Our Mission

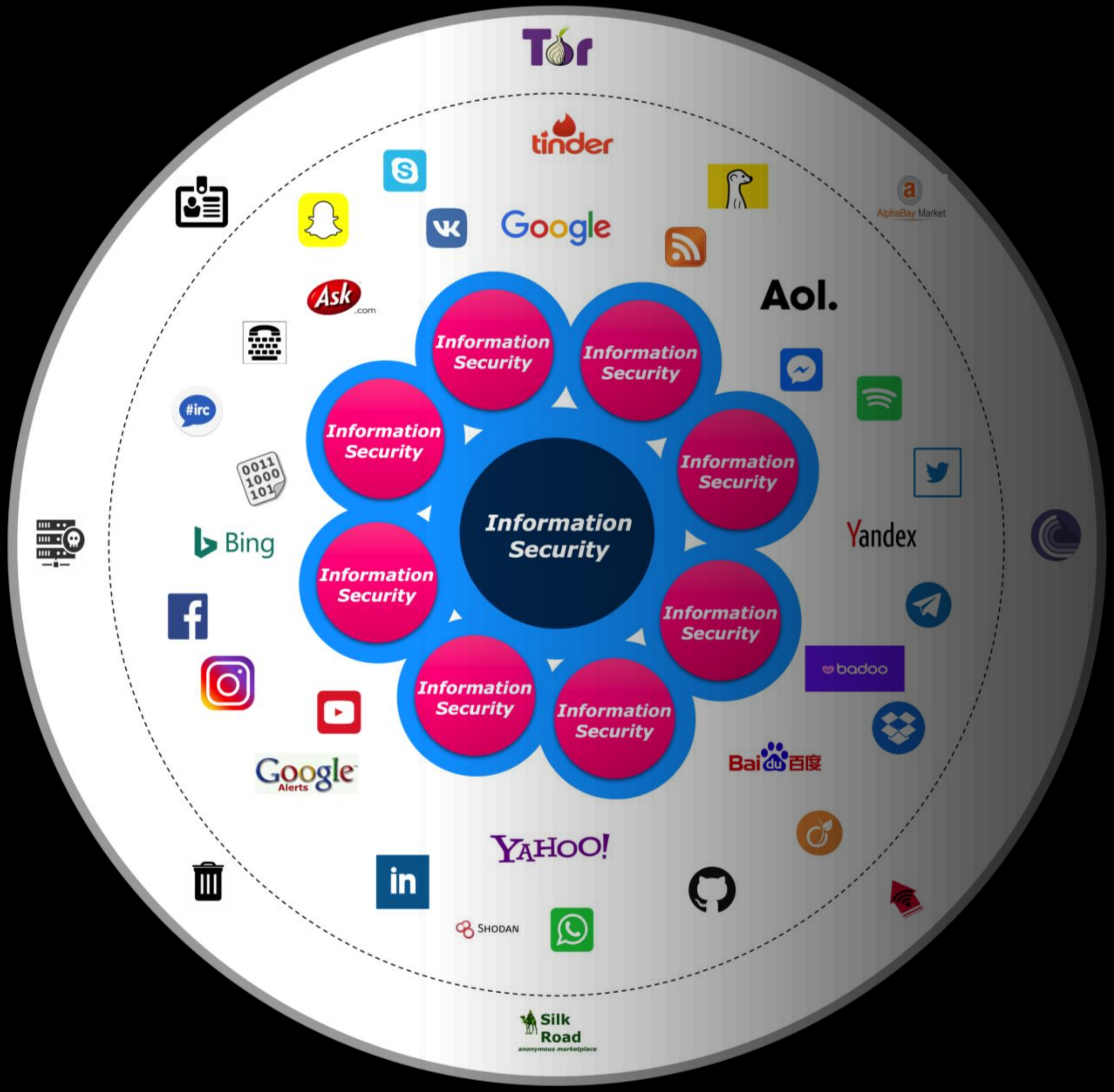
To introduce Digital Risk Intelligence as the link that makes Cyber Security an asset for Digital Transformation processes.

Cyber Security Trends

- Attack trends have changed, they are now increasingly **employee-centric**.
- Companies are "fortified" and therefore attackers seek easier and more profitable targets: **people**
- **90 %** of all security incidents **involve internal staff**
- A striking **89%** of security incidents are a **direct result** of **negligence** or **social engineering fraud**
- Incidents ratio increases **50% every 12 months**

What do we say?

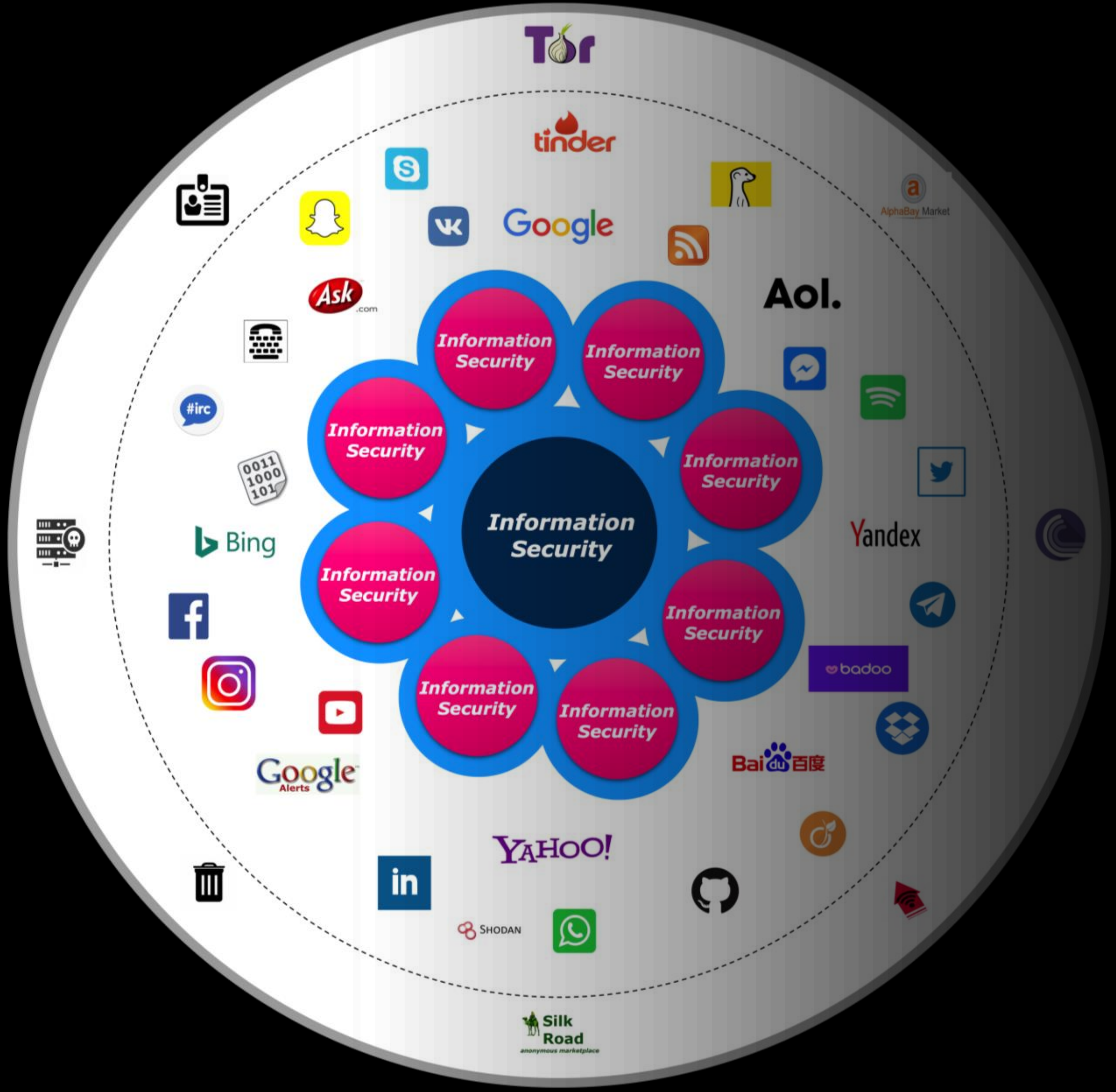
- **90** % of all security incidents **involve internal staff**
  - **Only 10% of all incidents are related to technology**
- A striking **89%** of security incidents are a **direct result** of **negligence** or **social engineering fraud**
  - **Only 11% of security incidents are "covered" by Traditional IT-Security or Information Security**



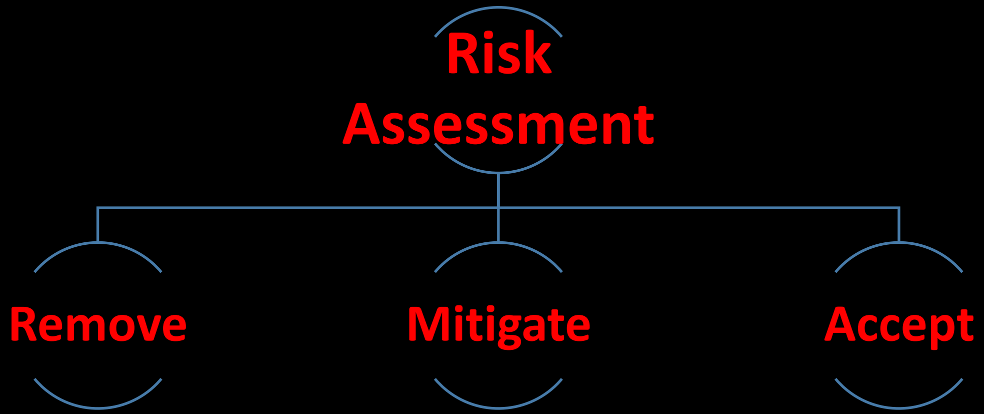
Digital Risk Landscape

Cyber Intelligence

MILAGRO
DIGITAL RISK INTELLIGENCE



Risk Based Security Work



MILAGRO
DIGITAL RISK INTELLIGENCE

Cyber Attacks Methodology

Looking for vulnerabilities

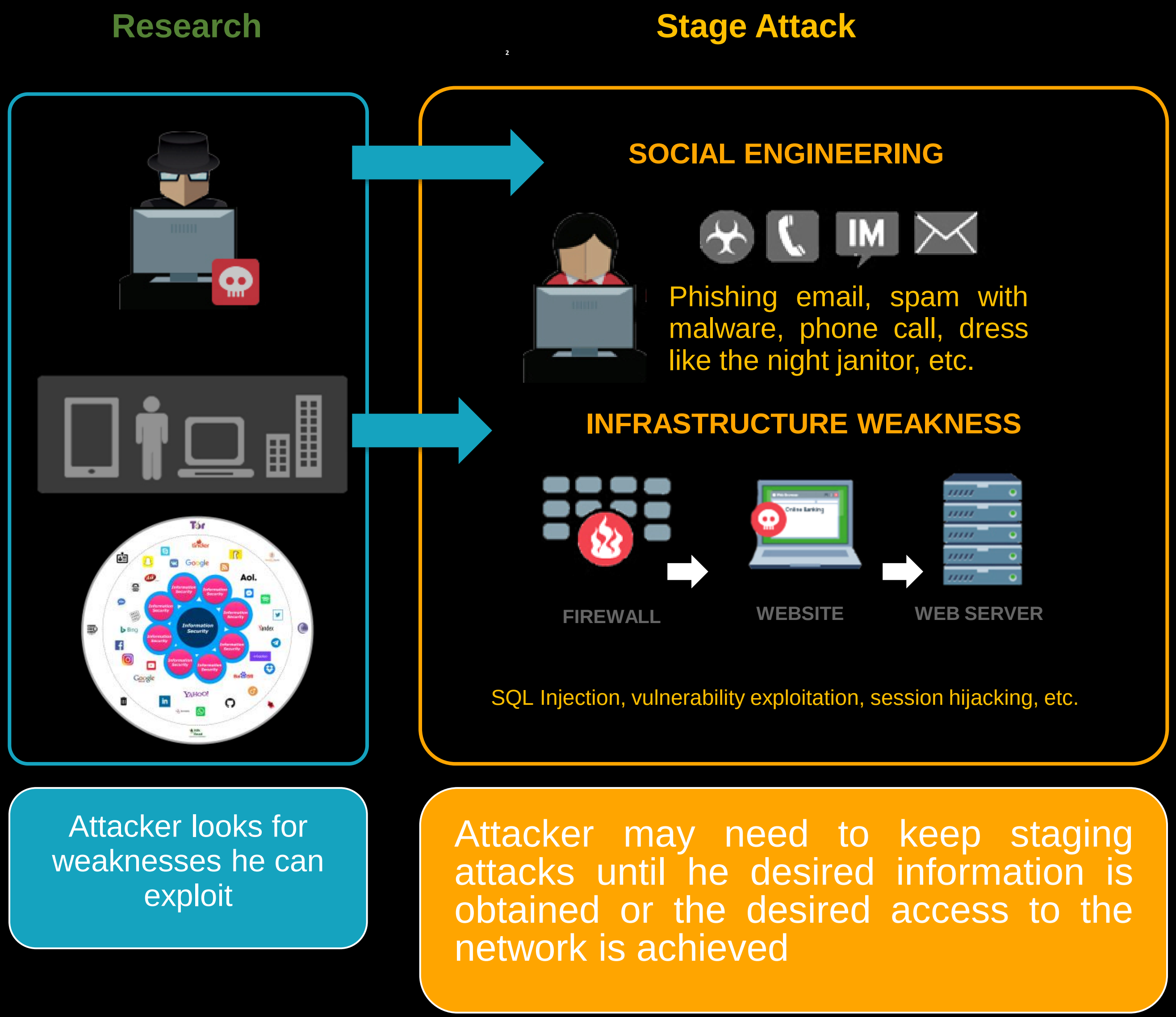
- From the outside-In

Analyzing Vulnerabilities

- Available exploits
- Easiest way In

Penetration Tactics

- Social Engineering: ex Phishing
  - Working from the inside
- Targeting Infrastructure
  - Vulnerabilities
  - Brutal Force



Research

Stage Attack

SOCIAL ENGINEERING

Phishing email, spam with malware, phone call, dress like the night janitor, etc.

INFRASTRUCTURE WEAKNESS

SQL Injection, vulnerability exploitation, session hijacking, etc.

Attacker looks for weaknesses he can exploit

Attacker may need to keep staging attacks until he desired information is obtained or the desired access to the network is achieved

MILAGRO

DIGITAL RISK INTELLIGENCE

Digital Transformation has changed the Security Landscape

The attack surface is bigger and outside the perimeter

MILAGRO
DIGITAL RISK INTELLIGENCE