**Integration Steps**

1. **Access Microsoft Sentinel**
   * Go to the **Azure Portal** → **Microsoft Sentinel** → **Data Connectors**.
2. **Deploy the SentinelOne Connector**
   * Search for **SentinelOne** in the connector gallery.
   * Click **Deploy to Azure** to launch the custom deployment template.
3. **Provide Required Inputs**
   * Enter SentinelOne API credentials (API token, domain, etc.).
   * Configure the polling interval and other parameters.
4. **Azure Function Deployment**
   * The deployment creates an **Azure Function App** that periodically pulls data from SentinelOne.
   * Logs are ingested into a custom table named SentinelOne\_CL in Log Analytics.
5. **Monitor the Integration**
   * Go to **Function App** → **Functions** → SentinelOneSentinelConnector → **Monitor**.
   * Use **Application Insights** for detailed diagnostics and log tracing.
6. **Validate in Sentinel**
   * Use KQL to query the SentinelOne\_CL table and verify data ingestion.