Working with Azure Security and Reporting Tools

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

Introduce Azure information protection

Discuss Azure monitor and service health

Introduce Azure key vault

Introduce Azure Sentinel

Introduce and demonstrate Azure security center

By the end of this module

- You will understand the core monitoring tools available in Azure
- Understand the benefits of these tools to your organization

Azure Information Protection and Security Monitoring Tools

What Is Azure Information Protection?

AIP is used to classify documents and emails

AIP applies labels to documents

Labeled documents can be protected

AIP labels

- Can be applied automatically
- Can be applied manually
- Can be recommended to users

Two Sides to AIP

Classification

Metadata is added to documents. Clear text and visual markings like headers, footers and watermarks

Protection

Azure rights management encrypts documents using rights management templates

Classifying and Protecting Existing Documents

Ideally documents and emails should be labeled and protected when they are created

You will probably have lots of existing documents in Azure and on-premises

For on-premise data stores you can use Azure information protection scanner

For cloud data stores we can use Microsoft cloud app security

Three Security and Reporting Resources

Azure monitor

Collect and analyze metric information for Azure and on-premises resources

Azure service health

Notifies you about Azure services and planned maintenance

Azure advanced threat protection

Detect and investigate attacks in Azure and on-premises

What Is Azure Monitor?

Collect, analyze and act on telemetry

Azure or on-premises

Troubleshooting and performance monitoring

Data collected by Azure monitor

- Metrics
- Logs

What Is Azure Service Health?

Notifies you about service status

Reports incidents and planned maintenance

Azure service health offers

- Personalized dashboards
- Configurable alerts
- Guidance and support

What Is Azure Advanced Threat Protection?

Monitor and analyze user activity

Identifies suspicious activity and events

Works with your on-premises Active Directory forest

Identifies

- Reconnaissance attacks
- Compromised credentials
- Lateral movements
- Domain dominance

Azure Key Vault

The Problem with Secrets

Secrets management

How do you control access tokens, passwords, API keys and other secrets?

Key management

How do you create and control encryption keys?

Certificate management

How do you provision, manage and deploy certificates?

What Is Azure Key Vault?

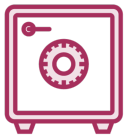
Centralize the storage or application secrets

Uses FIPS 140-2 level 2 validated HSMs

Enable logging to monitor how and when secrets are being used

Enables centralized administration of secrets

Azure Key Vault Recommendations



Use separate key vault for each application or environment

Take regular backups of your key vault

Turn on logging and set up alerts

Turn on soft delete and purge protection

Demo

Deploy Azure Key Vault

Show Azure Kay Vault security features

Show how ARM templates use secrets

Azure Security Centre and Azure Sentinel

Cloud Security Challenges

Rapid change

How do you make sure that changes to services meet your security requirements?

Complex attacks

Attacks are becoming more sophisticated. How do you keep up with new threats?

Skills shortage

Lots of information available but who monitors it?

Azure Security Center

Protect PaaS

No deployment needed, just works

Non-Azure services

Deploy monitoring agent

Compliance

Reports our compliance posture

Assessment

Continuous assessment of existing and new sources

Threat protection

Detect and prevent threats to IaaS and PaaS

Azure Sentinel

Cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution

A single solution for

- Collect date at cloud scale
- Detect previously undetected threats
- Investigate threats with artificial intelligence
- Respond to incidents rapidly

Azure Sentinel

Connect to your security sources with data connectors

Analyze your data using workbooks and analytics

Security automation and orchestration using playbooks

Deep investigation and hunting

Demo

Configure Azure security centre

View events collected by Azure security centre

Summary

Learned about Azure monitoring tools

Learned about Azure key vault

Learned about Azure information protection

In our next module

- Azure compliance and data protection standards