**Multiple-Choice Questions (MCQs)**

1. **After cloning the repo, which script must you run *first* to populate ChromaDB before starting the MCP servers?**  
   a) mcp\_mitre\_server.py  
   b) upload\_to\_chromadb.py  
   c) mcp\_memory\_server.py  
   d) requirements.txt  
   **Correct Answer:** b) upload\_to\_chromadb.py
2. **Which MITRE technique ID is returned in the sample query “Hijack Legit RDP Session to Move Laterally”?**  
   a) T1563.002  
   b) T1021.001  
   c) T1071.001  
   d) T1105  
   **Correct Answer:** a) T1563.002

**True/False Questions**

1. **True or False –** One of the key advantages MCP brings to blue-team operations is a fully *auditable* evidence chain for every LLM answer.  
   **Correct Answer:** True
2. **True or False –** Vector embeddings in ChromaDB allow analysts to retrieve relevant MITRE, detection rules and CISA advisories even when their query wording does **not** contain exact keywords.  
   **Correct Answer:** True
3. **True or False –** Starting the mcp\_mitre\_server.py before running upload\_to\_chromadb.py will still work because the server can index data on the fly.  
   **Correct Answer:** False

**Fill-in-the-Blank Questions**

1. **Which five-word mantra on Slide 1 summarises the benefits of an MCP-powered SOC?**  
   *(Write the five nouns in order: \_\_\_\_\_\_, \_\_\_\_\_\_, \_\_\_\_\_\_, \_\_\_\_\_\_, \_\_\_\_\_\_.)*  
   **Correct Answer:** Auditability, Speed, Explainability, Modularity, Consistency
2. **The demo notebook orchestrates queries in JSON-RPC, then logs the full Q&A to the \_\_\_\_\_\_ server so auditors can replay decisions.**  
   **Correct Answer:** memory
3. **Fill in the missing step for the SOC workflow: 1 Ingest → 2 Enrich → 3 \_\_\_\_\_\_ → 4 Log.**  
   **Correct Answer:** Generate analyst guidance with an LLM
4. **In the data-prep pipeline, name one of the three knowledge bases that are ingested and embedded into ChromaDB.**  
   **Correct Answer (any one):**
   * MITRE ATT&CK
   * Detection Rules (e.g., SIGMA/Splunk/Elastic)
   * CISA Advisories
5. **List two specific analyst actions recommended when an alert maps to MITRE technique T1563.002 (RDP session hijacking).**  
   **Correct Answer (any two):**
   * Review session logs for abnormal RDP redirects
   * Check for unexpected privilege escalation
   * Validate involved user accounts
   * Follow CISA mitigation steps