Comprehensive Implementation Guide: PRJ-AZURE-SEC-059 - Azure Security Solution with Defender and Sentinel

This guide provides a comprehensive, production-ready blueprint for deploying a unified, AI-powered security operations center (SOC) in Azure. The solution leverages **Microsoft Defender for Cloud** for Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP), and **Azure Sentinel** (now **Microsoft Sentinel**) for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).

---

1. Project Overview

The **PRJ-AZURE-SEC-059** project establishes a robust, centralized security monitoring and automated response platform within the Azure cloud environment. The core objective is to provide unified security management, advanced threat detection, and automated incident response across Azure, hybrid, and multi-cloud assets.

The solution is built upon the following core components:

- **Microsoft Defender for Cloud (MDC):** Provides continuous security posture management (CSPM) to identify misconfigurations and vulnerabilities, and workload protection (CWPP) for servers, databases, storage, and other services. It acts as the primary source of high-fidelity security alerts and recommendations.
- **Microsoft Sentinel (Azure Sentinel):** The cloud-native SIEM and SOAR solution. It ingests security data from MDC and other sources, uses machine learning and threat intelligence to detect sophisticated threats, and provides a centralized platform for investigation and incident management.
- **Azure Key Vault:** Used for secure storage of secrets, keys, and certificates. It is a critical resource protected by **Microsoft Defender for Key Vault**, demonstrating the solution's comprehensive workload protection capabilities.

- **Azure Policy and Governance:** Used to enforce security configurations, such as enabling Just-in-Time (JIT) VM access and Adaptive Network Hardening, ensuring a consistent security baseline.

This architecture moves security operations from a reactive, manual process to a proactive, automated, and intelligence-driven one, significantly improving an organization's security maturity.

2. Business Context

Modern cloud environments face an escalating volume and sophistication of cyber threats. The traditional perimeter-based security model is insufficient. This project directly addresses these challenges by delivering quantifiable business value through risk mitigation, cost savings, and efficiency gains.

The Problem

- **Fragmented Security Visibility:** Security teams often struggle with siloed tools and lack a unified view of security across diverse Azure services, on-premises infrastructure, and other cloud providers.
- **Alert Fatigue and Slow Response:** Manual security operations are overwhelmed by a high volume of low-fidelity alerts, leading to alert fatigue and slow incident response times that fail to keep pace with the speed of cloud-scale attacks.
- **Compliance Complexity:** Maintaining continuous compliance with multiple regulatory frameworks (GDPR, HIPAA, PCI DSS) is complex and resource-intensive without automated monitoring and reporting.

The Solution

The deployment of a unified security solution using Microsoft Defender for Cloud and Microsoft Sentinel provides a single pane of glass for security management, threat detection, and automated response.

Capability	Microsoft Defender for Cloud (MDC)	Microsoft Sentinel (SIEM/SOAR)
CSPM	Continuous assessment of security posture, secure score, and regulatory compliance.	Ingests MDC recommendations for compliance reporting.
CWPP	Advanced threat protection for specific workloads (VMs, SQL, Storage, Key Vault).	Ingests high-fidelity MDC alerts for centralized investigation.
SIEM	N/A	Centralized data ingestion, correlation, and threat detection using AI/ML.
SOAR	Automated response actions (e.g., JIT access)	Automated incident response playbooks (Logic Apps) for enrichment and remediation.

Business Value and ROI

The investment in this solution yields significant return on investment (ROI) through:

Metric	Quantified Value	Mechanism
Incident Response Time	**80% Reduction**	Automated SOAR playbooks (e.g., auto-isolation, ticket creation) eliminate manual steps, reducing the mean time to respond (MTTR) from hours to minutes.
Security Posture Improvement	**30-50% Increase in Secure Score**	Continuous CSPM from MDC provides prioritized, actionable recommendations, driving proactive remediation of misconfigurations.
Cost Savings (Analyst Time)	**$150,000+ Annually**	By consolidating security tools and automating Tier 1 and Tier 2 tasks, security analysts can focus on high-value threat hunting and investigation, rather than alert triage.
Risk Mitigation	**Near-Real-Time Threat Detection**	AI-powered detection and correlation across all data sources identify sophisticated threats like ransomware and APTs that evade traditional signature-based systems.
Audit Readiness	**Continuous Compliance Monitoring**	Automated reporting and evidence collection for GRC frameworks reduce audit preparation time by up to 60%.

Risk Mitigation

The solution is specifically engineered to detect and respond to the most critical threats in cloud environments:

- **Ransomware:** MDC detects suspicious file activity and Sentinel correlates this with network traffic anomalies, triggering playbooks to isolate affected resources.
- **Advanced Persistent Threats (APTs):** Sentinel's fusion technology correlates low-and-slow signals across multiple data sources (e.g., Azure AD sign-ins, Key Vault access) to identify multi-stage attacks.
- **Insider Threats:** Monitoring of privileged access (via JIT) and sensitive data access (via Defender for Storage/Key Vault) provides early warning of malicious or accidental misuse.

- **Misconfiguration Exploitation:** MDC continuously scans for misconfigurations (e.g., publicly exposed storage accounts, unencrypted databases) and provides remediation steps before they can be exploited.

3. GRC Mapping (Governance, Risk, and Compliance)

The architecture is designed to provide robust evidence and controls for major global compliance frameworks. The integration of MDC and Sentinel ensures that security controls are not only implemented but are also continuously monitored and auditable.

Compliance Frameworks and Control Mappings

Framework	Control/Requirement	Solution Component Mapping
Microsoft Cloud Security Benchmark	All Controls	MDC's Secure Score and Regulatory Compliance dashboard directly map to and assess adherence to this baseline.
NIST CSF	**DE.AE-1 (Baseline analysis)**	Sentinel's analytics rules and machine learning models establish and monitor deviations from normal activity.
ISO 27001:2022	**A.8.23 (Technical vulnerability management)**	MDC's vulnerability assessment (integrated with Qualys/Microsoft Defender Vulnerability Management) provides continuous scanning and reporting.
MITRE ATT&CK	Cloud Tactics & Techniques	Sentinel's built-in detection rules and hunting queries are mapped to the MITRE ATT&CK framework, allowing analysts to understand the context of an attack.
GDPR	**Article 32 (Security measures)**	Enforced through MDC's CWPP, RBAC, and Sentinel's incident management for rapid breach containment.
HIPAA	**§ 164.308(a)(6) (Security incident procedures)**	Sentinel's incident management and SOAR playbooks provide documented, repeatable, and automated procedures for handling security incidents involving ePHI.
PCI DSS v4.0	**Requirement 10 (Log monitoring)**	Sentinel centralizes all required logs (Azure Activity, Network Flow, System Logs) and provides continuous, automated monitoring and alerting.
SOC 2	**CC7.2 (System monitoring)**	Sentinel provides the continuous monitoring capability, while MDC ensures the system's security configuration is maintained.

Security Controls Implemented

The solution implements several key security controls:

1. **Cloud Security Posture Management (CSPM):** Provided by MDC's Secure Score and recommendations.
2. **Cloud Workload Protection Platform (CWPP):** Provided by MDC's specific plans (e.g., Defender for Servers, Key Vaults).
3. **Just-in-Time (JIT) VM Access:** Minimizes exposure of management ports by locking them down and only opening them on demand for a limited time.
4. **Adaptive Network Hardening:** Recommends Network Security Group (NSG) rules to further limit the attack surface based on actual traffic patterns.
5. **File Integrity Monitoring (FIM):** Tracks changes to critical operating system files, directories, and registry keys on Windows and Linux machines.

Audit Evidence

The platform automatically generates and retains the necessary evidence for compliance audits:

- **Security Alerts and Incident Records:** Stored in Sentinel, providing a complete timeline of the attack, investigation, and resolution.
- **Security Posture Assessments:** Historical Secure Score and regulatory compliance reports from MDC.
- **SOAR Playbook Execution Logs:** Detailed logs from Logic Apps proving that automated response actions were executed as designed.
- **Threat Intelligence Reports:** Integration with Microsoft and third-party threat intelligence feeds used in detection and investigation.

4. Prerequisites

Successful deployment requires specific accounts, tools, and configurations to be in place.

4.1. Azure Subscription and Permissions

- **Active Azure Subscription:** A valid subscription is required.
- **Required Roles:**
  - **Owner** or **Contributor** on the subscription to create resource groups, Log Analytics Workspaces, and Key Vaults.
  - **Security Admin** on the subscription to enable Microsoft Defender for Cloud plans.
  - **Sentinel Contributor** on the Log Analytics Workspace to manage Sentinel settings, analytics rules, and playbooks.

4.2. Local Tools

- **Azure CLI:** The command-line interface for managing Azure resources.
  - *Installation:* Follow the official Microsoft documentation for your operating system.
  - *Configuration:* Run `az login` and ensure the correct subscription is selected: `az account set --subscription "<Subscription ID or Name>"`.

4.3. Azure Service Prerequisites

- **Log Analytics Workspace:** An existing or new workspace is required to host Sentinel data. Sentinel is an application that runs on top of a Log Analytics Workspace.
- **Microsoft Defender for Cloud:** Must be enabled at the subscription level. The **Standard Tier** (now referred to as **Defender plans**) is required to access CWPP features like Defender for Key Vault and advanced threat detection.

5. Architecture Overview

The solution architecture is a hub-and-spoke model for security data, centered around the Log Analytics Workspace and Microsoft Sentinel.

Data Flow and Component Interaction

1. **Data Ingestion:** Raw security logs (e.g., Azure Activity, Azure AD, NSG flow logs, VM logs) are collected and streamed into the **Log Analytics Workspace**.
2. **Cloud Security Posture Management (CSPM): Microsoft Defender for Cloud** continuously assesses the configuration of all Azure resources against the Microsoft Cloud Security Benchmark. It generates **Recommendations** for misconfigurations (e.g., "Enable MFA on subscription accounts").
3. **Cloud Workload Protection Platform (CWPP):** MDC's specific Defender plans (e.g., Defender for Key Vault, Defender for Servers) monitor runtime behavior of workloads. When a threat is detected (e.g., suspicious Key Vault access pattern), MDC generates a **Security Alert**.
4. **SIEM Correlation:** Both MDC **Recommendations** and high-fidelity **Security Alerts** are automatically streamed into **Microsoft Sentinel**. Sentinel correlates these alerts with other ingested data (e.g., network logs, user activity) using its built-in analytics rules and Fusion technology to create a consolidated **Incident**.
5. **Incident Management:** Security analysts use the Sentinel Incident queue for investigation, leveraging features like the investigation graph and hunting queries.
6. **Automated Response (SOAR):** When an Incident meets a predefined condition (e.g., high severity, specific entity involved), a **Logic App (Playbook)** is automatically triggered. This playbook executes remediation actions, such as isolating a compromised VM, revoking a user's token, or creating a ticket in an external system (e.g., ServiceNow).

Key Architectural Principles

- **Centralization:** All security data and incident management are centralized in Sentinel, eliminating the need to switch between multiple consoles.
- **Defense-in-Depth:** The solution layers protection: CSPM for prevention, CWPP for runtime detection, and SIEM/SOAR for correlation and automated response.
- **Cloud-Native:** Leveraging Azure's native services ensures scalability, high availability, and seamless integration with other Azure resources.

6. Step-by-Step Implementation

This section provides the detailed, production-ready steps for deploying the core components using the Azure CLI.

6.1. Setup Environment Variables

Define variables to ensure consistency and ease of deployment. **Replace the placeholder values with your desired names.**

```
# --- Configuration Variables ---
RESOURCE_GROUP="rg-prj-azure-sec-059-security"
LOCATION="eastus" # Choose a region close to your primary resources
WORKSPACE_NAME="la-prj-azure-sec-059-sentinel"
KEY_VAULT_NAME="kv-prj-azure-sec-059-secrets"
SUBSCRIPTION_ID=$(az account show --query id -o tsv)

echo "Configuration Summary:"
echo "Resource Group: $RESOURCE_GROUP"
echo "Location: $LOCATION"
echo "Log Analytics Workspace: $WORKSPACE_NAME"
echo "Key Vault: $KEY_VAULT_NAME"
echo "Subscription ID: $SUBSCRIPTION_ID"
```

6.2. Create Resource Group

The resource group will logically contain all security components.

```
echo "Creating Resource Group: $RESOURCE_GROUP..."
az group create --name $RESOURCE_GROUP --location $LOCATION
```

6.3. Deploy Log Analytics Workspace

This workspace will serve as the data repository for Microsoft Sentinel. We use the `PerGB2018` SKU, which is the standard for Sentinel deployments.

```
echo "Creating Log Analytics Workspace: $WORKSPACE_NAME..."
az monitor log-analytics workspace create \
    --resource-group $RESOURCE_GROUP \
    --workspace-name $WORKSPACE_NAME \
    --location $LOCATION \
    --sku PerGB2018
```

6.4. Enable Microsoft Sentinel

Sentinel is enabled on top of the Log Analytics Workspace. This step registers the workspace as a Sentinel instance.

```
echo "Enabling Microsoft Sentinel on workspace: $WORKSPACE_NAME..."
WORKSPACE_ID=$(az monitor log-analytics workspace show --resource-group
$RESOURCE_GROUP --workspace-name $WORKSPACE_NAME --query id -o tsv)

# Sentinel onboarding via REST API call
az rest --method PUT \
    --uri
"/subscriptions/$SUBSCRIPTION_ID/resourceGroups/$RESOURCE_GROUP/providers/Micr
api-version=2020-01-01" \
    --body "{\"properties\": {}}"

echo "Sentinel enabled successfully."
```

6.5. Enable Microsoft Defender for Cloud Plans

We enable the Standard tier for the subscription and specifically enable **Defender for Key Vault** to align with the project's focus.

```
echo "Enabling Microsoft Defender for Cloud Standard Plans..."

# 1. Enable Defender for Servers (CWPP for VMs)
# This ensures auto-provisioning of the Log Analytics agent for data
collection
az security auto-provisioning-setting update \
    --name "default" \
    --auto-provision "On"

# 2. Enable Defender for Key Vault (CWPP for Key Vault)
az security pricing create -n KeyVaults --tier Standard

# 3. Enable Defender for the subscription (CSPM)
az security pricing create -n Subscriptions --tier Standard

echo "Defender for Cloud plans enabled."
```

6.6. Deploy Sample Azure Key Vault

Deploy a Key Vault instance to test the protection provided by Defender for Key Vault.

```
echo "Deploying Azure Key Vault: $KEY_VAULT_NAME..."
az keyvault create \
    --name $KEY_VAULT_NAME \
    --resource-group $RESOURCE_GROUP \
    --location $LOCATION \
    --enabled-for-deployment true \
    --sku standard
```

6.7. Configure Essential Data Connectors in Sentinel

While many connectors are best configured via the Portal or IaC, we can confirm the connection of the most critical built-in connectors via the CLI/REST API.

```
echo "Configuring essential data connectors (Azure Activity, Defender for Cloud)..."

# 1. Connect Azure Activity Log (Conceptual - often done via Portal/ARM)
# This is crucial for monitoring control plane operations.
# The following is a conceptual command, as full connector deployment is complex via simple CLI
# az monitor log-analytics workspace data-source create ...

# 2. Verify Defender for Cloud connector status
# The MDC connector is automatically enabled when Sentinel is onboarded to a workspace
# that has MDC enabled. We verify the connection in the Validation phase.

echo "Data connector configuration initiated. Review 'Data Connectors' in the Sentinel Portal."
```

6.8. Conceptual Deployment of a Sample SOAR Playbook

A production-ready SOAR playbook (Logic App) is essential for automated response. We outline the conceptual steps for a common scenario: **“Auto-Isolate VM on High-Severity Alert.”**

Playbook Logic:

1. **Trigger:** When a Microsoft Sentinel incident is created or updated.
2. **Condition:** Check if the incident severity is “High” and the alert provider is “Microsoft Defender for Cloud.”
3. **Action 1 (Enrichment):** Get details of the affected VM entity.
4. **Action 2 (Remediation):** Call the “Isolate VM” action (a pre-built Logic App action or a custom runbook) to apply a restrictive Network Security Group (NSG) rule to the VM.
5. **Action 3 (Notification):** Send an email or post a message to a Teams channel with incident details and the action taken.

Conceptual Deployment Steps (Requires Logic App JSON/Bicep):

1. **Create Logic App:** Define the Logic App resource in the same resource group.

2. **Assign Managed Identity:** Grant the Logic App's System Assigned Managed Identity the necessary RBAC roles (e.g., **Network Contributor** to modify NSGs, **Key Vault Secrets User** if interacting with Key Vault).
3. **Connect to Sentinel:** Attach the Logic App as a Playbook to a Sentinel Automation Rule.

This step is a placeholder for a full IaC deployment, emphasizing the need for a dedicated SOAR phase in a real project.

7. Validation & Testing

Verification ensures that the deployed components are correctly configured and the end-to-end security workflow is functional.

7.1. Verify Sentinel and MDC Status

1. **Portal Check:** Navigate to the Azure Portal, open the Log Analytics Workspace (`$WORKSPACE_NAME`), and confirm that **Microsoft Sentinel** is listed as a solution.
2. **Data Connectors:** In the Sentinel blade, navigate to **Data Connectors**. Verify that **Microsoft Defender for Cloud** and **Azure Activity** show a "Connected" status.
3. **Defender Status:** Navigate to **Microsoft Defender for Cloud**. Check the **Pricing and settings** blade and confirm that the subscription and the Key Vault are set to the **Standard** tier.

7.2. Simulate a Security Alert (Key Vault)

To test the end-to-end flow, we simulate a threat against the protected Key Vault.

1. **Simulate Threat:** Attempt a suspicious action on the Key Vault (e.g., repeated failed access attempts from a non-whitelisted IP, or a mass secret deletion attempt).
2. **Verify Alert in MDC:** Within 5-10 minutes, a **Security Alert** should appear in the Microsoft Defender for Cloud alerts blade, specifically related to the Key Vault.
3. **Verify Incident in Sentinel:** The MDC alert should be automatically ingested by Sentinel and appear as a **High Severity Incident** in the Sentinel **Incidents** blade.

7.3. Validate SOAR Playbook Execution

If a sample SOAR playbook was deployed (e.g., for high-severity alerts):

1. **Trigger Playbook:** Manually run the playbook against the newly created Key Vault incident, or wait for the automation rule to trigger it.
2. **Check Logic App Run History:** Navigate to the deployed Logic App in the Azure Portal. Check the **Run history** to confirm the run was successful (green checkmark).
3. **Verify Action:** Confirm the intended action was executed (e.g., a notification email was received, or a test VM was successfully isolated).

8. Troubleshooting

This section provides solutions for common deployment and operational issues.

Issue	Potential Cause	Resolution
No data in Sentinel	Data connectors are not enabled, or the Log Analytics agent is not reporting.	1. Verify the status of the **Microsoft Defender for Cloud** and **Azure Activity** connectors in Sentinel. 2. For VMs, ensure the Log Analytics agent is installed and the VM's firewall allows outbound traffic to the Log Analytics endpoint.
SOAR Playbook failure	Logic App permissions are incorrect (RBAC) or the trigger condition is not met.	1. Check the Logic App run history for detailed error messages. 2. Ensure the Logic App's Managed Identity has the necessary RBAC roles (e.g., **Sentinel Responder**, **Network Contributor**).
High Cost	Log Analytics data ingestion is too high.	1. Review Log Analytics usage reports. 2. Implement **Data Collection Rules (DCRs)** to filter out noisy, non-security-relevant logs. 3. Adjust the Sentinel commitment tier (see Cost Optimization).
Defender for Cloud alerts are missing	The specific Defender plan for the resource is not enabled (e.g., Defender for Storage is off).	1. Check the **Pricing and settings** in MDC. 2. Ensure the required Defender plan is set to **Standard** for the relevant resource type.
JIT Access not working	The VM is not onboarded to MDC, or the NSG is manually configured.	1. Ensure the VM is in a subscription with Defender for Servers enabled. 2. Verify that the JIT policy is assigned and not overridden by manual NSG rules.

9. Cost Optimization

Security solutions can be a significant operational expense. Strategic configuration is key to maximizing protection while minimizing costs.

9.1. Sentinel Commitment Tiers

Azure Sentinel offers commitment tiers that provide a significant discount (up to 60%) compared to the Pay-As-You-Go rate for data ingestion.

- **Strategy:** Accurately estimate your daily ingestion volume (in GB) and select the corresponding commitment tier (e.g., 100 GB/day, 200 GB/day).
- **Action:** Monitor usage for the first 30 days and adjust the tier monthly. If you exceed the tier, the overage is charged at the tier's discounted rate, not the full Pay-As-You-Go rate.

9.2. Log Analytics Data Retention and Archiving

Data retention is a major cost driver.

- **Hot Data (Active Analytics):** Keep data in the active Log Analytics tier only for the minimum required period (e.g., 90 days for immediate investigation).
- **Archived Logs:** Use the **Archived Logs** feature for long-term, low-cost storage (up to 7 years) to meet regulatory requirements (e.g., GDPR, HIPAA). This data is significantly cheaper to store but requires a retrieval process (Restore) for analysis.

9.3. Selective Defender for Cloud Plans

Only enable the paid Defender plans (Standard tier) for the resources that genuinely require advanced CWPP features.

- **Example:** If you only have a few critical Key Vaults, enable Defender for Key Vault only on the subscription containing those critical assets. If you have non-production VMs that do not host sensitive data, consider excluding them from the Defender for Servers plan.
- **Cost-Benefit Analysis:** Always weigh the cost of the Defender plan against the risk of the workload being compromised.

10. Security Best Practices

Beyond the core deployment, adopting these best practices ensures the long-term security and maintainability of the SOC solution.

10.1. Role-Based Access Control (RBAC)

Implement the principle of least privilege for all security personnel accessing Sentinel and Defender.

- **Sentinel Roles:**
  - **Sentinel Reader:** Can view data, incidents, and workbooks. Ideal for Tier 1 analysts.
  - **Sentinel Responder:** Can manage incidents (change status, assign ownership) and run playbooks. Ideal for Tier 2 analysts.
  - **Sentinel Contributor:** Can create and edit analytics rules, workbooks, and playbooks. Ideal for SOC engineers.
- **Defender Roles:**
  - **Security Reader:** Can view security posture and alerts.
  - **Security Administrator:** Can manage security policies and view everything.

10.2. Multi-Factor Authentication (MFA) and Conditional Access

Enforce strong identity controls for all users, especially those with privileged access to the security console.

- **MFA:** Enforce MFA for all users accessing the Azure Portal and any security-related applications.
- **Conditional Access:** Implement Conditional Access policies in Azure AD to restrict access to the security resource group (`$RESOURCE_GROUP`) based on:
  - **Device Compliance:** Only allow access from corporate-managed, compliant devices.
  - **Trusted Locations:** Restrict access to known SOC IP ranges.

10.3. Continuous Monitoring and Tuning

Security is not a one-time deployment. The solution requires continuous maintenance.

- **Secure Score Review:** Daily review of the Microsoft Defender for Cloud Secure Score to prioritize and remediate the most impactful recommendations.

- **Alert Tuning:** Regularly review false positives in Sentinel. Tune analytics rules, suppression rules, and Fusion rules to increase the signal-to-noise ratio and prevent alert fatigue.
- **Threat Hunting:** Proactively use Sentinel's hunting queries to search for threats that have not yet triggered an alert, leveraging the MITRE ATT&CK framework.

10.4. Log Retention Policy Enforcement

Ensure that the Log Analytics retention settings meet all regulatory and internal audit requirements. Use Azure Policy to enforce the minimum required retention period across all security-relevant Log Analytics Workspaces.

10.5. Infrastructure as Code (IaC)

For production environments, the entire deployment should be managed via IaC (Bicep, Terraform). This ensures repeatability, version control, and compliance.

Conceptual Bicep Snippet (Expanded):

```
// main.bicep
param location string = resourceGroup().location
param workspaceName string = 'la-prj-azure-sec-059-sentinel'
param keyVaultName string = 'kv-prj-azure-sec-059-secrets'

// 1. Log Analytics Workspace
resource workspace 'Microsoft.OperationalInsights/workspaces@2021-12-01-
preview' = {
  name: workspaceName
  location: location
  properties: {
    sku: {
      name: 'PerGB2018'
    }
    retentionInDays: 90 // Enforce 90-day retention
  }
}

// 2. Microsoft Sentinel Onboarding
resource sentinel 'Microsoft.SecurityInsights/onboardingStates@2021-10-01' = {
  name: 'default'
  scope: workspace
  properties: {}
}

// 3. Azure Key Vault
resource keyVault 'Microsoft.KeyVault/vaults@2023-07-01' = {
  name: keyVaultName
  location: location
  properties: {
    sku: {
      family: 'A'
      name: 'standard'
    }
    tenantId: subscription().tenantId
    enabledForDeployment: true
    enableRbacAuthorization: true // Use RBAC for access control
  }
}

// 4. Enable Defender for Key Vault (Pricing)
resource defenderKeyVaultPricing 'Microsoft.Security/pricings@2023-01-01' = {
  name: 'KeyVaults'
  properties: {
    pricingTier: 'Standard'
  }
```

```
}

output workspaceId string = workspace.id
output keyVaultUri string = keyVault.properties.vaultUri
```

11. Cleanup

To remove all deployed resources and avoid future charges, execute the following command. **Use with caution, as this is irreversible.**

```
echo "Deleting resource group: $RESOURCE_GROUP..."
az group delete --name $RESOURCE_GROUP --yes --no-wait
echo "Cleanup initiated. The resource group will be deleted in the
background."
```

End of Implementation Guide