1. Network-Based Intrusions (e.g., DDoS, MitM, DNS spoofing)
2. Application-Level Intrusions (e.g., SQL Injection, XSS, RCE)
3. Endpoint-Based Intrusions (e.g., malware, keyloggers, exploiting outdated OS)
4. Social Engineering Intrusions (e.g., phishing, pretexting, baiting)
5. Insider Threats (e.g., data theft by employees, accidental leaks)
6. Supply Chain and Third-Party Intrusions (e.g., SolarWinds supply chain attack)
7. Physical Intrusions (e.g., theft of servers, unauthorized physical entry)

Section 2: Comparison of Internal vs. External Breaches

This section compares internal and external breaches, highlighting their characteristics, motivations, and difficulty of detection. External breaches are typically opportunistic, financially motivated, or state-sponsored, while internal breaches are often intentional (malicious) or accidental (negligent).