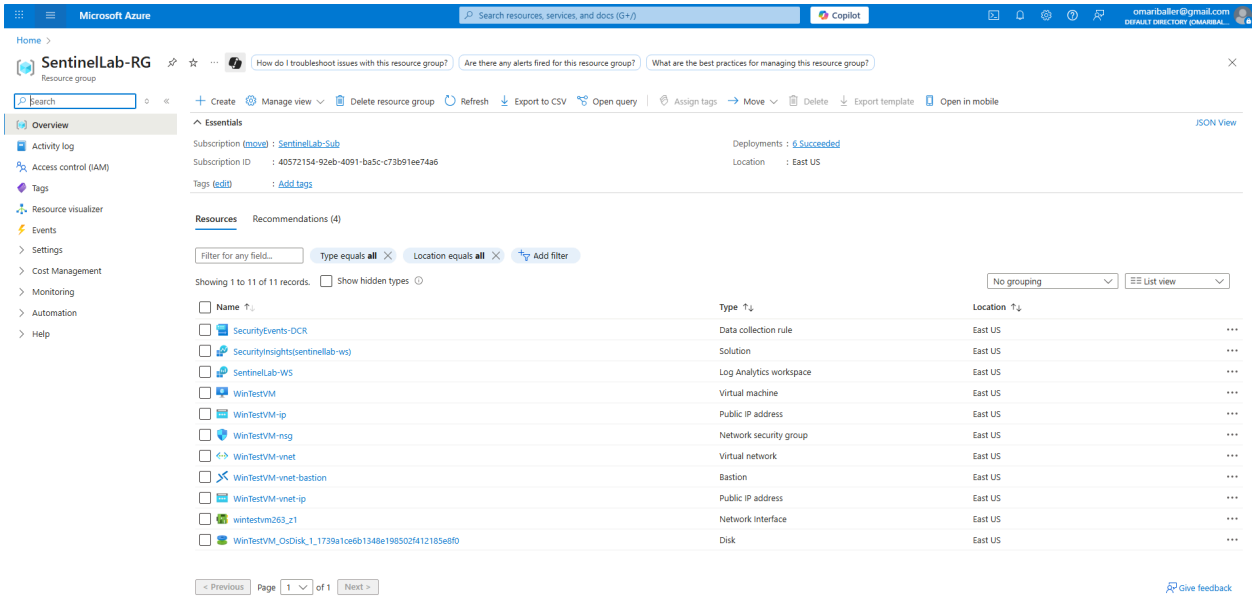
HEADER: Lab Overview

Screenshot:



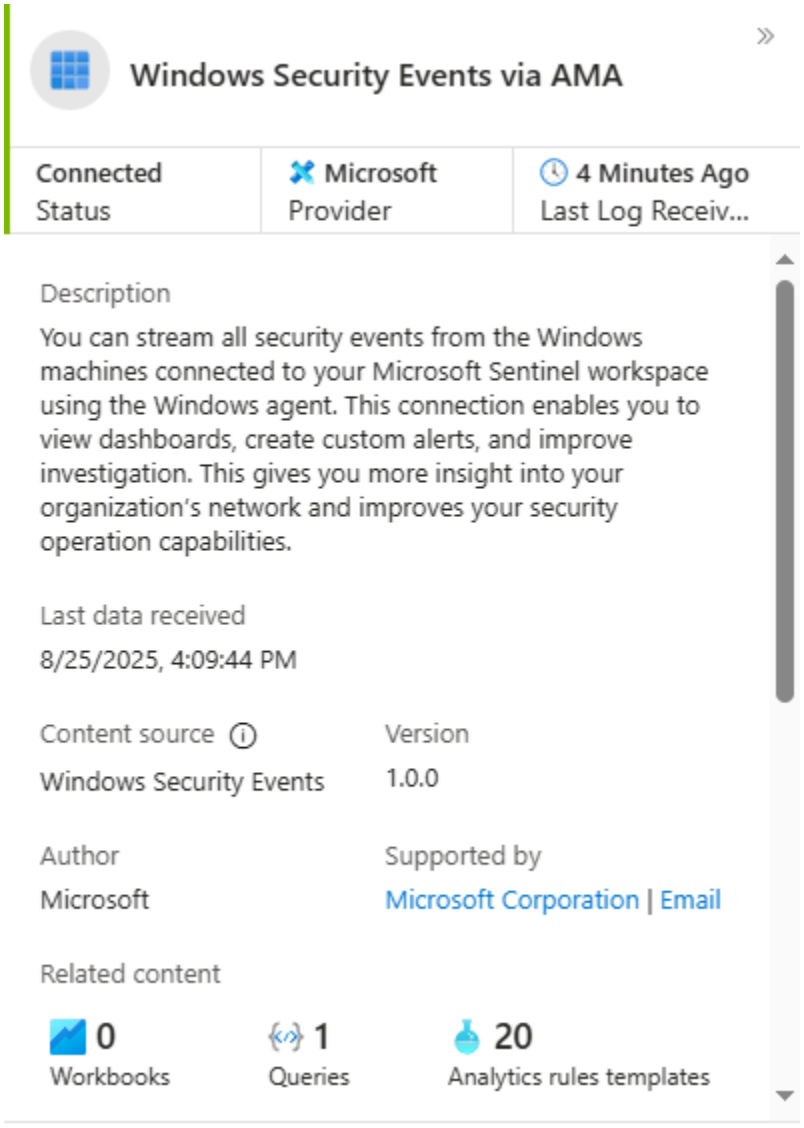
Caption:

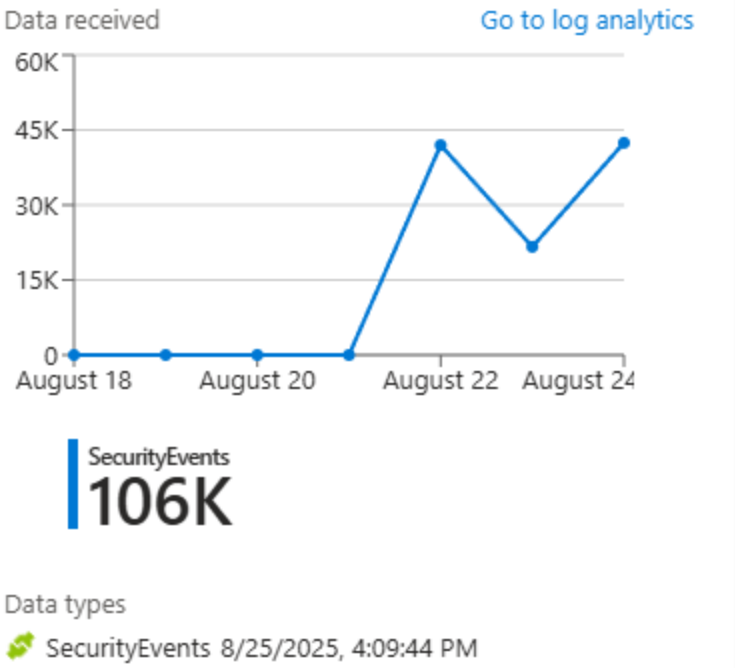
Azure Resource Group showing the full detection lab setup: WinTestVM (Windows 11 test machine), Sentinel Log Analytics Workspace, Data Collection Rule (DCR), and associated networking resources.

This lab simulates a real-world SOC environment. Logs are collected from a Windows VM via Sysmon + Windows Security Events and ingested into Microsoft Sentinel through the workspace. Custom analytics rules were created to detect brute force attempts and failed logon floods, mapped to MITRE ATT&CK tactics

HEADER: Data Ingestion

Screenshots:



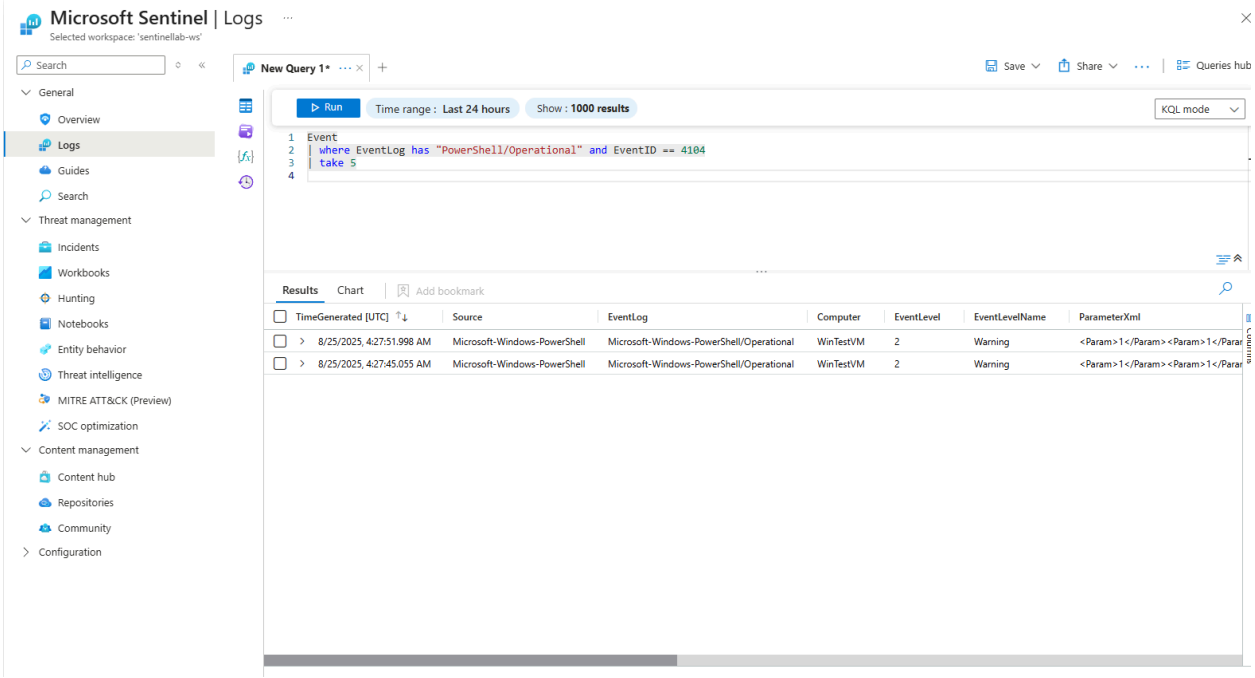


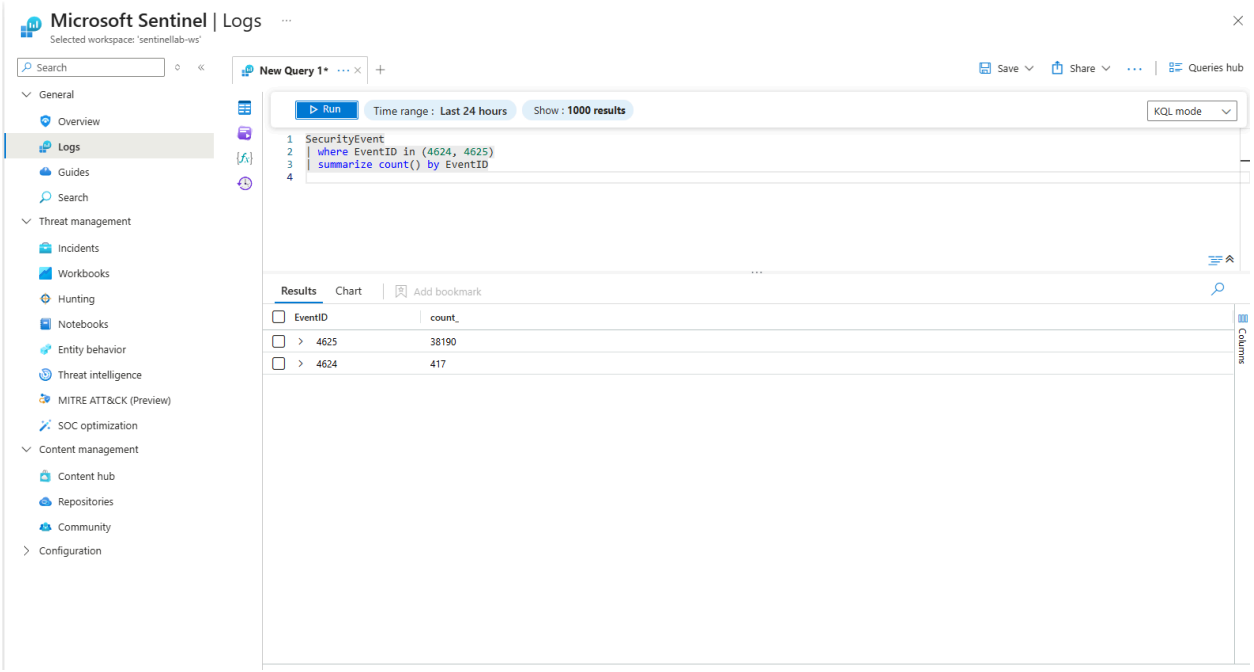
Caption:

Windows Security Event logs were ingested into Microsoft Sentinel using the Azure Monitor Agent (AMA). The connector page confirms the successful configuration of the Data Collection Rule (`SecurityEvents-DCR`) and shows active log data flowing from the WinTestVM into the workspace.

HEADER: Raw Logs Validation

SCREENSHOT:



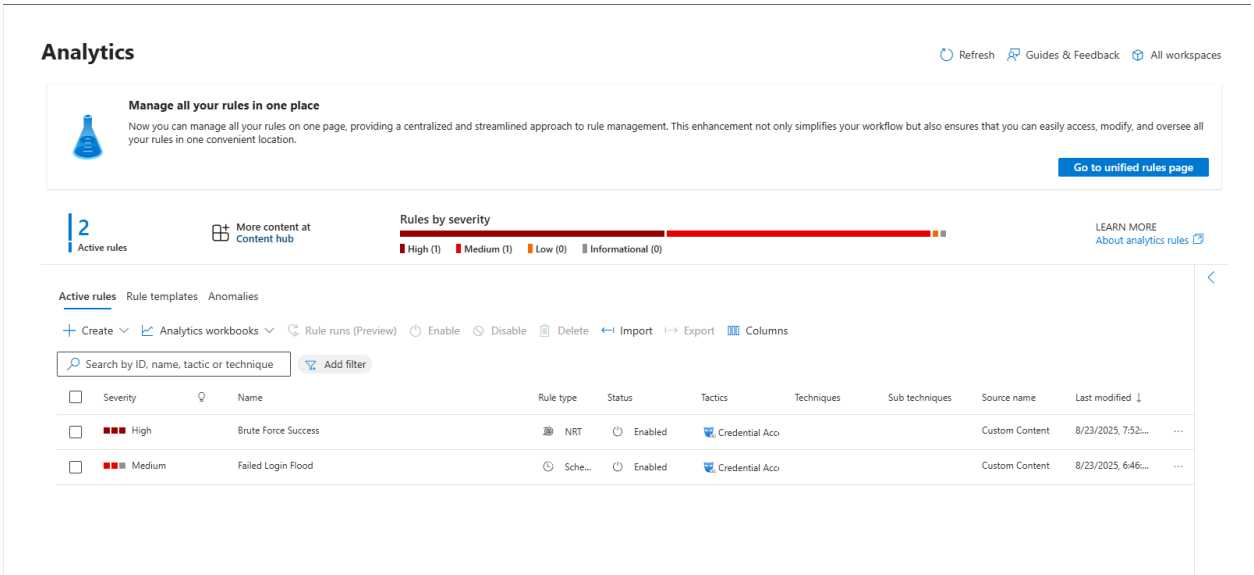


CAPTION:

To validate ingestion, KQL queries were executed against the Log Analytics Workspace. EventID **4104** confirmed PowerShell script block logging, while EventIDs **4624** (successful logon) and **4625** (failed logon) confirmed authentication events. These raw events provide the foundation for building custom detection rules.

HEADER: Detection Rules

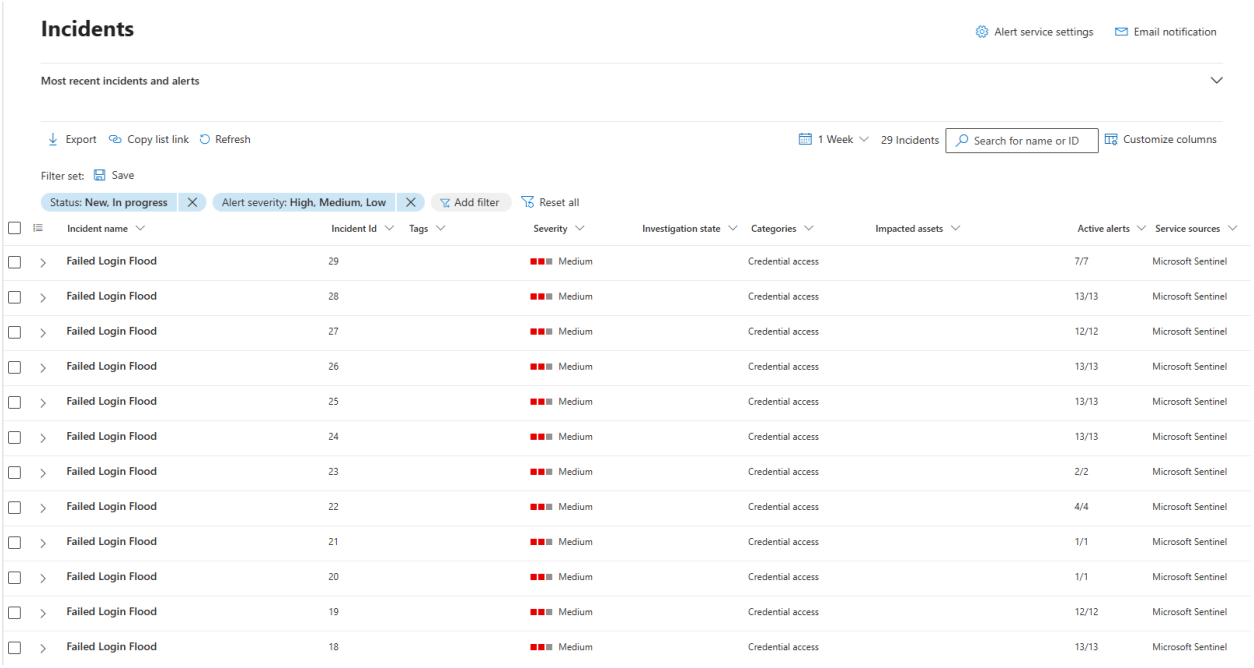
SCREENSHOT:



CAPTION:

Two custom analytics rules were created in Sentinel to simulate common SOC detections: **Failed Login Flood** (detects repeated failed authentication attempts) and **Brute Force Success** (detects credential stuffing that eventually succeeds). Each rule was mapped to the MITRE ATT&CK framework under the **Credential Access** tactic, with severities assigned appropriately.

HEADER: Incidents



CAPTION:

Simulated brute force activity was generated by intentionally failing repeated logins against the WinTestVM. Microsoft Sentinel successfully correlated these events and triggered multiple incidents, visible in the Incidents page. This confirmed end-to-end detection: data ingestion → log validation → rule detection → incident creation.