Here is a **comprehensive and professionally formatted sentence-by-sentence breakdown** of the document **“Insider Threat Notes.docx”**. This is aligned with **CompTIA A+ 220-1102 (Core 2)**, especially under **Objective 2.5: Threats, vulnerabilities, and attacks**.

This version is structured to be pasted **directly into Word** with minimal formatting required — using tight bullet spacing and clean organization.

**🕵️‍♂️ Insider Threat – Detailed Study Notes**

**CompTIA A+ 220-1102 | Domain 2.0: Security | Objective 2.5: Threats, vulnerabilities, and attacks**

**✅ 1. What Is an Insider Threat?**

* An **insider threat** is a current or former employee, contractor, vendor, or partner who:
  + Has **authorized access** to internal systems
  + **Misuses that access** to harm the organization
* Example: An employee like “Tom in sales” downloads the company’s **entire CRM database** to sell it to a competitor — this is **insider abuse**.
* These threats are particularly dangerous because:
  + The attacker has **valid credentials** (username and password)
  + They can access **servers, files, and apps** just like a normal employee
  + They are **difficult to detect** using traditional security tools

**🛑 2. Why Are Insider Threats Hard to Detect?**

* Unlike external threats, insiders already have:
  + **Network access**
  + **Permissions and privileges** to do damage
* Security systems typically trust authenticated users, making **malicious insiders** hard to spot unless unusual behavior is observed.

**🔍 3. Detecting Insider Threats**

* Best detection method is through **active observation and a security-aware culture**.
* Encourage employees to:
  + **Monitor each other’s actions**
  + Ask questions like:

“Hey, why are you downloading 10GB of files at 2 a.m.?”

* This raises awareness of behaviors that don’t align with **normal business needs**.

**🚩 4. Behavioral Indicators**

* Warning signs may include:
  + Open **discontent with the company**
  + Verbal threats or wishing harm on the organization
  + Disgruntled attitude or desire for revenge
* If a person expresses anger or intent to hurt the company:
  + They should be **carefully offboarded**
  + Their network access must be revoked immediately

**🎬 5. Pop Culture Example: Jurassic Park**

* The movie offers a fictional but useful insider threat example:
  + A **disgruntled IT admin** creates a **logic bomb** in the system
* **Logic bomb** = a type of malware that:
  + Executes based on a **trigger** (like a time or event)
  + In this case: a **script** runs daily to check for an input code
* If no code is entered (e.g., employee is absent or leaves):
  + The system **automatically releases dinosaurs** by opening cage doors
  + Spoiler: The admin is killed, the system fails, and chaos follows
* This logic bomb was meant to **punish the organization** after the employee left.

**💣 6. Logic Bombs Explained**

* A logic bomb is malicious code designed to:
  + Activate under certain conditions (e.g., on a specific **date** or after a **missed input**)
  + Cause intentional damage (e.g., delete files, leak data, or shut down systems)
* Real-world logic bomb examples may:
  + **Wipe a hard drive**
  + **Encrypt data (ransomware style)**
  + **Leak sensitive files to public sources** (e.g., WikiLeaks)

**🧾 7. Summary Table – Insider Threat vs Logic Bomb**

| **Concept** | **Definition** |
| --- | --- |
| Insider Threat | A person with legitimate access who misuses it for sabotage or data theft |
| Logic Bomb | Malicious code triggered by a time or event to cause disruption or destruction |
| Disgruntled Employee | A common insider threat profile — may deploy logic bombs or steal data |
| Detection Strategy | Culture of questioning unusual behavior, monitoring login activity |
| Prevention | Least privilege, auditing, access revocation at termination |

**📘 8. CompTIA A+ 220-1102 Exam Relevance**

✅ **Yes – Insider threats and logic bombs are directly included in Objective 2.5.**

You must be able to:

* Recognize behaviors and risks of insider threats
* Understand what a logic bomb is and how it operates
* Know methods to detect, mitigate, and prevent insider misuse