# Threat Hunting Process Development

1. Research Threat Hunt Process
2. Create Query Pack for Hunts
3. Document Process for Hunters
4. Deploy Hunt Pack to All Workspaces
5. **Research Threat Hunt Process**:
    - Understand the purpose and objectives of threat hunting.
    - Explore existing threat hunting methodologies and best practices.
    - Identify relevant threat intelligence sources.
    - Determine the scope and focus areas for your threat hunts.
    -
6. **Create KQL Query Pack for Threat Hunts**:
    - Develop a set of **KQL (Kusto Query Language)** queries tailored to your organization's environment.
    - These queries should target specific indicators of compromise (IoCs), suspicious behaviors, or known attack patterns.
    - Consider using threat intelligence feeds and historical data to inform your query development.
    -
7. **Document Process for Hunters**:
    - Create comprehensive documentation for threat hunters:
        - **Standard Operating Procedures (SOPs)**: Detailed step-by-step instructions for conducting threat hunts.
        - **Playbooks**: Specific scenarios and response actions.
        - **Data Sources and Collection Methods**: Specify which logs, telemetry, and data sources to analyze.
        - **Tools and Platforms**: Document the tools (e.g., SIEM, EDR) used during threat hunts.
        - **Communication Channels**: Define how hunters collaborate and report findings.
        - **Escalation Paths**: Outline procedures for escalating critical findings.
        -
8. **Deploy Hunt Pack to All Client Environments in Windows Azure**:
    - Package your KQL query pack along with any necessary scripts or configurations.
    - Deploy the hunt pack to all relevant client environments hosted in **Windows Azure**:

    - **Azure Virtual Machines**: Ensure the queries are scheduled to run periodically.
    - **Azure Sentinel**: Utilize built-in query capabilities or custom workbooks.
    - **Azure Security Center**: Integrate threat hunting into security policies.
- Monitor the effectiveness of the hunt pack and iterate as needed.

Remember that threat hunting is an iterative process, and continuous improvement is essential. Regularly review and update your threat hunting procedures based on new threat intelligence, evolving attack techniques, and organization changes.

references:
(*https://www.reliaquest.com/blog/build-a-cyber-threat-hunting-plan-with-this-step-by-step-process/*)

*Cyber Threat Hunting: Types, Methodologies, Best Practices (knowledgehut.com)*