PROJECT PHASE 1
SYNOPSIS

❖ PROJECT TITLE:

AZURE CLOUD DETECTION LAB USING SENTINEL

PROBLEM DEFINITION:

The goal of the project is to create a cloud environment that is secure and can be used to detect and respond to cyber threats. The project will use Microsoft Sentinel, a cloud-native SIEM and SOAR solution, to collect, store, and analyze data from various sources in the Azure cloud environment. The project will also use KQL, a powerful query language, to query and analyze logs and time-series data.

PROBLEM OBJECTIVE:

Configure and deploy a secure Azure environment that can be used to detect and respond to cyber threats. This problem objective is specific, measurable, achievable, relevant, and time-bound. It is specific because it identifies the specific tasks that need to be completed, such as configuring Azure resources, using data connectors, and understanding Windows security event logs. It is measurable because it can be quantified, such as by the number of Azure resources that are configured or the number of security events that are detected. It is achievable because it is realistic and within the scope of the project. It is relevant because it is directly related to the goal of the project, which is to create a secure Azure environment. And it is time-bound because it has a specific deadline, such as the end of the project.

PROPOSED PLAN OF WORK:

1) Configure and Deploy Azure Resources such as Log Analytics Workspace, Virtual Machines, and Azure Sentinel.
2) Implement Network and Virtual Machine Security Best Practices.
3) Utilize Data Connectors to bring data into Sentinel for Analysis.
4) Understand Windows Security Event logs.
5) Configure Windows Security Policies.
6) Utilize KQL to query Logs
7) Write Custom Analytic Rules to detect Microsoft Security Events.
8) Utilize MITRE ATT&CK to map adversary tactics, techniques, detection, and mitigation procedures.

METHODOLOGY:

Part 1: Setup Lab Resources

Step 1: Create Free Azure Account.

Step 2: Create a Resource Group.

Step 3: Deploy a Virtual Machine.

Step 4: Create Log Analytics Workspace and Deploy Sentinel.

Part 2: Getting Data into Sentinel.

Part 3: Generating Security Events.

Part 4: Kusto Query Language

Part 5: Writing Analytic Rule and Generating Scheduled Task.

Part 6: MITRE ATT&CK

Detection: As observed. monitoring and logging of specific windows event id was used to detect this activity. However, MITRE also has more recommendations for detection. **Mitigation:** MITRE ID M1019 – User Account Management suggests that user account privileges should be limited to only authorize admins to create scheduled tasks on remote systems.

TECHNOLOGY:

Microsoft Sentinel: Microsoft Sentinel, also known as Azure Sentinel, is a cloud-native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution offered by Microsoft.

Azure Log Analytics Workspace: An Azure Log Analytics workspace is a central repository for collecting, storing, and analyzing log and telemetry data from various sources in the Microsoft Azure cloud environment.

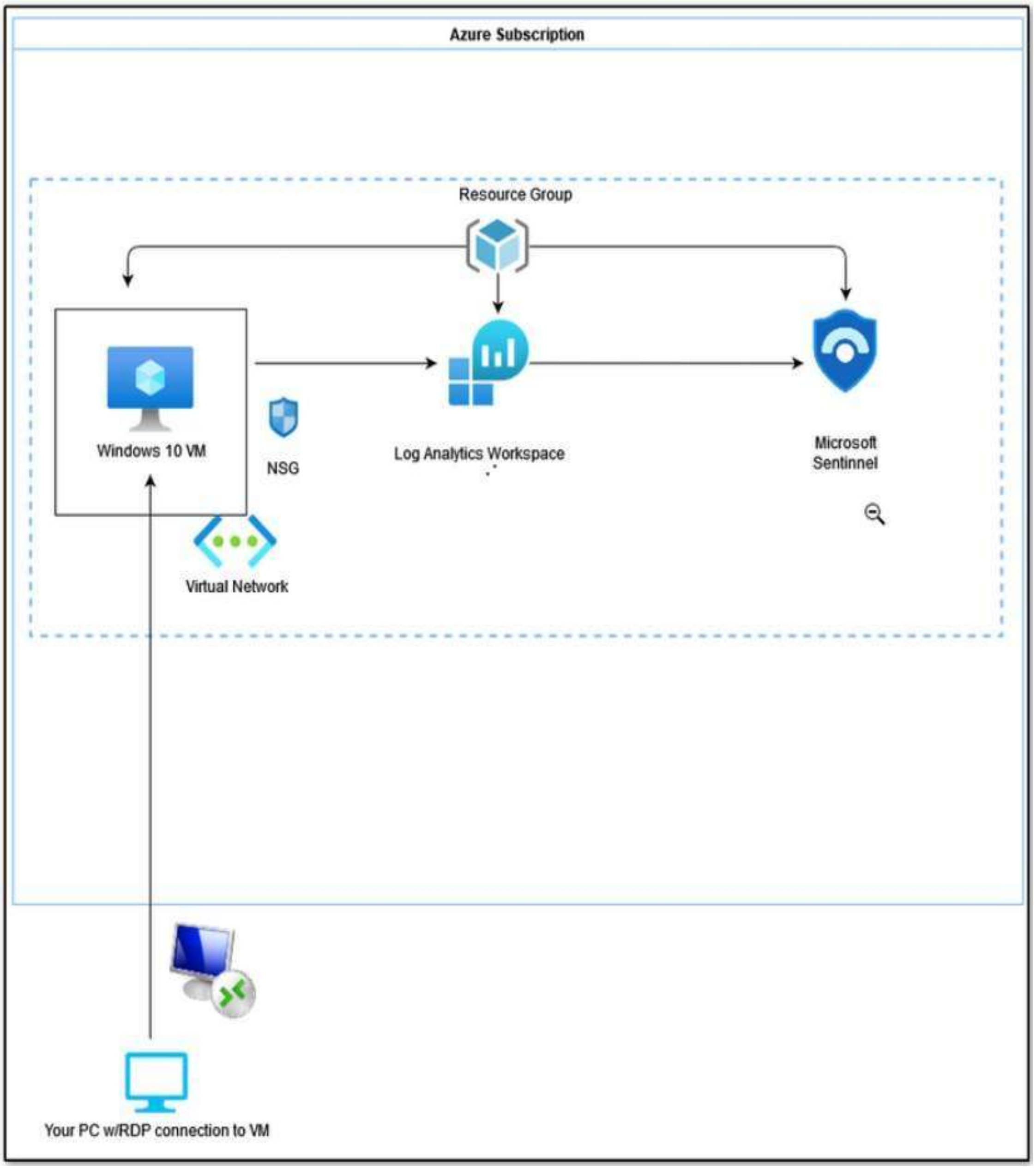
Features are:

1. Data Collection
2. Data Retention
3. Third-party Integration
4. Visualization and Dashboards
5. Integration with Azure Monitor and Solutions
6. Query and Analytics
7. Monitoring and Alerting.

KQL: Kusto Query Language (KQL) is a powerful query language used in Azure Monitor, Azure Log Analytics, and Azure Data Explorer to query and analyze logs and time-series data. It allows you to extract meaningful insights and perform data analysis on various types of data stored in these services.

MITRE ATT&CK: MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base and framework that provides valuable insights into the tactics, techniques, and procedures (TTPs) used by cyber adversaries during different stages of the cyberattack lifecycle

Topology:



FUNCTIONAL SPECIFICATION:

Building a Cloud Security lab for detection and monitoring.

PROJECT SCOPE:

1. The Azure Cloud Detection Lab Project is a hands-on learning experience focused on security operations and threat detection in Microsoft Azure. The lab guides participants through the setup and configuration of Azure resources, including Log Analytics Workspace, Virtual Machines, and Azure Sentinel (formerly known as Azure Sentinel), which is a cloud-based SIEM/SOAR solution.

2. The lab covers various aspects of security monitoring and analysis, utilizing data connectors to collect and analyze data from Windows Security Event logs. Participants learn to configure Windows Security Policies, utilize Kusto Query Language (KQL) to query logs, and write custom analytic rules to detect Microsoft Security Events.

3. One of the critical components of the lab is integrating MITRE ATT&CK, a knowledge base and framework that outlines adversary tactics, techniques, and procedures used in cyberattacks. Participants learn to map adversary tactics and techniques to detection and mitigation procedures, helping them gain insights into potential threats and improve security measures.

4. The lab concludes by demonstrating how to create a custom analytic rule for detecting suspicious scheduled task creation, simulating a potential persistence technique. By monitoring and analyzing security events, the participants gain valuable skills in threat detection and incident response.

5. Overall, the Azure Cloud Detection Lab Project provides participants with a practical understanding of SIEM, threat detection, and security best practices in the Azure cloud environment, helping them develop valuable skills sought after by security positions, particularly on the blue team side

Roll No	Name of Students	Name of Guide
12	Manana Sharma	
70	Gaurav Singh	
71	Prasanna Tangade	

- **Approved by:** Dr.C.Dadiyala