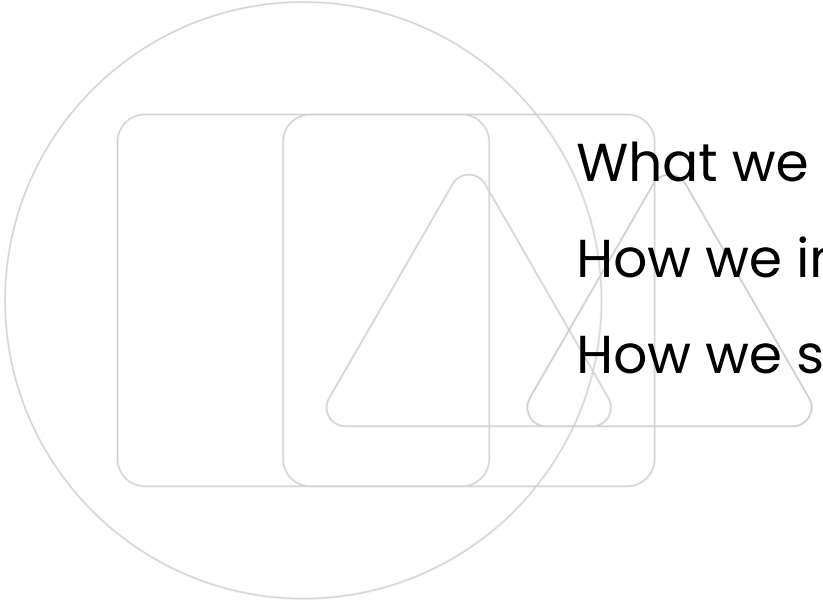
kirey group

Banche e Sicurezza 2021

# Machine Learning applicato alla Cybersecurity: la nuova generazione di tecnologie di Detection & Response

25-26 Maggio

kirey group



What we believe

How we innovate

How we secure

# What we believe

**Rendiamo**
**accessibile l'innovazione**
e trasformiamo il potenziale tecnologico
in valore economico.

# We shape your business

We are Kirey Group

kirey group

**Abilitiamo le aziende di tutto il mondo all'innovazione,
grazie alla nostra offerta integrata di consulenza e tecnologie.
Vogliamo essere protagonisti della rivoluzione digitale. Insieme.**



## System Integration

Diamo forma alle migliori soluzioni tecnologiche integrando le tecnologie della nostra IT Factory con le migliori disponibili sul mercato.

## Advising

Diamo forma alla collaborazione tra realtà diverse. I nostri esperti si uniscono al team dell'azienda creando un gruppo collaborativo. In questo modo abilitiamo le aziende ai nuovi modelli di business e progettiamo soluzioni ad alto valore tecnologico.

## R&D

Diamo forma in anticipo alle metodologie e tecnologie del futuro investendo costantemente nelle attività di Ricerca e Sviluppo, fondamentali Innovare e Rinnovare. Per questo abbiamo fondato Kubris®: Innovation Center dedicato alla progettazione, sviluppo e implementazione di soluzioni personalizzate basate sulle ultime tendenze tecnologiche.

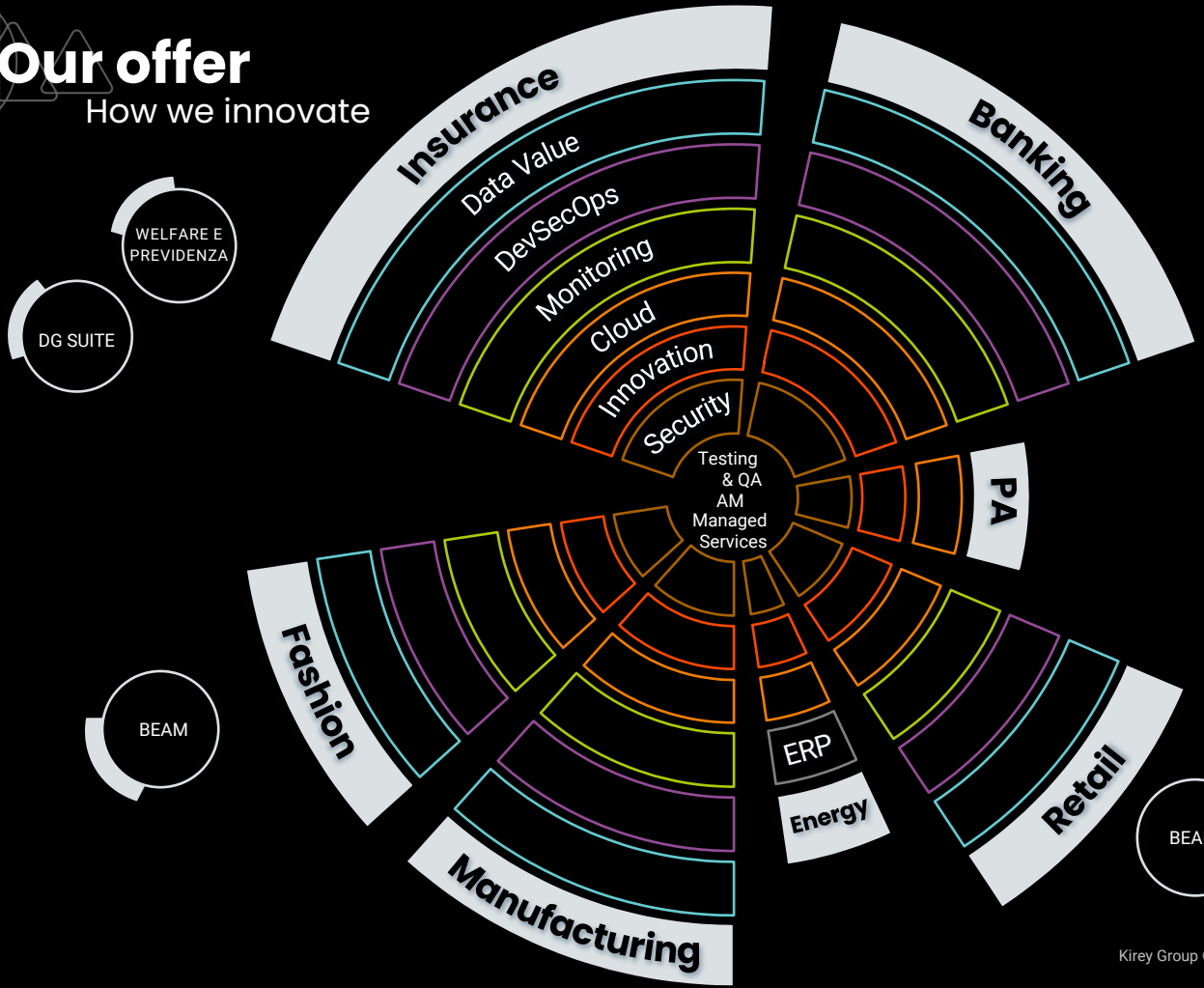
# How we innovate

**Abbiamo maturato competenze e sviluppato soluzioni** per aiutare le aziende a definire specifiche roadmap verso l'innovazione digitale

# Our offer

## How we innovate

kirey group




**SOLUTIONS**:

- DATA VALUE
- DEVSECOPS
- MONITORING
- CLOUD
- INNOVATION
- SECURITY

**SERVICES**:

TESTING & QA
APPLICATION
MAINTENANCE
MANAGED SERVICES

# La Cybersecurity ed il mondo delle Banche

## Le sfide da affrontare, quali sono i pericoli, chi sono gli attaccanti

kirey group

Il contesto odierno ci obbliga a confrontarci con le problematiche derivanti dalla sicurezza dei sistemi IT

### Le sfide

La **normativa**, la **disponibilità del servizio** (BC, DR), il **rischio reputazionale** (data breach) e le **compliance** a cui dover aderire alzano costantemente l'asticella degli sforzi indirizzati a migliorare la propria postura di sicurezza

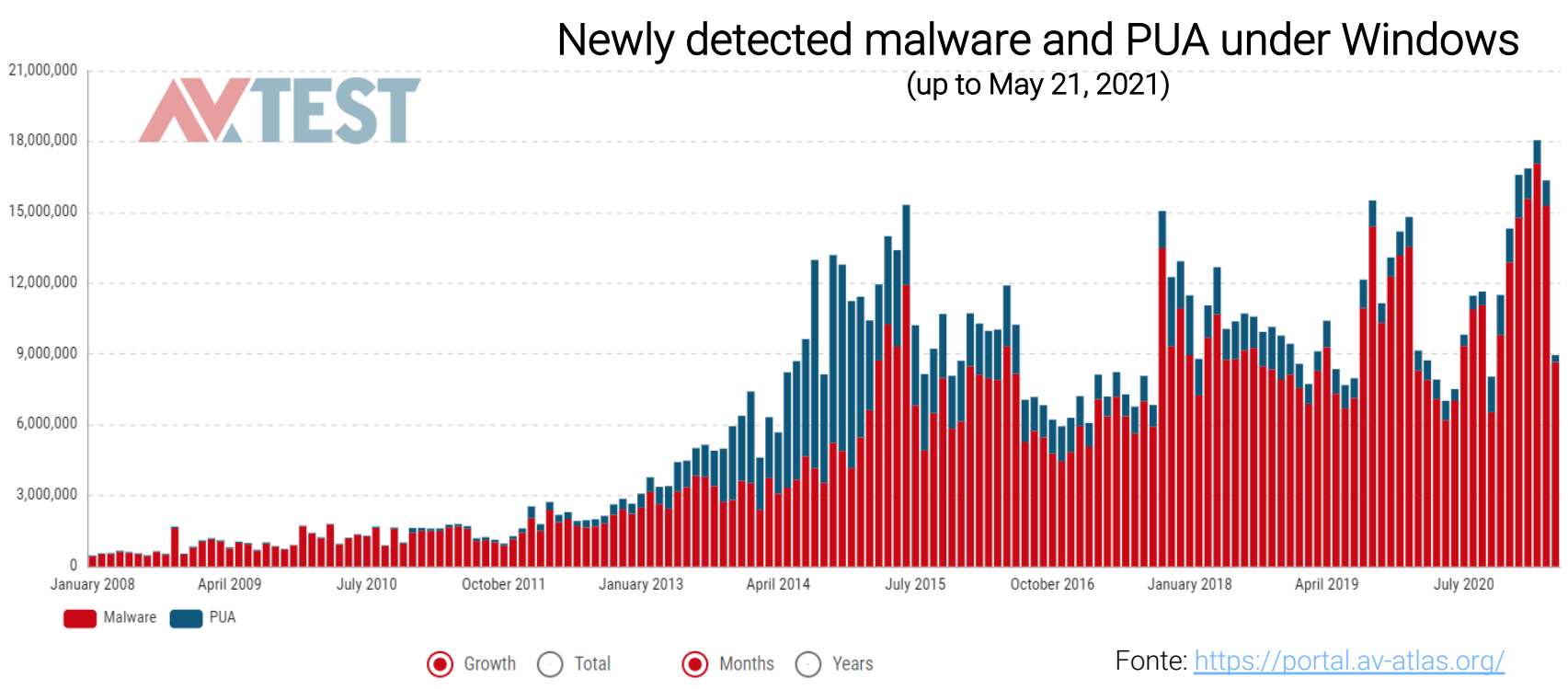
### I pericoli

Tutto il servizio ruota intorno all'infrastruttura IT. **Anche solo un componente debole** o progettato erroneamente può mettere in crisi l'intero sistema.
Anche i **processi** dell'organizzazione non possono prescindere dal tenere in considerazione il **rischio IT**

### Gli attaccanti

Non è più il ragazzo con la felpa col cappuccio (sempre che lo sia mai stato) ma **vere e proprie organizzazioni criminali** dotate di risorse e capacità d'investimento con lo scopo preciso di creare profitto (illecito)

# Malware: magnitudo e intensità




Fonte: https://portal.av-atlas.org/

# La superficie d'attacco: intensità

Dove oggi si concentra maggiormente il rischio

kirey group

## I sistemi esposti

L'accesso da Internet per i clienti (web, app) ai loro profili, le informazioni presenti sui sistemi, la possibilità di intervenire sui propri parametri. Le future integrazioni verso sistemi terzi (reporting, consolidation, integrazioni per M&A, ecc.).

## Le infrastrutture

La sicurezza dei sistemi che erogano i servizi è un punto nevralgico che può introdurre ulteriori rischi se non viene gestita con un processo adeguato di patch e change management. Come per i sistemi esposti, utilizzare ciclicamente servizi di Penetration Test aiuta a verificare lo stato generale della security delle proprie architetture.

## Il personale

La conoscenza da parte del personale dei possibili problemi di sicurezza e dei vettori d'attacco (phishing, social engineering, ecc.) è l'ulteriore difesa che è necessario mettere in campo. L'istruzione dei propri dipendenti e l'utilizzo di fornitori che hanno messo in atto un percorso di Awareness è un requisito chiave per aumentare la capacità di respingere gli attacchi più sofisticati.

# Come ridurre il rischio

Alcune possibili contromisure da adottare

kirey group

## Monitoraggio

- Implementazione di strumenti di controllo e di difesa dei propri sistemi AUTOMAZIONE!!
- Attività di verifica periodica (Vulnerability Assessment e Penetration Test)

## SOC

- Operatori in grado d'analizzare gli attacchi in corso e supportare le attività di contrasto
- Strumenti di correlazione che evidenzino anomalie comportamentali degli utenti e sui sistemi

## Servizi gestiti di sicurezza

- Fornitori con personale qualificato per la gestione e l'implementazione dei servizi
- Integrazione di strumenti per una migliore capacità d'intercettazione delle minacce

## Security Awareness

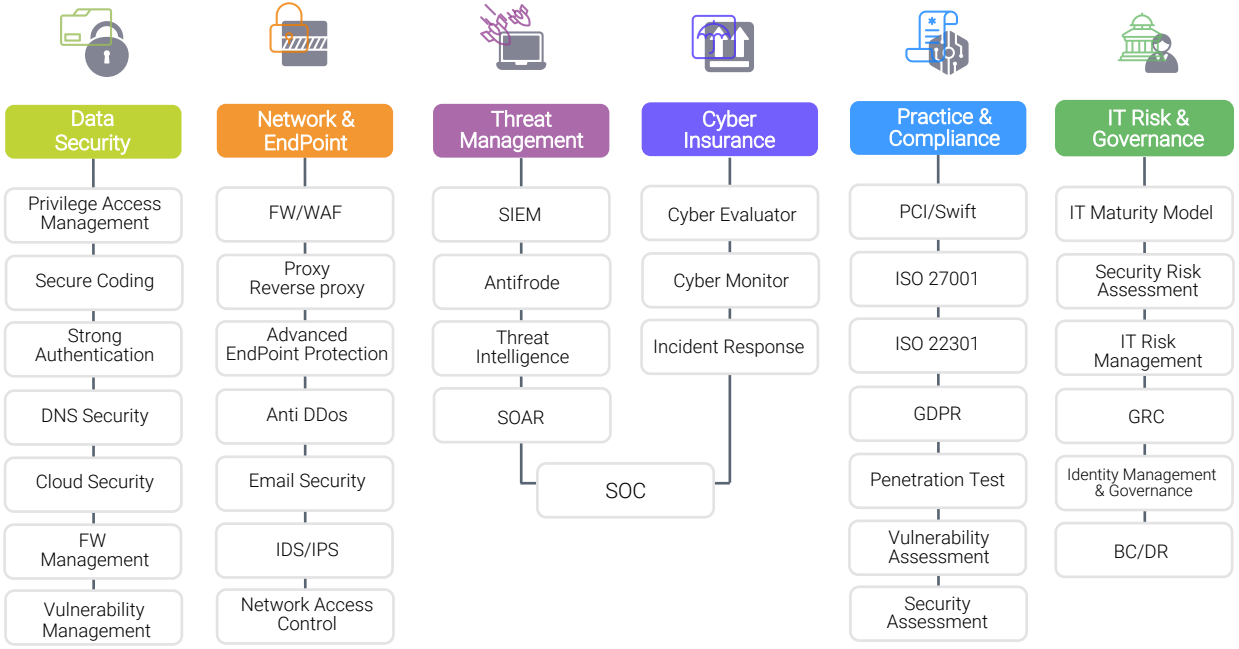
Formazione del proprio personale per minimizzare il rischio di attacchi basati su Social Engineering o Phishing ed in generale diffondere una cultura di base sui fondamentali della sicurezza informatica

# Security

## How we secure

kirey group

Un mondo **digitale** e **iperconnesso** porta ad attacchi informatici più intelligenti. Proponiamo l'adozione di una **prospettiva resiliente**: partendo dai processi e dall'infrastruttura espandiamo la diffusione della cultura del rischio a tutti i livelli dell'organizzazione. In questo modo è possibile concentrarsi sul business caratteristico e sulla mission aziendale.



# kirey group

## We Shape Your Business

www.kireygroup.com
info@kireygroup.com
57, Via Benigno Crespi
20159 Milan