**Test 2**

**Problem Analysis Project: SIEM Lab Deliverable**

**8832028**

**Paul Jose**

# **Module-1 Setting up the environment**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 1 Created Log Analytics Workspace

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 2 Created Log Analytics Workspace.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 3 Enabled Play books

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 4 Sentinel Dashboard

# **Module-2 Data Connectors**

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

Figure 5 Azure Sentinel Data Connectors

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

Figure 6 Azure Activity Data Connectors

Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 7 Azure monitor agent

# Module 3 Analytics Rule

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 8Microsoft Analytics Rule

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 9 Analytics rule from Microsoft Entra ID.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 10 Rule for high and medium alerts from Microsoft Defender for Cloud.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 11 Custom Rule for Microsoft Follina Attack.

# Module 4

# Incident Management

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 12 Incident Dashboard

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 13 Attempts to sign in disabled accounts

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Figure 14 Investigation Status**

Interfaz de usuario gráfica

Descripción generada automáticamente

**Figure 15 Created Automation Rule For False Positives**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Figure 16 WorkBook**

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

**Figure 17 Threat Hunt for Microsoft Follina**

**References**

Azure-Sentinel/Solutions/Training/Azure-Sentinel-Training-Lab/Modules/Module-1-Setting-up-the-environment.md at master · Azure/Azure-Sentinel. (n.d.). GitHub. Retrieved June 22, 2024, from <https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Training/Azure-Sentinel-Training-Lab/Modules/Module-1-Setting-up-the-environment.md>

Microsoft-Sentinel-Queries/Detect-Follina-Exploitation.kql at main · le0li9ht/Microsoft-Sentinel-Queries. (n.d.). GitHub. Retrieved June 22, 2024, from https://github.com/le0li9ht/Microsoft-Sentinel-Queries/blob/main/Detect-Follina-Exploitation.kql