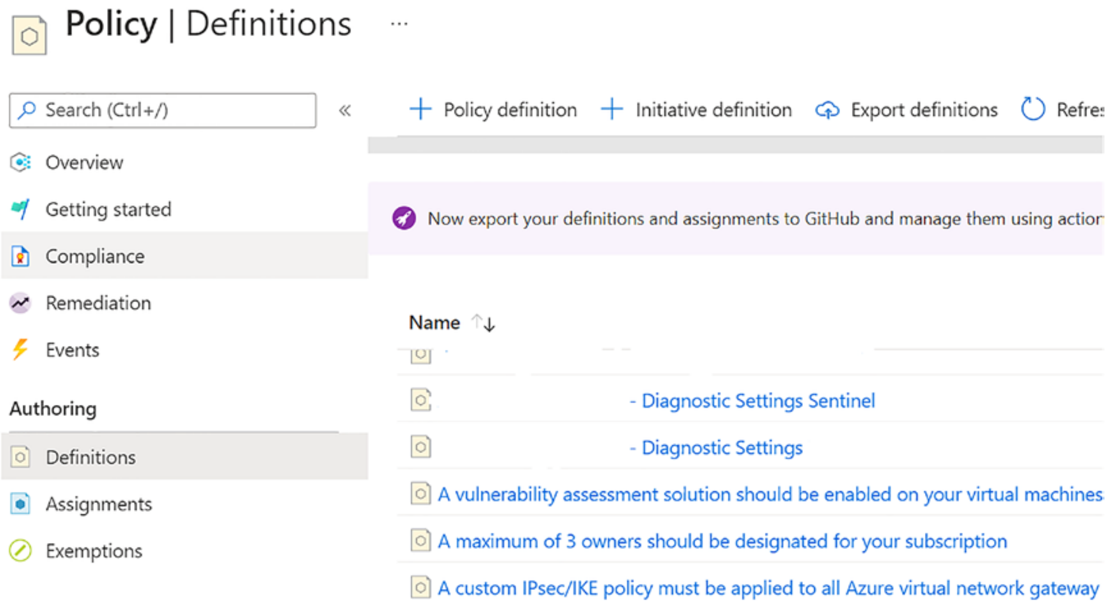
This chapter covers the following topics:

- Setting up security policies
- Advanced observability
- Azure Monitor
- Azure Sentinel

Setting Up Security Policies

Microsoft Defender applies security initiatives to Azure subscriptions. These initiatives contain security policies that can be enforced at a subscription level or resource group level. Every security policy includes things like the type of resources that can be deployed and enforces the tags for all resources. As shown in Figure 7-1, you can view policy definitions and initiatives on the Azure Portal.

S. Lad, *Azure Security For Critical Workloads*, https://doi.org/10.1007/978-1-4842-8936-5_7



Policy | Definitions ...

Now export your definitions and assignments to GitHub and manage them using actior

- Diagnostic Settings Sentinel

- Diagnostic Settings

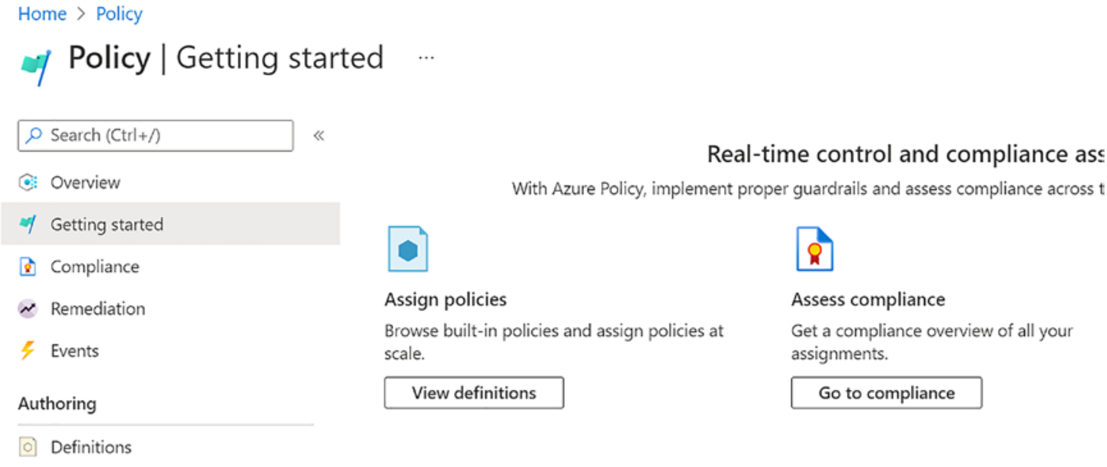
A vulnerability assessment solution should be enabled on your virtual machines

A maximum of 3 owners should be designated for your subscription

A custom IPsec/IKE policy must be applied to all Azure virtual network gateway

Figure 7-1. *Security policies and initiatives*

– Security policy: An Azure security policy is a rule about the specific security conditions that the security team wants to control. There are also various built-in definitions available to control what type of resources can be deployed or enforce tags on various resources. Apart from the built-in policies, you can also create custom security policies. See Figure 7-2.



Home > Policy

Policy | Getting started ...

Real-time control and compliance ass

With Azure Policy, implement proper guardrails and assess compliance across t

Assign policies

Browse built-in policies and assign policies at scale.

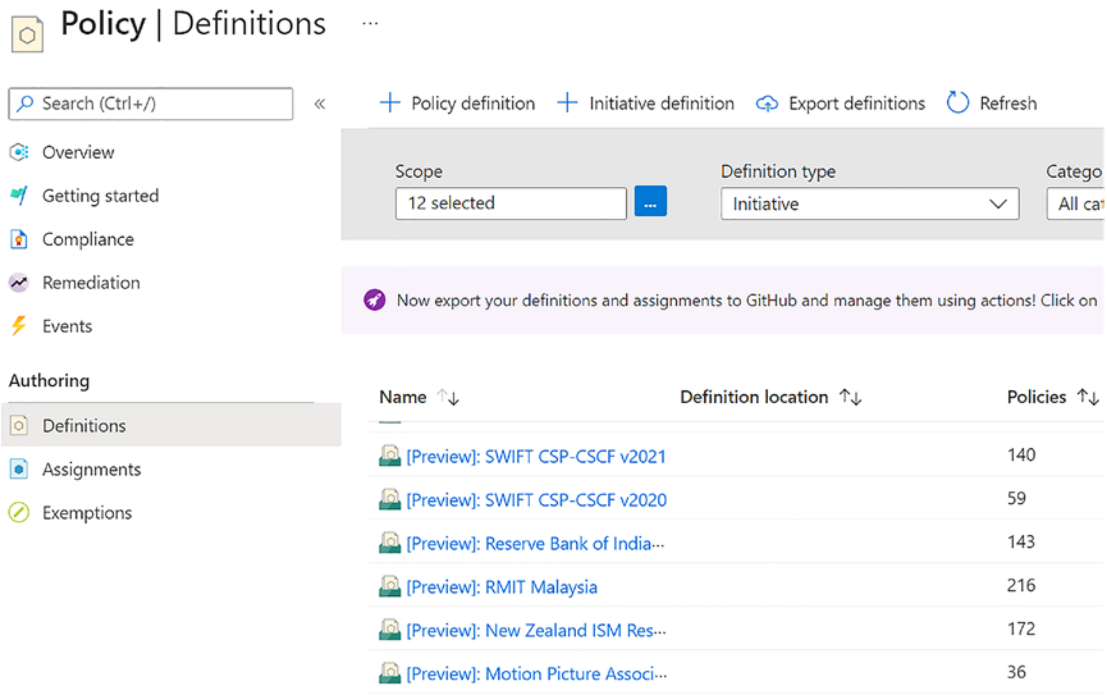
Assess compliance

Get a compliance overview of all your assignments.

Figure 7-2. *Overview of security policies*

In order to implement policy definitions, you need to create them and assign the policies. You can assign these policies using Azure CLI, PowerShell, or the Azure Portal.

– Security policy initiative: Azure policy initiative is a collection of policy definitions or rules that are grouped together for a specific goal. This simplifies the management of policies by grouping policies together into a single item. It also helps ensure the security requirements of the regulators. Figure 7-3 shows an example overview of the security initiatives.



Scope: 12 selected

Definition type: Initiative

Catego: All cat

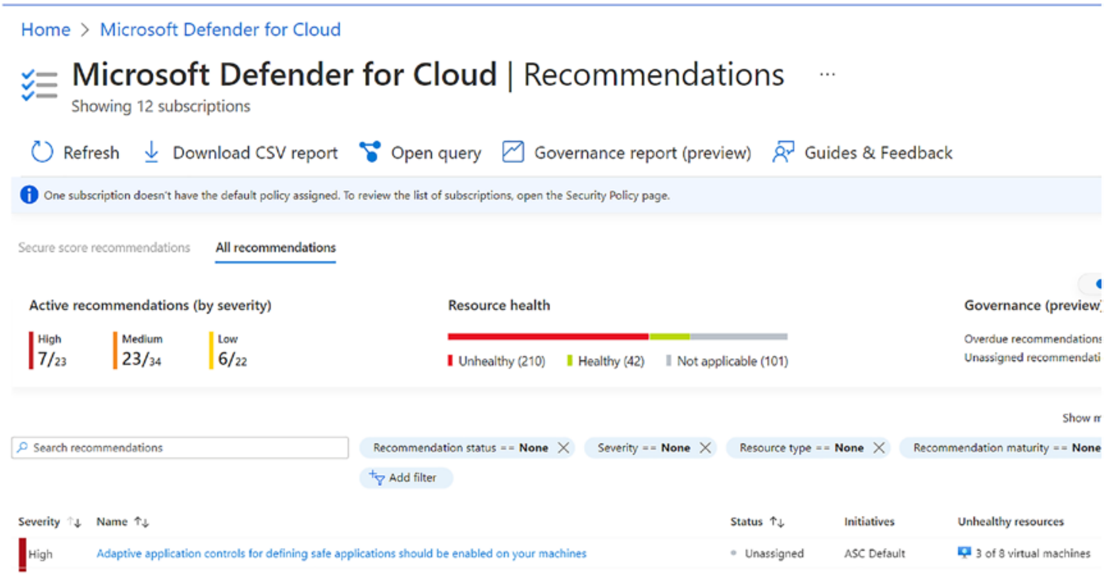
Now export your definitions and assignments to GitHub and manage them using actions! Click on

Name	Definition location	Policies
[Preview]: SWIFT CSP-CSCF v2021		140
[Preview]: SWIFT CSP-CSCF v2020		59
[Preview]: Reserve Bank of India...		143
[Preview]: RMIT Malaysia		216
[Preview]: New Zealand ISM Res...		172
[Preview]: Motion Picture Associ...		36

Figure 7-3. *Overview of security initiative*

– With security initiatives, you can define the desired configurations of the workloads to ensure the security compliance of the company. You can use Azure Policy to manage policies and initiatives and assign them to subscriptions or management groups.

- Security recommendations: Defender for cloud periodically analyzes the compliance status of the resources to identify potential security misconfigurations and weakness. Azure Defender for cloud also provides recommendations to fix these security issues. These recommendations mainly come by validating the policies against the resources that don't meet the requirements. See Figure 7-4.
- You can take required actions based on the recommendations from the Defender cloud. Each recommendation has the following information:
- Short description
- Steps to implement the recommendation
- Impacted resources


Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Recommendations ...
Showing 12 subscriptions
Refresh
Download CSV report
Open query
Governance report (preview)
Guides & Feedback
Secure score recommendations
All recommendations
Show m
Search recommendations
Add filter

One subscription doesn't have the default policy assigned. To review the list of subscriptions, open the Security Policy page.

Active recommendations (by severity)

High	Medium	Low
7/23	23/34	6/22

Resource health

Unhealthy (210) Healthy (42) Not applicable (101)

Governance (preview

Overdue recommendations

Unassigned recommendati

Recommendation status == None ✕ Severity == None ✕ Resource type == None ✕ Recommendation maturity == None

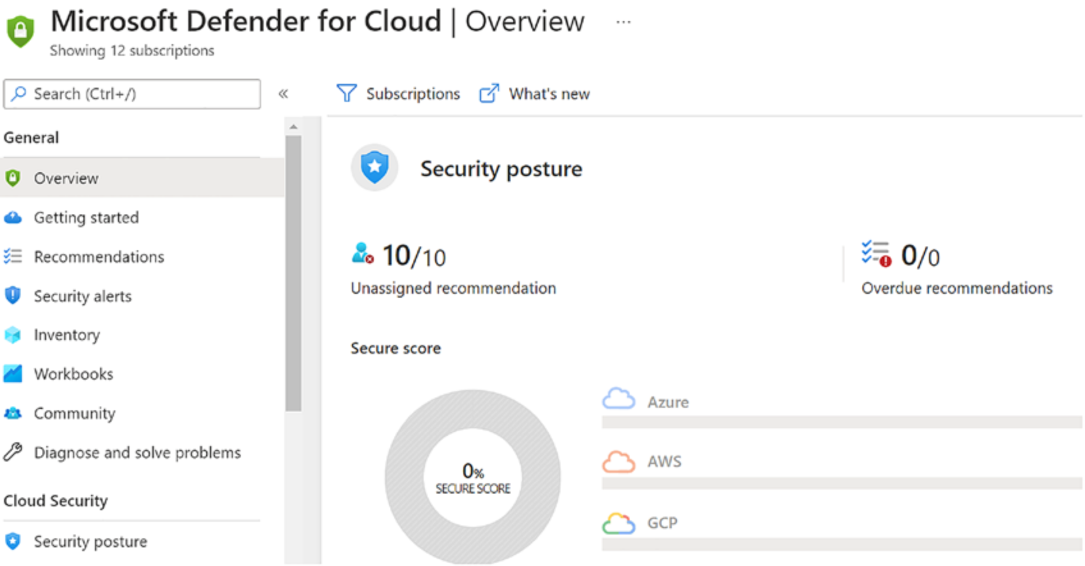
Severity ↑↓	Name ↑↓	Status ↑↓	Initiatives	Unhealthy resources
High	Adaptive application controls for defining safe applications should be enabled on your machines	Unassigned	ASC Default	3 of 8 virtual machines

Figure 7-4. Recommendations by Defender for cloud

The main goals of Microsoft Defender are to:

- Understand the current security situation
- Effectively and efficiently improve the security

You can achieve this using the secure score. Defender for cloud checks the cloud resources for security issues and then groups them to determine a single score. See Figure 7-5.


Microsoft Defender for Cloud | Overview

Showing 12 subscriptions

Security posture

10/10 Unassigned recommendation

0/0 Overdue recommendations

Secure score

0% SECURE SCORE

Azure

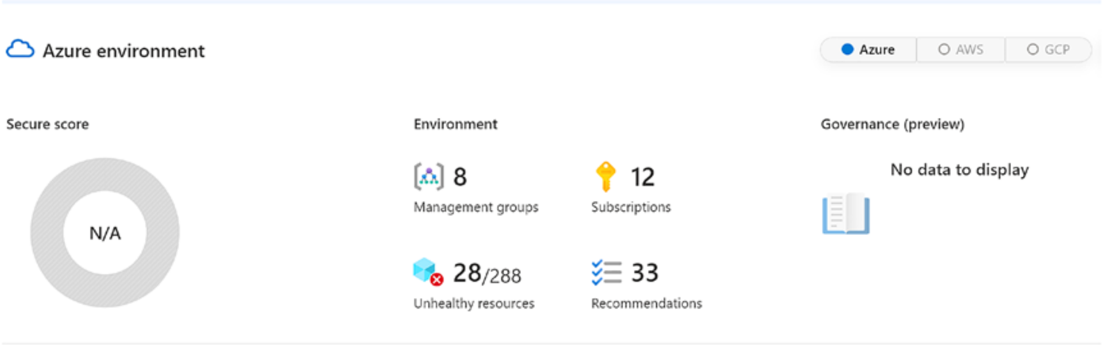
AWS

GCP

Figure 7-5. *Posture score*

Once you open the overview page of Microsoft Defender for cloud, you can view the secure score for the security posture. The secure score is represented as a percentage.

If you want to understand the score at a granular level, click Explore Security Posture from the Overview page. See Figure 7-6.


Azure environment

Secure score

N/A

Environment

8 Management groups

12 Subscriptions

28/288 Unhealthy resources

33 Recommendations

Governance (preview)

No data to display

Figure 7-6. *Security posture details*

Advanced Observability

In order to proactively monitor applications, you need to monitor resources to maintain security posture and check the vulnerabilities. You can enable alerts for suspicious activities to find security issues and events.

You need to consider the following points to monitor security related events:

- Use Azure Native tools to monitor the application, infrastructure, and workload
- Create a security operations center or SecOps team
- Monitor the traffic and access requests for the application
- Identify and discover common risks to improve the security score in Microsoft Defender
- Use industry standard protocols and benchmarks to improve the security posture of an organization
- Send logs and alerts to the central log management system
- Enable frequent internal and external audit compliance
- Regularly test security design and implementation

Microsoft Azure provides various monitoring tools to observe the operations and detect behavior:

- Microsoft Defender for cloud: This is a cloud security posture management and cloud workload protection platform for on-premises as well as public cloud resources. See Figure 7-7.

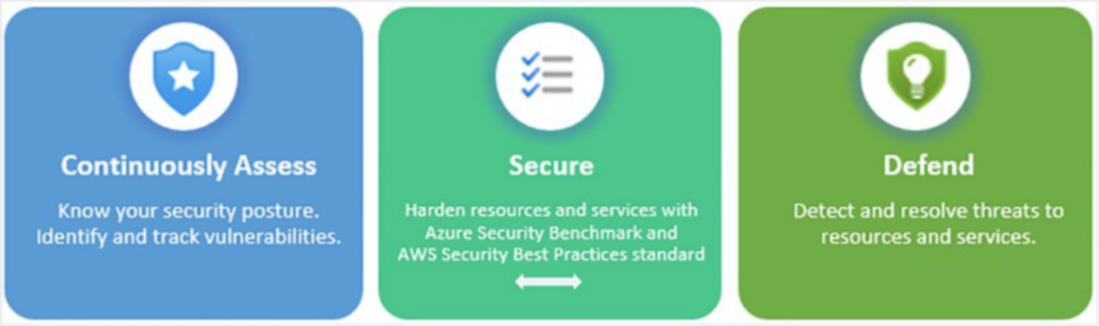
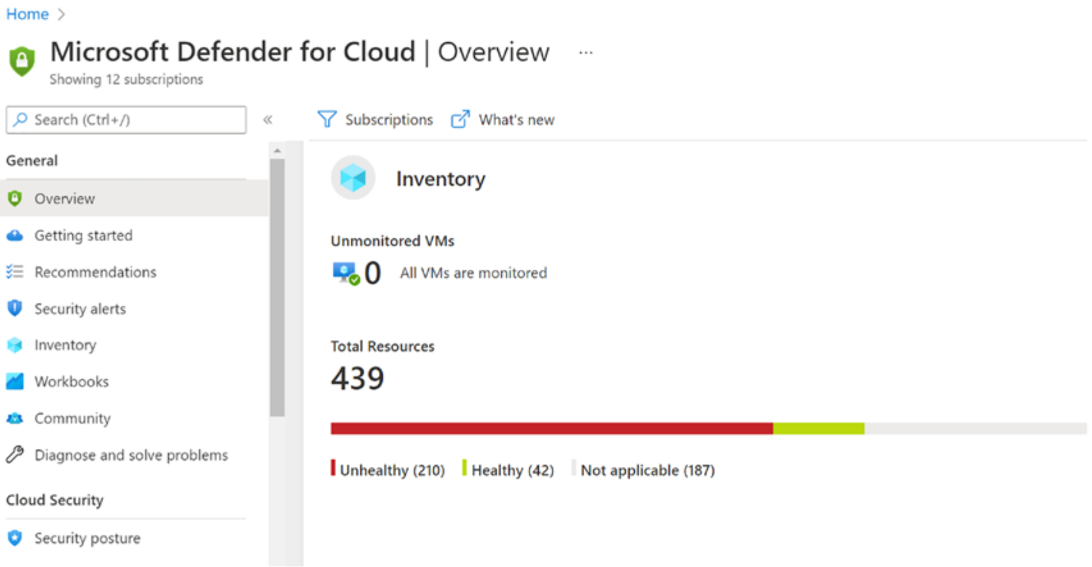

Continuously Assess
Know your security posture. Identify and track vulnerabilities.
Secure
Harden resources and services with Azure Security Benchmark and AWS Security Best Practices standard
Defend
Detect and resolve threats to resources and services.

Figure 7-7. *Microsoft Defender for cloud lifecycle*

Defender for cloud maintains the following information to assess your cloud application:

- Defender for cloud secure score: It continuously assesses the security posture so that you can track and improve security efforts.
- Defender for cloud recommendations: It secures the application or workload by providing step-by-step actions that can protect the application from known security risks.
- Defender for cloud alerts: This defends your workload in real-time so your team can act immediately and prevent security events. See Figure 7-8.



Unmonitored VMs
0 All VMs are monitored

Total Resources
439

Unhealthy (210) Healthy (42) Not applicable (187)

Figure 7-8. *Microsoft Defender for cloud*

- Microsoft Sentinel: Sentinel uses native security information event management (SIEM) and security orchestration solutions in Azure. It provides a bird's eye view across the enterprise to monitor and detect volumes of alerts and resolution of the issues. See Figure 7-9.

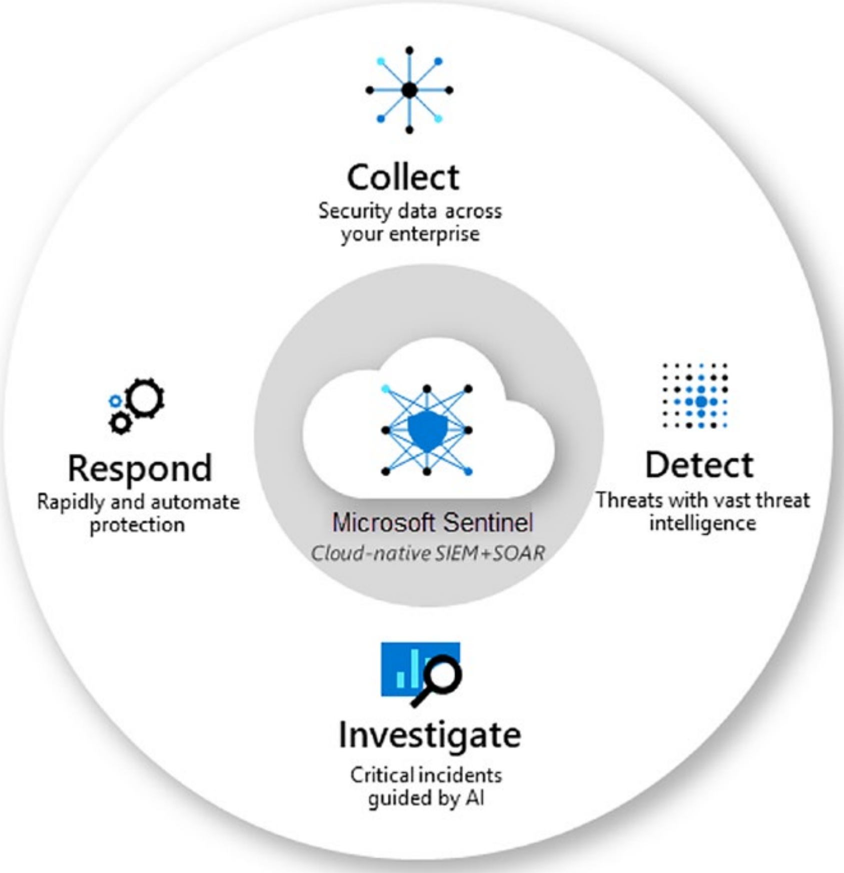
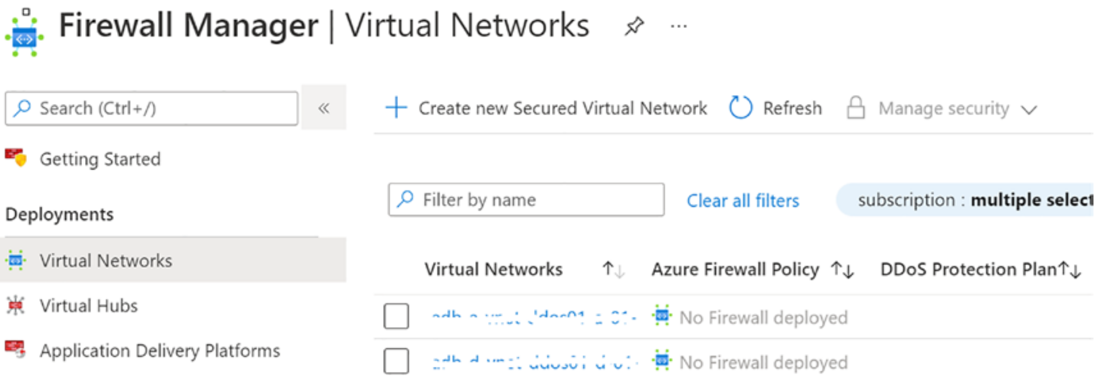

Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Microsoft Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

Figure 7-9. *Microsoft Sentinel*

Microsoft Sentinel performs the following activities to improve the overall security of the application. With Microsoft Sentinel, you can perform security orchestration, automation, and response for any security threats:

- Collect data at a scale
- Detect undetected threats if any
- Check threats with artificial intelligence
- Act on the incidents rapidly
- Azure DDOS protection, which mainly focuses on defending against distributed denial of service attacks; see Figure 7-10.



Firewall Manager | Virtual Networks

subscription : **multiple select**

□	Virtual Networks	Azure Firewall Policy	DDoS Protection Plan
□	[illegible]	No Firewall deployed	
□	[illegible]	No Firewall deployed	

Figure 7-10. *Azure DDOS Protection*

- Azure Rights Management: Protects files and emails across multiple devices.

- Azure Governance Visualizer: Collects insights and information into the policies, and includes role-based access control, Azure blueprints, and subscriptions

Most cloud architecture has compute, networking, data, and identity components and each of these components needs to be monitored closely in terms of security and related issues. Microsoft Defender for cloud has built-in features that monitor the security posture of all these services. You can follow these best practices to configure Microsoft Defender for various services:

- IaaS and PaaS Security: In the IaaS model, you can create various infra services and they will be hosted on Azure. Microsoft Azure provides assurance that the resources will be isolated and security patches and updates will be done in a timely manner. In order to control this in a better manner, you can host the complete IaaS solution on-premises or in a data center. For example, you can create your own virtual network, storage, and host entities. You have a shared responsibility when you consider the reference of PaaS components. See Figure 7-11.

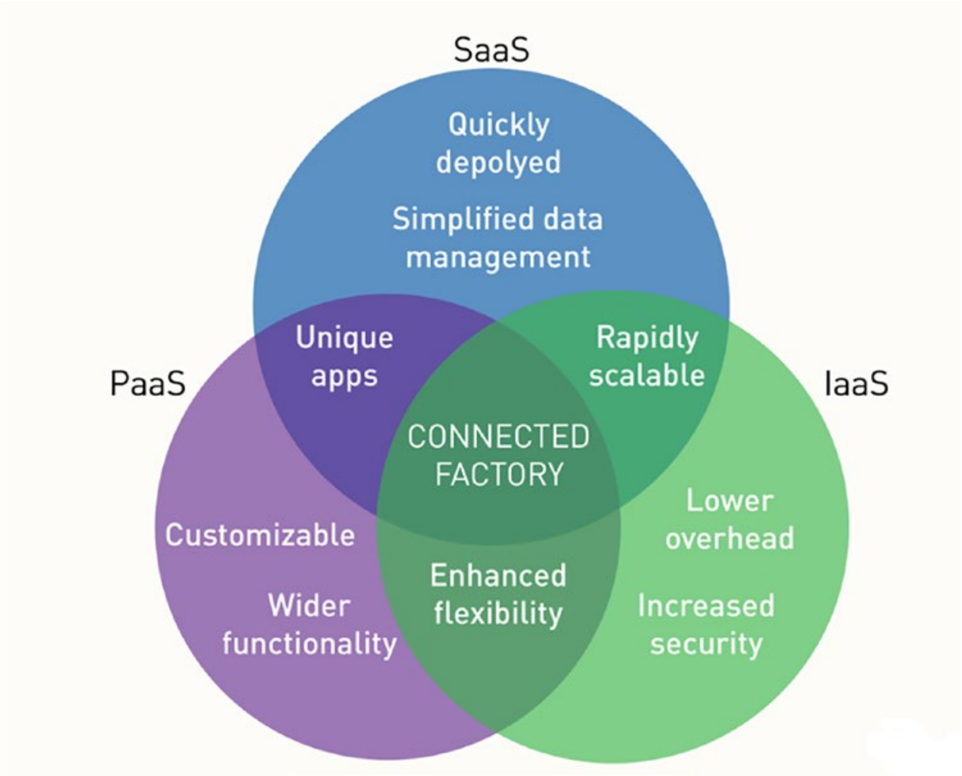


Figure 7-11. *Azure PaaS/SaaS responsibility*

- Virtual machines: For Windows and Linux VMs, use Microsoft Defender to take the advantage of free services for missing OS patching, security misconfigurations, and network security. For example, virtual machines don't have vulnerability scanning solutions to check for security threats. Microsoft Defender for servers watches network movement to and from these virtual machines.

Observability means how well you understand what is happening in the system by collecting logs, metrics, and traces. Observability in the cloud is very hard to achieve.

Azure Monitor

Azure Monitor maximizes the availability and overall performance of the application. See Figure 7-12.

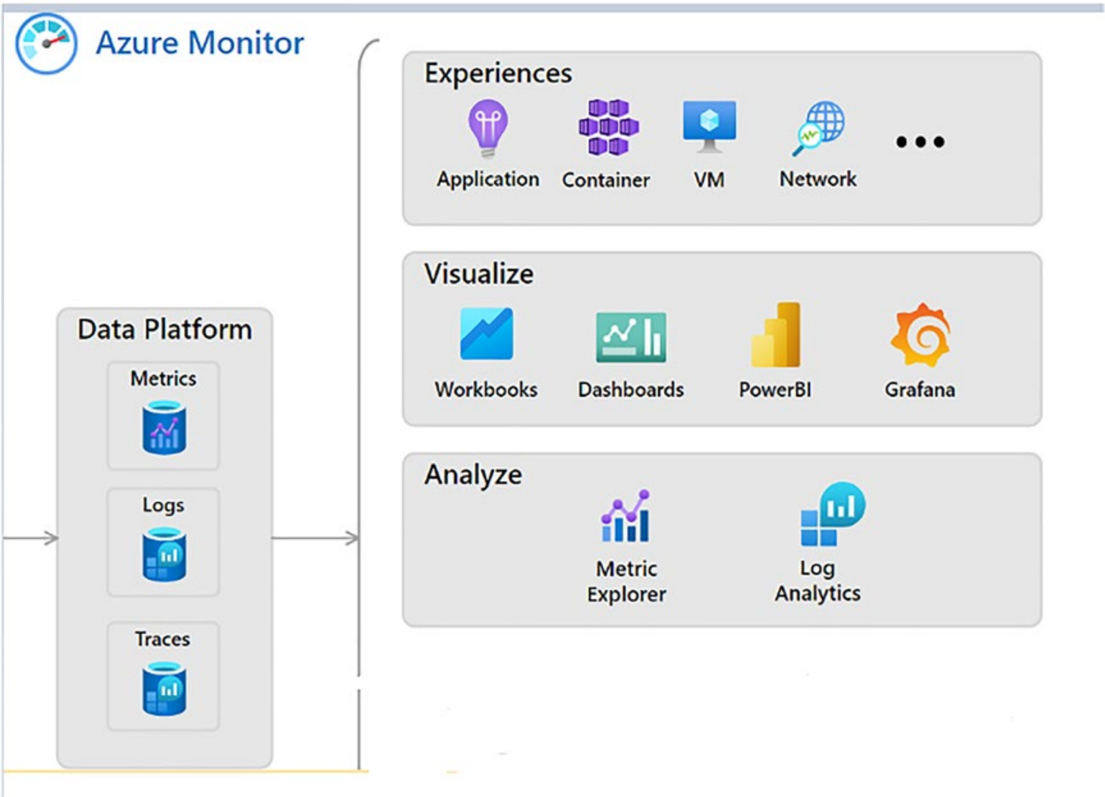


Figure 7-12. *Azure Monitor: Applications*

All data collected by Azure Monitor is stored in two formats (see Figure 7-13):

- Metrics
- Logs

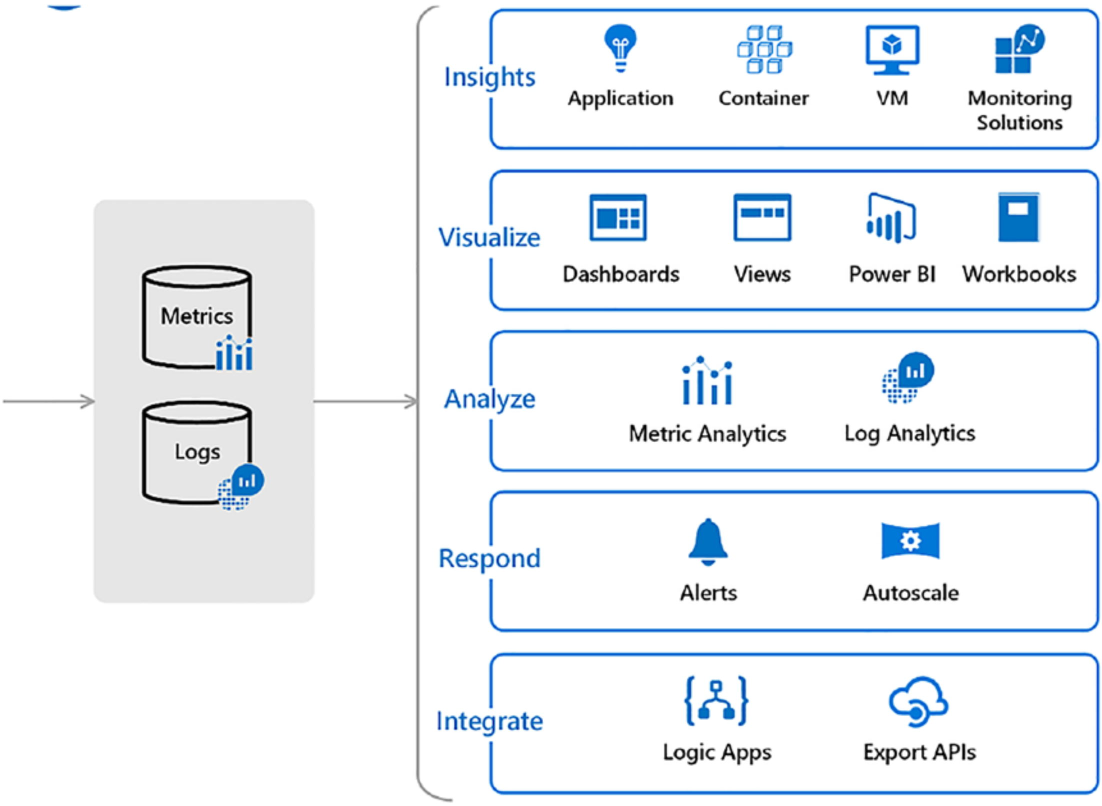


Figure 7-13. *Azure Monitor metrics and logs*

Metrics are numerical values that describe the system at a particular point in time. Metrics are lightweight and efficient and store near real-time logs. Logs contain different kinds of data that is stored in the form of records with sets. For many Azure resources, data is collected by Azure Monitor in the Overview page. For example, you can view the chart and dashboards interactively. See Figure 7-14.

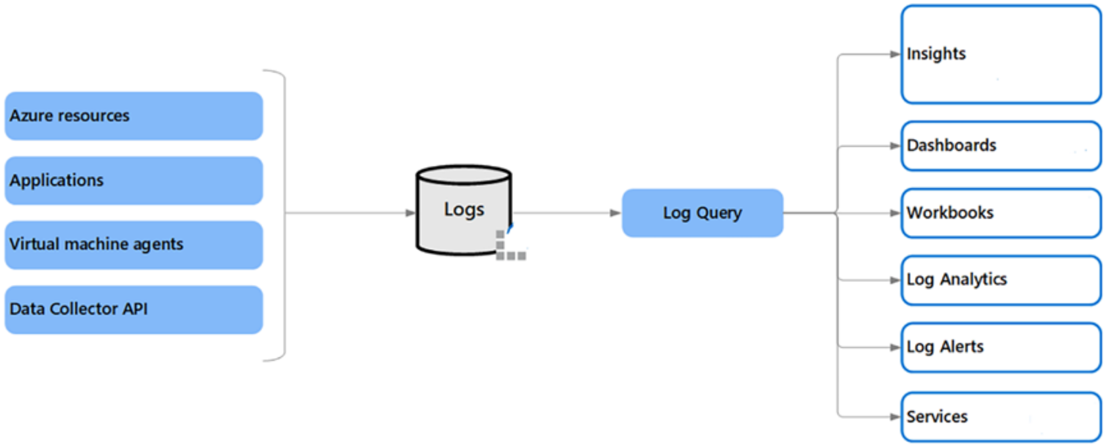


Figure 7-14. *Azure Monitor metrics explorer*

Logs collected by Azure Monitor will be analyzed with queries to get, consolidate, and collect data. You can create and test queries using log analytics. You can use the kusto query language, which is similar to the SQL language, to log queries.

Azure Monitor collects data from various sources. It mainly consists of the following information:

- Application monitoring data: Collects data about the performance and functionality of the source code written on various Azure services.
- Operating system logs: Collect all the logs of the guest operating system data running on Azure, on-premises, or on another public cloud.
- Azure service monitoring data: Contains all the monitoring data from various Azure services.
- Azure subscription monitoring data: Contains all data about the operation and management of the Azure subscription and related information. You can enable diagnostics to extend the data you collect by Azure Monitor. You can also enable logging with Application Insights to collect exceptions, requests, and page views. See Figure 7-15.

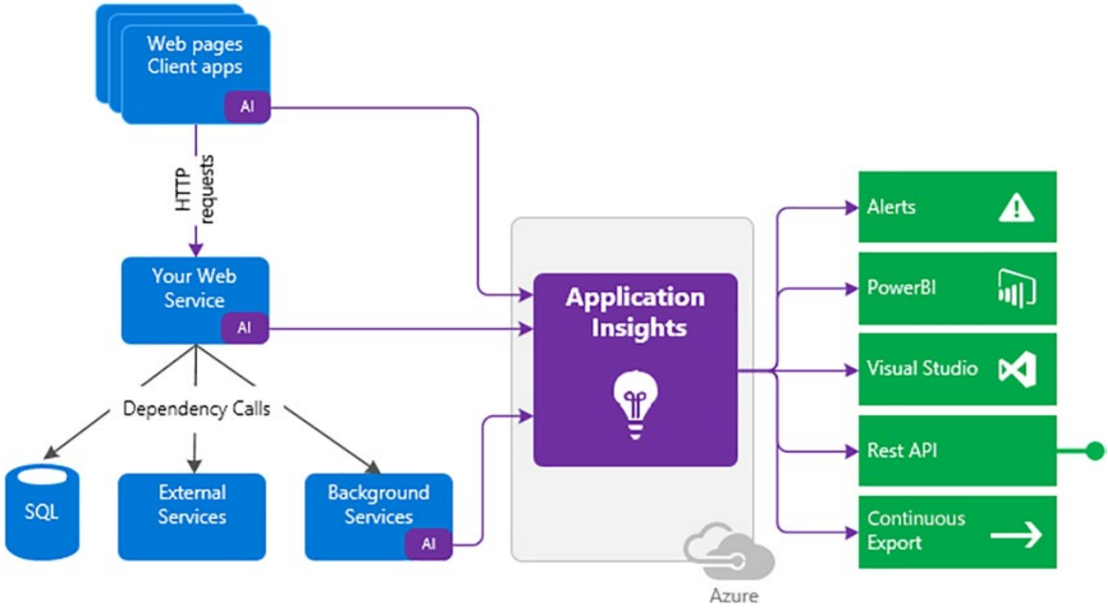


Figure 7-15. *Application Insights*

With Application Insights, you can monitor extensible application performance. Application Insights supports various platforms like .NET, Node.Js, Java, and Python. Application Insights can be used with on-premises or public cloud sources. You can also easily integrate application insights with DevOps processes.

Container Insights monitor the performance of the container workload that's deployed to the Kubernetes cluster. You can improve the performance of the cluster by collecting metrics from controllers, nodes, and containers. Once the container logs are connected, you can enable the monitoring of the Kubernetes clusters. See Figure 7-16.

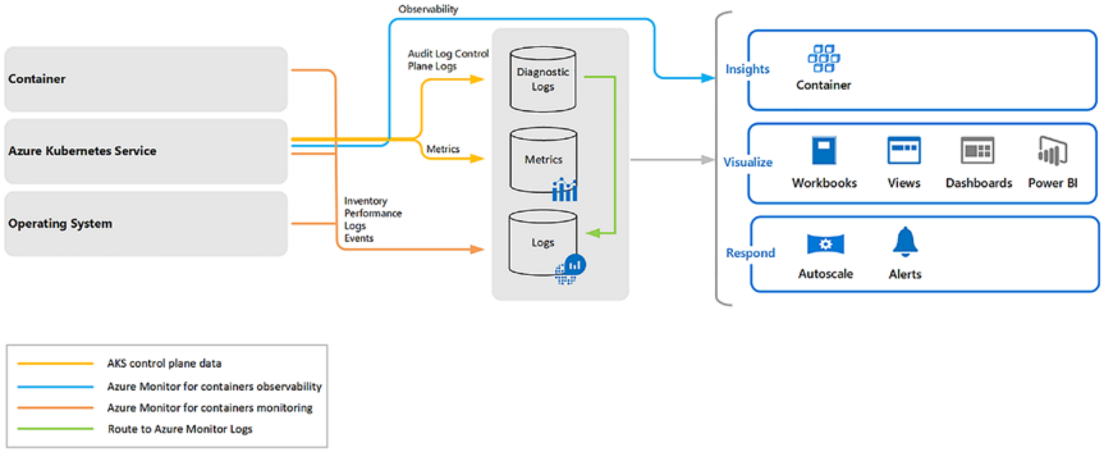
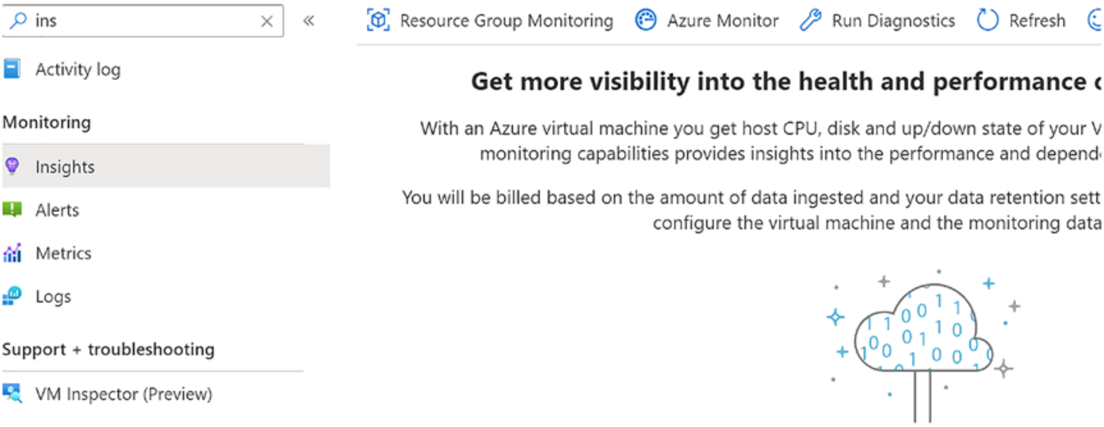


Figure 7-16. *Container Insights*

VM Insights helps organizations monitor the Azure VMs at scale. Overall health and performance are monitored for the Windows and Linux VMs to identify different processes and interdependencies. See Figure 7-17.



Get more visibility into the health and performance o

With an Azure virtual machine you get host CPU, disk and up/down state of your V
monitoring capabilities provides insights into the performance and depend

You will be billed based on the amount of data ingested and your data retention sett
configure the virtual machine and the monitoring data

Figure 7-17. *VM Insights*

Alerts in Azure Monitor help detect and address issues before they are identified by end users. See Figure 7-18.

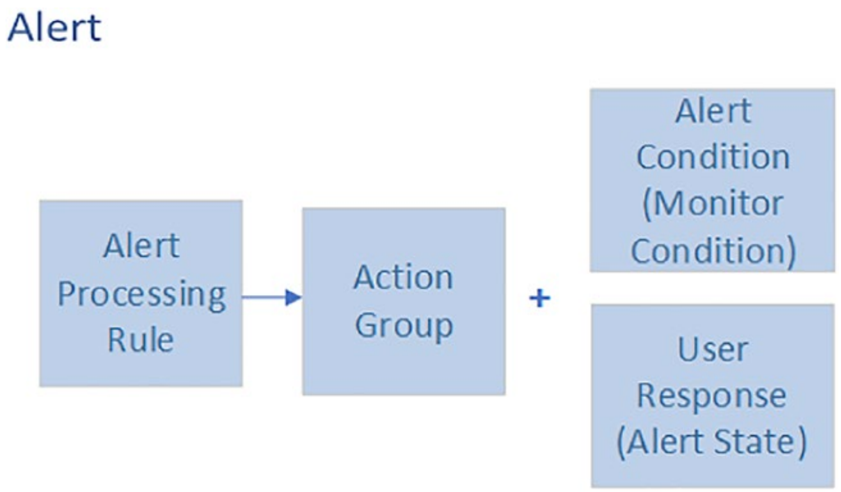
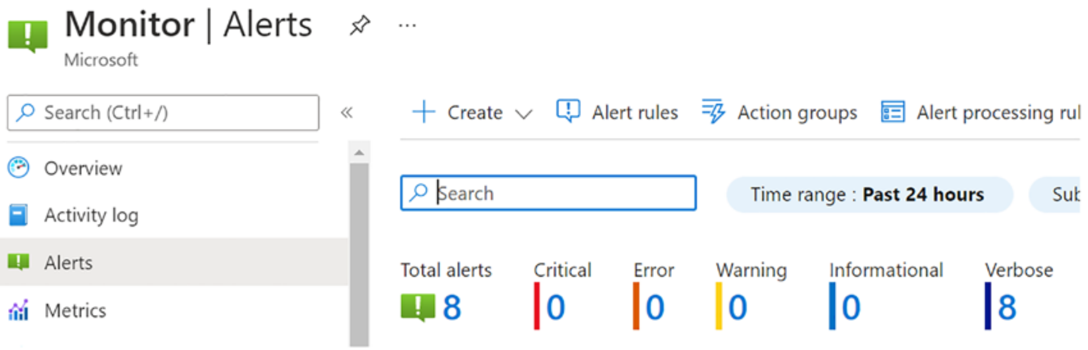

Alert
Alert Processing Rule
Action Group
+
Alert Condition (Monitor Condition)
User Response (Alert State)

Figure 7-18. *Alerts*

You can create alerts, either on metrics or on log data, based on the Azure Monitor Data platform. Alert rules monitor the operational logs. Alert rules capture the signal and check if the criteria is met. If the conditions are met, an alert will be triggered. See Figure 7-19.



Total alerts	Critical	Error	Warning	Informational	Verbose
8	0	0	0	0	8

Figure 7-19. *Azure Monitor Alerts*

You can create alert rules using the following combinations:

- Resources to be monitored
- Signal from the resource
- Conditions

Once an alert is triggered, the following sequence of events will unfold:

- The alert processing rule applies the fired alerts. With alert processing rules, you can add or suppress the action groups and apply filters or rules based on a predefined schedule.
- Actions groups trigger the notification based on the workflow to inform the users that alerts have been triggered.
- Notifications methods such as email, SMS, or push notifications
- Automation Runbooks
- Azure functions
- ITSM incidents
- Logic apps
- Webhooks
- Secure webhooks
- Event hubs
- An alert condition is set by the system. When the alert is fired, the alert monitor's condition is set to fired.

Azure Monitor also supports integration with various partners to collect data. With auto-scale, you can set the right amount of resources to handle the application workload. By enabling this feature, you can save on the cost by removing idle resources. While configuring auto-scaling, you can specify the minimum and maximum number of instances and logic to increase or decrease resources. See Figure 7-20.

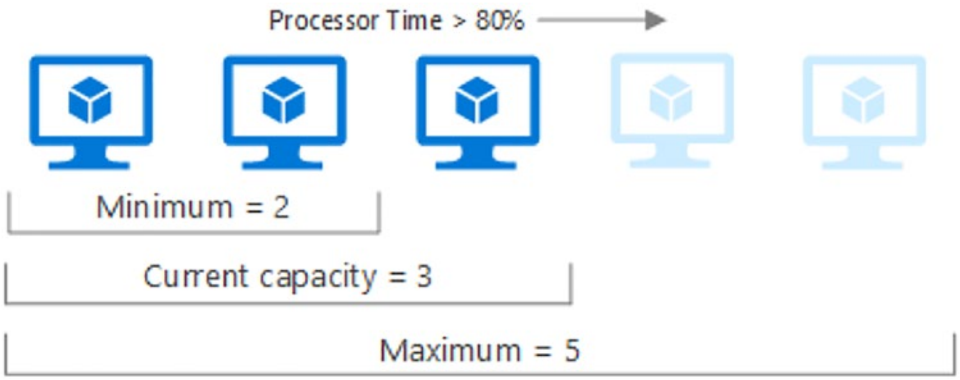
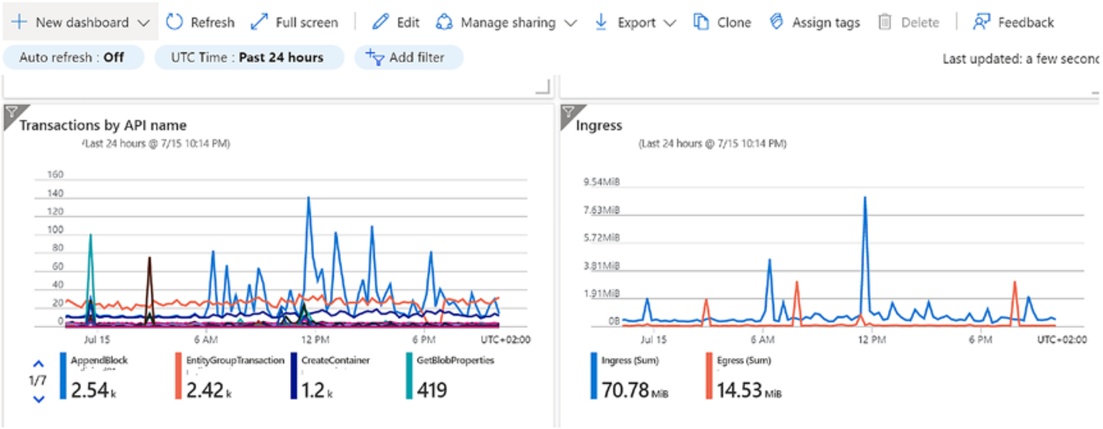


***Figure 7-20.** Auto-scaling*

Azure Dashboards allows you to combine different types of data into a single pane. Once the dashboard is ready, you can share it with the end users. For example, you can create a dashboard that combines tiles that shows metrics, activity logs, and the output of the log query. See Figure 7-21.



Auto refresh : **Off**

UTC Time : **Past 24 hours**

Last updated: a few seconc

***Figure 7-21.** Azure Dashboards*

Azure also has a feature called a *workbook,* which provides a flexible way to perform data analysis and create rich visuals using the Azure Portal. See Figure 7-22.

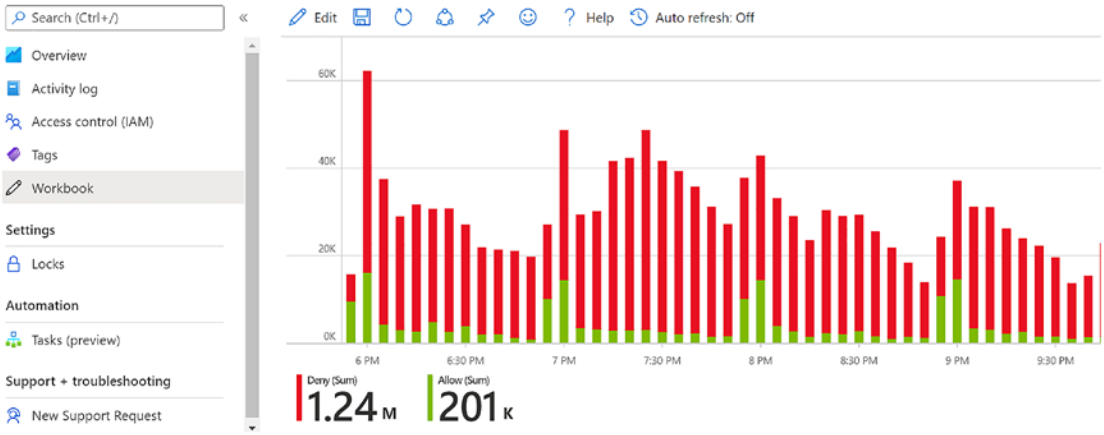


Figure 7-22. *An Azure workbook*

You can use an Azure workbook with Insights or create your own predefined templates.

Power BI is a business analytics service that provides interactive visualizations using various data sources. It is an effective way to make the data available within and outside your organization. You can also automatically import data from Azure Monitor. See Figure 7-23.

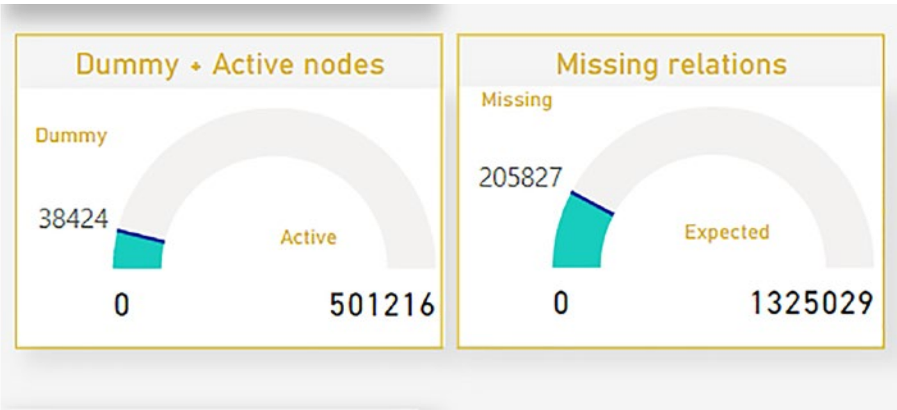
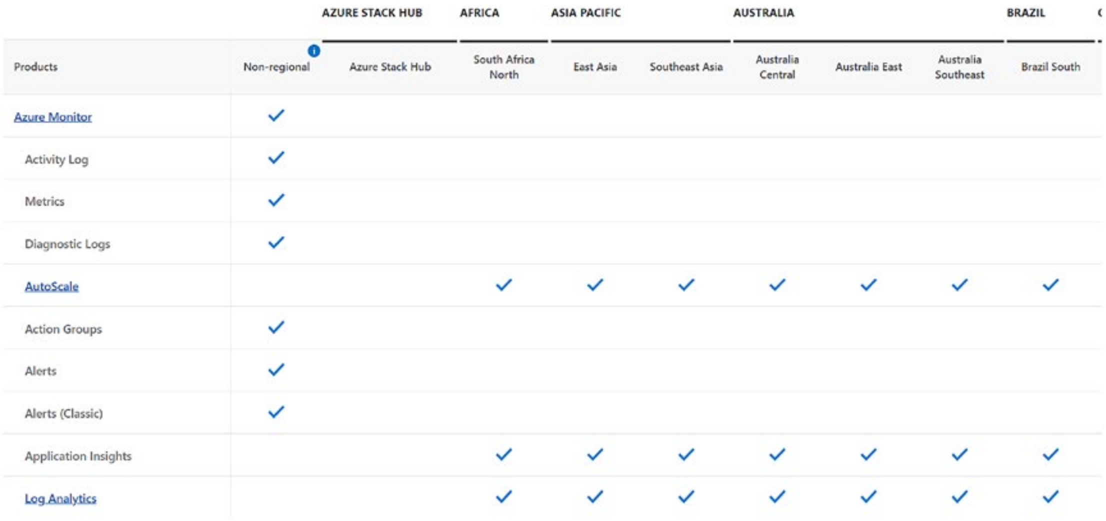


Figure 7-23. *Power BI reports*

Azure Sentinel

Azure Sentinel is a cloud-native, security information, and event management (SIEM) solution, as well as a security orchestration, automation, and response (SOAR) solution.

Microsoft Sentinel has many connectors available for Microsoft solutions, which are out-of the box solutions and provide real-time integration with external tools including Microsoft 365 Defender, Azure AD, and Microsoft Defender for cloud apps. In addition, you can use the REST API to connect various data sources from Azure Sentinel. Microsoft Sentinel can run its workspaces in almost every region where log analytics is generally available. There might be regions where log analytics become generally available and it can take some time for Sentinel to become generally available. See Figure 7-24.



		AZURE STACK HUB	AFRICA	ASIA PACIFIC		AUSTRALIA			BRAZIL
Products	Non-regional	Azure Stack Hub	South Africa North	East Asia	Southeast Asia	Australia Central	Australia East	Australia Southeast	Brazil South
Azure Monitor	✓								
Activity Log	✓								
Metrics	✓								
Diagnostic Logs	✓								
AutoScale			✓	✓	✓	✓	✓	✓	✓
Action Groups	✓								
Alerts	✓								
Alerts (Classic)	✓								
Application Insights			✓	✓	✓	✓	✓	✓	✓
Log Analytics			✓	✓	✓	✓	✓	✓	✓

Figure 7-24. *Azure Sentinel regional availability*

Before you set up Microsoft Sentinel, you need to have the following prerequisites and resources in place:

- Log analytics workspace
- Azure subscription
- Contributor permission for the subscription where you want to deploy Microsoft Sentinel
- Contributor or reader permission to the resource group
- Additional permission to connect to the data sources

If you want to enable Microsoft Sentinel, you need to go to the Azure Portal and select the subscription where Sentinel will be created. See Figure 7-25.

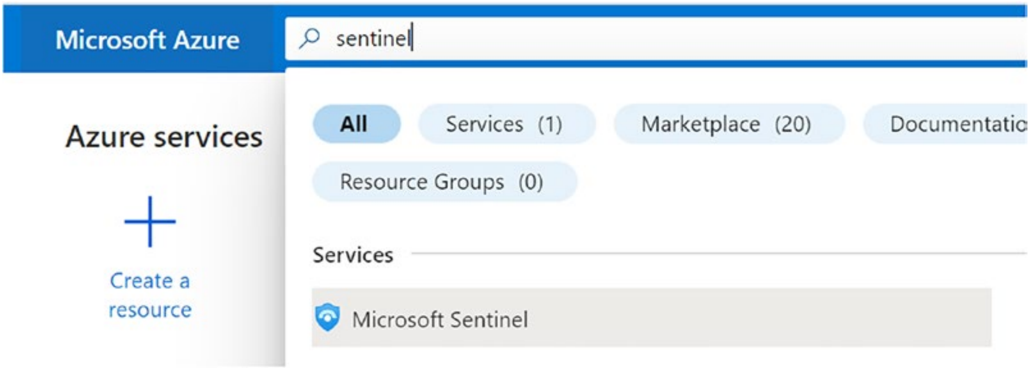


Figure 7-25. *Enable Azure Sentinel*

Click the Add button and then select the existing workspace that you want to use or create a new workspace. It is also possible to run Microsoft Sentinel from more than one workspaces, but data is always isolated to a single workspace. See Figure 7-26.

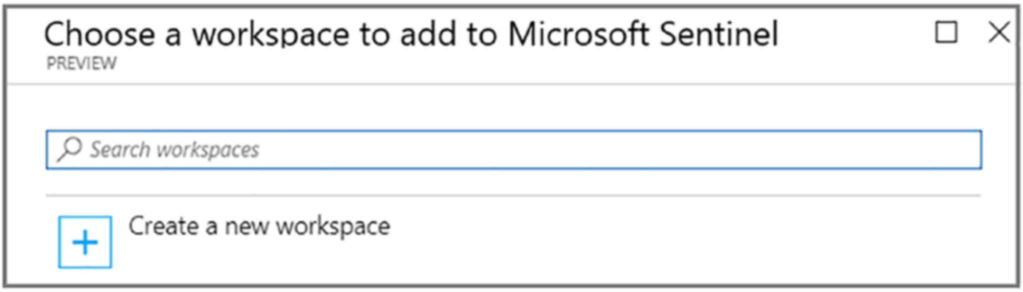


Figure 7-26. *Enable Azure Sentinel*

Select Add Microsoft Sentinel. Microsoft Sentinel ingests data from various services by connecting services and sending the events and logs to itself. For physical and virtual machines, you can install a log analytics agent, which will collect the logs and forward them to Microsoft Sentinel.

You can also integrate Microsoft Sentinel with various security services. It is empowered by the components that will send the data to the workspace and becomes stronger through interactions. Logs can be ingested directly into Microsoft Sentinel to provide a full picture of events and incidents. For example, Microsoft Sentinel ingests data from other Microsoft services and partner platforms. See Figure 7-27.

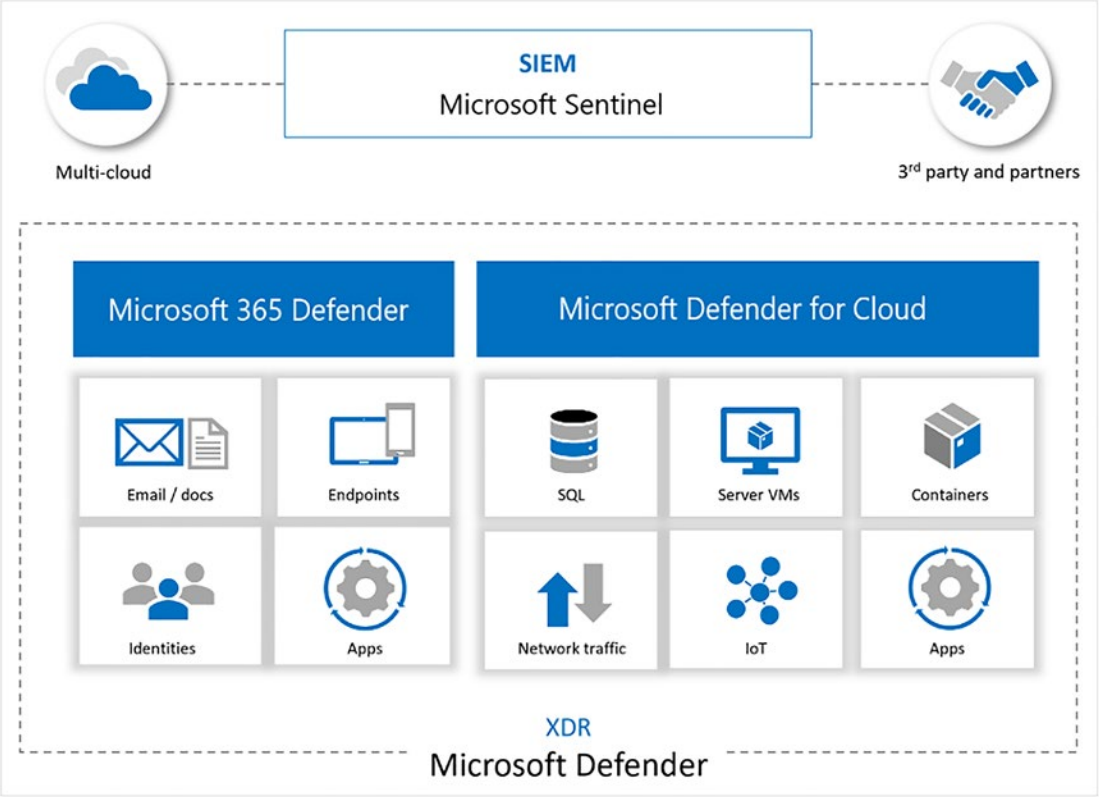


Figure 7-27. *Azure Sentinel with Microsoft Defender*

Apart from sending data, Microsoft Sentinel has various other features:

- Uses information with machine learning
- Creates visualizations with workbooks
- Runs playbooks with alerts
- Integrates with partner platforms
- Integrates and fetches enrichment feeds from threat intelligence platforms

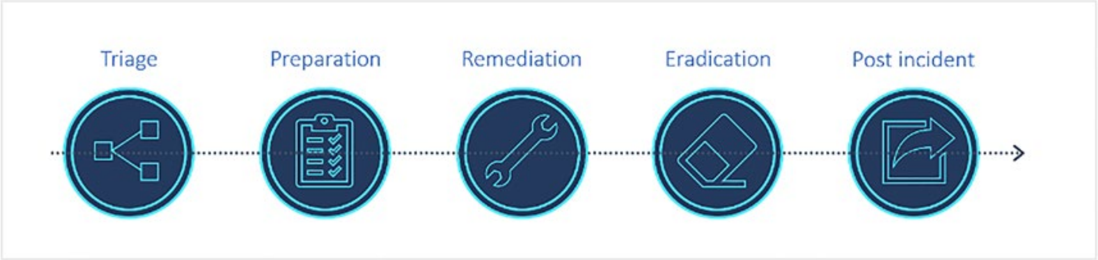


***Figure 7-28.** Incident management and response process*

You can also use Microsoft Sentinel to manage incidents and respond to responses in case of failures. See Figures 7-28 and 7-29.

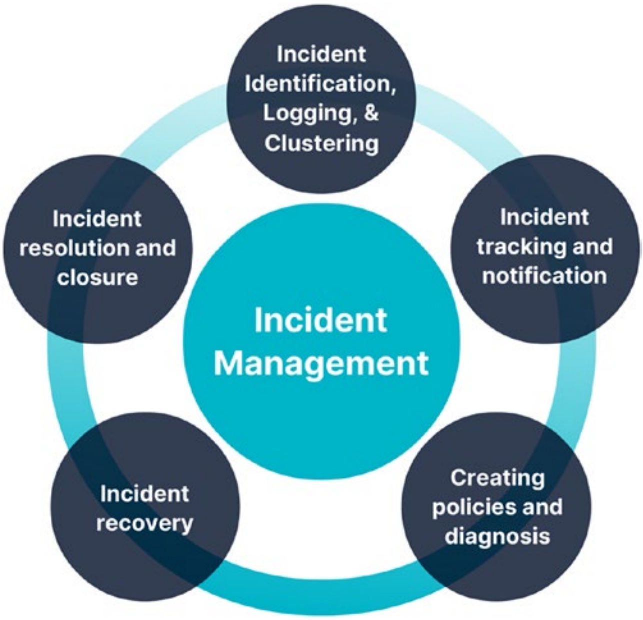

Incident Identification, Logging, & Clustering
Incident tracking and notification
Creating policies and diagnosis
Incident recovery
Incident resolution and closure
Incident Management

***Figure 7-29.** Incident management and response process*

Content in Microsoft Sentinel includes the following:

- Data connectors: Microsoft Sentinel has many out-of-the-box connectors to start ingesting data to Microsoft Sentinel. For example, Microsoft 365 Defender connector is a service to the service connector that integrates data from Office 365, Azure AD, and so on. See Figure 7-30.

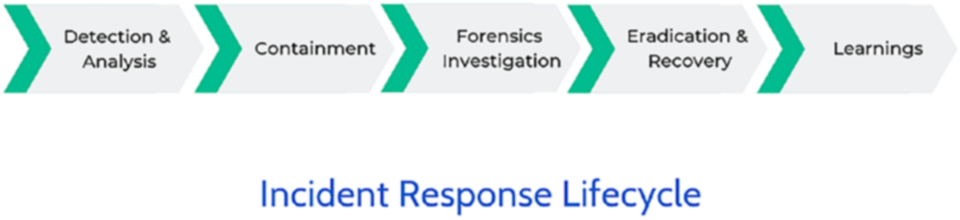


***Figure 7-30.** Azure Sentinel connectors*

- Parsers: These parsers provide log formatting in the Advanced Security Information Model (ASIM) formats to support their use across Microsoft Sentinel.

- Workbooks: These provide monitoring, visualization, and interactivity with data using Microsoft Sentinel. See Figure 7-31.

4.5M +27K
EVENTS
89 +2
ALERTS
29
NEW
3
INVESTIGATED
9
CLOSED

***Figure 7-31.** Workbooks visualization*

- Hunting queries: These queries are used by the Security Operations Team (SOC) team to hunt for threats in Microsoft Sentinel. See Figure 7-32.

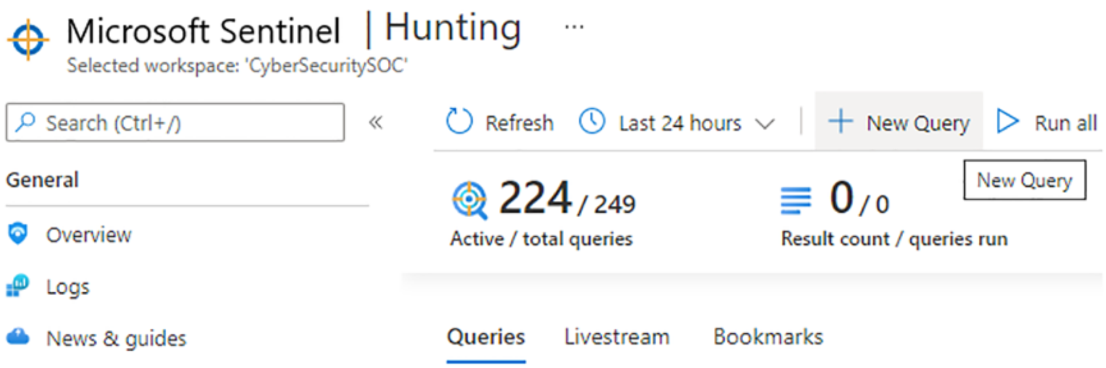


Figure 7-32. *Microsoft Sentinel hunting queries*

Hunting dashboards provide built-in, ready-made queries to get started and familiar with tables and query language. Queries run on the data stored in the log tables. These built-in queries are developed by the Microsoft security researchers. See Figure 7-33.

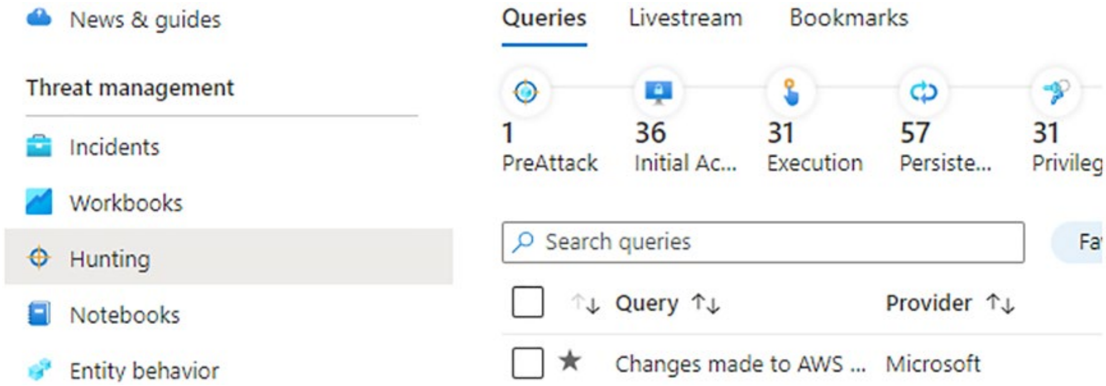
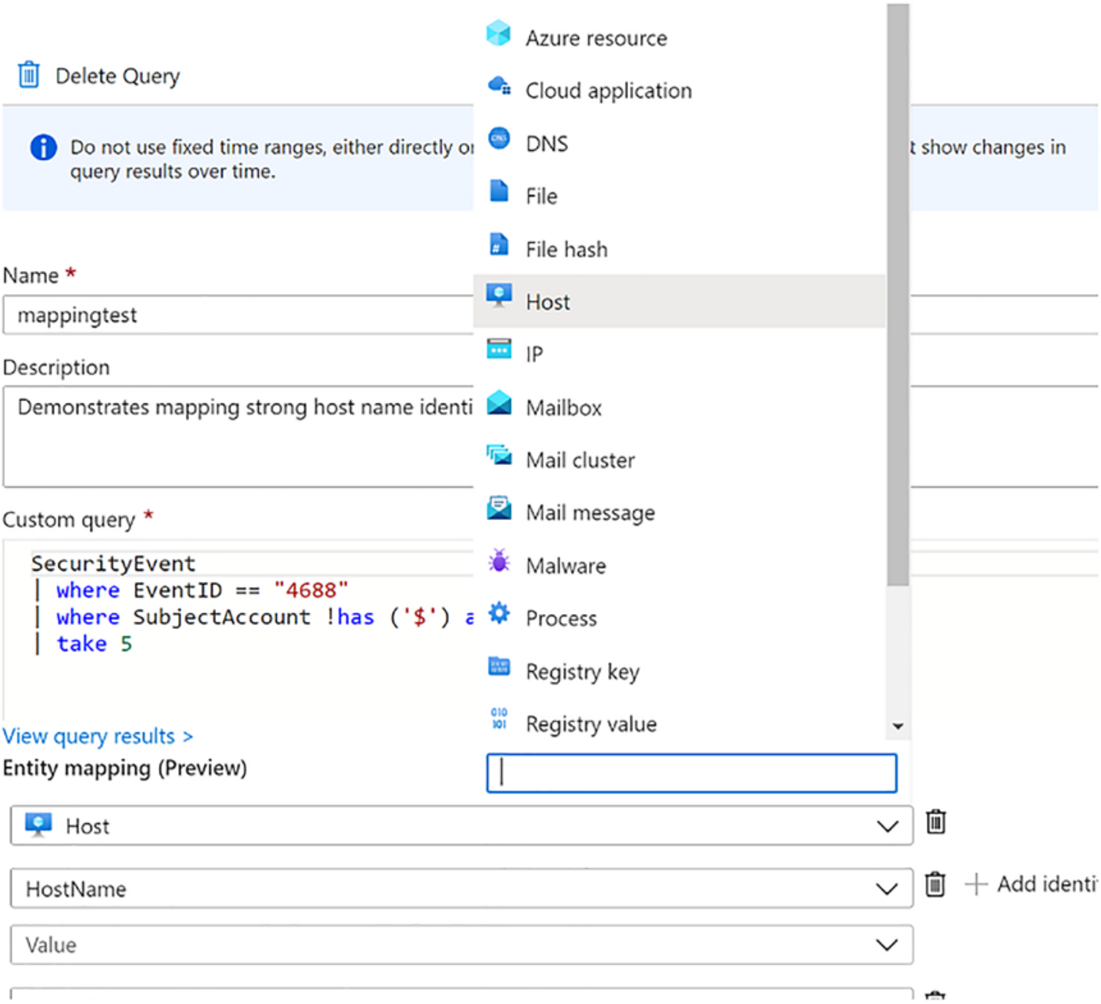


Figure 7-33. *Microsoft Sentinel hunting custom queries*

You can also create custom queries or modify existing queries and then share them with users who belong to the same tenant.

To create a new query, select New Query and then select Create. Click the Create Entity Mapping and then select the entity type, identifiers, and columns.

Typical hunting queries start with the table or parser name followed by the operators, separated by the pipe character. See Figure 7-34.



Delete Query

Do not use fixed time ranges, either directly o[...] query results over time. [...]t show changes in

Name *

mappingtest

Description

Demonstrates mapping strong host name identi

Custom query *

```
SecurityEvent
| where EventID == "4688"
| where SubjectAccount !has ('$') a
| take 5
```

View query results >

Entity mapping (Preview)

Host

HostName

Value

Figure 7-34. *Microsoft Sentinel hunting create new queries*

– Playbooks and Azure Logic App custom connector: This provides features for the automated investigations, remediations, and response scenarios in Microsoft Sentinel. Playbooks in Microsoft Sentinel are based on workflows, like Azure logic apps, which can be used to schedule, automate, and orchestrate workflow across the enterprise.

Azure Logic app communicates with other systems and services using these connectors:

- Custom connectors
- Managed connectors
- Microsoft Sentinel connectors
- Triggers
- Actions
- Dynamic fields

Conclusion

This chapter explained how to secure data stored in the cloud and how to provide secure access to that data. You also learned about the various ways to classify data and make it available for downstream users and applications in a secure manner. Finally, you also learned about the various data encryption patterns and related models used while working with public cloud providers, such as Azure, Google, AWS, and so on.