

Sprint 5 Review: Configure security operations and monitoring

- ✓ Sprint Status - **Complete**
- ✓ Project Status - 71% Complete
- ✓ Items Completed - 16 Tasks
- ✓ Sprints Left for Completion - 2
- ✓ Project on Budget - **Yes**

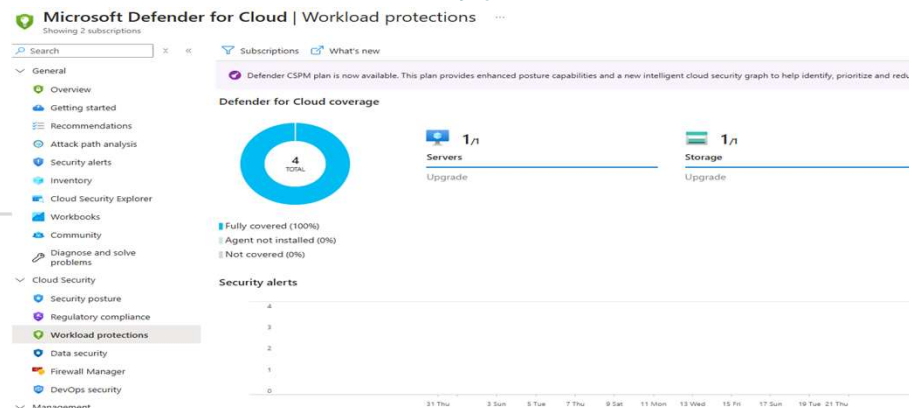
Things to Demo	Quick Updates	What is Next
Task 1 Complete Setup Microsoft Defender for Cloud (Secure Score, workload protection)		Sprint 6 Conduct integration testing and User Acceptance Training (UAT)
Task 2 Complete Configure Microsoft Sentinel with data connectors and analytics rules	Data Connector Microsoft Entra ID ticket submitted to Microsoft. Pending response.	
Task 3 Complete Test and validate automated threat response workflows		

Sprint 5 - Task 1 Captures

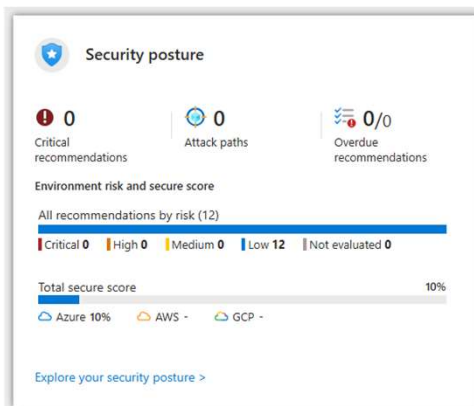
Setup Microsoft Defender for Cloud (Secure Score, workload protection)

<https://learn.microsoft.com/en-us/training/modules/microsoft-defender-cloud-security-posture/3-secure-score>

DataWorks 100% of
workload protections



DataWorks Secure Score

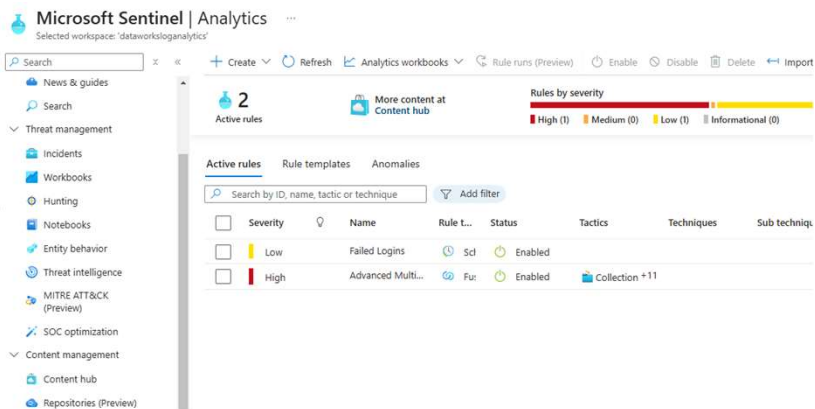


Sprint 5 - Task 2 Captures

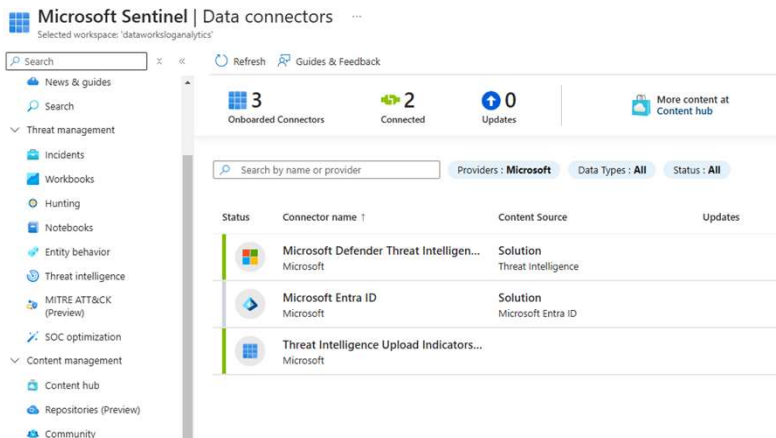
Configure Microsoft Sentinel with data connectors and analytic rules

<https://learn.microsoft.com/en-us/training/modules/security-monitoring-automation-solutions/3-microsoft-sentinel-data-connectors>

DataWorks Failed Login
Analytics rule created



DataWorks data connectors
connected, Pending resolution to
Microsoft Entra ID Connector



Sprint 5 - Task 3 Captures

test and validate automated threat response workflows

<https://learn.microsoft.com/en-us/training/modules/security-monitoring-automation-solutions/6-respond-threats-by-using-playbooks-with-automation-rules-microsoft-sentinel>

DataWorks Failed Login
Incident Created, assigned
severity, assigned owner,
and assigned tags

The screenshot displays the Microsoft Sentinel 'Incidents' page. The left sidebar shows the navigation menu with 'Incidents' selected under 'Threat management'. The main content area shows a summary of incident counts: 1 Open incident, 1 New incident, and 0 Active incidents. Below this, there's a search bar and filters for Severity (All), Status (2 selected), and Incident Provider name (All). A table lists the incidents, with one incident visible: Medium severity, Incident number 1, Title Failed Login, Alerts 0, Incident provider name Azure Sentinel, and Alert product name Azure Sentinel.

Severity	Incident number	Title	Alerts	Incident provider name	Alert product name
Medium	1	Failed Login	0	Azure Sentinel	Azure Sentinel