

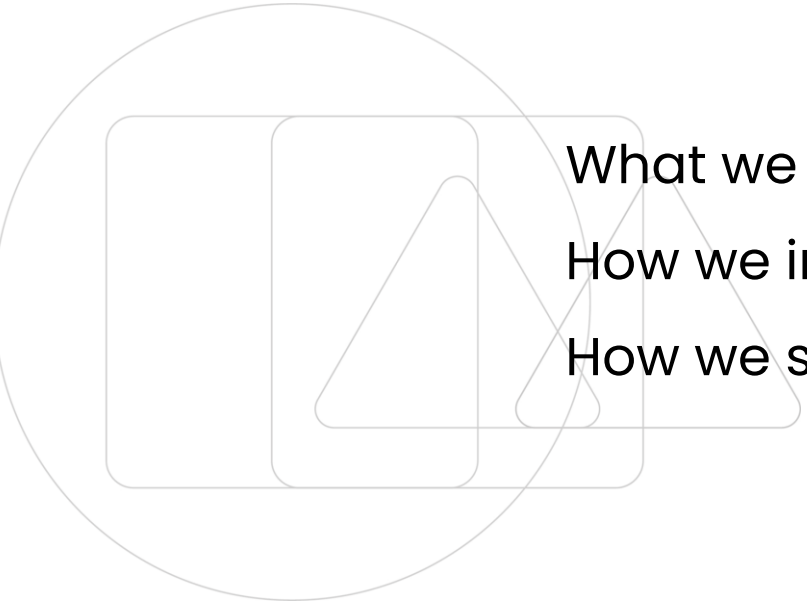


kirey group

GLI ENTI DEL WELFARE ALLA PROVA DEL CYBER RISK

Le sfide della Cybersecurity per i fondi pensione e gli enti del welfare

Martedì 18 maggio
Ore 11.10 – 11.30



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

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.

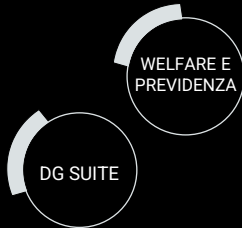
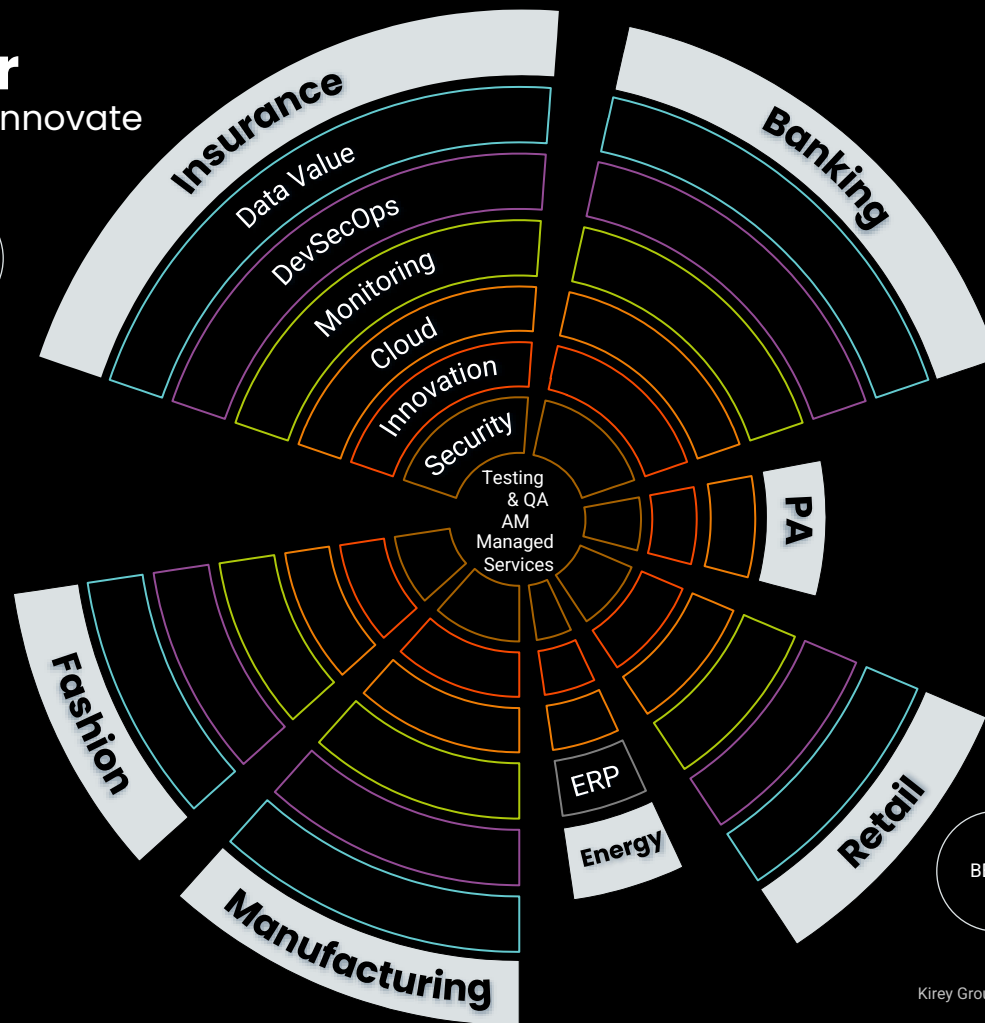
How we innovate

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



Our offer

How we innovate

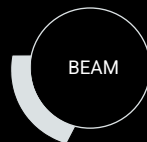


SOLUTIONS:

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

SERVICES:

- TESTING & QA
- APPLICATION
- MAINTENANCE
- MANAGED SERVICES



La Cybersecurity ed il mondo del Welfare

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

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

Major Security Events più recenti

Bloomberg the Company & Its Products

HOME MAIL NOTI

BR

yahoo!finanza

Home Finanza Il mio

REUTERS Reuters

Redazione
14 aprile 2021

f

Si parla di

Twitter

di Makiko
ven 14 maggio

Colonial Pipeline

Costco

BREAKING NEWS

Biden to speak on

Data Manager Online
il portale dell'ICT professionale

SOFTWARE ▼ HARDWARE ▼ WEB E SOCIAL MERCATO ▼ IT TOP100 WHITE PAPERS #WECHANGEIT

Home > Software > Sicurezza > Aumentati del 767% gli attacchi ransomware mirati rivolti a vittime di alto...

Software Sicurezza

Aumentati del 767% gli attacchi ransomware mirati rivolti a vittime di alto profilo

Di Redazione Data Manager Online - 26 Aprile 2021

Mi piace 0

Share

f

Twitter

P

WhatsApp

in

✉

Telegram

Colonial Pipeline



La superficie d'attacco

Dove oggi si concentra maggiormente il rischio



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



Monitoraggio

- Implementazione di strumenti di controllo e di difesa dei propri sistemi
- Attività di verifica periodica (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

Il modello vincente nello sviluppo applicativo

01 Prodotti

Soluzioni leader di mercato sia in ambito di sviluppo applicativo che in quello della sicurezza

Advising & Progetti 02

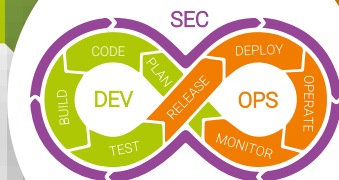
- Advising scelta della piattaforma e della sua integrazione nel contesto esistente
- Design e setup della piattaforma
- Formazione delle risorse del cliente

03 Service Operations

- MSS - Managed Security Services
- Sinergia con i servizi Ops

Supporto 04

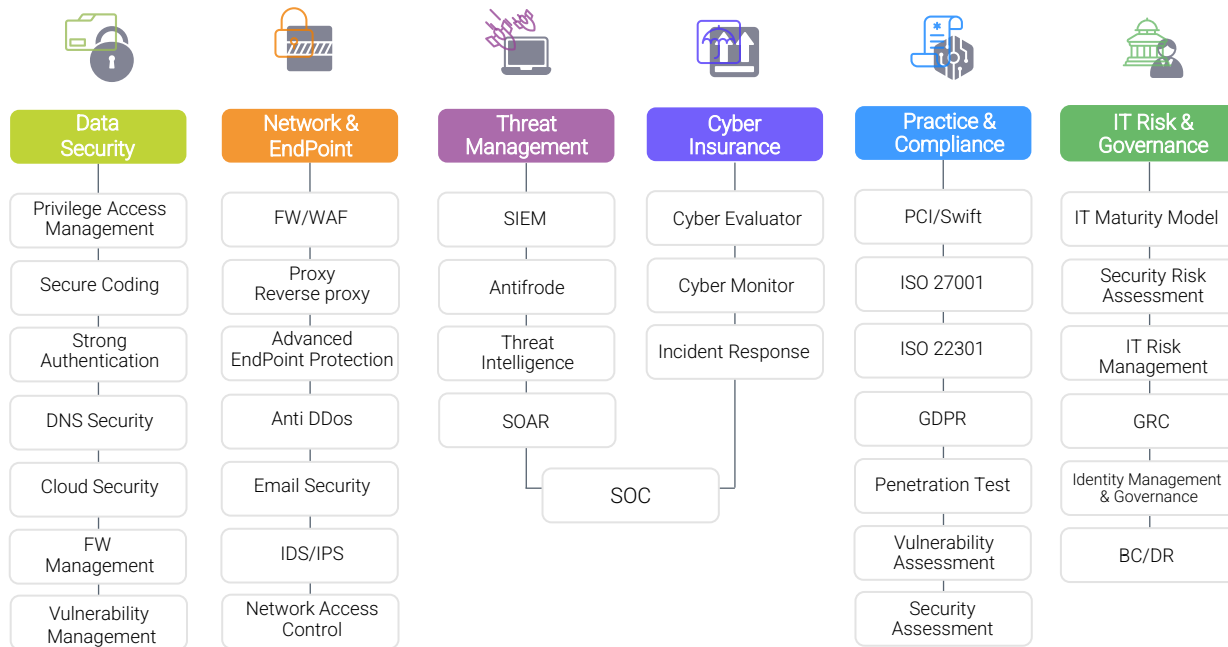
Security Engineer certificati dedicati alle richieste di supporto sulla tecnologia



Security

How we secure

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



La presentazione e le notizie sono a unico scopo informativo e solo per la circolazione privata, non devono essere riprodotte, ri-usate, pubblicate, copiate su supporti, pubblicate su siti o in altro modo senza il consenso scritto di Kirey Group o di sue società controllate. La presente non costituisce un'offerta per l'acquisto o la vendita di qualsiasi cosa in esso menzionata. Non intendono essere una descrizione completa delle condizioni o degli sviluppi riguardanti il materiale contenuto all'interno. Gli utilizzatori sono invitati a fruire delle informazioni a proprio rischio; non saremo responsabili per eventuali perdite dirette o indirette derivanti dal loro uso. A meno che non specificamente indicato, Kirey non è responsabile del contenuto di questa presentazione e/o delle opinioni dei presentatori. Situazioni individuali, pratiche e standard locali possono variare nel tempo.

