Cloud-Based Security Monitoring System Using Microsoft Sentinel

Challa Hema Sundar Yadav

GitHub: https://github.com/monkeydsundar/sundar

# Introduction

Cloud environments face constant threats such as brute-force attacks and unauthorized access. This project leverages Microsoft Sentinel to build a scalable and proactive cloud-native security monitoring system. The solution detects and responds to threats in real-time using advanced analytics and automation.

# System Architecture

The system architecture consists of several integrated Azure components working together to provide comprehensive threat monitoring and response.

Key Components:

* • Microsoft Sentinel: Central SIEM platform
* • Data Connectors: Connect to Azure AD, Office 365, and Virtual Machines
* • Log Analytics Workspace: Central log storage and analytics
* • Logic Apps (Playbooks): Automate incident response
* • Workbooks: Custom dashboards for real-time threat visualization

[Architecture Diagram Placeholder – see image in the final version]

# Setup and Configuration

1. Deploy Microsoft Sentinel in Azure Portal

2. Configure data connectors for Azure AD, Office 365, and Virtual Machines

3. Create analytics rules to detect brute-force attempts

4. Configure playbooks for automated response

5. Set up workbooks for dashboards

# Detection Rules

Example: Brute-force attempts on Azure AD

SigninLogs  
| where ResultType != 0  
| summarize FailedAttempts = count() by UserPrincipalName, IPAddress, bin(TimeGenerated, 5m)  
| where FailedAttempts > 5

# Incident Response Playbooks

• Lock out user accounts upon brute-force detection

• Apply firewall rules to block malicious IP addresses

• Send real-time alerts to the SOC team

## Playbook Import Instructions

1. Open Logic App in Azure

2. Switch to code view, paste JSON, save

3. Create automation rule and connect playbook

# Visualization and Dashboards

Interactive dashboards show:

* • Overview of brute-force attempts
* • Geographic distribution of attacks
* • Incident response timelines

# Future Enhancements

• Integration with external threat intelligence

• Machine Learning for anomaly detection

• Multi-cloud support (AWS, GCP)

# Conclusion

This project demonstrates a real-world cloud-native SIEM implementation using Microsoft Sentinel. With detection, automation, and visualization, it forms a strong foundation for securing modern cloud infrastructures.  
  
GitHub: https://github.com/monkeydsundar/sundar