Installation Steps – Log Engineering & Parser Auto-Generator

Prerequisites

- Microsoft Security Copilot access enabled
- Microsoft Sentinel workspace already provisioned
- User has appropriate permissions to deploy KQL functions in the target workspace

---

Step 1: Install the Agent

1. Open **Microsoft Security Copilot**.
2. Navigate to the **Agent Store**.
3. Search for **Log Engineering & Parser Auto-Generator**.
4. Select the agent and click **Install**.

Step 2: Connect Required Permissions

1. When prompted, approve access to:
    - The target **Microsoft Sentinel / Log Analytics workspace**
    - Required Sentinel APIs for KQL function deployment
2. Confirm that permissions are scoped correctly to the intended workspace.

Step 3: Configure Agent Inputs

1. Open the agent configuration panel.
2. Provide the required inputs:
    - **Sample Logs**: Raw or representative log data to be analyzed
    - **Workspace ID**: The Sentinel workspace where parsers will be deployed
3. Save the configuration.

Step 4: Run a Validation Test

1. Select **Test Agent**.
2. Review the generated analysis, parser output, and validation feedback.
3. Confirm that:
    - Fields are correctly parsed
    - ASIM mappings are appropriate
    - No ingestion or syntax errors are reported

Step 5: Deploy to Production

1. Once validation is complete, select **Publish** or **Deploy**.
2. The agent will deploy KQL parsers and supporting artifacts into the workspace.
3. Review the deployment status confirmation.

Step 6: Operational Use

- Use the agent for:
    - New log source onboarding
    - Parser regeneration after schema changes
    - Accelerated Sentinel deployments across environments
- Monitor ingestion health and parser performance through Sentinel.

Post-Installation Notes

- The agent operates in an **advisory and governed mode**.
- No destructive actions are performed.
- All outputs are explainable and reviewable before and after deployment.