INFOSECTRAIN
Educate. Excel. Empower.

MOST BREACHES START WITH ACCESS NOT ATTACKS

No exploits *No advanced malware.* *Just exposure.*

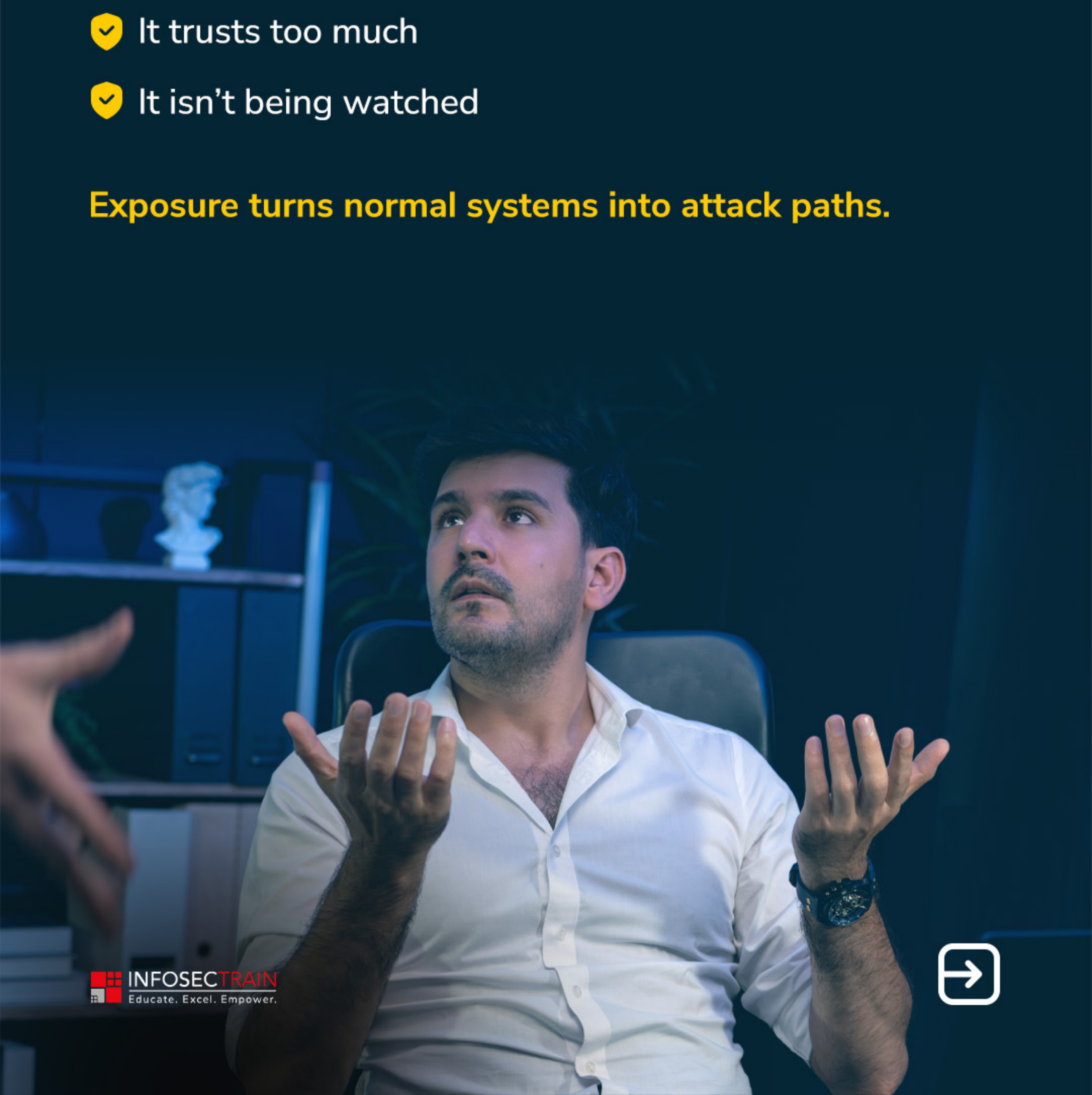
www.infosectrain.com

What Overexposed Really Means

A system is exposed when

- It’s reachable when it shouldn’t be
- It trusts too much
- It isn’t being watched

Exposure turns normal systems into attack paths.



Network & Internet Exposure

Where Exposure Starts

- Open ports
- Exposed APIs
- Public cloud storage

Anything public will be discovered.

INFOSECTRAIN
Educate. Excel. Empower.

Identity Exposure

Who Has More Access Than They Need

- Weak IAM policies
- Default or reused passwords
- Missing multi-factor authentication
- Excessive permissions

Identity is the new perimeter.

Maintenance Exposure

When Old Systems Stay Vulnerable

- Unpatched software
- Outdated TLS
- Unsupported components

Known weaknesses attract attackers.

INFOSECTRAIN
Educate. Excel. Empower.

Visibility Exposure

When No One Is Watching

- No logging
- Logs not reviewed
- Alerts ignored

Attacks last longer when visibility is missing.

INFOSECTRAIN
Educate. Excel. Empower.

Why This Leads to Breaches

From an Attacker’s View

- Easy access
- Low effort
- Low chance of detection

Misconfigurations reduce attacker risk.

INFOSECTRAIN
Educate. Excel. Empower.

Key Takeaway

Attackers don’t need zero-days
when environments are overexposed.

Reduce exposure, and breaches drop dramatically.

INFOSECTRAIN

Educate. Excel. Empower.