OSINT ATTACK CHAIN

1. Discovery

Passive observation begins: social media profiles, company websites, domain registrations, and people search engines reveal initial data.

2. Correlation

Attacker connects public data points: email reuse, usernames, photos, or family connections.

3. Profiling

An operational picture of the target emerges: lifestyle habits, travel patterns, digital behaviors, and routines.

4. Access Pathways

Vulnerabilities are identified: exposed credentials, unsecured apps, physical address, or linked metadata.

5. Exploitation

The adversary uses the discovered exposure: phishing, impersonation, blackmail, physical surveillance, or data compromise.

6. Sustained Access

Persistence is established through malware, impersonation, or recurring data collection via unmonitored channels.