Grant Thornton

Grant Thornton – Security Agents

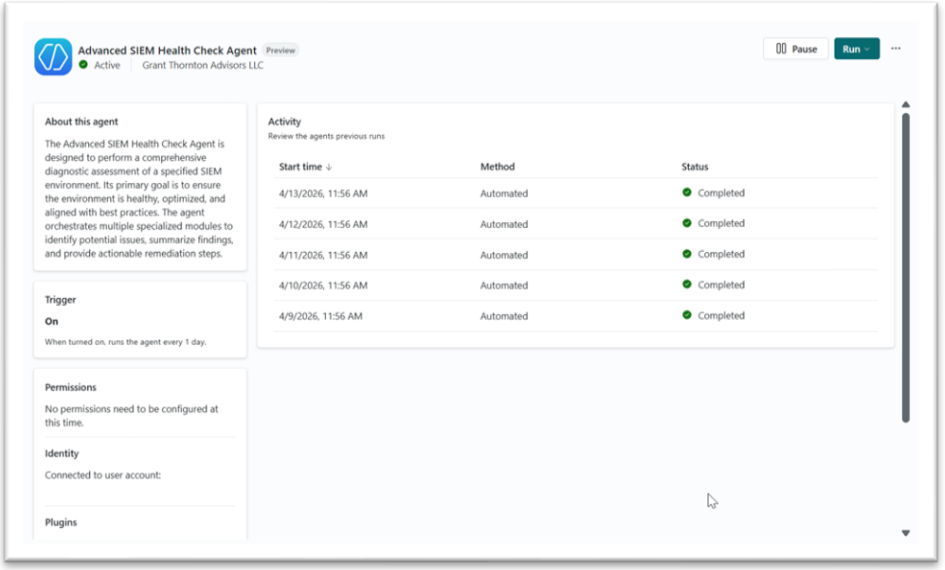
Advanced SIEM Health Check Agent

Security Copilot Agent – Agent Management Functionality

The Advanced SIEM Health Check Agent enables streamlined, Copilot-driven assessment of Microsoft Sentinel health and configuration from a single, centralized interface.

The Advanced SIEM Health Check Agent is designed to be launched and managed directly from the Microsoft Security Copilot agent management experience. From this centralized view, users can configure required inputs, initiate health assessments, and review summarized findings produced by the agent. The agent integrates seamlessly with Microsoft Sentinel to execute health checks across data ingestion, analytics rules, and incident activity, ensuring users can quickly understand the overall state of their SIEM environment without leaving the Copilot interface.

Advanced SIEM Health Check Agent

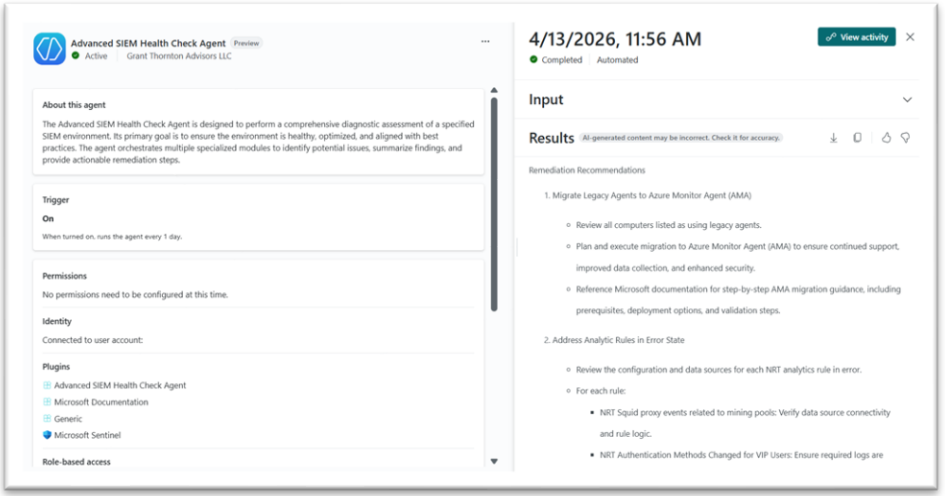


Security Copilot Agent Functionality

This slide demonstrates how the Advanced SIEM Health Check Agent provides clear, actionable insights into Microsoft Sentinel health using Copilot-driven analysis.

Within Microsoft Security Copilot, the Advanced SIEM Health Check Agent orchestrates multiple specialized skills to perform a comprehensive diagnostic review of a Sentinel workspace. The agent evaluates ingestion health, detection rule stability, and recent incident activity to identify misconfigurations, operational risks, and optimization opportunities. Findings are consolidated into clear summaries with actionable insights, enabling security teams to efficiently assess environment health and prioritize remediation using natural language interactions.

Advanced SIEM Health Check Agent



Agent Installation Instructions

The following steps describe how to deploy, configure required connection values, and run the Advanced SIEM Health Check Agent using Microsoft Security Copilot.

1. **Install the Agent:** Deploy the agent through the Microsoft Security Copilot agent framework, making it available within the tenant's Copilot environment.

2. **Provide Required Connection Parameters:** Configure the agent by supplying specific required values needed to establish a connection, including Tenant ID, Subscription ID, Resource Group Name, and Microsoft Sentinel Workspace Name.

3. **Configure Agent Scope and Access:** Use the provided values to define the target Azure and Sentinel resources the agent will assess, ensuring proper permissions and workspace visibility.

4. **Execute the Agent:** Run the agent using Copilot prompts either on demand or on a scheduled basis to perform SIEM health assessments.

5. **Review Assessment Output:** Review returned results within Copilot, including SIEM health findings, configuration observations, and identified gaps.

6. **Apply Recommended Actions:** Follow the agent's recommended guidance and next steps to remediate issues and improve Microsoft Sentinel reliability, configuration, and effectiveness.