Syntho Quest

PHYSICAL SECURITY VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Scope: Assess physical security of facilities (office, data center, branch, labs): perimeter, access control, doors/gates, locks, CCTV, alarms, badge systems, visitor processes, supply-chain deliveries, staff/social engineering, and secure areas (server rooms, comms closets).

Goal: Identify real-world vulnerabilities that enable unauthorized access, theft, sabotage or data exposure; produce prioritized fixes and retest plan.

Core focus areas (must test)

- Perimeter & approach: fencing, lighting, signage, blind spots, vehicle access controls.
- Physical access controls: door locks, magnetic locks, turnstiles, mantraps, badge readers, tailgating risk.
- CCTV & monitoring: camera coverage, blind spots, camera tamper risk, recording retention, remote access.
- Alarms & sensors: intrusion detection, door contacts, motion sensors, alarm response process.
- Reception & visitor processes: ID checks, escort procedures, badge issuance & return.
- Portable device & media security: laptop docking, unattended devices, printing/printing trays, shred bins.
- Lock picking & physical bypass: weak locks, emergency exits, server rack locks, cable entry points.
- Power & environmental controls: UPS, generator access, HVAC controls, fire suppression access.
- Supply chain & maintenance: contractor access, third-party vendors, delivery handling.
- Social engineering & staff behavior: spear-phishing, vishing, tailgating, dumpster diving.

Business Associate: vivek
Email: contact@synthoquest.com
Mobile: +91-8333801638 (whats app)