

The Solution in Action: Sentinel Health Check Agent

Maintaining the health of a Microsoft Sentinel workspace is complex and time consuming. It requires continuous monitoring, configuration checks, and performance tuning. To simplify this, we've introduced an AI Agent designed to evaluate and optimize Sentinel health automatically.

Agent Description

An AI-powered agent that automatically evaluates and optimizes the health of a Microsoft Sentinel workspace. It monitors log ingestion, configuration, and performance. Beyond monitoring, it can create detailed remediation steps to resolve problems, generate KQL queries to assist with investigations, and provide intelligent troubleshooting guidance to accelerate root cause analysis of health-related issues. This functionality is trained on Microsoft documentation and is designed to enhance operational efficiency through proactive health checks and automated recommendations.

Value add for you team

- ✓ Checks for duplicate logs in Sentinel workspace
- ✓ Detects and reports errors in log ingestion
- ✓ Enables faster detection and response to health issues
- ✓ Improves data quality and reliability through automated monitoring
- ✓ Conducts regularly scheduled Automates time-consuming health checks

Technologies Leveraged



Target Audience

Security Analysts	SIEM Engineers	Cloud Admins
-------------------	----------------	--------------