# Threat Model: Targeted Harassment of a Technical Individual

## ■ Victim Profile

• Autistic quant / fintech engineer
• Works on proprietary strategies, simulations, AI models
• Sensory sensitive — susceptible to intrusive noise/light/EM disruptions
• Often operates from a fixed workstation or lab space

## ■ Attacker Motives

| Threat Actor | Motive |
|---|---|
| Corporate competitor | Steal or suppress trading algorithms, slow down research |
| Cybercriminals | Extract intellectual property for profit |
| State-sponsored actor | Talent denial, behavioral study, disruption of financial infrastructure |
| Harasser / stalker | Psychological harm, coercion, nuisance interference |

## ■ Likely Tactics

| Vector | Examples |
|---|---|
| Cyber | Network probing, phishing, IoT compromise, IP theft |
| EM/Side-Channel | Power-line injection, low-level EM interference, TEMPEST-style snooping |
| Psychological | Noisy environments, light flicker harassment, triggering sensory overload |
| Social | Disinformation, recruitment attempts, reputation sabotage |

## ■ Countermeasures

| Layer | Defensive Measure |
|---|---|
| Physical | LED/coil randomizer to create noise floor for subtle EM interference |
| Network | Hardened VPN, firewall, zero-trust access |
| Behavioral | Scheduled breaks, social engineering awareness |
| Analytical | Logging environmental data (EMF meters, audio, light flicker) to correlate with symptoms/events |

This threat model frames the LED/coil jammer as a legitimate physical-layer cybersecurity control, similar to a firewall — but operating on the electromagnetic environment to reduce attack surface.