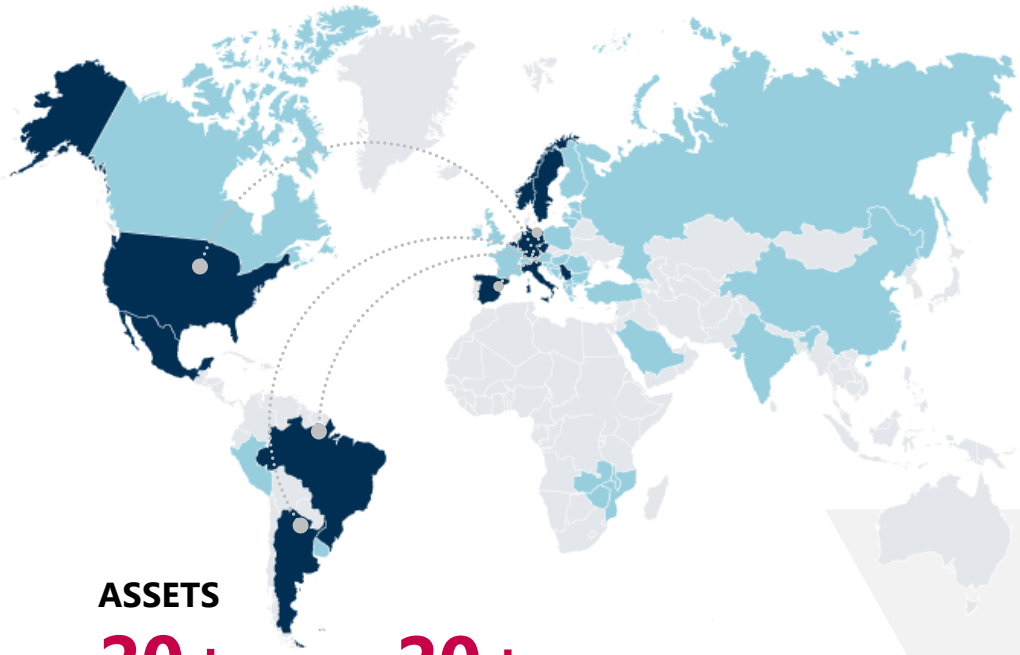
# Engineering Innovation

Where Business Meets Technology

# Our Mission

We help our **partners** achieve their **goals**,
**co-designing innovative solutions** and leveraging
the opportunities of a **continuous technology evolution**.
We help them **transform their Business**
based increasingly on **new core values**
and **digital ecosystems**.

# At a Glance



## A GLOBAL COMPANY

**12.000+**
Associates

**40+**
Offices around the world

**Global HQ**
Rome, Italy

**Worldwide**
Delivery

**Based in**
EUROPE, NORTH AMERICA, LATIN AMERICA

## RESEARCH & INNOVATION

**6**
Development labs

**70+**
Live Research Projects

**250+**
Innovators

**40 Mil €**
Investments

**450+**
Data Scientists & Researchers

## TRAINING

**IT & Management School «Enrico della Valle»**
Our own Academy

**150k**
Training hours

## ASSETS

**20+**
Companies within the Group

**20+**
Proprietary solutions for all market sectors

**10+**
Cross-BU Competence Centers

**16k+**
Projects in 2019

**4** Data Centers

**20 petabyte**
Data Handled

**22.000**
Servers managed

**250.000**
Workplaces managed

**Tier IV**

## WHAT WE DO

**€ 1,274 Bn** FY19

**40+ YEARS** OF CONTINUOUS GROWTH

The World **We Live In**

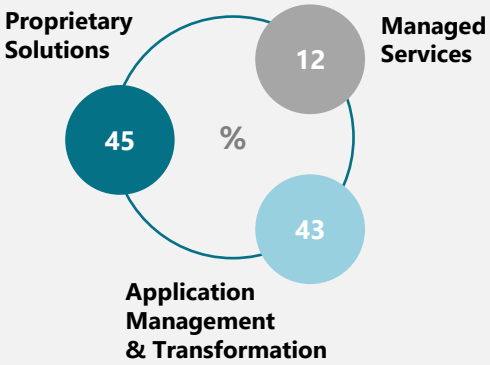
- Smart Energy & Utilities
- Digital Media & Communication
- Augmented City
- Smart Transportation

The World **We Work In**

- Digital Finance
- Digital Industry
- Digital Retail & Fashion
- Smart Agriculture

The World **That Looks After Us**

- Smart Government
- E-Health
- Digital Defense, Aerospace & Homeland Security



# Our Approach

## Explore & Upskill
Research & Innovation
IT & Management Academy
M&A & Startup Observatory

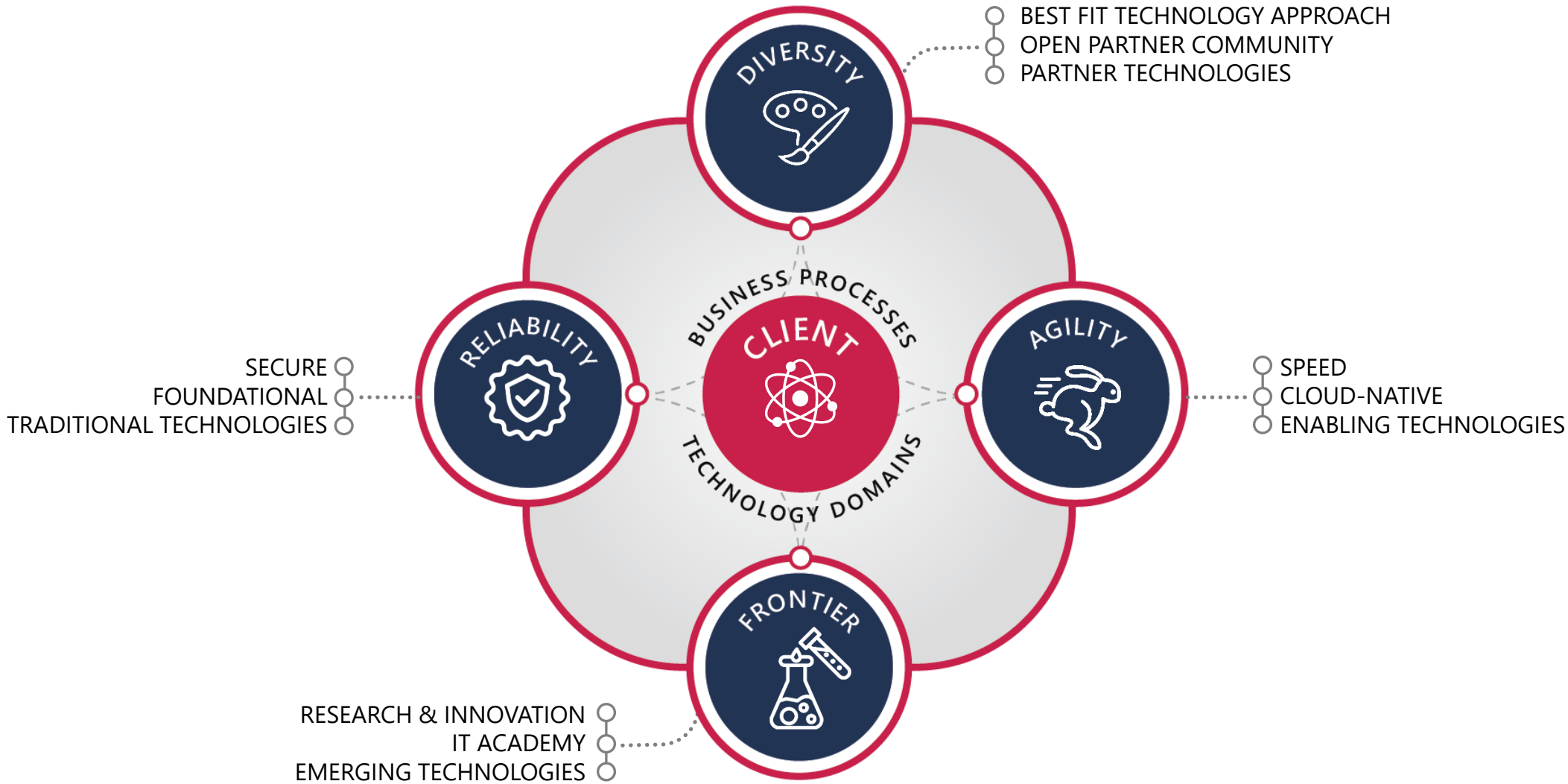
## Strategy & Design
Business Consulting
Processes & Services Redesign
UX & Usability/Accessibility

## Implement & Integrate
Traditional & Enabling Technologies
Proprietary & Partner Solutions
Project Management

## Manage & Evolve
Application Management & Transformation
Managed Services
Digital Workplace

© Engineering

# Our Value Proposition




© Engineering

# Enabling Technologies

**AI & Advanced Analytics**

**Intelligent Automation** (RPA)

**Internet of Things**

**AR / MR / VR**

**Blockchain**

**Digital Twin**

**Cloud**

**Cybersecurity**

# Our Portfolio

## THE WORLD WE LIVE IN

- AUGMENTED CITY
- SMART ENERGY & UTILITIES
- SMART TRANSPORTATION
- DIGITAL MEDIA & COMMUNICATION

## THE WORLD WE WORK IN

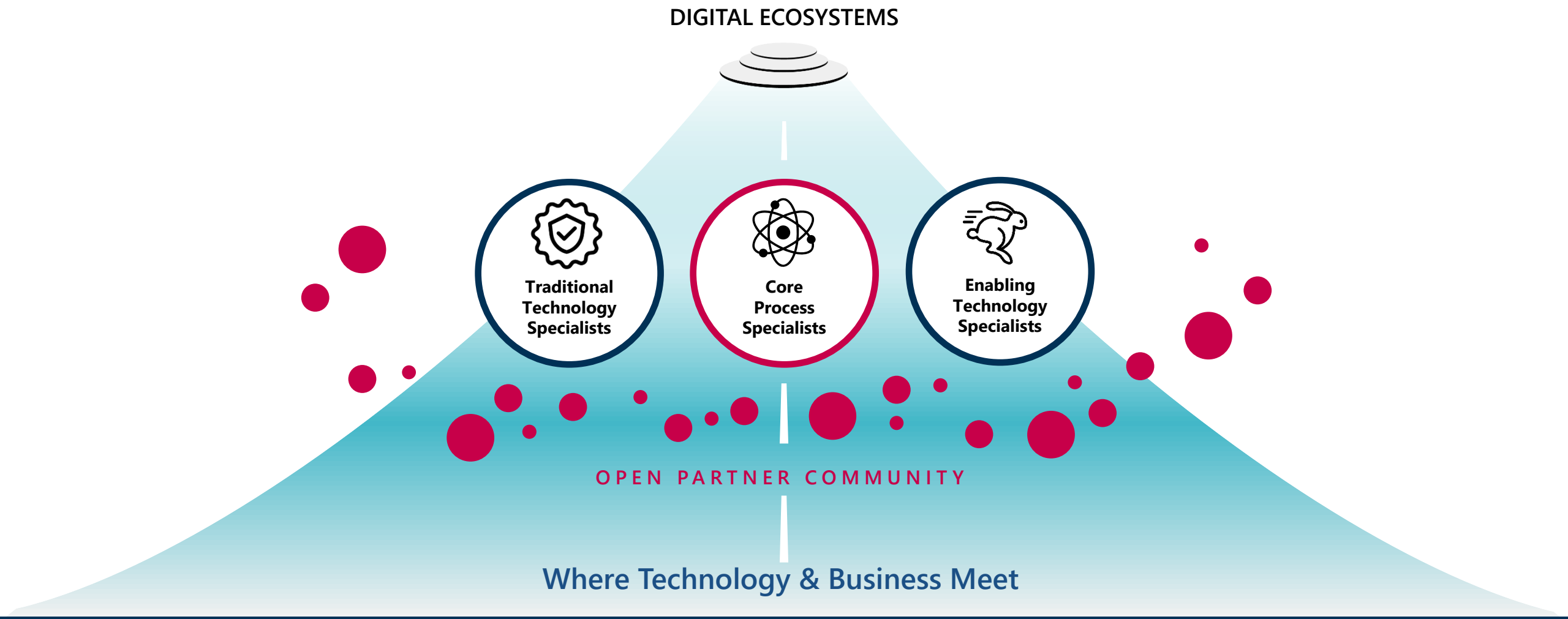
- DIGITAL INDUSTRY
- DIGITAL FINANCE
- DIGITAL RETAIL & FASHION
- SMART AGRICULTURE

## THE WORLD THAT LOOKS AFTER US

- SMART GOVERNMENT
- E-HEALTH
- DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

© Engineering

# Enabling Digital Transformation




**ENABLING TECHNOLOGIES**

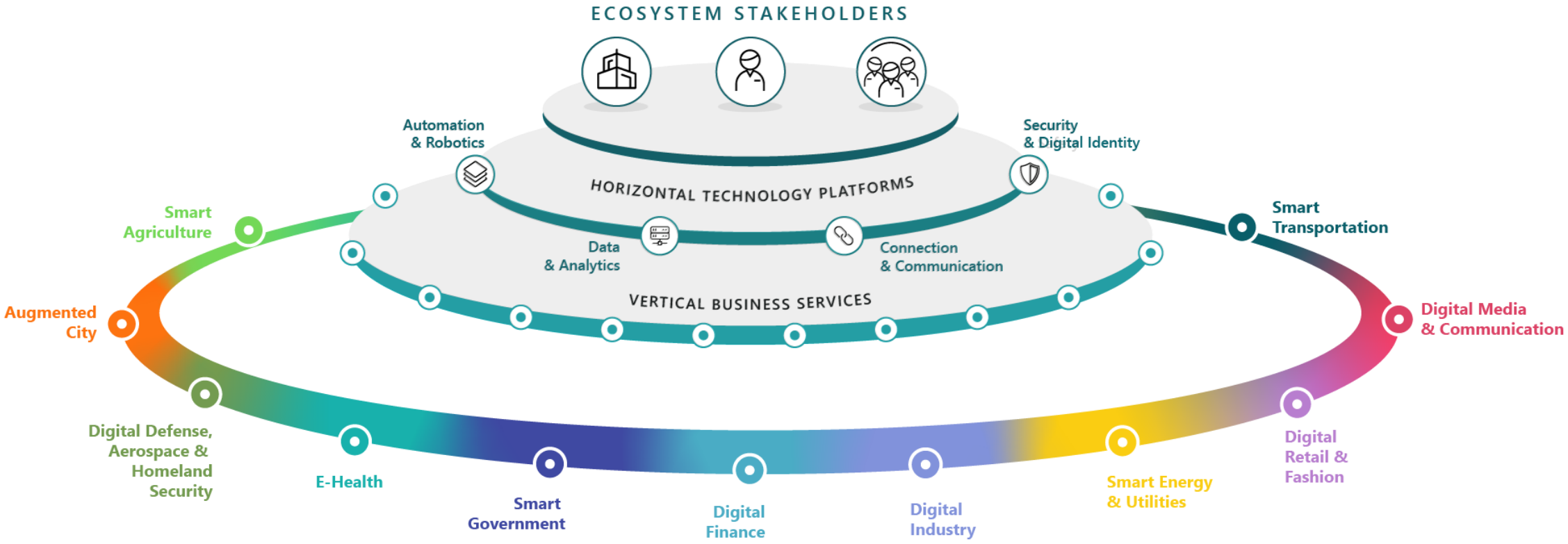
AI & Advanced Analytics | Cloud | Cybersecurity | IoT | Intelligent Automation (RPA) | AR / MR / VR | Blockchain | Digital Twin

CONTINUOUS RESEARCH AND INNOVATION ON EMERGING TECHNOLOGIES

CONTINUOUS UPSKILLING AND TRAINING IT ACADEMY

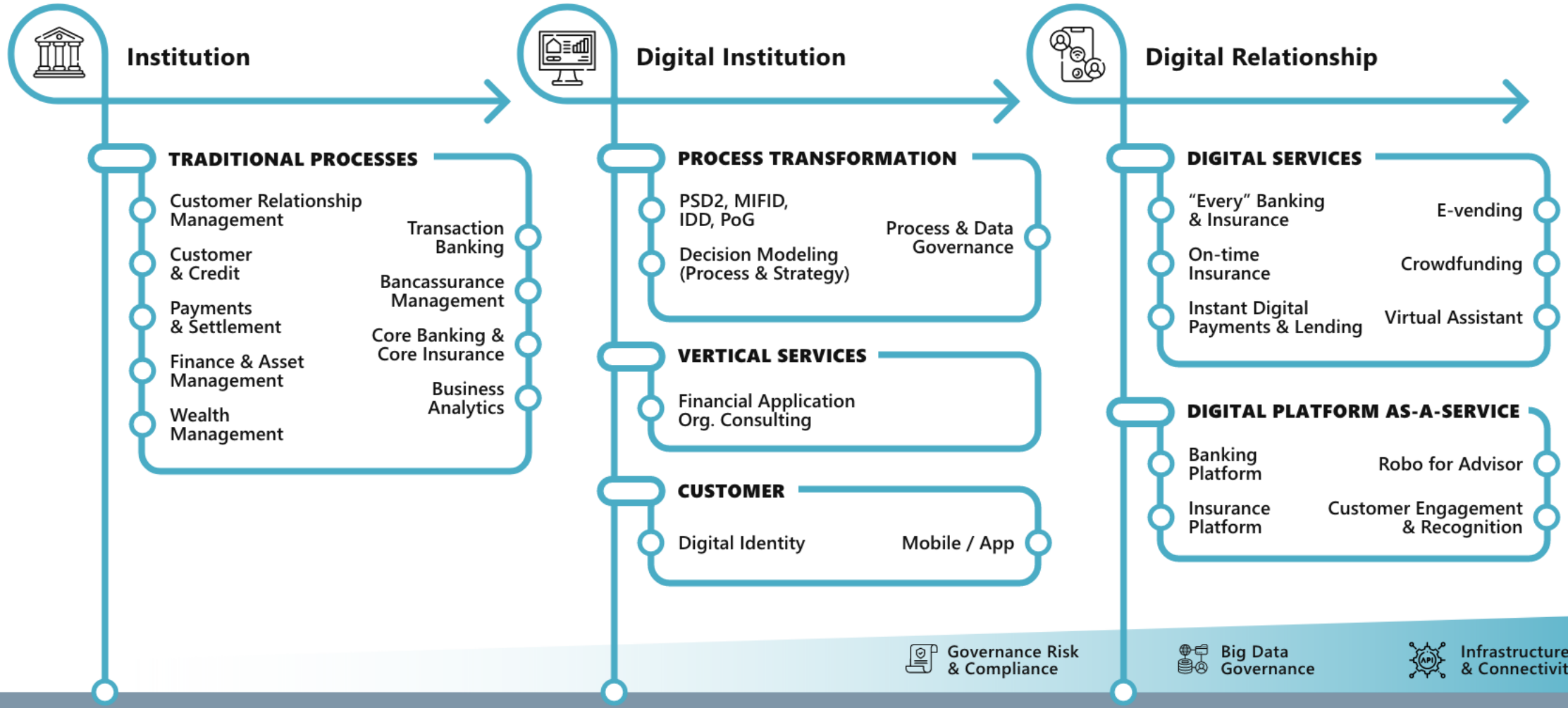
STARTUP AND INCUBATOR LABS

# Composing solutions to enable digital ecosystems




© Engineering

# Digital Finance



ENABLING TECHNOLOGIES

# Cybersecurity

## WHAT

The collection of **skills, structures, processes, technologies** used to **protect Data, Applications and Infrastructures** from unauthorized access, damage or attacks.

## HOW

- **Governing digital identities** (regulations, risks)
- **Blocking cyber attacks** (detection, intervention)
- **Safeguarding data** (cloud, assets)

## WHY

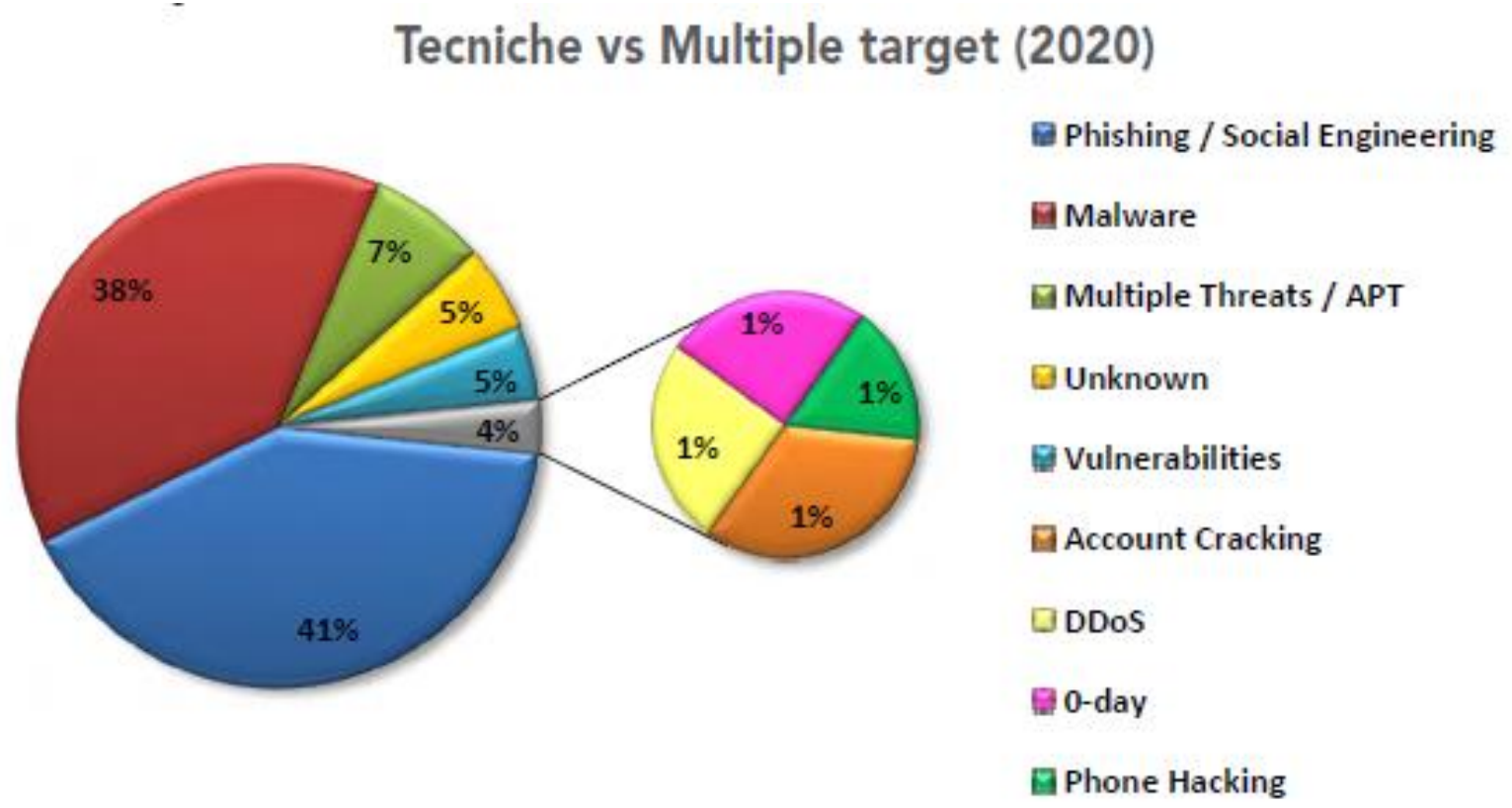
The **exponential growth** in **data quantity and value** increases the importance of adopting **cyber technologies**, methodologies, skills and IT security to protect company assets and data from the risk of attacks.

## WHERE

- We are **our first customers** of our Cybersecurity services
- We provide **IT security services** for IT applications, systems, networks, and managed services to detect cyber threats and deal with them, also through **our SOC**, adopting dedicated **policies / techniques**
- We provide hosting for **22,000 servers** at our **4 data centers,** protecting **+20 PB of data**, managing **+43.2B events** and intercepting +123B known vulnerabilities each day
- We support **large organizations**, both public and private, operating in global scenarios

## HOW IT WILL EVOLVE

- Automation and AI will **increase the usability** of threat information
- The **spread of IoT sensors** will require stronger methods of data protection, authentication, validation
- **Centralized platforms** to provide services to users
- Greater **awareness** of companies
- Greater **dependence** on virtual space

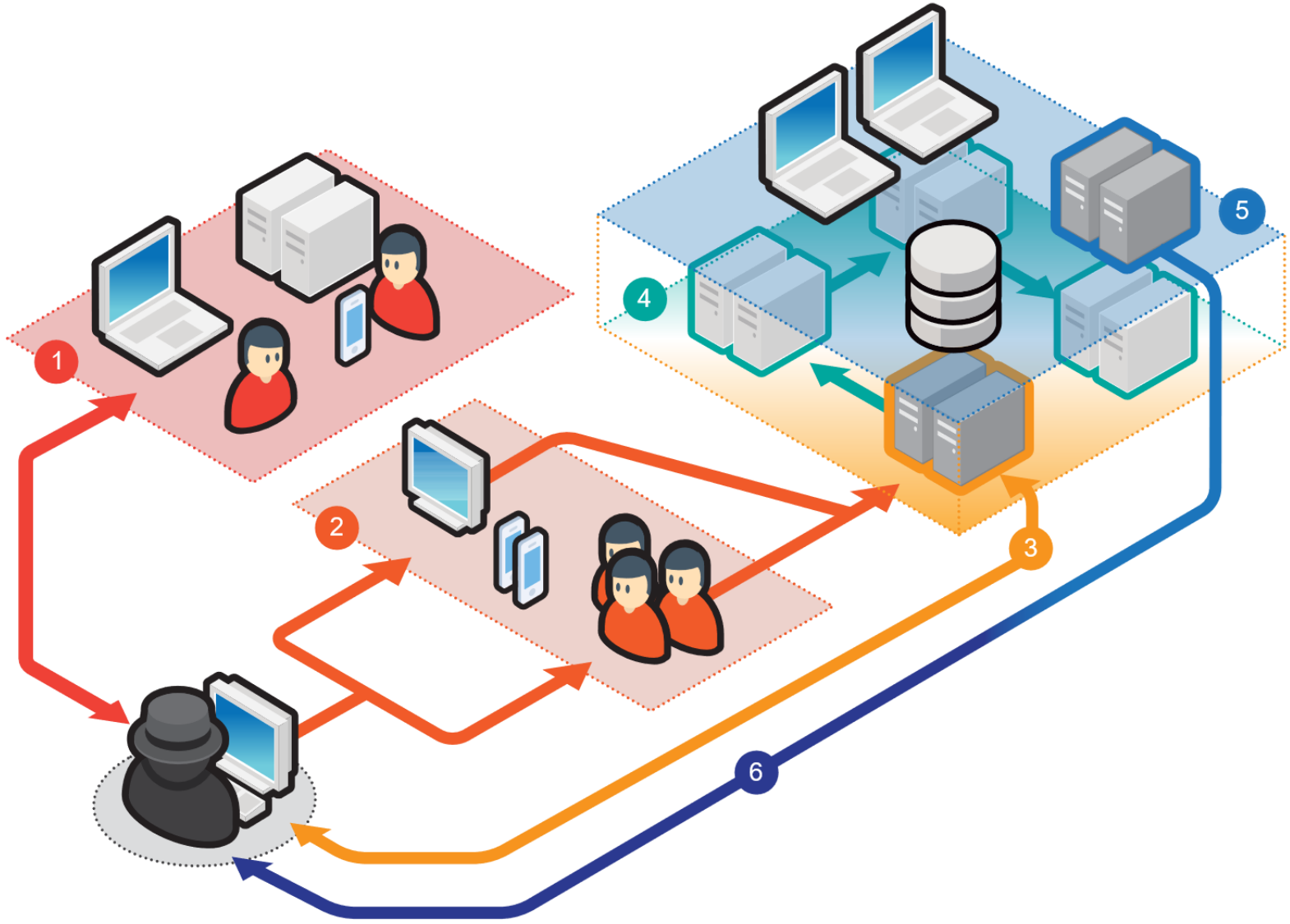



# Tecniche su Multi Target

© Engineering

# RISK-BASED APPROACH

1. INTELLIGENCE GATHERING
2. POINT OF ENTRY
3. C&C COMMUNICATION
4. LATERAL MOVEMENT
5. ASSET DISCOVERY
6. DATA EXFILTRATION




© Engineering

# Phishing – Quali sono i rischi



## Settore Finance: l'obiettivo preferito dagli hacker

Il settore **Finance** continua ad essere un **obiettivo sensibile** per gli hacker di tutto il mondo: negli ultimi 7 anni, infatti, questo settore è risultato per 6 volte **il più attaccato**. Nel **2020**, le imprese dei settori Finance e Technology hanno subito da sole il **17%** di tutti gli attacchi*.

## Attacchi Web: phishing e furto di credenziali

Il **43%*** delle attività criminali, contro i settori più colpiti dell'area EMEA, proviene da **attacchi via web**

Il **75%** degli attacchi contro obbiettivi dell'**area EMEA** hanno avuto **origine** all'interno della stessa area

Il **73%** di tutte le attività ostili rientra in quattro categorie: **attacchi via web, reconnaissance, servizi specifici e attacchi brute-force**

## ***Cyber-Threats*: un'evoluzione continua**

In un contesto tecnologico sempre più interconnesso, le **minacce** e le **tecniche di attacco** sono in **continua evoluzione**. Diventa quindi fondamentale che ogni tipo di business sia costantemente aggiornato in termini di ***cybersecurity***. Ad oggi, l'**83%**** dei business affonda, o riesce a malapena a stare a galla, di fronte all'ondata crescente delle ***minacce cyber***.

© Engineering

# AUTENTICAZIONE ADATTIVA

La protezione contro questo tipo di truffa è sempre lo stesso: **quando viene chiesto di fare un'operazione "anomala", bisogna fare un passaggio di verifica in più**. È quella che si chiama "**autenticazione adattiva**", che già vediamo utilizzata dai servizi online più evoluti. Viene identificato un comportamento "normale", che richiede un'autenticazione semplice; quando viene richiesta un'operazione anomala, che sia per il tipo di operazione, la sua rischiosità, ma anche l'area geografica o il dispositivo da cui viene richiesta, allora si passa ad esempio ad un'autenticazione più forte, o si richiede una verifica telefonicamente, o comunque si fa un ulteriore passaggio di validazione della richiesta che ha anche il risultato di "allertare" la potenziale vittima del fatto che qualcosa stia succedendo, nel caso non fosse lui l'autore dell'operazione.

© Engineering

# Overview Percorso Cyberculture

**Modulo**
***Cybersecurity Health check***

Verificare il livello di conoscenza dei dipendenti sulla sicurezza delle informazioni e il grado di resilienza rispetto alle minacce phishing, delineando le priorità di intervento per rafforzare la Cybersecurity Culture

1

**Modulo**
***Cybersecurity Awareness***

Trasformare gli utenti in protagonisti attivi e consapevoli della Cybersecurity, facendo conoscere loro i rischi più comuni, promuovendo l'attitudine a comportarsi in modo prudente

2

**Modulo**
***Cybersecurity Training***

Consolidare il livello di conoscenza delle tematiche di sicurezza mediante attività di formazione erogabili al Top Management, al Line Management e a tutti i dipendenti aziendali

3

© Engineering

# Modulo 1:
## *Cybersecurity Health check*

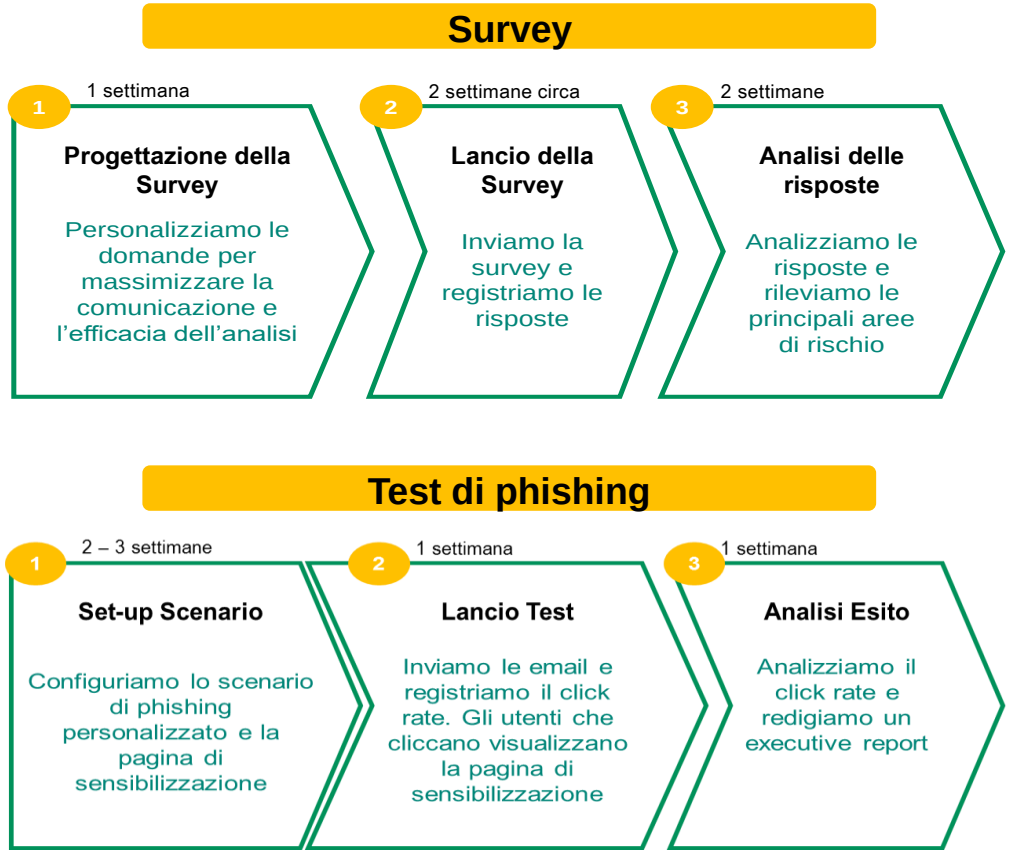
**OBIETTIVO**: verifichiamo il livello di conoscenza da parte dei dipendenti sulla sicurezza, al fine di delineare le priorità di intervento volte a rafforzare la Cybersecurity Culture

- **La Survey** indaga **le abitudini e i comportamenti** dei dipendenti, evidenziando i possibili **rischi di cybersecurity**, **attraverso poche domande** su temi, rispetto ai quali, **il fattore umano può fare la differenza:** es. password security, phishing.

  L'analisi delle risposte consente di costruire un **percorso personalizzato**, il cui obiettivo ultimo è **cambiare paradigma** costruendo insieme una **cultura di cybersecurity.**

- **Il test di phishing** consiste nell'invio di un'**e-mail simile a quelle utilizzate dai criminali informatici**. Un motore logico registra in forma anonima le reazioni degli utenti (es. il click sul link presente nell'e-mail).

  Oltre a verificare **il reale livello di consapevolezza** viene **erogato un contenuto formativo mirato**, **veloce e di forte impatto**, poiché associato all'azione rischiosa appena eseguita.




© Engineering

# Modulo 2:
## *Cybersecurity Awareness*

**OBIETTIVO:** creare consapevolezza, facendo conoscere le minacce ed i rischi più comuni di Cybersecurity, promuovendo l'attitudine a comportarsi in modo prudente

Il **programma "Cybersecurity awareness"** ha l'obiettivo di migliorare il livello di consapevolezza del personale.

Si compone delle seguenti iniziative:

- **Campionato Cybersecurity**: campionato finalizzato all'attività di training, svolto attraverso la sana competizione tra squadre
- **Digital Poster/Cartellonistica/ Gadget**: materiale distribuito nelle aree condivise (mense, aree ristoro, ascensori, aree stampa), per veicolare i messaggi chiave di sicurezza
- **Cybersecurity Space**: newsletter che affronta temi specifici di cybersecurity, pubblicabile ad esempio sulla intranet aziendale
- **Workshop:** eventi cybersecurity, in cui si affrontano argomenti e discussioni sulle principali tematiche in ambito, o sulle iniziative in programma da avviare o concluse

**Veicolare le informazioni attraverso semplici strumenti…**

Le iniziative del programma veicolano:

- informazioni di **riconoscimento**, che aiutano l'utente/lettore a riconoscere una situazione critica
- informazioni di **rischio**, che aiutano l'utente/lettore a valutare la criticità della situazione e dargli la giusta importanza
- informazioni di **comportamento**, che aiutano l'utente/lettore ad adottare comportamenti adeguati alla minaccia

**…con una comunicazione efficace**

Formati accattivanti

Contenuti fruibili ovunque


Linguaggio divulgativo

Metodologia efficace

© Engineering

# Modulo 3:
# *Cybersecurity Training*

**OBIETTIVO**: eleviamo e consolidiamo il livello di conoscenza delle tematiche di sicurezza mediante attività di formazione personalizzate ed erogabili a target mirati di popolazione aziendale

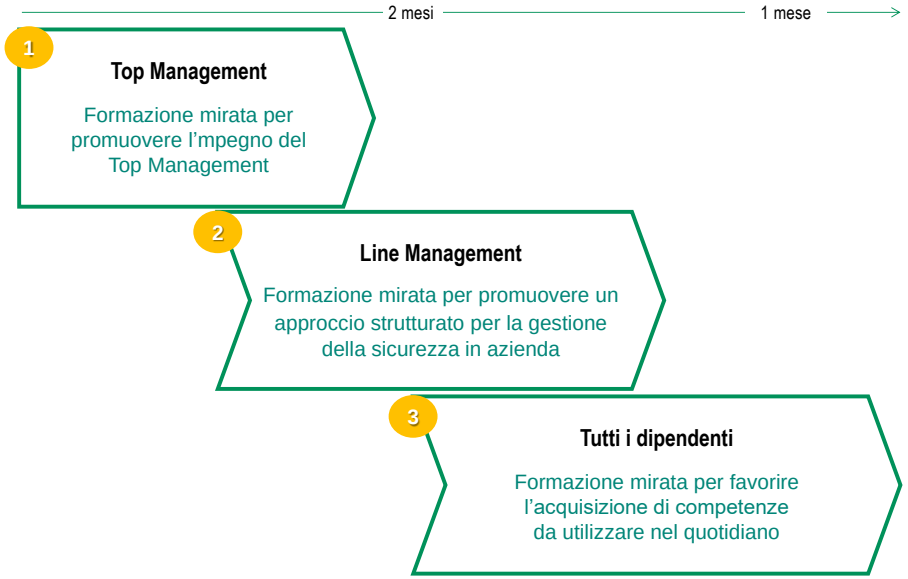
**L'attività di training** può essere erogata in modalità differenti, in funzione delle specifiche esigenze dell'organizzazione, ad esempio prevedendo sessioni in aula e/o moduli di e-learning.

Con riferimento al target di popolazione aziendale, è auspicabile un **approccio mirato e progressivamente inclusivo**, prevedendo moduli per il:

- **Top management**: il quale comprende che la cybersecurity ha una rilevanza business, promuovendo committment e una gestione strutturata della sicurezza in azienda
- **Line management**: il quale, beneficiando del committment del Top Management, diventa promotore e sostenitore della sicurezza in azienda
- **Tutti i dipendenti**: i quali, attraverso piani di formazione strutturati nel tempo, accrescono le loro conoscenze in materia, facilitando il contenimento degli incidenti di sicurezza

Briefing in piccoli gruppi

Esempi pratici e business case




© Engineering

# Cybersecurity

www.eng.it

Engineering Ingegneria Informatica SpA

@EngineeringSpa

LifeAtEngineering

gruppo.engineering