POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Osservatorio
Cybersecurity & Data Protection

Cybersecurity: don’t look up

Febbraio 2022

Osservatorio Cybersecurity & Data Protection

Ricerca 2021

PARTNER

accenture, Almaviva, Assolombarda, BlackBerry, CrowdStrike, Cybersel, ERMES Intelligent Web Protection, Horizon Security, Innovery Group Gold Business Partner IBM, Lutech, Microsoft, Minsait An Indra company, Posteitaliane, Rai, Reply Spike, TIM, Vargroup Platinum Business Partner IBM, vodafone business, WHITEJAR.IO Powered by Unguess, WIIT The Premium Cloud, Yarix a vargroup company

SPONSOR

blue is underwriting, Cyber Guru, Huawei, Thales, zscaler

SUPPORTER

aditinet secure, together, Cryptonet Labs

IN COLLABORAZIONE CON

Cefriel Politecnico di Milano, Politecnico Milano 1863 Dipartimento di Elettronica, Informazione e Bioingegneria

CON IL PATROCINIO DI

ANRA Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali, Assintel Associazione Nazionale Imprese ICT, Clusit Associazione Italiana per la Sicurezza Informatica

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Indice

Introduzione

Cybersecurity: don't look up

Guarda il video dell'evento su **osservatori.net**

Con la nuova normalità del lavoro, basata sullo smart working e sulla ricerca di un nuovo equilibrio nel delicato rapporto tra organizzazione e individui e nella società nel suo complesso, gli attacchi cyber non hanno conosciuto crisi e anzi si confermano in costante crescita, come evidenziano i dati del Rapporto Clusit che registrano 1.053 incidenti gravi nel primo semestre del 2021, con un +15% rispetto all'anno precedente.

Le organizzazioni, dalla loro parte, confermano un crescente interesse per le tematiche di cybersecurity, evidenziato da una spesa in aumento del 13% rispetto all'anno precedente, un ritmo di crescita mai così elevato negli ultimi anni, per un mercato che complessivamente vale 1,55 miliardi di euro.

Le confortanti dinamiche di spesa trovano ancor più concretezza nelle previsioni per il nuovo anno. Secondo le rilevazioni condotte dall'Osservatorio Digital Transformation Academy, la security rappresenta infatti la voce più importante in una lunga lista di aree di investimento digitale per il 2022 per le grandi aziende per il secondo anno di fila e, per la prima volta, si attesta al primo posto anche tra le priorità dichiarate delle PMI, dopo la lusinghiera seconda piazza dell'anno precedente.

In questo scenario si è mosso l'Osservatorio Cybersecurity & Data Protection, promosso dalla School of Management del Politecnico di Milano. L'Osservatorio, al suo settimo anno di Ricerca, intende rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche della cybersecurity e della data protection e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.

"Cybersecurity: don't look up" è il titolo scelto per rappresentare la Ricerca di quest'anno: le organizzazioni si stanno muovendo nella direzione che vede la cybersecurity un elemento chiave per il proprio business e proprio in questo momento non bisogna abbassare la guardia, ma "guardare in alto" verso le nuove insidie e mettere in atto azioni strategiche di lungo periodo.

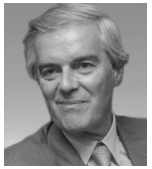
Introduzione

Cybersecurity: don't look up

Guarda il video dell'evento su **osservatori.net**

Lo scenario è sempre più preoccupante dal punto di vista degli attacchi, tuttavia ci sono importanti elementi di contesto che possono aiutare l'ecosistema cyber italiano a crescere. Il PNRR e la nascita dell'Agenzia per la Cybersicurezza Nazionale sono l'occasione per fare sistema e coordinare misure di supporto alla sicurezza e per favorire la crescita di professionalità cyber in tutta la filiera di mercato, oltre che nella Pubblica Amministrazione.

Comitato Scientifico



Umberto Bertelè
Chairman degli Osservatori Digital Innovation

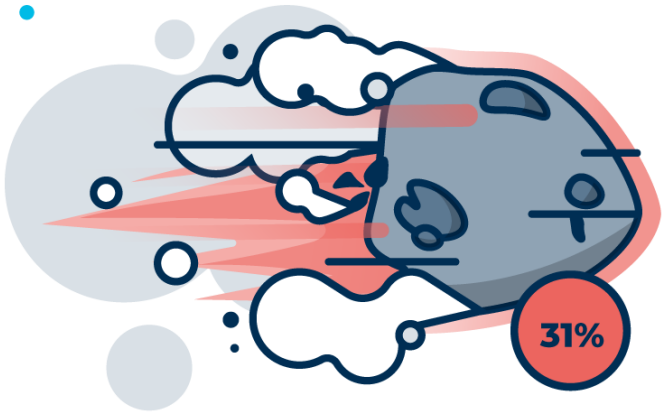
Alessandro Perego
Direttore Scientifico, Osservatori Digital Innovation

Andrea Rangone
Comitato Scientifico, Osservatori Digital Innovation

Mariano Corso
Comitato Scientifico, Osservatori Digital Innovation


CYBERSECURITY:
DON'T LOOK UP

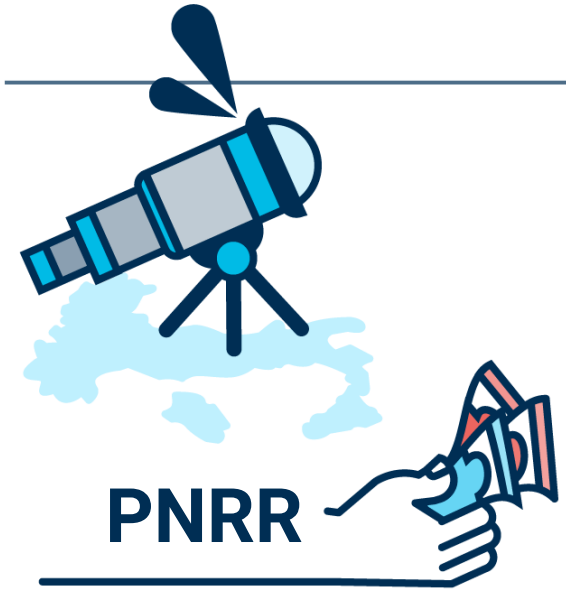
IL CONTESTO GENERALE



ULTERIORE AUMENTO
DEGLI ATTACCHI DURANTE IL 2021
DOPO LA CRESCITA NEI PRIMI MESI
DEL 2020

NECESSITÀ DI
RAFFORZAMENTO DELLE INIZIATIVE
DI SENSIBILIZZAZIONE RIVOLTE AL PERSONALE
PER LE NUOVE MODALITÀ DI LAVORO

REVISIONE COMPLETA
DELLA STRATEGIA DI GESTIONE
DELLA SICUREZZA INFORMATICA
DEFINITA IN PRECEDENZA



MISSIONE 1
COMPONENTE 1
(M1C1)

6,14 MLD € PER LA DIGITALIZZAZIONE
DELLA PA TRA CUI
623 MLN €
IN CYBERSECURITY

MISSIONE 4
COMPONENTE 2
(M4C2)

1,61 MLD €
PER LA CREAZIONE DI ALMENO
10 PARTENARIATI TRA 15 TEMI

UN PARTENARIATO
SUL TEMA
CYBERSECURITY

+

AGENZIA PER
LA CYBERSICUREZZA
NAZIONALE

ASSUNZIONE PERSONALE

ENTRO DICEMBRE 2023
FINO A 300 SPECIALISTI

ENTRO DICEMBRE 2027
FINO A 800 SPECIALISTI

IL MERCATO DELLA SECURITY 2021

2021
1'545 MLN €

2020
1'370 MLN €

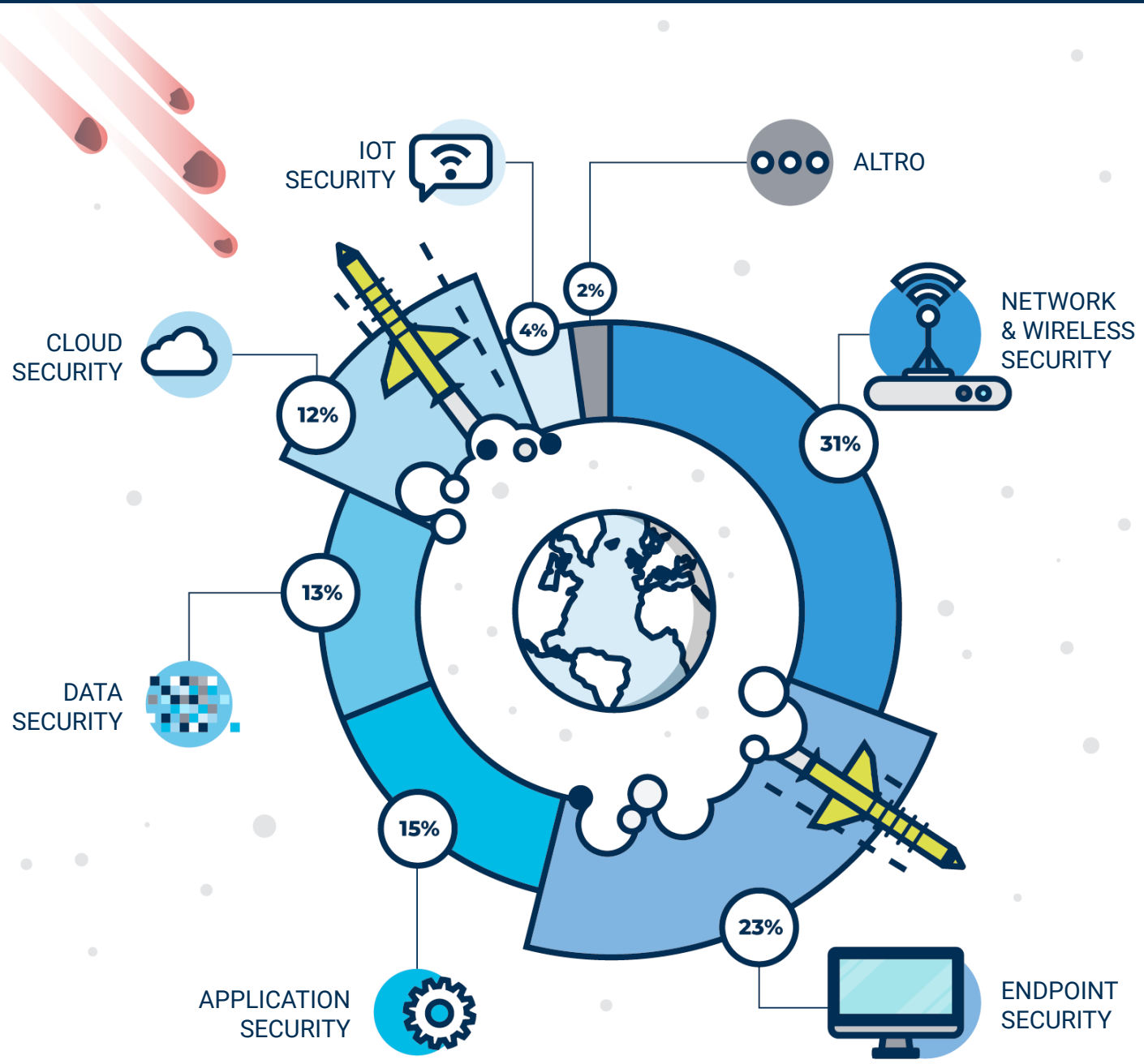
2019
1'317 MLN €

2018
1'190 MLN €

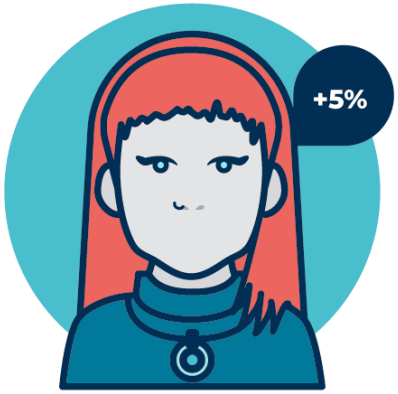
2017
1'090 MLN €

2016
976 MLN €

TIPOLOGIA DI SICUREZZA
CON MAGGIORE CRESCITA
2021 VS 2020



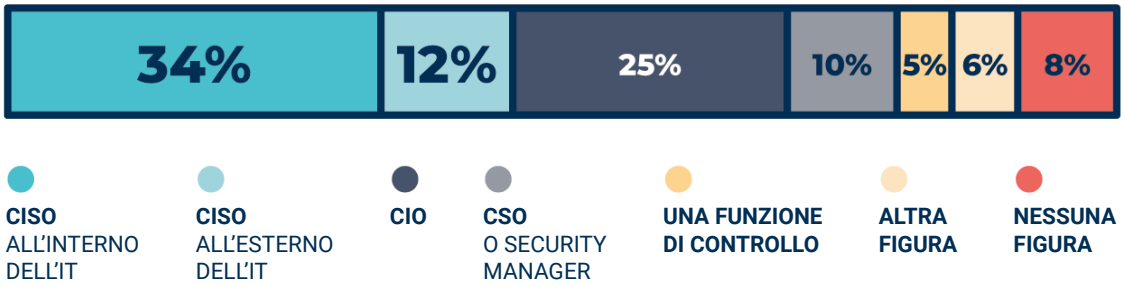
LA GESTIONE DELLA CYBERSECURITY E DEL RISCHIO CYBER



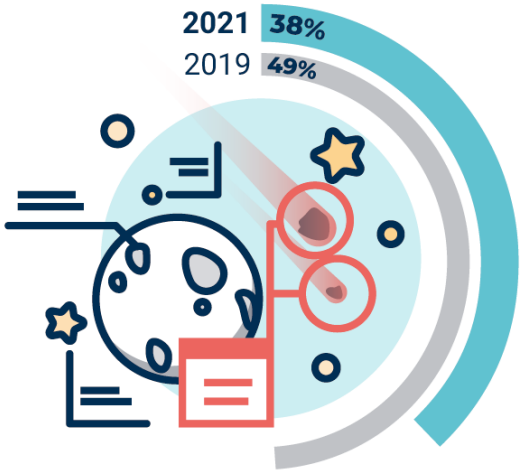
46%

LA RESPONSABILITÀ DELLA SICUREZZA INFORMATICA È AFFIDATA AL

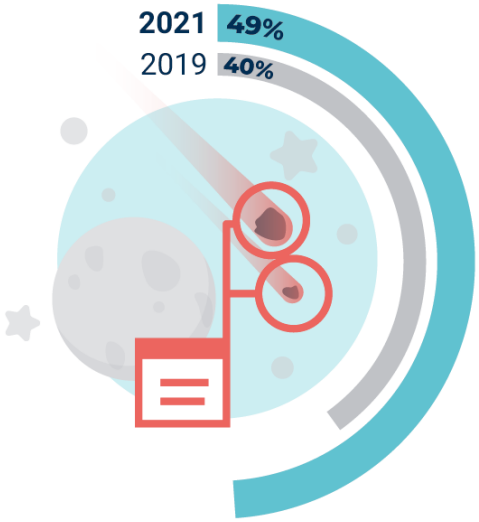
CISO



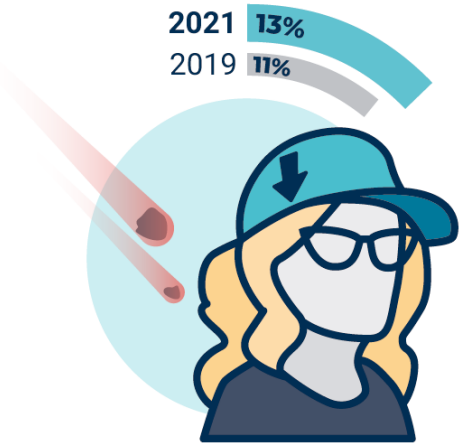
IL PROCESSO DI GESTIONE DEL RISCHIO CYBER



VIENE GESTITO ALL'INTERNO DI UN **PROCESSO INTEGRATO** DI RISK MANAGEMENT AZIENDALE



VIENE GESTITO COME **RISCHIO A SÉ STANTE** ALL'INTERNO DI UNA SINGOLA FUNZIONE



NON VIENE MONITORATO COSTANTEMENTE

L'IMPATTO DEI TREND DEL DIGITALE SULLA SECURITY

ECOMMERCE & PAYMENT

OT SECURITY

BIG DATA ANALYTICS

SUPPLY CHAIN SECURITY

DEVSECOPS E SECURITY BY DESIGN

63%

DIGITAL IDENTITY

67%

SMART E REMOTE WORKING

80%

CLOUD

LE PRIORITÀ DELLE AZIENDE

Il contesto di riferimento

Il panorama di riferimento per la cybersecurity sta vivendo un momento di grande turbolenza: nella "nuova normalità", caratterizzata prevalentemente da modalità di lavoro che prevedono l'alternanza tra casa e ufficio, gli attacchi informatici sono sempre più frequenti e significativi, in un trend di intensificazione e recrudescenza del fenomeno che prosegue ormai da diversi anni.

Dallo sfruttamento di vulnerabilità sempre più critiche fino alla sempre maggiore diffusione di **ransomware** con ripercussioni disastrose, stiamo assistendo a una vera e propria guerra cyber. Tra le tendenze rilevate nel 2021, preoccupano gli attacchi rivolti a infrastrutture critiche, quelli che prendono di mira sistemi sanitari e quelli indirizzati all'intera supply chain, che generano impatti a cascata su tutte le aziende fornitrici, clienti o utilizzatrici di un servizio o un prodotto.

Secondo le ultime rilevazioni del **Clusit**, **solo nel primo semestre 2021, sono stati ben 1.053 gli incidenti di tipo grave**, ossia che hanno avuto un impatto significativo in termini economici e di reputazione sulle organizzazioni colpite, in crescita del 15% rispetto al primo semestre del 2020.

A fronte dello scenario delineato e con il protrarsi dell'emergenza sanitaria, la reazione delle grandi imprese, secondo quanto emerso dalla Survey dell'Osservatorio condotta su 132 grandi organizzazioni operanti in Italia, è orientata verso il tentativo di accrescere la consapevolezza della popolazione aziendale in merito ai rischi e alle minacce informatiche. **Il 54% delle grandi realtà ravvisa infatti la necessità di rafforzare le iniziative di sensibilizzazione rivolte al personale** rispetto ai comportamenti da tenere nelle nuove modalità di lavoro.

L'attenzione rivolta alla materia è ai suoi massimi storici: i sistemi di gestione dell'information security e della data protection si collocano al primo posto tra le priorità di investimento in logica prospettica in materia di innovazione digitale, sia per le grandi e grandissime imprese, in cui la prima posizione viene occupata per il secondo anno consecutivo, sia – per la prima volta in assoluto – per le realtà di dimensioni minori.

Va però considerato anche il rovescio della medaglia: un terzo del campione dichiara di aver effettivamente rilevato un **ulteriore aumento degli attacchi informatici nell'ultimo anno (31%)**, che va a sommarsi alla crescita già significativa affrontata durante i primi mesi della situazione emergenziale. Nel 5% dei casi, inoltre, la complessità dello scenario da affrontare ha indotto le aziende a rivedere completamente la strategia di gestione della sicurezza informatica precedentemente definita.

Il PNRR e l'introduzione dell'Agenzia per la Cybersicurezza Nazionale

L'attenzione al tema della cybersecurity viene confermata dal quadro istituzionale, da cui emerge l'introduzione di misure significative in materia.

All'interno del Piano Nazionale di Ripresa e Resilienza (PNRR), la cybersicurezza ricopre un ruolo rilevante, dopo essere passata in subordine per diversi anni. L'attenzione al tema si concretizza negli **investimenti previsti nella Missione 1, con 623 milioni di euro mirati a dotare la Pubblica Amministrazione di presidi e competenze di cybersecurity**, e nella **Missione 4, con ulteriori fondi a sostegno della ricerca su tematiche innovative**[1].

Obiettivo del Piano, che secondo le rilevazioni dell'Osservatorio è stato accolto caldamente da più soggetti coinvolti, quali Telco, operatori di infrastrutture critiche ed enti della Pubblica Amministrazione, è quindi favorire la digitalizzazione e l'innovazione dell'intero Paese, con un ruolo da protagonista della cybersecurity.

La principale novità riguarda tuttavia l'introduzione di una struttura parastatale predisposta ad affrontare le

Approfondisci il tema:
REPORT

Priorità dell'innovazione digitale per le imprese nel 2022: trend di investimento

Note

1. Nella Missione 4 sono previsti investimenti da 1,6 miliardi di euro, per la creazione di 15 partenariati allargati (di cui uno dedicato alla sicurezza informatica) estesi a università, centri di ricerca, imprese e progetti di ricerca di base.

minacce informatiche: l'Agenzia per la Cybersicurezza Nazionale (ACN). Attiva dallo scorso settembre, è nata con l'obiettivo di predisporre una strategia di sicurezza cibernetica a livello di sistema Paese, diventando un vero e proprio punto di riferimento a livello nazionale e internazionale per imprese e istituzioni e sostenendo campagne di sensibilizzazione e di creazione di una cultura diffusa di cybersicurezza.

Dalla Survey erogata dall'Osservatorio, le imprese si dimostrano aperte e disponibili a lavorare con il nuovo ente. In particolare, il 17% di esse ha già stabilito la volontà di collaborare con l'Agenzia, la metà delle organizzazioni (53%) è in attesa di linee guida e indicazioni, mentre un ulteriore 22% vuole approfondire meglio il ruolo dell'organismo nell'ottica di individuare possibili opportunità future.

Il mercato e lo scenario della cybersecurity in Italia

Il mercato della cybersecurity nel 2020 aveva incassato il colpo inferto dalla pandemia, riuscendo però a mantenere un debole tasso di crescita positivo (+4%) nonostante un'economia in forte contrazione. Il rallentamento della spesa era stato confermato anche dall'analisi dell'offerta cybersecurity, i cui indicatori finanziari avevano subito una frenata in termini di crescita.

Nel 2021 gli investimenti tornano invece ad aumentare in maniera florida: **il mercato della cybersecurity ha raggiunto un valore di 1,55 miliardi di euro, registrando un +13% rispetto al 2020**. Il ritmo di crescita non è mai stato così elevato, nemmeno in periodo pre-Covid. A conferma di ciò si registra un 60% di grandi organizzazioni che ha visto un aumento del budget dedicato alle attività di sicurezza informatica, contro il 51% del 2019 (nel 2020 la stessa percentuale si fermava al 40%).

Un ulteriore dato a riprova della dinamicità del mercato riguarda il numero di operazioni straordinarie che hanno riguardato aziende italiane impegnate nel settore servizi e soluzioni in ambito security: nel 2021 l'Osservatorio ha censito 13 operazioni di acquisizione, aggregazione e quotazione, che hanno visto il coinvolgimento di ben 24 diverse realtà, per un giro d'affari pari a diverse centinaia di milioni di euro.

Dalla scomposizione del mercato nelle diverse componenti di spesa si conferma un mix analogo a quanto rilevato lo scorso anno:

- 52% per soluzioni di security, quali Vulnerability Management e Penetration Testing, SIEM, Identity and Access Management, Intrusion Detection System, Data Loss Prevention, Risk and Compliance Management e Threat Intelligence.
- 48% per servizi, quali servizi professionali e servizi gestiti (Managed Services).

In termini di tipologia di spesa, **gli aspetti di security più tradizionali continuano a coprire le quote maggiori del mercato**, con la categoria Network & Wireless Security che si conferma al primo posto nel mix con il 31% della spesa, seguita da Endpoint Security (23%) e Application Security (15%). **Gli aumenti di investimento più corposi riguardano la spesa in Endpoint Security e in Cloud Security**: da un lato, la protezione dei dispositivi continua a essere un elemento cruciale nel contesto delle nuove modalità di lavoro, dall'altro l'adozione di applicazioni e piattaforme in Cloud, sempre più diffusa ed estesa anche in seguito al protrarsi della situazione di emergenza sanitaria, rende necessaria un'attenzione alla salvaguardia dei sistemi sulla nuvola.

Nonostante la dinamica di crescita, **il rapporto tra spesa in cybersecurity e PIL continua ad apparire limitato se paragonato a ciò che avviene a livello internazionale**: la relazione si mantiene infatti stabile a un tasso dello 0,08%, sempre lontano dalle cifre di altri Paesi del G7. Insieme al Giappone, però, l'Italia è l'unica nazione a non aver registrato nel 2021 una diminuzione di tale rapporto.

I trend del digitale e le implicazioni sulla sicurezza

La pervasività assunta dalla trasformazione digitale, accelerata significativamente anche dal contesto pandemico, impone alle organizzazioni di indagare le implicazioni sulla sicurezza informatica introdotte dalle nuove soluzioni e dai nuovi approcci, in termini di potenziali minacce e rischi generati.

Approndisci il tema:
REPORT

Il panorama di riferimento per la cybersecurity e lo scenario di mercato 2021

Per il secondo anno consecutivo sono il **Cloud** e le nuove modalità di lavoro in **Smart e Remote Working** a confermarsi come i trend che generano il maggiore impatto sul modello di gestione della security all'interno delle grandi organizzazioni italiane. Il primo, per il quale si attesta all'80% la quota di aziende che dichiara un impatto rilevante o molto rilevante, è legato a una ormai radicata propensione a migrare dati, applicazioni e infrastrutture in ambienti cloud, che rende necessaria per le organizzazioni l'introduzione di nuove competenze dedicate e di opportuni strumenti di controllo, monitoraggio e orchestrazione. Il secondo trend (rilevante per il 67% delle imprese) è sostenuto dal protrarsi della pandemia e dalle nuove modalità di lavoro, che rendono necessario implementare soluzioni a tutela del perimetro aziendale.

Completa il podio il paradigma della **Digital Identity** (63%), che dopo essere passato in sordina per diverso tempo sperimenta un picco di attenzione. L'accelerazione è dettata dalla crescente necessità di assicurare agli utenti aziendali la possibilità di accedere a risorse e dati critici anche da remoto, utilizzando un'identità digitale sicura e certificata, tramite l'implementazione di soluzioni di gestione di accessi e privilegi, sistemi di autenticazione multi-fattore o approcci passwordless.

L'organizzazione della cybersecurity, il ruolo del CISO e le iniziative di sensibilizzazione

Nel delicato contesto attuale, assumono ancora più rilevanza che in passato gli aspetti organizzativi di gestione della sicurezza all'interno delle organizzazioni, dal ruolo ricoperto dalla figura del **Chief Information Security Officer (CISO)** fino alla creazione di una cultura diffusa in materia all'interno delle aziende.

Dopo anni in cui l'organizzazione della cybersecurity risultava pressoché cristallizzata, nel 2021 la responsabilità della sicurezza informatica torna a crescere e, nel 46% delle imprese, è affidata a un CISO formalizzato, che riporta principalmente all'interno della Direzione IT (34%)

Approndisci il tema:
REPORT

Scelte organizzative, competenze e responsabilità in materia di cybersecurity

e ha un team dedicato a supporto nella maggior parte dei casi (78% delle realtà).

Un ulteriore importante aspetto riguarda le azioni implementate per aumentare l'awareness del personale aziendale sulle tematiche di cybersecurity e data protection. **Il 58% delle realtà ha definito un piano di formazione strutturato, volto a sensibilizzare tutti gli attori coinvolti nei processi aziendali**, mentre una porzione di aziende (11%) ha scelto invece di focalizzarsi sulla formazione di alcune specifiche funzioni, considerate più a rischio o più sensibili. Sono poi presenti casi in cui sono state implementate azioni di sensibilizzazione meno strutturate e sporadiche (30%), mentre solo nell'1% delle organizzazioni le attività di formazione per i dipendenti non sono previste.

La gestione del rischio cyber all'interno delle organizzazioni

Anche il processo di gestione del **rischio cyber** assume una rilevanza sempre più cruciale per le organizzazioni nel contesto emergenziale, specialmente per quanto riguarda la mitigazione di scenari legati all'interruzione di business o al downtime di rete, che impediscono di garantire la regolare operatività aziendale.

La situazione legata al Covid-19 ha però lasciato uno strascico negativo in termini di approccio al rischio cyber, aumentando la difficoltà nell'adottare una visione olistica e strategica e generando preoccupanti silos. La fotografia che emerge dai dati della Survey evidenzia un generale peggioramento nel processo di gestione da parte delle organizzazioni: sebbene il numero complessivo di aziende che affrontano il rischio cyber rimanga circa invariato, si attesta al 38% la quota di realtà che dichiara di gestirlo in un processo integrato di risk management aziendale, mentre il resto del campione lo tratta come un rischio a sé stante all'interno di una singola funzione o addirittura non monitora costantemente il rischio cyber.

Cybersecurity: don't look up

Con il protrarsi della situazione di emergenza sanitaria, la consapevolezza in merito all'importanza della

cybersecurity si sta consolidando, non solo nelle organizzazioni di maggiori dimensioni, ma anche in realtà meno strutturate, con diversi segnali positivi: dall'importante rimbalzo nella dinamica del mercato alla diffusione del CISO, in crescita dopo anni di immobilità.

Il primo passo è stato compiuto: le organizzazioni hanno posto le basi per rendere la cybersecurity un elemento chiave per la strategicità del loro business, intraprendendo un percorso strutturato verso una nuova fase per la sicurezza informatica.

L'Italia rimane però all'ultimo posto tra i Paesi del G7 nel rapporto tra spesa cybersecurity e PIL. In aggiunta, il mercato del cybercrime, alimentato da floridi finanziamenti, corre veloce, con nuove tipologie di attacco sempre più crude e sofisticate in grado di mettere in ginocchio anche le realtà più consolidate.

Le organizzazioni non devono quindi abbassare la guardia e adagiarsi su quanto costruito quest'anno, ma al contrario, muoversi nella formulazione di una strategia a lungo termine, tenendo alta la guardia.

Da questo punto di vista, lasciano ben sperare il PNRR e l'introduzione dell'Agenzia per la Cybersicurezza Nazionale: occasione per garantire il coordinamento tra i diversi soggetti e la valorizzazione delle competenze cyber, verso la costruzione di un fronte comune contro i malintenzionati.

Mariano Corso
Responsabile Scientifico

Gabriele Faggioli
Responsabile Scientifico

Alessandro Piva
Direttore della Ricerca

Glossario

Cybersecurity: don't look up

Al fine di facilitare la lettura di questo Executive Summary, viene proposto un glossario che sintetizza le principali definizioni utilizzate.

Application Security
strumenti per la protezione delle applicazioni aziendali e per il loro sviluppo secondo standard di security by design.

Chief Information Security Officer (CISO)
figura responsabile del presidio dell'information security in azienda. Si occupa di definire la visione strategica, di implementare programmi per la protezione degli asset informativi e di definire processi per limitare i rischi legati all'adozione delle tecnologie digitali.

Cloud Security
strumenti e soluzioni per la protezione dei diversi possibili ambienti Cloud, sia considerando il modello di servizio (IaaS, PaaS o SaaS) sia considerando il modello di implementazione (Cloud privato, pubblico, ibrido o multi-Cloud).

Data Loss Prevention (DLP)
soluzioni per il monitoraggio dei dati presenti in azienda al fine di prevenirne la perdita per furto, a seguito di un attacco informatico o errore.

Endpoint Security
protezione di ciascun dispositivo connesso alla rete:
smartphone, tablet, notebook, PC, ma anche terminali dei registratori di cassa, stampanti, scanner, fotocopiatrici e altri dispositivi.

Identity and Access Management (IAM)/ Privileged Access Management (PAM)
soluzioni che permettono la gestione e il monitoraggio di autorizzazioni e privilegi di accesso degli utenti a infrastrutture, applicazioni e dati critici.

Intrusion Detection System (IDS)
soluzioni che monitorano il traffico di rete per identificare e bloccare gli accessi non autorizzati a un determinato sistema o dispositivo.

Managed Services
si intendono i servizi offerti in maniera continuativa da provider esterni all'organizzazione per garantire il supporto e la manutenzione dei sistemi informativi aziendali (es. SOC).

Network e Wireless Security
strategie, procedure e tecnologie pensate per proteggere l'infrastruttura cablata e wireless della rete aziendale da danni e da accessi impropri, oltre che soluzioni per il monitoraggio dell'utilizzo del web da parte degli utenti e strumenti per la protezione della posta elettronica.

Ransomware
particolare categoria di malware in grado di bloccare le funzionalità di un dispositivo e cifrare i dati contenuti al suo interno, rendendoli inaccessibili sino al pagamento di un riscatto in denaro (tipicamente richiesto in criptovaluta).

Rischio cyber
qualsiasi rischio di perdita finanziaria, distruzione o danno alla reputazione di un'organizzazione dovuta ad un malfunzionamento del sistema informativo.

Risk and Compliance Management
soluzioni volte ad analizzare il livello di esposizione al rischio cyber dei sistemi informatici aziendali e garantire la conformità a standard, framework e normative in materia di sicurezza delle informazioni e protezione dei dati.

Security Information and Event Management (SIEM)
soluzioni per il monitoraggio degli eventi di sicurezza in grado di raccogliere e analizzare dati provenienti da più fonti e segnalare in tempo reale eventuali anomalie e criticità al personale che si occupa di security.

Glossario

Cybersecurity: don’t look up

Threat Intelligence

soluzioni che sfruttano Big Data Analytics e algoritmi di Artificial Intelligence e Machine Learning per raccogliere informazioni, monitorare e analizzare in real-time i rischi e le minacce di sicurezza, al fine di mettere in atto piani di protezione in ottica preventiva.

Vulnerability Management/Penetration Testing

soluzioni volte a individuare e misurare il grado di gravità delle vulnerabilità e testare la sicurezza di sistemi, applicazioni o reti, anche attraverso la simulazione di attacchi da parte di malintenzionati.

La mission dell'Osservatorio e gli obiettivi della Ricerca

L'Osservatorio Cybersecurity & Data Protection intende conoscere, comprendere e affrontare le nuove minacce alla sicurezza informatica supportando le aziende nella scelta delle tutele più opportune, rendendole consapevoli dell'importanza del monitoraggio e del controllo delle attività e mostrando loro le tecniche e le tecnologie a supporto della cybersecurity adottabili.

In continuità con le edizioni passate, l'Osservatorio si focalizza sui seguenti obiettivi:

- quantificare il mercato della sicurezza informatica in Italia, identificando i trend che lo caratterizzano;
- analizzare e confrontare le diverse modalità di gestione del rischio cyber;
- identificare le competenze e i ruoli coinvolti nella gestione della cybersecurity;
- stimare lo stato di adozione di sistemi e soluzioni di cybersecurity e data protection nelle organizzazioni italiane.

L'Advisory Board

Al fine di favorire un confronto continuativo e indirizzare la Ricerca sui trend di maggiore valore per le aziende, l'Osservatorio si avvale di un Advisory Board, ossia un ristretto gruppo di indirizzo composto da Executive che si occupano della gestione della cybersecurity e della data protection all'interno di grandi organizzazioni appartenenti a diversi settori merceologici.

I Workshop a porte chiuse

L'Osservatorio ha organizzato nel 2021 quattro workshop tematici a porte chiuse, erogati in modalità ibrida, al fine di discutere e validare i risultati ottenuti dalla rilevazione empirica:

- *Trend emergenti e use case aziendali in ambito cybersecurity e data protection* (7 maggio 2021);
- *Modelli organizzativi e competenze per la gestione della cybersecurity e data protection* (25 giugno 2021);
- *L'offerta tecnologica in ambito cybersecurity & data protection* (1° ottobre 2021);
- *Le modalità di gestione del rischio cyber nel contesto di evoluzione istituzionale* (24 novembre 2021).

Il Percorso Autorità

Nel corso del 2021 sono stati organizzati una serie di

incontri di approfondimento con le Autorità, focalizzati sulla discussione di un tema specifico attinente agli ambiti della cybersecurity e data protection insieme ad alcuni referenti delle principali istituzioni in materia.
In particolare, sono stati organizzati 2 incontri ad ampia partecipazione di pubblico:

- *Il Data Protection Officer all'interno delle complessità organizzative pubbliche e private* (25 maggio 2021);
- *GDPR e Cloud Provider: la compliance e la sicurezza dei dati* (15 settembre 2021).

Il Tavolo di Lavoro "Security Readiness"
Durante la Ricerca 20201 sono proseguiti i lavori del Gruppo di Lavoro di approfondimento verticale dal titolo "Security Readiness". Il Gruppo di lavoro si è posto l'obiettivo di fornire degli strumenti che permettano alle aziende di valutare in modo strutturato il proprio livello di maturità e di elaborare una strategia di medio-lungo termine per la gestione della security.

Le Survey
A partire da un modello comune di indagine, sviluppato in funzione degli obiettivi della Ricerca, sono stati definiti i questionari che sono stati sottoposti a CISO, CSO, CIO, Risk Manager, Chief Risk Officer, DPO e Responsabili della compliance di imprese di piccole, medie e grandi dimensioni e Pubbliche Amministrazioni di diversa natura.

Survey CISO – Grandi imprese
La rilevazione ha visto il coinvolgimento di 132 organizzazioni italiane di grandi dimensioni, aventi un numero di addetti superiore a 249. La Survey è mirata a stimare il mercato e lo stato di adozione di sistemi di cybersecurity nelle aziende italiane, indagare l'impatto sulla gestione della sicurezza generato dai trend dell'innovazione digitale e identificare le strutture di governance e i processi messi in campo dalle organizzazioni per una corretta gestione della cybersecurity e della data protection.

Survey Compliance
La rilevazione ha visto il coinvolgimento di 90 organizzazioni italiane di piccole, medie e grandi dimensioni. La Survey ha avuto come obiettivo quello di misurare e quantificare l'effort che le aziende dedicano alle attività di valutazione della sicurezza e della compliance dei fornitori di servizi cloud alla normativa sulla protezione dei dati personali.

Survey PMI

La Ricerca, svolta in collaborazione con l'Osservatorio Innovazione Digitale nelle PMI, ha coinvolto un campione di piccole e medie imprese rappresentativo della popolazione aziendale italiana, in termini di settore merceologico, dimensione e distribuzione geografica. Sono state analizzate 503 imprese con un numero di addetti compreso tra 10 e 249 suddivise in quattro aree territoriali (nord-ovest, nord-est, centro, sud e isole), per due classi dimensionali (piccole aziende tra 10 e 49 addetti e medie aziende tra i 50 e i 249 addetti).

La quantificazione del mercato

La metodologia di stima del mercato ha seguito un approccio caratterizzato da una triplice prospettiva:

- top-down, tramite il coinvolgimento dei principali vendor del settore: in particolare sono stati analizzati tramite interviste dirette, telefoniche o fonti secondarie, oltre 100 organizzazioni operanti nel territorio italiano;
- bottom-up, tramite la rilevazione della spesa in soluzioni e servizi di information security da parte delle organizzazioni italiane end-user stratificate per classe dimensionale e settore di mercato;
- fonti secondarie, analizzando ricerche e studi dei principali vendor e analisti internazionali.

Per l'analisi del rapporto mercato cybersecurity e PIL sono state utilizzate ulteriori informazioni reperite da fonti secondarie, in particolare:

- per il PIL italiano i valori pubblicati dal Ministero dell'Economia e delle Finanze (**www.mef.gov.it**);
- per i valori del PIL degli stati esteri i valori di Data World Bank (**www.data.worldbank.org**) al cambio euro/dollaro del 15/12/2021;
- per i tassi di crescita del PIL, i valori presi dal Fondo Monetario Internazionale di ottobre 2021 (**www.imf.org/en/Publications/WEO/weo-database/2021/October**);
- per il mercato cybersecurity degli stati esteri i valori da Statista (**www.statista.com**).

Il panorama di riferimento per la cybersecurity e lo scenario di mercato 2021 ↗

Il Report analizza il mercato della cybersecurity in Italia e le principali aree di investimento delle aziende, l'impatto sulla gestione della sicurezza generato dai trend dell'innovazione digitale e le principali sfide, tecnologiche e normative, che attendono le organizzazioni nel prossimo futuro.

Scelte organizzative, competenze e responsabilità in materia di cybersecurity ↗

Il Report mira ad analizzare come le scelte organizzative delle aziende in materia di presidio e responsabilità di cybersecurity stiano evolvendo, evidenziando il cambiamento in atto. Vengono illustrate le diverse configurazioni adottate e le figure specialistiche introdotte dalle organizzazioni.

La gestione del rischio cyber e l'evoluzione del contesto normativo ↗

Il Report analizza l'evoluzione del processo di gestione del rischio cyber all'interno delle organizzazioni, soffermandosi sulle azioni implementate dalle diverse realtà aziendali nella gestione del rischio legato agli attacchi informatici e nell'adeguamento al contesto normativo.

L'offerta tecnologica in ambito cybersecurity ↗

Il Report illustra il mercato dell'offerta tecnologica in ambito cybersecurity, analizzando le diverse categorie di offerta messe a disposizione per la sicurezza delle organizzazioni e proponendo un framework di classificazione originale sviluppato dall'Osservatorio.

Approfondisci il tema di ricerca su osservatori.net con i Report online

↗ **Scopri i Report online**

Gli Osservatori Digital Innovation organizzano diversi Programmi tematici, composti da Workshop e Webinar, con l'obiettivo di aiutare a comprendere quali effetti abbia l'evoluzione tecnologica nelle nuove strategie digitali, attraverso la discussione dei risultati emersi dalle Ricerche annuali.

Tutti gli eventi possono essere seguiti in diretta oppure on demand sulla piattaforma osservatori.net

Approfondisci il tema di ricerca su osservatori.net con il Programma tematico dedicato

↗ **Scopri il Programma tematico**

Programma tematico dedicato:
Cybersecurity & Data Protection (2022):

OT/ICS CYBERSECURITY: MINACCE DI OGGI E CONTROMISURE PER RESILIENZA E CONTINUITÀ OPERATIVA
Webinar – 24/01/2022

LA RIVOLUZIONE DEL CLOUD NATIVE COMPUTING, VELOCITÀ E SICUREZZA
Webinar – 28/02/2022

IL MERCATO DELLA CYBERSECURITY E IL PROTRARSI DELLA SITUAZIONE DI EMERGENZA SANITARIA
Webinar – 07/03/2022

ON-BOARD AUTOMOTIVE SECURITY
Webinar – 22/03/2022

IL LIVELLO DI COMPLIANCE E SICUREZZA DEI FORNITORI
Webinar – 01/04/2022

PCI DSS 4.0 FINALMENTE DISPONIBILE: NOVITÀ, IMPATTI E SCADENZE
Webinar – 15/04/2022

TREND DELL'INNOVAZIONE DIGITALE E CYBERSECURITY
Webinar – 09/06/2022

L'IMPORTANZA DEL MONITORAGGIO SULLE INFRASTRUTTURE IT
Webinar – 24/06/2022

MODELLI ORGANIZZATIVI E COMPETENZE PER LA CYBERSECURITY
Webinar – 07/07/2022

I RANSOMWARE: LE NUOVE TECNICHE D'ATTACCO E COME DIFENDERSI
Webinar – 19/07/2022

DALLA BUSINESS CONTINUITY ALLA RESILIENZA OPERATIVA
Webinar – 06/09/2022

I SERVIZI NELLE SMART CITY: FRUIBILITÀ, CYBERSECURITY E PRIVACY
Webinar – 22/09/2022

POTENZIARE LE SOLUZIONI DI SICUREZZA CON LA THREAT INTELLIGENCE
Webinar – 04/10/2022

L'IMPORTANZA DELL'ADOZIONE DI UN CYBERSECURITY FRAMEWORK ADEGUATO ALLA SPECIFICA REALTÀ AZIENDALE
Webinar – 25/10/2022

MODALITÀ DI GESTIONE DEL RISCHIO CYBER E COMPLIANCE NORMATIVA
Webinar – 16/11/2022

Approfondisci il tema di ricerca su osservatori.net con il Programma tematico dedicato

↗ **Scopri il Programma tematico**

LA CERTIFICAZIONE DELLA SICUREZZA DEI PRODOTTI ICT

Webinar – 17/11/2022

ANALISI E GESTIONE DEL RISCHIO

Webinar – 13/12/2022

Approfondisci il tema di ricerca su osservatori.net con il Programma tematico dedicato

↗ **Scopri il Programma tematico**

Gruppo di Lavoro

Cybersecurity: don't look up

Guarda il video dell'evento su **osservatori.net**

Mariano Corso
Responsabile Scientifico

Gabriele Faggioli
Responsabile Scientifico

Alessandro Piva
Direttore

Giorgia Dragoni
Ricercatrice Senior

Ivan Antozzi
Ricercatore

Martina Broggi
Community & Event Coordinator

Jacopo Polverino
Analista

Nicola Ciani
Analista

Supporto specialistico:

Luca Bechelli
Senior Advisor

Anna Cataleta
Senior Advisor

Enrico Frumento
Cybersecurity Senior Specialist, CEFRIEL

Anna Italiano
Senior Advisor

Un ringraziamento speciale a
Andrea Antonielli

Per qualsiasi commento e richiesta di informazioni:
alessandro.piva@polimi.it

Advisory Board

Cybersecurity: don't look up

Guarda il video dell'evento su **osservatori.net**

Luca Bertoglio
Global CISO, Marelli

Massimo Cottafavi
Head of Cyber & Operations Security, Snam

Mirco Destro
Information Systems Director, Vimar

Michele Fabbri
Cyber Security Group Director,De Nora

Elisa Garavaglia
Security Governance, Assicurazioni Generali

Mirko Giardetti
Digital Innovation Manager, LUBE Industries

Vinicio Mazzei
Privacy Officer and Digital Governance and Compliance Manager, Saipem

Simone Pezzoli
Chief Information Security Officer, Autostrade per l'Italia

Roberto Puricelli
CISO EMEA, Marelli

Riccardo Roncon
CISO, Gruppo ITAS Assicurazioni

Corrado Salvemini
Head of IS Security, Stella McCartney

Daniele Sangion
Head of Cyber Security for Third Party Security Program, UniCredit

Advisory Board

Cybersecurity: don’t look up

Alessio Setaro
Cyber Security Leader di Leroy Merlin Italia | CISO Global per il gruppo Adeo

Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di **fare cultura in tutti i principali ambiti di Innovazione Digitale**. Oggi sono un punto di riferimento qualificato sull'Innovazione Digitale in Italia che integra attività di Ricerca, Comunicazione e Aggiornamento continuo.

La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese.

La **Mission** degli Osservatori è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di innovazione digitale in Italia.

I fattori distintivi

Le attività degli Osservatori Digital Innovation sono caratterizzate da 4 fattori distintivi.

1. **Ricerca**. Le attività di ricerca sono svolte da un team di oltre 100 tra Professori, Ricercatori e Analisti impegnati su più di 40 differenti Osservatori che affrontano tutti i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione.
2. **Aggiornamento**. Osservatori.net è il punto di riferimento per l'aggiornamento professionale sull'innovazione digitale. Il portale è una fonte unica di informazioni e dati basati su Pubblicazioni, Webinar e Workshop realizzati da analisti ed esperti con un know-how unico e distintivo. Il tutto è erogato tramite una piattaforma multimediale e interattiva per l'aggiornamento a distanza.
3. **Comunicazione**. Attraverso Convegni, Media e Pubblicazioni gli Osservatori diffondono buone pratiche, esperienze e cultura legata all'innovazione digitale, realizzando ogni anno oltre 5000 uscite stampa e 200 eventi pubblici.
4. **Networking**. Gli Osservatori aggregano la più ampia community di decisori della domanda, dell'offerta e delle Istituzioni, che collabora e sviluppa relazioni concrete nelle numerose occasioni di interazione per contribuire alla diffusione dell'Innovazione Digitale in Italia.

Gli Osservatori sono classificabili in 3 macro categorie:

1. **Digital Trasformation**, che include gli Osservatori che analizzano in modo trasversale i processi di innovazione digitale che stanno profondamente trasformando il nostro Paese;
2. **Digital Solutions**, che raggruppa gli Osservatori che studiano in modo approfondito specifici ambiti applicativi e infrastrutturali relativi alle nuove tecnologie digitali;
3. **Verticals**, che comprende gli Osservatori che analizzano l'innovazione digitale in specifici settori o processi.

Digital Transformation:
Agenda Digitale | Design Thinking for Business | Digital Transformation Academy | Innovazione Digitale nelle PMI | Smart Working | Startup Hi-tech | Startup Intelligence

Digital Solutions:
5G & Beyond | Artificial Intelligence | Big Data & Business Analytics | Blockchain & Distributed Ledger | Cloud Transformation | Cybersecurity & Data Protection | Data Center (Tavolo di Lavoro) | Digital B2b | eCommerce B2c | Innovative Payments | Internet of Things | Mobile B2c Strategy | Multicanalità | Omnichannel Customer Experience | Quantum Computing & Communication | Space Economy

Verticals:
Business Travel | Cloud per la PA (Tavolo di Lavoro) | Connected Car & Mobility | Contract Logistics "Gino Marchet" | Digital Content | Digital Identity | Digital Procurement (Tavolo di Lavoro) | Droni | EdTech | eGovernment | Export Digitale | Fintech & Insurtech | Food Sustainability | HR Innovation Practice | Innovazione Digitale nei Beni e Attività Culturali | Innovazione Digitale nel Pharma (Tavolo di Lavoro) | Innovazione Digitale nel Retail | Innovazione Digitale nel Turismo | Internet Media | Life Science Innovation | Professionisti e Innovazione Digitale | Sanità Digitale | Smart AgriFood | Smart City (Tavolo di Lavoro) | Smart Working nella PA (Tavolo di Lavoro) | Supply Chain Finance | Tech Company – Innovazione del Canale ICT | Transizione Industria 4.0

Si segnalano di seguito gli Osservatori correlati ai temi trattati in questo documento:
Artificial Intelligence | Big Data & Business Analytics | Cloud Transformation | Digital Identity | Digital Innovation Academy | Internet of Things | Smart Working | Transizione Industria 4.0

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Il punto di riferimento per l'aggiornamento Executive sull'Innovazione Digitale

In un contesto in cui l'innovazione digitale ha sempre più rilevanza per la competitività delle imprese e il cambiamento incessante caratterizza le nuove tecnologie, aggiornarsi è fondamentale per tutti i professionisti a vari livelli aziendali.

Gli Osservatori Digital Innovation rappresentano una fonte unica di conoscenza sull'Innovazione Digitale sviluppata da un team di 90 Ricercatori e Professori del Politecnico di Milano, che da anni punta a fornire a professionisti, manager e imprenditori

Avrai a tua disposizione: piattaforma **multimediale** e **interattiva**, ricerca **indipendenti** e **rigorose**, **analisti** e **esperti** con un know-how unico al servizio di **manager e professionisti**.

Report
caratterizzati da formati innovativi, consentendo una rapida ricerca delle informazioni di proprio interesse

Workshop e Webinar Premium
della durata di circa 4 ore (Workshop) e 1 ora (Webinar), durante i quali i partecipanti possono confrontarsi con analisti ed esperti

Programmi tematici
che raggrupano Workshop e Webinar in percorsi focalizzati su un particolare tema. Aiutano a comprendere gli effetti dell'evoluzione tecnologica attraverso la discussione dei risultati emersi

Inizia la prova gratuita oppure Abbonati ora e intraprendi il tuo percorso di crescita

Avrai a tua disposizione la più completa raccolta di analisi, dati e framework sull'Innovazione Digitale

↗ Inizia la prova gratuita

↗ Scegli l'Abbonamento

Per informazioni contatta Andrea Vanazzi

02 2399 4813 | 342 9212906
andrea.vanazzi@osservatori.net

↗ Contattaci

School of Management del Politecnico di Milano

www.som.polimi.it

La **School of Management del Politecnico di Milano**, costituita nel 2003, accoglie le molteplici attività di ricerca, formazione e consulenza nel campo dell'economia, del management e dell'industrial engineering, che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili.

La School of Management possiede la "Triple crown", i tre accreditamenti più prestigiosi per le Business School a livello mondiale: EQUIS, ricevuto nel 2007, AMBA (Association of MBAs) nel 2013, e AACSB (Advance Collegiate Schools of Business, ottenuto nel 2021).

Nel 2017 è la prima business school italiana a vedere riconosciuta la qualità dei propri corsi erogati in digital learning nei master Executive MBA attraverso la certificazione EOCCS (EFMD Online Course Certification System). Inserita nella classifica del Financial Times delle migliori Business School d'Europa dal 2009, oggi è in classifica con Executive MBA, Full-Time MBA, Master of Science in Management Engineering, Customised Executive programmes for business e Open Executive programmes for managers and professionals. Nel 2021 l'International Flex EMBA si posiziona tra i 10 migliori master al mondo nel Financial Times Online MBA Ranking.

La Scuola è presente anche nei QS World University Rankings e nel Bloomberg Businessweek Ranking.

La Scuola è membro di PRME (Principles for Responsible Management Education), Cladea (Latin American Council of Management Schools) e di QTEM (Quantitative Techniques for Economics & Management Masters Network).

Fanno parte della Scuola: il Dipartimento di Ingegneria Gestionale del Politecnico di Milano e MIP Graduate School of Business che, in particolare, si focalizza sulla formazione executive e sui programmi Master.

Le attività della School of Management legate all'Innovazione Digitale si articolano in Osservatori Digital Innovation, che fanno capo per le attività di ricerca al Dipartimento di Ingegneria Gestionale, e Formazione executive e programmi Master, erogati dal MIP.

MIP Politecnico di Milano Graduate School of Business

Gli **Osservatori Digital Innovation** sono fortemente integrati con le attività formative della Scuola:
nel senso che rappresentano un'importante sorgente per la produzione di materiale di insegnamento e di discussione per i corsi e traggono anche spesso linfa vitale dalle esperienze di coloro che partecipano ai corsi (in particolare a quelli post-universitari erogati dal MIP)
o vi hanno partecipato nel passato.

In sinergia con gli Osservatori, il MIP Politecnico di Milano Graduate School of Business ha lanciato diverse iniziative nell'ambito Digital Innovation:

- *Master Executive MBA* con possibilità di scegliere corsi elective focalizzati sui temi della Digital Business Transformation;
- *Percorso Executive* in Gestione Strategica dell'Innovazione Digitale;
- *Corsi brevi* Digital Innovation.

Per maggiori informazioni si veda il sito
www.mip.polimi.it

Sostenitori della Ricerca

Cybersecurity: don't look up

Partner

- Accenture
- Almaviva
- Assolombarda
- BlackBerry
- CrowdStrike
- Cybersel
- Ermes - Intelligent Web Protection
- Horizon Security
- Innovery
- Lutech
- Microsoft
- Minsait
- Poste Italiane
- Rai
- Spike Reply
- TIM
- Var Group – Yarix
- Vodafone Business
- WhiteJar - Unguess
- Wiit

Sponsor

- Blue Underwriting
- Cyber Guru
- Huawei
- Thales
- Zscaler

Supporter

- Aditinet Consulting SpA
- CryptoNet Labs

In collaborazione con

- CEFRIEL
- DEIB

Con il patrocinio di

- ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
- Assintel
- CLUSIT

accenture

Accenture è un'azienda globale di servizi professionali con capacità avanzate in campo digitale, cloud e security. Combinando un'esperienza unica e competenze specialistiche in più di 40 settori industriali, fornisce servizi in ambito Strategy & Consulting, Interactive, Technology e Operations, sostenuta dalla più ampia rete di Advanced Technology e Intelligent Operations centers a livello mondiale. I nostri 674.000 talenti combinano ogni giorno tecnologia e ingegno umano, servendo clienti in oltre 120 paesi. Accenture abbraccia la potenza del cambiamento per creare valore e successo condiviso per i clienti, le persone, gli azionisti, i partner e le comunità.

Marco Valsecchi
Managing Director, Security Strategy & Risk ICEG Lead

marco.valsecchi@accenture.com
www.accenture.it

AlmavivA

AlmavivA è sinonimo di innovazione digitale. Esperienze consolidate, competenze uniche, ricerca continua e una profonda conoscenza dei diversi settori di mercato, pubblico e privato, ne fanno il Gruppo leader italiano nell'Information & Communication Technology.

AlmavivA accompagna i processi di crescita del Paese raccogliendo la sfida che le realtà enterprise devono affrontare per rimanere competitive nell'epoca del Digitale, innovando il proprio modello di business, la propria organizzazione, la cultura aziendale e l'ICT.

La presenza in Italia è un riferimento di valore per AlmavivA. E a partire dalle solide competenze Made in Italy di AlmavivA è nato un network globale che opera attraverso 43 sedi in Italia e 24 all'estero, con un'importante presenza in Brasile, oltre che negli Stati Uniti, Colombia, Tunisia, Romania, Arabia Saudita e a Bruxelles, centro nevralgico della UE. Con 45.000 persone, 10.000 in Italia e 35.000 all'estero, AlmavivA è il 5° Gruppo privato italiano per numero di occupati al mondo, con un fatturato pari a 891 milioni di euro nel 2020.

Fra i principali player di riferimento nel settore Cybersecurity, AlmavivA garantisce un livello del tutto nuovo di conoscenza e comprensione delle minacce cyber alle organizzazioni che vogliano dedicarsi in sicurezza all'innovazione e alla crescita del proprio business predisponendo strategie di actionable cybersecurity a protezione di asset e dati critici.

Con un approccio modulare e scalabile che guarda alla sicurezza a livello di ecosistema, AlmavivA ha creato un panel completo e diversificato di servizi di nuova generazione, tecnologie e prodotti proprietari e di mercato, che tiene conto da un lato di uno scenario di rischio sempre più complesso e sofisticato dall'altro della continua evoluzione specifica delle principali Industry.

Roger Cataldi
CISO e Head of CyberSecurity Practice & Consulting

r.cataldi@almaviva.it
www.almaviva.it

ASSOLOMBARDA

Assolombarda è l'associazione delle imprese che operano nella Città Metropolitana di Milano e nelle province di Lodi, Monza e Brianza, Pavia.

Assolombarda, per dimensioni e rappresentatività, è l'associazione più importante di tutto il Sistema Confindustria. Esprime e tutela gli interessi di circa 6.800 imprese di ogni dimensione, nazionali e internazionali, produttrici di beni e servizi in tutti i settori merceologici. E conta più di 412.000 addetti.

L'associazione tutela gli interessi delle imprese associate nel rapporto con gli interlocutori istituzionali e gli stakeholder del territorio attivi in vari ambiti: formazione, ambiente, cultura, economia, lavoro, società civile. Offre, inoltre, servizi di consulenza specialistica in tutti i settori di interesse aziendale.

Miriam Ieraci
Funzionario Assolombarda Area Industria, Energia e Innovazione

miriam.ieraci@assolombarda.it
www.assolombarda.it

BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world.

The company secures more than 500M endpoints including over 195M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems.

Massimo Iarossi
Regional Sales Manager Italy&Malta

miarossi@blackberry.com
www.blackberry.com/us/en

CROWDSTRIKE

CrowdStrike, leader della sicurezza informatica a livello globale, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint, del workload e delle identità creata appositamente per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon® applica l'intelligenza artificiale a livello del cloud per offrire protezione e visibilità istantanee sull'intera azienda e prevenire gli attacchi sugli endpoint e sui workload all'interno e all'esterno della rete della rete. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni giorno CrowdStrike Falcon crea correlazioni in tempo reale tra più di 1.000 miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite. Con la piattaforma cloud CrowdStrike Falcon, i clienti godono di protezione più efficace, migliori prestazioni e un time-to-value immediato. C'è solo una cosa da ricordare su CrowdStrike: We stop breaches.

Luca Nilo Livrieri
Sales Engineer Manager – Southern Europe

luca.nilolivrieri@crowdstrike.com
www.crowdstrike.com

Cybersel nasce nel 2011 come spin-off di una realtà fondata nel 2003 e giunta fino a oggi attraverso continue evoluzioni. Cybersel vanta una lunga esperienza nel coniugare le esigenze tecnologiche delle aziende con la ricerca delle soluzioni di sicurezza informatica più innovative.

La nostra missione prevede la ricerca a livello internazionale delle tecnologie più avanzate e avveniristiche da proporre sui propri mercati di riferimento, oggi l'Italia, UK e la Francia.

Il nostro modello commerciale può essere considerato come una "boutique" delle tecnologie avanzate: offre ai nostri clienti una ricercata gamma delle migliori soluzioni e garantisce un rapporto basato su competenza professionale e tecnologica mentre ai nostri partner produttori delle tecnologie assicurano una vera rappresentanza locale della loro organizzazione.

In sintesi, Cybersel è un consulente delle tecnologie per il cliente e una base operativa virtuale del produttore.

La crescita e l'evoluzione esponenziale degli attacchi informatici degli ultimi anni hanno sicuramente condizionato l'interesse delle aziende, spingendole ad adottare misure di protezione sempre più sofisticate. Per questo motivo Cybersel è oggi specializzata nella proposta di soluzioni che aiutano le aziende ad affrontare il tema sempre più prioritario legato alla Cyber Security. Cyber Risk Management, Cyber Security Posture, Breach Attach Simulation sono alcuni dei temi che oggi proponiamo ai nostri clienti.

Claudia Bagnato
Marketing Manager

claudia.bagnato@cybersel.eu
www.cybersel.eu/it

ERMES
Intelligent Web Protection

La nostra storia. **Ermes** è nata nel 2017 come spin-off del Politecnico di Torino grazie all'idea di un gruppo di ricercatori di Electronic e Telecommunication Engineering che aveva intuito che il Web sarebbe cambiato drasticamente di lì a poco. Il nostro prodotto. L'85% dei cyberattacchi di successo sfrutta l'interazione umana e colpisce i bersagli nelle prime 21 ore dalla sua creazione, ed i sistemi di protezione tradizionali che adottano un approccio reputazionale falliscono nell'individuazione di tali minacce dal ciclo di vita breve. Ermes, grazie al suo approccio comportamentale basato su algoritmi di AI brevettati, riduce la finestra di esposizione alle minacce da giorni a minuti garantendo una protezione complessiva real-time del 99% sul Web ed incrementandola del 25% rispetto alle principali soluzioni presenti sul mercato. I nostri clienti e partner diretti. Siamo scelti dalle migliori aziende di tutti i settori come KPMG, Carrefour, Reale Mutua, Bonelli Erede, Sol Group, International School of Monaco. Il nostro prodotto è distribuito da Techdata ed Icos a più di 40 partner in 4 diversi continenti. Le nostre persone.

Siamo pienamente convinti che le persone facciano la differenza! Vantiamo un esperto team di leadership con 45+ anni di esperienza ed internamente abbiamo redatto un programma per i nostri top player fondato su OKR specifici ed un piano di ricompensa dedicato. La nostra idea di sostenibilità. Crediamo che sia impossibile creare valore senza preservare il mondo in cui viviamo. Per questo, nel 2020 abbiamo adottato un piano interno con l'obiettivo di diventare un'azienda a 0 emissioni nette di CO2 entro il 2024. Inoltre, la tecnologia di Ermes garantisce una maggiore sostenibilità attraverso l'energia risparmiata riducendo la larghezza di banda della rete del 30% e salvando 150 alberi all'anno per ogni 1.000 dispositivi che utilizzano Ermes.

Andrea Filippo Marini
CBO

a.marini@ermes.company
www.ermes.company

HORIZON SECURITY

Horizon Security Azienda italiana specializzata nell'erogazione di servizi di consulenza in ambito Cyber & Information Security.
Opera da svariati anni sui più importanti mercati nazionali ed internazionali, affiancando i maggiori Gruppi Industriali, Finanziari, Assicurativi, dell'Energia e dei Servizi nell'affrontare le nuove sfide per la protezione del proprio business.
Attraverso una costante attività di formazione e di investimenti nella Ricerca, Horizon Security è in grado di proporre servizi e soluzioni all'avanguardia ed al passo con i continui mutamenti degli scenari tecnologici e normativi.
Può contare su un team di professionisti qualificati e specializzati esclusivamente nell'ambito Cyber & Information Security, si propone come il partner ideale per soddisfare le esigenze delle aziende Enterprise negli ambiti:

- Strategy & Governance – Supportare le organizzazioni ad allineare ed integrare gli aspetti di Cyber Security rispetto alle priorità e dinamicità del proprio busienss e di compliance.
- Defensive Technology – Supportare le organizzazioni a definire ed adottare efficienti programmi tecnologici e relativi processi al fine di migliorare il livello di maturità in ambito Cyber Security.
- Threat & Incident Management – Supportare le organizzazioni a mantenere il proprio programma di Cyber Security in linea al continuo evolversi del business e landscape tecnologico, fornendo un'adeguata visibilità e gestione dei rischi Cyber.
- Operational Technology Security – Supportare le organizzazioni ad estendere i propri programmi di Cyber Security al contesto Operational Technology (OT) attraverso l'adozione di adeguati framework, processi e tecnologie.
- Emerging Technology Risks – Supportare le organizzazioni ad adottare ed implementare le tecnologie emergenti attraverso un approccio basato sul rischio Cyber.

Massimiliano Luraghi
Senior Manager

massimiliano.luraghi@horizonconsulting.com
www.horizonsecurity.it

INNOVERY GROUP
Gold Business Partner IBM

Innovery è una società multinazionale con sede in Italia, Spagna e Messico. Gestita da un team di professionisti e di grande esperienza, l'azienda si concentra sul mercato della Finanza, Industria, Utility, Energia, Retail e Telecomunicazioni e Pubblica Amministrazione.

Dal 2019, a seguito dell'entrata nell'azionariato di Wise Equity, il Gruppo mira ad accelerare ulteriormente la sua espansione favorendo la crescita organica, facendo leva sulle relazioni esistenti e costruendone di nuove, e attuando una strategia di M&A per sviluppare prodotti, servizi e mercati a livello internazionale. Il successo che l'azienda ha ricevuto in questi anni è dovuto alla vasta gamma di soluzioni e servizi personalizzati che offriamo ai nostri clienti. I nostri obiettivi sono quelli di continuare a stabilire partnership con i più importanti leader del mondo ICT e di costruire relazioni più forti con i nostri clienti basate su professionalità, supporto e servizi rapidi e affidabili, e offrire tecnologie e soluzioni utili a risolvere con successo le richieste attuali e crescenti. Nei prossimi tre anni, il piano di crescita dell'azienda si concentra sui miglioramenti ergonomici e lo sviluppo tecnologico negli attuali uffici, oltre ad aprirne di nuovi in tutto il mondo e ad ampliare l'offerta di servizi e soluzioni.

La nostra azienda ,composta da professionisti altamente qualificati, sta assumendo un ruolo di primo piano nel mondo dell'Information and Communications Technology, che è pieno di stimoli e in costante sviluppo.

Negli ultimi anni, Innovery ha accelerato il suo percorso di crescita attraverso l'acquisizione e l'integrazione di aziende altamente specializzate e innovative, consolidando così la sua posizione in Europa. Nel 2020 il gruppo ha raggiunto un fatturato di oltre 46 milioni di euro, con un organico di 350 dipendenti distribuiti tra Italia, Spagna e Messico.

Maria Mozzillo
Marketing & communications coordinator

maria.mozzillo@innovery.net
innovery.net

LUTECH

Il **Gruppo Lutech**, leader in Italia e player europeo nei servizi e soluzioni ICT, supporta la digital evolution delle aziende Clienti grazie alle competenze di oltre 2.700 professionisti e all'approccio end-to-end. Il Gruppo Lutech guida i propri Clienti nella sfida della Digital Trasformation con un'offerta all'avanguardia che unisce tre anime: LutechTechnology, che progetta, implementa e mette in sicurezza soluzioni di Hybrid Cloud Technology, LutechDigital, impegnata nella creazione della migliore customer experience e nella valorizzazione dei dati di Clienti, prodotti e performance aziendali, e LutechProducts, leader in soluzioni e prodotti proprietari specifici per ogni mercato. Le strategie di cybersecurity devono tener conto della costante mutazione genetica dei cyber attacchi e dei rischi della sicurezza delle informazioni. Per questo Lutech adotta un approccio olistico e multidisciplinare in grado di rinforzare tutte le componenti di difesa in modo congiunto.
L'approccio dei servizi di Security Advisory Lutech segue un modello consolidato:

- ASSESS: realizziamo assessment mirati per consentire al nostro Cliente di conoscere il grado di maturità del proprio sistema di gestione della cybersecurity.
- DESIGN: progettiamo piani specifici e personalizzati per i nostri Clienti rispettando il giusto equilibrio tra le esigenze di business e l'obiettivo di protezione dei dati e delle infrastrutture
- BUILD: grazie alle competenze di tutto il Gruppo Lutech siamo in grado di implementare le più svariate soluzioni tecnologiche
- OPTIMIZE: una volta che i processi sono in produzione affianchiamo il Cliente nel continuo miglioramento e nell'ottimizzazione degli stessi.

A conferma dell'approccio end-to-end, grazie al Next-Generation Security Operations Center-NG SOC, Lutech assicura la gestione completa della governance e dell'operatività legate alla sicurezza ai propri Clienti.

Roberto Leone
Advisory Practice Manager

r.leone@lutech.it
www.lutech.it

Microsoft

Fondata nel 1975, **Microsoft** abilita le organizzazioni pubbliche e private in tutto il mondo a realizzare i loro progetti di trasformazione digitale con nuovi scenari di innovazione, come Cloud Computing e Intelligenza Artificiale. La missione dell'azienda è sostenere persone ed organizzazioni ad ottenere di più, grazie alla tecnologia e al digitale. Microsoft vanta una lunga esperienza nel settore delle tecnologie innovative e oggi milioni di utenti stanno già utilizzando servizi e dispositivi sviluppati da Microsoft e dai suoi partner per il lavoro e il tempo libero. L'azienda ha inoltre maturato una profonda conoscenza in ambito Cloud Computing ed Artificial Intelligence, estendendo i vantaggi di queste tecnologie a tutti i campi di applicazione, dal business al consumer fino ai temi sociali.

Microsoft Italia è parte integrante e attiva dell'area Western Europe di Microsoft. Fondata nell'ottobre del 1985, la filiale dell'azienda di Redmond è presente sul territorio italiano con due sedi principali a Milano e Roma. Conta oltre 850 dipendenti e 10.000 aziende partner presenti sul territorio che impiegano oltre 350.000 professionisti su tecnologie Microsoft. È anche grazie a loro che la filiale italiana è diventata uno dei protagonisti dell'evoluzione digitale del nostro Paese, accompagnando milioni di imprese nel processo di trasformazione del loro business attraverso le nuove tecnologie. Microsoft Italia è inoltre impegnata a supportare studenti e docenti nell'adozione di tecnologie digitali per migliorare la didattica e l'apprendimento, fornendo competenze digitali.

Luba Manolova
Director, Business Group Lead Microsoft 365 Modern Work & Cybersecurity

luba.manolova@microsoft.com
www.microsoft.com

minsait
An Indra company

Minsait, Società di Indra (www.minsait.com), è l'Azienda leader nella consulenza negli ambiti della Digital Transformation e delle Information Technologies in Spagna e America Latina. Possiede un alto grado di specializzazione e conoscenza del settore, grazie alle sue capacità di integrare il mondo core con il mondo digitale, alla sua leadership nell'innovazione e nella trasformazione digitale e alla propria flessibilità. In questo modo la società focalizza l'offerta su proposte di valore ad alto impatto, basate su soluzioni end-to-end, con un notevole grado di segmentazione, che le consente di raggiungere risultati tangibili per i propri clienti in ogni settore con un focus sulla trasformazione. Le proprie capacità e leadership si riflettono nella suite di prodotti proprietari, sotto il marchio Onesait, e nella vasta gamma di servizi offerti.
In Italia Minsait conta più di 3000 professionisti che lavorano su tutto il territorio nazionale. La società ha sviluppato competenze avanzate in ambiti innovativi come Content & Process Technologies, Customer Experience Technologies, Solutions Architects e Data & Analytics, che consentono di offrire soluzioni e servizi ad alto valore aggiunto nei mercati in cui opera. Minsait ha localizzato in Italia il proprio centro di eccellenza globale per le tecnologie Customer Experience, completando la sua vasta presenza geografica con una consolidata capacità locale di produzione e delivery grazie ai centri di Napoli, Matera e Bari.
Nel 2020 Minsait ha rafforzato le proprie capacità e offering in Italia nella Cybersecurity con l'incorporazione nel Gruppo Indra di Net Studio, azienda italiana leader nelle soluzioni di identità digitale e access management. Net Studio ha un team di oltre 80 esperti e importanti clienti nei settori dell'industria, della finanza e dell'energia che gli hanno permesso di crescere rapidamente negli ultimi anni. Il suo portafoglio di soluzioni comprende: la governance delle identità digitali; la gestione delle identità; la gestione degli accessi; la gestione degli account privilegiati e la governance dei dati.

Francesco Casertano
Cybersecurity Managing Director

fcasertano@minsait.com
www.minsait.com/en

Posteitaliane

Con 159 anni di storia, una rete di oltre 12.785 Uffici Postali, 125 mila dipendenti, 569 miliardi di euro di attività finanziarie totali e 35 milioni di clienti, Poste Italiane è parte integrante del tessuto economico, sociale e produttivo del Paese e rappresenta una realtà unica in Italia per dimensioni, riconoscibilità, capillarità e fiducia da parte della clientela.

Poste Italiane è oggi la più grande realtà del comparto logistico in Italia ed è leader nel settore finanziario, assicurativo e dei servizi di pagamento.

Nel corso del 2021 Poste Italiane ha continuato il progressivo processo di trasformazione della rete logistica per consolidare la rete di distribuzione più capillare del Paese e renderla sempre più efficiente.

Questi importanti risultati collocano l'Azienda in una posizione privilegiata per cogliere le opportunità legate alla crescita dell'e-commerce, grazie anche a un consolidato know-how nel settore dei pagamenti e del digitale.

L'Azienda riveste un ruolo importante nel Paese, dando un forte contributo alla filiera produttiva e all'economia nazionale: investendo e operando insieme agli altri operatori della sua catena del valore, genera risultati positivi non solo attraverso il proprio business, ma anche generando esternalità tramite l'attivazione di una catena di fornitura locale.

Negi ultimi quattro anni, Poste Italiane ha intrapreso un'importante percorso di sostenibilità orientato a promuovere gli elementi distintivi della propria strategia aziendale, trasformare le sfide del mercato in opportunità di creazione di valore condiviso e concorrere allo sviluppo del proprio livello di reputazione. Oggi la sostenibilità è considerata una componente integrante delle attività, dei processi e della strategia aziendale.

www.posteitaliane.it

Rai è la Media Company italiana di servizio pubblico attiva in diversi comparti del mercato delle comunicazioni: Tv, Radio, Digital, Cinema, Home Video, Editoria. L'offerta, totalmente gratuita, comprende 14 canali Tv, 12 canali radio, le piattaforme multimediali RaiPlay e RaiPlay Sound (con relative App), i portali RaiNews (disponibile anche via App), Raisport.rai, Raicultura, a cui si aggiunge l'App RaiPlay Yoyo. Il Gruppo è presente anche su YouTube, MSN, Facebook, Twitter e Instagram con profili/account di canali e di programmi televisivi e radiofonici. Alla controllata Rai Com è affidata la commercializzazione dei canali Rai all'estero, a Rai Cinema le attività di acquisizione, produzione e distribuzione dei contenuti cinematografici e audiovisivi, a Rai Pubblicità la gestione in esclusiva delle comunicazioni commerciali su tutti i mezzi e le piattaforme Rai e a Rai Way la distribuzione e la manutenzione del segnale radiotelevisivo.

Federico Bertoni
Responsabile Analisi di Scenario

federico.bertoni@rai.it
www.rai.it

REPLY
SPIKE

Spike Reply è la società del gruppo Reply specializzata nei servizi di consulenza e nelle soluzioni integrate di cyber security e data protection. Spike supporta i propri clienti nello sviluppare e mantenere nel tempo un efficace programma di gestione del rischio cyber, in linea con gli obiettivi strategici e la propensione al rischio dell'organizzazione. In particolare, Spike Reply, supporta i propri clienti creando e mantenendo un Programma di Cyber Security per governare, analizzare, proteggere, rilevare e rispondere al panorama delle minacce, sviluppando metodologie e implementando soluzioni adeguate a mettere in sicurezza i processi, le architetture e le applicazioni del proprio clienti rispetto alle minacce in costante evoluzione. Attraverso un'ampia rete di partnership, Spike Reply aiuta inoltre i clienti nel selezionare le soluzioni di sicurezza più appropriate e innovative per proteggersi dai rischi e dalle minacce cyber.

Sonia Crucitti
Partner

s.crucitti@reply.com
www.reply.eu

TIM

TIM è il gruppo leader in Italia e in Brasile nel settore ICT, sviluppa infrastrutture fisse, mobili, cloud e datacenter e offre servizi e prodotti per le comunicazioni e l'intrattenimento, ponendosi all'avanguardia delle tecnologie digitali. Il Gruppo si compone di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e pubbliche amministrazioni, anche in partnership con gruppi di primaria importanza: **Noovle** è la cloud company di TIM, **Olivetti** è il polo digitale con focus sullo sviluppo di soluzioni Internet of things, **Telsy** opera nel settore della cybersecurity e **Sparkle** realizza e mette a disposizione infrastrutture e servizi internazionali. In Brasile, **TIM Brasil** è uno dei principali player nel mercato delle telecomunicazioni e leader nella copertura 4G. Nello sviluppo del business il Gruppo ha fatto propri obiettivi di tutela dell'ambiente e di inclusione sociale con l'intento di ottenere un impatto concreto e rilevante e diventare **carbon neutral nel 2030**. Con il progetto **Operazione Risorgimento Digitale** – la prima grande scuola di Internet gratuita – vengono diffuse competenze digitali al Paese, mentre **Fondazione TIM** è l'espressione dell'impegno sociale di TIM.

Cristiano Alborè
Portfolio Development Director di Telsy

cristiano.albore@telsy.it
www.gruppotim.it

VARGROUP Platinum Business Partner IBM | YARIX a vargroup company

Yarix è la società a capo della divisione Digital Security di **Var Group** – player di riferimento in Italia nel settore dei servizi e delle soluzioni digitali per le imprese - e una delle aziende italiane più riconosciute, innovative e autorevoli nel comparto della sicurezza informatica: da 20 anni fornisce servizi e soluzioni di cyber security, business continuity e disaster recovery a industrie, enti governativi e militari, aziende del comparto sanitario e università. Dispone di un Cognitive Security Operation Center tra i più evoluti in Italia e si avvale di team specializzati in defensive e offensive security, Cyber Threat Intelligence, Incident Response. Il 2014 ha visto l'avvio di una strategia di crescita finalizzata alla creazione di un polo di eccellenza per la gestione globale della sicurezza delle imprese. Attraverso un processo di acquisizioni che ha portato all'integrazione di realtà col maggiore potenziale e le competenze più evolute in Italia, Var Group e Yarix offrono alle aziende italiane – che affrontano le sfide dell'innovazione tecnologica e della trasformazione digitale – un nuovo livello di protezione fondato su un approccio olistico alla Security.

Var Group, con un fatturato di 480 milioni di Euro al 30 aprile 2021, oltre 2700 collaboratori, 23 sedi in tutta Itali e 8 all'estero in Spagna, Germania, Austria, Romania, Svizzera e Cina, è uno dei principali partner per l'innovazione digitale. L'offerta Var Group trae la sua forza dalla profonda conoscenza dei processi aziendali e dall'integrazione di più elementi. È frutto del lavoro di Business Unit focalizzate nello sviluppo di progetti di: Customer Experience, Digital Process, Digital Industries, Digital Cloud, Digital Security, Smart Services, Cognitive & Advanced Analytics e Business Technologies Solutions.

Elena Vidotto
Marketing Manager, Digital Security

elena.vidotto@yarix.com
www.vargroup.it

vodafone business

Vodafone è una delle principali società di telecomunicazioni in Europa e Africa. Il nostro purpose – Connect for a better future – la nostra esperienza e il nostro raggio d'azione ci danno l'opportunità unica di guidare un cambiamento positivo per la società. Le nostre reti permettono a famiglie, amici, aziende e governi di restare connessi e, come ha dimostrato l'emergenza COVID-19, svolgiamo un ruolo fondamentale per economie e settori critici, come l'istruzione e la sanità. Siamo il più grande operatore di rete mobile e fissa d' Europa e il più grande provider di connettività IoT del mondo. In Africa la nostra piattaforma tecnologica M-Pesa consente a oltre 45 milioni di persone di accedere a pagamenti e servizi finanziari mobili. Gestiamo reti mobili e fisse in 21 Paesi e siamo presenti con accordi di partnership nel mercato della rete mobile di altri 48. Al 30 settembre 2020 Vodafone contava più di 300 milioni di clienti di rete mobile, più di 27 milioni di clienti di rete fissa a banda larga, oltre 22 milioni di clienti TV e oltre 112 milioni di dispositivi IoT connessi. A giugno 2019 Vodafone Italia ha lanciato il 5G su rete commerciale, prima in Italia, a Milano e 28 comuni dell'area metropolitana, a Roma, Torino, Bologna e Napoli. A Milano, capitale europea del 5G, Vodafone ha superato il 90% di copertura 5G della popolazione. Vodafone ha lanciato nel 2019 Vodafone Business e varato un piano di investimenti di 240 milioni incrementali in 5 anni per creare servizi e competenze che integrano le nuove tecnologie di connettività e convergenza – dal 5G alle soluzioni di rete virtualizzate configurabili dal cliente (Software Defined Network) – con applicazioni e servizi che risolvono problemi di business attraverso l'adozione del digitale in tutti gli elementi della catena del valore: dai processi industriali alla supply chain, dal controllo e ridisegno dei processi, fino allo sviluppo e all' erogazione dei prodotti e servizi ai clienti. Le nuove applicazioni e i nuovi servizi saranno realizzati, sia attraverso lo sviluppo diretto di piattaforme da parte di Vodafone (IoT, Analytics, Cloud), sia con la creazione di un ecosistema di partnership nazionali e internazionali. Vodafone sta facendo passi importanti anche per minimizzare il proprio impatto ambientale. In Italia, la rete Vodafone è già alimentata al 100% da fonti rinnovabili tramite l'acquisto di energia prodotta esclusivamente da fonti rinnovabili certificate per la propria rete e anche per i propri uffici. Inoltre, prima tra le aziende di telecomunicazioni, Vodafone Italia ha anticipato gli obiettivi di zero emissioni proprie di gas a effetto serra al 2025.

Gabriele Scialò
Product Manager Security

gabriele.scialo@vodafone.com
www.vodafone.it/portal/Aziende

//WHITEJAR.IO
POWERED BY UNGUESS

In Italia, **WhiteJar** è la prima piattaforma di bug security testing che coinvolge una community di hacker etici reclutati nel crowd secondo elevati standard di competenza tecnica e reputazione. Si tratta del servizio di cybersecurity offerto da UNGUESS, prima conosciuta come AppQuality.

La piattaforma lavora interamente il concetto di collaborazione e di conoscenza collettiva, coinvolgendo quindi una intelligenza umana ed allargata nella ricerca comune di vulnerabilità dei sistemi informatici proponendo anche una soluzione a quelli eventualmente trovati: le situazioni da testare sono infatti esposte a una moltitudine di differenti approcci e competenze tecniche. L'azienda cliente di WhiteJar ha il pieno controllo della comunicazione con la community, cercando vulnerabilità che, una volta scoperte, consentiranno di essere rimediate e alle quali corrisponderà una ricompensa per l'Ethical Hacker che l'ha scovata.

Si tratta di un modello competitivo che porta a creare report accurati, che contengono le vulnerabilità individuate e i suggerimenti di remediation.

Aldo Fucelli Pessot del Bo
Head of Cybersecurity

aldo.delbo@unguess.it
whitejar.io

WIIT
THE PREMIUM CLOUD

WIIT SpA è uno dei principali player europei nel mercato del Cloud Computing con soluzioni di Hybrid Cloud e Hosted Private Cloud per Applicazioni Critiche. Il Gruppo, quotato sul segmento STAR di Borsa Italiana, si rivolge a clienti con importanti esigenze di continuità: aziende leader nei propri settori che cercano nel partner tecnologico di riferimento elevati livelli di efficienza e sicurezza, nonché la capacità di scalare per rispondere a fabbisogni via via crescenti. WIIT è presente sul mercato con 9 sedi in Italia e 5 all'estero, oltre 400 dipendenti e 12 DC di classe Enterprise di cui il principale è certificato Tier IV dall'Uptime Institute. La strategia di WIIT è focalizzata su competenze e servizi di eccellenza, grazie ai continui investimenti in asset tecnologici e all'attività di M&A che viene condotta in maniera sistematica, da 4 anni, da un team dedicato, sia in Italia che all'estero: il progetto CLOUD4EUROPE, nato nel 2020 con l'acquisizione del provider tedesco myLoc Managed IT e sviluppato da ulteriori operazioni, ha l'obiettivo di creare il leader europeo nel Cloud delle Applicazioni Critiche. Il modello di deploy Hybrid Cloud di WIIT permette, infatti, di garantire elevati livelli di servizio costituiti da ambienti On Premises, Private e Public, col fine ultimo di garantire la Business Continuity globale dei processi aziendali. La capacità di gestire le principali suite applicative ha il suo fiore all'occhiello in ambito SAP, dove WIIT vanta 6 certificazioni per la gestione continuativa delle piattaforme tecnologiche SAP e SAP HANA in modalità PaaS, collocandosi tra i pochi partner SAP al mondo con il maggior numero di certificazioni di Outsourcing Operations. Il modello di WIIT è rafforzato dalla piattaforma proprietaria di Cyber Security as a Service, il cui framework è stato premiato sia nel 2018 che nel 2020 ai Digital360 Awards.

Giuseppe Colosimo
Cyber Security Director

Giuseppe.colosimo@wiit.cloud
www.wiit.it

blue is underwriting

BLUE è un'agenzia ad alta competenza per la sottoscrizione di coperture assicurative per professionisti, per le figure apicali delle imprese e per la tutela della sicurezza CYBER.

Polo di riferimento tecnico, grazie alle autonome capacità di sottoscrizione delegate dalle più importanti Compagnie internazionali del segmento, propone un modello di approccio al rischio cyber di cui è parte centrale e innovativa HAIKU®, una web-application proprietaria - frutto di una specifica ricerca - che, grazie a un algoritmo di stima del livello complessivo di rischio - che auto-apprende dalla propria esperienza - è capace di raccogliere e analizzare le informazioni correlate al perimetro di un dominio.

Cyber Guru

Cyber Guru (www.cyberguru.it) nasce in Italia nel 2017 con l'obiettivo di contribuire a creare una cultura diffusa della sicurezza informatica, ridefinendo il concetto di Cyber Security Awareness attraverso lo sviluppo di soluzioni innovative in grado di agire efficacemente sul fattore umano e trasformare l'anello debole della catena difensiva, nella prima linea di difesa contro il Cyber Crime. Le soluzioni della piattaforma Cyber Guru, attraverso percorsi di apprendimento educativi e stimolanti, si rivolgono a tutti coloro che non ricoprono ruoli specialistici in ambito Cyber Security. Ogni elemento di Cyber Guru è stato progettato e realizzato per massimizzare l'efficacia del contributo formativo, minimizzando l'effetto dispersivo e annullando i costi di gestione. Le soluzioni progettate sulla base di un approccio metodologico esclusivo, consentono alle organizzazioni di formare e addestrare i propri dipendenti a un uso corretto delle tecnologie digitali, aumentando il livello di protezione di individui e organizzazioni. Automazione, Intelligenza Artificiale e Gamification, sono solo alcune delle caratteristiche che rendono la piattaforma Cyber Guru unica nel suo genere.
I 3 percorsi formativi della piattaforma consentono di sviluppare programmi di addestramento fortemente sinergici:

- Cyber Guru Awareness: un innovativo sistema integrato di e-learning che consente di coinvolgere tutta l'organizzazione in un percorso di apprendimento particolarmente coinvolgente, basato su una metodologia di formazione continua.
- Cyber Guru Phishing: un innovativo sistema di apprendimento esperienziale adattivo, che ha lo scopo di aumentare la resistenza dell'organizzazione agli attacchi phishing e che produce risultati efficaci grazie alla sua metodologia avanzata e alle caratteristiche di automazione e di intelligenza artificiale.
- Cyber Guru Channel: un percorso di formazione video basato su una metodologia induttiva, realizzato con tecniche di produzione avanzata, tipiche delle serie TV, e basato su uno storytelling particolarmente coinvolgente.

Camilla Bassi
Fondatore e Amministratore Delegato

camilla.bassi@blueunderwriting.com
blueunderwriting.com

Maurizio Zacchi
Marketing & Digital Learning Manager

maurizio.zacchi@cyberguru.eu
www.cyberguru.it

HUAWEI

Founded in 1987, **Huawei** is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. We have more than 197,000 employees, and we operate in more than 170 countries and regions, serving more than three billion people around the world. Innovation has been fundamental to Huawei's survival and development over the past three decades. In this time we have continuously invested over 10% of our annual revenue back into R&D and in 2020 we had approximately 105,000 R&D employees, accounting for 53,4% of our total workforce. We are committed to bringing digital to every person, home and organization for a fully connected, intelligent world. To this end, we will:

- Drive ubiquitous connectivity and promote equal access to networks;
- Provide the ultimate computing power to deliver ubiquitous cloud and pervasive intelligence;
- Build digital platforms to help all industries and organizations become more agile, efficient, and dynamic;
- Redefine user experience with AI, making it more personalized for people across all scenarios, whether they're at home, in the office, or on the go.

Alida Zentai
R&D Legal Manager

alida.zentai@huawei.com
www.huawei.com

THALES

Thales (Euronext Paris: HO) is a global leader in advanced technologies, investing in digital and "deep tech" innovations – connectivity, big data, artificial intelligence, cybersecurity and quantum computing – to build a confident future crucial for the development of our societies. The Group provides its customers – businesses, organisations and governments – in the defense, aeronautics, space, transport, and digital identity and security domains with solutions, services and products that help them fulfil their critical role, consideration for the individual being the driving force behind all decisions.
Thales has 81,000 employees in 68 countries. In 2020 the Group generated sales of €17 billion.

Anna Sangalli
Sales & Lead Management Specialist

anna.sangalli@thalesgroup.com
www.thalesgroup.com/it

Zscaler accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange basata su SAS è la più grande piattaforma di sicurezza cloud in linea al mondo.

Alessio Stellati
Country Manager

astellati@zscaler.com
www.zscaler.com

aditinet secure, together

Aditinet Consulting SpA è una società italiana nata nel 2004 che offre consulenza e servizi in ambito Cybersecurity, Networking e Cloud Security. La nostra azienda ha un respiro internazionale, avendo aperto nel corso degli anni anche una sede a Londra e una sede a Pristina. Il nostro impegno è quello di accompagnare i clienti lungo un percorso di Trasformazione Digitale in Sicurezza, con un modello di business che ci vede attivi dalle prime fasi di consulenza, alla progettazione, al set-up fino all'assistenza durante tutto il ciclo di vita dei sistemi. Un ruolo importante è rivestito dai nostri Managed Services interni di SOC (Security Operation Center) e NOC (Networking Operation Center).

CRYPTONET LABS

CryptoNet Labs si occupa di Cybersecurity in tutte le sue declinazioni e, grazie all'esperienza ultraventennale del suo team, supporta il mercato in tre aree di intervento:

- Consulting & Compliance, dove affianchiamo il cliente, per accompagnarlo in un percorso di certificazione e per supportarlo in modo proattivo o reattivo nel prevenire o risolvere problemi di Cybersecurity, sia su specifiche esigenze puntuali sia con collaborazioni protratte nel tempo;
- Security Services & Products, che comprende le attività di Offensive Security, dedicate al security testing in molteplici ambiti tecnologici, e i nostri interventi di Defensive Security, dedicati all'integrazione di soluzioni proprietarie o di nostri partner negli ambienti dei clienti, per innalzarne il livello di sicurezza;
- Managed Services, che offre soluzioni "as a service" per la certificazione della sicurezza delle applicazioni e la protezione proattiva dalle minacce con il nostro servizio di Bodyguard Digitale basato su tecniche di Cyber Threat Intelligence.

Cryptonet Labs è certificata ISO 9001 e ISO 27001 per progettazione ed erogazione di servizi in ambito di Cybersecurity, dispone di un Laboratorio di prova accreditato da Accredia secondo lo standard ISO/IEC 17025 per l'esecuzione di Vulnerability Assessment ed è qualificata come QSA company dal PCI Council.

Marco Gornati
Sales Director

Marco.gornati@aditinet.it
www.aditinet.it

Stefano Taino
CEO

stefano.taino@cryptonetlabs.it
www.cryptonetlabs.it

Cefriel
POLITECNICO DI MILANO

Cefriel, fondato nel 1988 da università, imprese e amministrazioni locali per promuovere la collaborazione e la condivisione di conoscenze tra mondo della ricerca, tessuto economico e società, è il partner di Ricerca, Innovazione e Formazione che da oltre 30 anni accompagna le imprese nazionali e internazionali nel loro percorso di innovazione digitale, dall'ideazione dei prodotti e servizi, alla loro realizzazione, messa in esercizio e gestione in un processo ripetibile nel tempo. Cefriel è abilitatore e scientific trusted advisor per un uso responsabile delle tecnologie digitali a servizio dello sviluppo e della crescita sostenibile dell'impresa. Cefriel per la Cybersecurity. In ambito Cybersecurity, Cefriel è partner strategico per le imprese per l'analisi, la progettazione e lo sviluppo di strumenti per la gestione della sicurezza delle informazioni, soprattutto nei settori in cui la confidenzialità, l'integrità e la disponibilità delle informazioni sono fattori critici. Cefriel mette a disposizione delle aziende la propria "doppia anima":

- l'anima "Sapiens" in quanto, grazie alla propria posizione di attore scientifico e terza parte indipendente, è in grado di indirizzare le aziende nella comprensione dei propri rischi Cyber e nelle scelte strategiche da compiere per minimizzarli;
- l'anima "Faber" in quanto è in grado di mettere a terra alcune delle azioni di remediation identificate tramite progetti di innovazione o azioni di formazione mirate.

Sfide

- Comprendere le minacce. Comprendere in modo continuativo le nuove minacce alla sicurezza e i problemi legati alle tecnologie emergenti (continuous security).
- Gestire i rischi cyber. Ridurre l'esposizione ai rischi per la sicurezza informatica in modo sostenibile, lavorando anche sul fattore umano.
- Promuovere la cultura cyber. Diffondere e promuovere i "Key Facts" della Cybersecurity anche ai non specialisti, visto che gli attacchi impattano sia sull'operatività che sul business.

Come vincerle? La risposta di Cefriel:
Cefriel si occupa di sicurezza informatica affrontandone tutti i diversi aspetti in tre contesti: innovazione, ricerca, formazione. Promuove un approccio olistico che include il fattore umano, la governance e le tecnologie, al fine di garantire nel tempo la sicurezza e la sua sostenibilità, in termini non soltanto economici, ma anche di tecnologie, processi, persone e conoscenze.
Tre in particolare i fattori distintivi di questa risposta:

- l'autorevolezza di Cefriel come ente dalla costituency istituzionale no-profit
- la stretta connessione fra innovazione e ricerca e la intrinseca interdisciplinarità
- la sinergia di competenze ed esperienza che permea l'offerta formativa e di innovazione.

Cefriel risponde ai bisogni delle aziende offrendo il proprio Sustainable Cybersecurity PlaybookTM, un insieme di best practice e metodologie per ridurre in modo sostenibile il rischio cyber su uno o più pillar di un'azienda (esperti di cybersecurity, dipendenti e top management, sistemi informativi, dispositivi sul campo, top management...).
I servizi offerti:
Il Sustainable Cybersecurity PlaybookTM raccoglie cinque servizi specifici, alcuni di natura multidisciplinare, ma con un chiaro focus sulla Sicurezza Informatica:

- Servizio Smart Cybersecurity Posture Analysis – "Test before invest" – Cefriel fornisce all'organizzazione la Big Picture dei rischi cyber, con relativo piano di remediation con cui minimizzarli.
- Servizio Identity Management Assessment – "Raise your walls for an Identity Management viewpoint" – Cefriel è in grado di valutare il grado di sicurezza di una piattaforma di Identity Management sia in modo white-box che black-box.
- Servizio Integrated Social-Driven Vulnerability Assessment, Training – SDVA, Training – "Enforce the Employees resiliency bringing the human factor into the equation" – Cefriel può misurare il rischio derivante dal fattore umano per pianificare azioni di formazione mirate ai dipendenti di un'azienda.
- Servizio Full Spectrum Vulnerability Assessment – FSVA – "Enforce the Incident Response Team resiliency" – Cefriel è in grado di misurare il rischio derivante dal fattore umano mediante la simulazione di una campagna d'attacco completa, che testa la responsiveness del team di incident management.
- Servizio Data Visualization for Security - Dataviz 4 Security – "Give actionable information also to non-Cybersecurity People to manage your Cyber Security risks" – Cefriel supporta l'identificazione, definizione e rappresentazione di Key Security Indicator e Key Risk Indicator, anche a beneficio dei non addetti ai lavori.

Enrico Frumento
Cybersecurity Senior Domain Specialist

enrico.frumento@cefriel.com
www.cefriel.com

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA

Il **Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB)** è uno dei più grandi dipartimenti di ICT in Europa. Con circa 840 collaboratori, tra personale di ricerca strutturato, collaboratori esterni, studenti di dottorato e personale tecnico e amministrativo, il Dipartimento costituisce una realtà vitale in grado di sostenere la formazione, la ricerca di base, la ricerca applicata e l'attività di trasferimento tecnologico alle imprese.

La qualità della ricerca scientifica è l'obiettivo principale del DEIB, perseguito secondo i più elevati standard internazionali di qualità. All'interno del dipartimento sono presenti competenze eccellenti e consolidate, sia a livello nazionale che internazionale, nei settori dell'automazione, dell'informatica, dell'elettronica, della bioingegneria, dell'ingegneria elettrica e delle telecomunicazioni.

La qualità del lavoro di ricerca è testimoniata dalla vasta rete di collaborazioni con le migliori istituzioni internazionali, che fa del Dipartimento uno dei principali attori dello scenario mondiale dell'innovazione scientifica e tecnologica.

L'ambiente di ricerca del DEIB comprende anche la società consortile CEFRIEL e dodici spin-off.

www.deib.polimi.it

Sostenitori della Ricerca – Con il Patrocinio di

Cybersecurity: don't look up

ANRA è l'associazione che dal 1972 raggruppa i risk manager e i responsabili delle assicurazioni aziendali in Italia. Opera attraverso la sede di Milano e vari corrispondenti regionali e ha come obiettivo principale la diffusione della cultura d'impresa attraverso la gestione del rischio in azienda. È diventata negli anni il principale interlocutore istituzionale in Italia sulle tematiche di risk e insurance management. A livello internazionale fa parte di FERMA (in Europa) e IFRIMA (network globale). Annovera tra le sue attività convegni e workshop, corsi di formazione, erogazione di informazione altamente qualificata, momenti di networking e supporto professionale. ANRA è costituita da oltre 630 Soci, Risk Officer, Risk Manager ed Insurance Manager le cui aziende rappresentano complessivamente un fatturato di oltre 600 miliardi (pari a circa il 39% del PIL). Nella sua attività di supporto a manager ed imprese, ANRA si appoggia a molti partner, come enti universitari, società di consulenza, compagnie assicurative, broker, società di servizio nell'ambito del rischio d'impresa: con le loro competenze specifiche, tutti questi attori portano valore aggiunto ai membri dell'associazione e alle loro imprese.

Assintel è l'associazione nazionale di riferimento delle imprese ICT e rappresenta le aziende che lavorano nell'ecosistema tecnologico e digitale. Aderisce a Confcommercio – Imprese per l'Italia, entro cui è punto di riferimento per tutti i temi e le iniziative che mirano a diffondere la cultura dell'Innovazione nel tessuto imprenditoriale locale e nazionale, mettendo in contatto Domanda e Offerta e stimolando un approccio empatico al mercato. Da qui l'orizzonte si estende all'insieme di stakeholder, pubblici e privati, verso i quali si fa promotrice di politiche, strategie e azioni che incidano sullo sviluppo del Sistema Paese. L'associazione interpreta, traduce e comunica le esigenze dell'ecosistema di partnership composto da operatori globali e locali che operano su tutto il territorio nazionale e nei diversi segmenti del mercato ICT: è un vero business network, capace di creare relazioni, sinergie e opportunità concrete per le aziende socie. L'associato è al centro del programma di Assintel: dalle sue esigenze nascono le strategie, i servizi e gli eventi. Far parte di un'associazione di categoria è strumento fondamentale per consentire all'azienda di entrare in un network di imprese che condividono esigenze e approcci al mercato, di avere una posizione più forte sul mercato, di usufruire di canali privilegiati di accesso alle risorse e ai finanziamenti, di far sentire la propria voce sui tavoli di discussione politici regionali e nazionali. Cuore dell'offerta di Assintel è la gamma di servizi per l'azienda - attraverso la collaborazione delle strutture territoriali - e soprattutto lo sviluppo di iniziative strategiche per il mercato ICT. Iniziative ed eventi anche in modalità digitale, ricerche e analisi di scenario, incontri territoriali di networking, la presenza istituzionale a prestigiosi eventi e fiere di settore, i progetti in collaborazione con le Istituzioni, la formazione finanziata, le convenzioni, i gruppi di lavoro settoriali sono solo alcune delle iniziative che Assintel sviluppa per i propri associati.

Stefano Barboni
Membro del Comitato per la Digitalizzazione dei Rischi

stefano.barboni@riesko.com
www.anra.it

Davide Giribaldi
Coordinatore del Gruppo di lavoro Cybersecurity

davide.giribaldi@encyberisk.it
www.assintel.it

Il **Clusit**, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più autorevole associazione italiana nel campo della sicurezza delle informazioni. Oggi rappresenta oltre 700 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Collabora con diversi Ministeri ed Agenzie Governative, con le Forze dell'Ordine, con il Garante per la Privacy, con Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Banca d'Italia, Confindustria e Confcommercio. Tra le attività ed i progetti per il 2022, ci sono: la realizzazione di 28 webinar, in collaborazione con gli Osservatori del Politecnico di Milano; la produzione di un libro sul tema del Rischio, a cura della Clusit Community for Security; il Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria, arrivato alla 17a edizione; 2 Security Summit, conferenze specialistiche in versione ibrida (in streaming e parzialmente on site) dal 15 al 17 marzo a Milano e in novembre a Roma; 12 Atelier della Security Summit Academy; 4 eventi verticali, dedicati ai settori Energy & Utilities (26 maggio), Healthcare (16 giugno), Finance (22 settembre) e Industriale/Manifatturiero (20 ottobre); i Rapporti Clusit, due all'anno, con pubblicazione a marzo e ottobre, sul Cyber-crime e sullo stato della sicurezza delle informazioni e delle reti in Italia; il Mese Europeo della Sicurezza Informatica, campagna di sensibilizzazione della Commissione Europea e dell'ENISA che si svolge ogni anno in ottobre, coordinata in Italia da Clusit.

Paolo Giudice
Segretario Generale

pgiudice@clusit.it
www.clusit.it

Ringraziamenti

Cybersecurity: don't look up

Si ringraziano inoltre le organizzazioni che, oltre alle aziende sostenitrici, sono state coinvolte nella Ricerca e vi hanno partecipato attivamente:

3F Filippi, A2A, Acciaieria Arvedi, Acea, ACI - Automobile Club D'Italia, Acsm - Agam, Aeroporto G. Marconi Di Bologna, Afv Acciaierie Beltrame, Agos Ducato, Alcantara, Alia Servizi Ambientali, Allianz, Alpiq Energia, Amg Energia, Amissima Assicurazioni, Ansaldo Energia, Arca Vita, Arera - Autorità Di Regolazione Per Energia Reti e Ambiente, Arnoldo Mondadori Editore, Arpa Industriale, Arriva Italia, Ascopiave, Assaeroporti - Associazione Italiana Gestori Aeroporti, Assicurazioni Generali, Asst Papa Giovanni XXIII, Ausl Valle D'Aosta, Automobili Lamborghini, Autorità Di Sistema Portuale Del Mar Tirreno Centro Settentrionale, Autorità Nazionale Anticorruzione, Autostrade per l'Italia, Aviva, Axa Assicurazioni, Banca Carige, Banca Generali, Banca Ifis, Banca Mediolanum, Banca Profilo, Banca Progetto, Banca Sella, Banco Bpm, Banco Desio, Bayer, Bitron Industrie, Bnp Paribas Cardif Vita, Bonfiglioli, Bosch, Bottega Verde, Brandart Image Packaging, Bricoman, Bartolini Corriere Espresso, Butali, Bwh Hotel Group, Calvi Holding, Calzedonia, Camera di Commercio di Torino, Carel Industries, Cassa Di Risparmio Di Volterra, Cellularline, Cesar di Barbarossa Enio & F.Lli, Chiesi Farmaceutici, Cira - Centro Italiano Ricerche Aerospaziali, Cnh Industrial, Cnp Unicredit Vita, Coca-Cola Hbc Italia, Cofidis, Comifar Distribuzione, Consob, Consorzio Servizi Bancari, Comune Di Firenze, Comune Di Milano, Consip, Coop Alleanza 3.0, Corte Dei Conti, Credit Suisse, Credito Valtellinese, Crif, Danieli & C., De Nora, Bff Banking Group, Dfree, Dhl Express Italia, Dolce & Gabbana, Dolomiti Energia Holding, Ducati Motor Holding, Edison, Electrolux Italia, Enav, Enel, Eni Gas e Luce, Esprinet, Evoca, Fecs Group, Ferrovie Dello Stato Italiane, Fiditalia, Florim Ceramiche, Gamenet, Gei - Gestione Energetica Impianti, Generalfinance, Gewiss, Gi Group, Gnutti Carlo, Goglio, Grandi Navi Veloci, Gruppo Ab, Gruppo Agsm, Gruppo Ermenegildo Zegna, Gruppo Feltrinelli, Gruppo FCA, Gruppo Hera, Gruppo Itas, Gruppo Lube, Gruppo Pellegrini, Gruppo Percassi, Gucci, Humanitas, Iccrea Banca, Illimity Bank, Inail, Ineos, Infocamere, Intesa Sanpaolo, Iren, Italcementi, Italgas, Italia Distribuzioni, Italiana Assicurazioni, Italiaonline, Italo, Izsler, Johnson Electric, Julia Portfolio Solutions, Kiko, Leroy Merlin, Lima, Liomatic, Lottomatica, Luxottica,

Ringraziamenti

Cybersecurity: don't look up

Maire Tecnimont, Marcegaglia, Marelli, Mediaworld, Midi Europe, Ministero Dell'Interno, Multi-Color Corporation, Multimedica, Octo Telematics, Ori Martin, Paydo, Pelliconi & C., Permastelisa, Pfizer Italia, Philip Morris International, Pirelli, Profumerie Douglas, Prysmian Group, Publiacqua, Randstad, Regione Lazio, Rexroth, Rina, Rivacold, Roche Diagnostic, Sacbo, Saipem, Salvatore Ferragamo, Sedamyl, Siram, Sisal, Snam, Societe Generale Securities Services, Spal Automotive, Stefano Ricci, Stella Mccartney, Stmicroelectronics, Technip Italy, Telespazio, Tenova, Terna, Texa, Transmec Group, Unicoop Firenze, Unicredit, Unifarm, Unipolsai, Vimar, Virgin Active, Vittoria Assicurazioni, Vorwerk Italia, Webuild, Wittur Group.

PARTNER

SPONSOR

SUPPORTER

IN COLLABORAZIONE CON

CON IL PATROCINIO DI

Illustrazioni: *Silvia Re*
Impaginazione: *Danilo Galasso*, *Emanuela Micello* e *Stefano Erba*

osservatori.net