**Sentinel Setup Guide:**

**Step 1: Enable Microsoft Sentinel**

1. Sign in to the **Azure Portal** ([https://portal.azure.com](https://portal.azure.com/)).
2. Search for **Microsoft Sentinel** in the search bar.
3. Click **Create Microsoft Sentinel**.
4. Select an existing **Log Analytics Workspace** or create a new one.
5. Click **Add** to enable Sentinel on the workspace.

**Step 2: Connect Data Sources**

1. In Sentinel, go to the **Data Connectors** section.
2. Browse or search for a connector (e.g., Azure AD, Microsoft Defender, Syslog, Windows Security Events).
3. Click on the connector and select **Open Connector Page**.
4. Follow the instructions to configure the connection.
5. Enable **log ingestion** for analysis.

**Step 3: Create Analytic Rules**

1. Navigate to **Analytics** in Sentinel.
2. Click **Create Rule** > **Scheduled Query Rule**.
3. Define a rule name and set the query logic (e.g., failed login attempts, suspicious network activity).
4. Set up **alert thresholds** and actions.
5. Click **Save** to activate the rule.

**Step 4: Set Up Incident Response**

1. Go to **Incidents** in Sentinel.
2. Click **Create Playbook** to automate incident response actions.
3. Use **Azure Logic Apps** to define automated responses (e.g., notify admins, block IPs, isolate machines).
4. Activate the playbook to handle security alerts efficiently.

**Step 5: Visualize Threats with Workbooks**

1. Navigate to **“**workbooks**”** in Sentinel.
2. Select a built-in template or create a custom dashboard.
3. Configure visualizations to monitor security events in real-time.