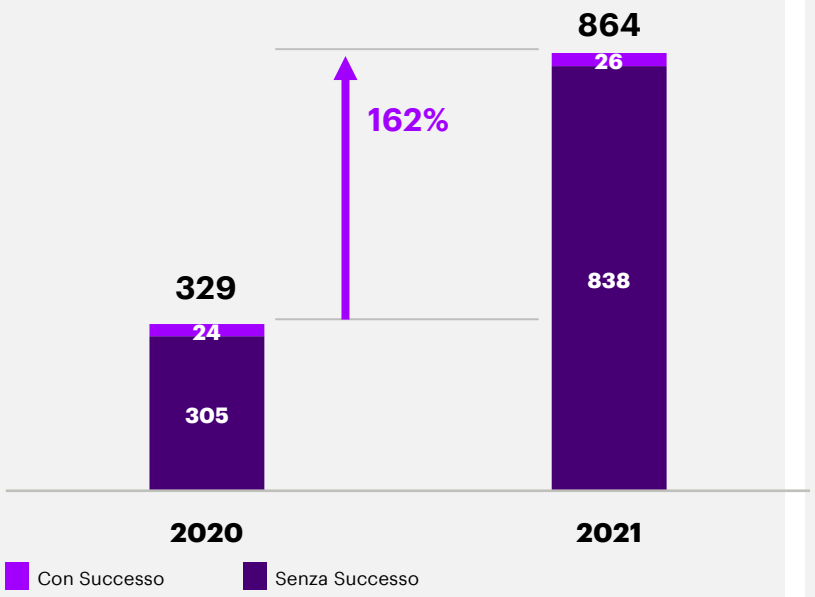
Cybersecurity: nuove frontiere di innovazione per rispondere alle crescenti minacce

ABI LAB Forum | 24 Marzo 2022 Marco Valsecchi, Accenture Security

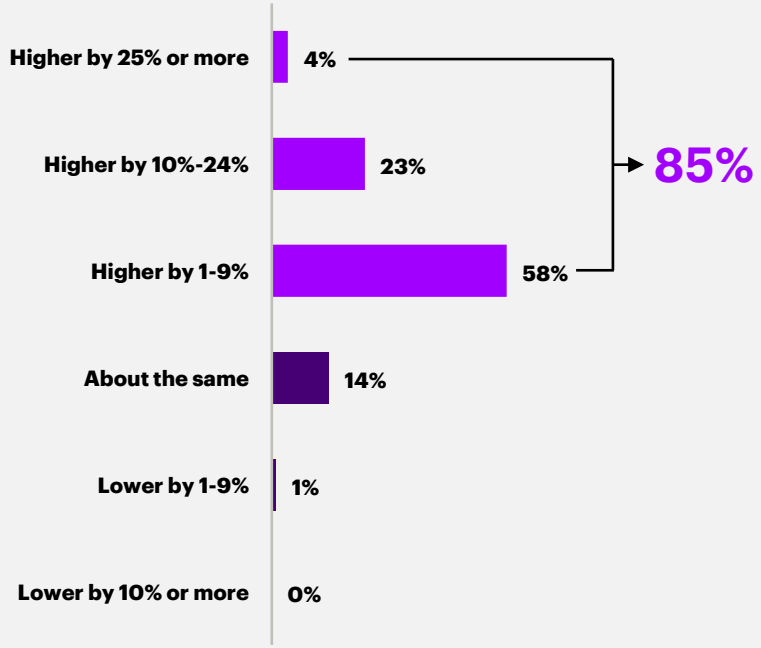
accenture

Lo stato della cybersecurity

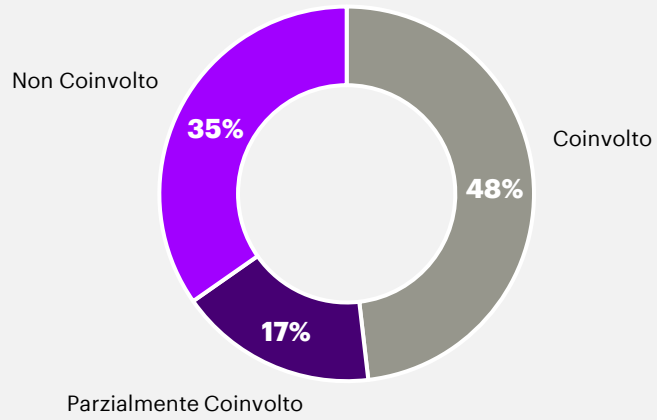
864 attacchi mediamente identificati per azienda, con un incremento del 162% rispetto al 2020



L'85% delle organizzazioni ha incrementato lo spending in sicurezza



Il 35% delle strutture di Sicurezza non è ancora coinvolto nelle valutazioni in merito all'implementazione di soluzioni cloud



Fonte: Accenture State of Cybersecurity Resilience surveys
Wave 3 report published in January 2020 (N=4,644) and Wave 4 report published in November 2021 (N=4,244)
FS N=922

Quali sono i driver che guidano la strategia di cyber security?

Elementi chiave da considerare

NEW RULES

Sono sempre più numerosi i requisiti normativi cui le Banche devono adempiere

Tecnologie e risorse necessarie non sempre sufficienti. I requisiti devono essere affrontati con una strategia univoca

NEW THREATS

Nuove minacce con impatto sui dati e sulla continuità dei servizi richiedono approcci complessi

Servizi di threat intelligence avanzati sono necessari per anticipare le possibili minacce di sicurezza

NEW BUSINESS

Nuovi modelli di business abilitati dalla PSD2 devono essere supportati da controlli specifici

L'accesso ai dati bancari dei clienti da terze parti deve essere adeguatamente controllata

NEW TECH

Nuove tecnologie introducono nuovi rischi di sicurezza ma abilitano anche nuove funzionalità di controllo

L'introduzione di nuove tecnologie (cloud, quantum computing, IA, ...) deve incrementare I livelli di sicurezza

NEW PARTNERS

Il numero di terze parti coinvolte cresce in funzione della specializzazione delle competenze richieste

Il controllo di una molteplicità di fornitori richiede approcci industriali e standard

Il continuo cambiamento del contest esterno, nuove minacce e nuovi servizi di business impattano il livello di sicurezza. Un approccio completo, flessibile e scalabile è necessario per garantire nel tempo un Sistema resiliente e robusto

Metodologia per piani di cyber security

ENTERPRISE WIDE

Tutti i sistemi e di dati aziendali devono essere presidiati in modo coerente

… (non dimentichiamoci qualche pezzo)

EXTENDED ECOSYSTEM COVERAGE

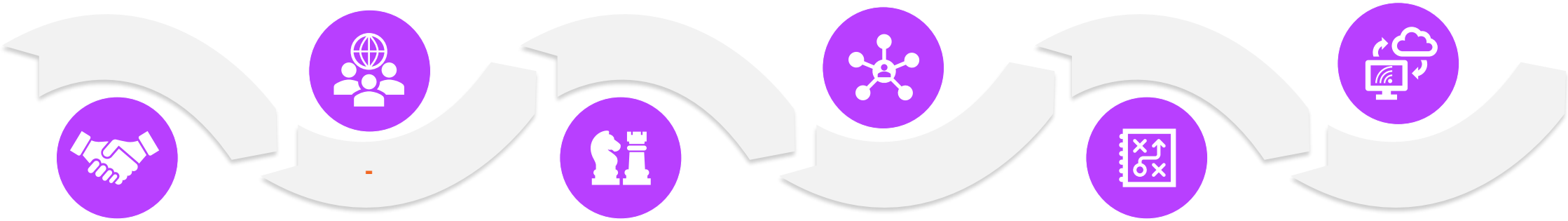
Proteggere la propria azienda significa contribuire alla sicurezza del sistema bancario

… (e la nostra vita quotidiana)

TECHNOLOGY ENABLED

Il modello e l'architettura di sicurezza sono più importanti della singola tecnologia

… (solo la tecnologia non aiuta)



RISK DRIVEN

La strategia di cyber security deve basarsi sull'accettazione cosciente dei rischi residui

… (si può accettare di correre dei rischi purché sia noto)

EXPOSURE FOCUSED

Non è sufficiente rispondere ai requisiti normativi ma è necessario rendere efficaci le contromisure sul perimetro aziendale

… (la carta aiuta, ma non basta)

SPEED

La rincorsa alla sicurezza non è un approccio corretto. Deve essere nativa in ogni sistema e processo aziendale

… (la rincorsa non funziona… si arriva troppo tardi)

Cosa non può mancare ...

AUTOMAZIONE

Stante l'estensione dei requisiti da coprire e del perimetro dei servizi da presidiare non è sostenibile prevedere una crescita esponenziale delle risorse. Solo l'automazione consente di ottimizzare la gestione, in particolare nelle fasi di «Detect» and «Respond»

INTEGRAZIONE

La velocità di risposta richiesta alle minacce cyber richiede che, una volta identificato l'alert, si proceda immediatamente ad eseguire azioni preventive e reattive sui sistemi di sicurezza. Solo l'integrazione delle piattaforme consente di gestire rapidamente e in modo fattivo le risposte

ANALISI

La dinamicità delle minacce di sicurezza rende inadatte forme di reazione statica agli eventi di sicurezza. Per intercettare fenomeni nuovi, dinamici e complessi, è necessario ricorrere all'adozione di soluzioni basate su analytics e IA applicate alla cyber security

DORA regulation

CONTESTO

- L'obiettivo primario di DORA è **l'armonizzazione** delle **regole** esistenti afferenti la **gestione delle ICT** ("Information and Communication Technology"), affrontando tematiche di **Governance, ICT Risk Management e Incident Reporting** al fine di assicurare la **resilienza operativa** contro i **rischi** delle **ICT**
- **L'entrata in vigore** di DORA ("Digital Operational Resilience Act") è prevista per la **prima metà del 2022** e la sua **applicazione** dovrà avvenire in maniera **uniforme** in tutti i paesi dell'**UE**
- L'applicazione di **DORA** interesserà **tutti gli operatori del settore finanziario** ed i rispettivi **fornitori di servizi ICT**

CONTENUTI PRINCIPALI

ICT Governance

Aggiornare le regole esistenti sulla governance ICT in linea con le rispettive strategie aziendali

ICT Risk Management

Requisiti e principi chiave sulla gestione del rischio ICT

ICT Incident Reporting

Monitoraggio e segnalazione di incidenti legati alle TIC

Digital Operational Resilience Testing

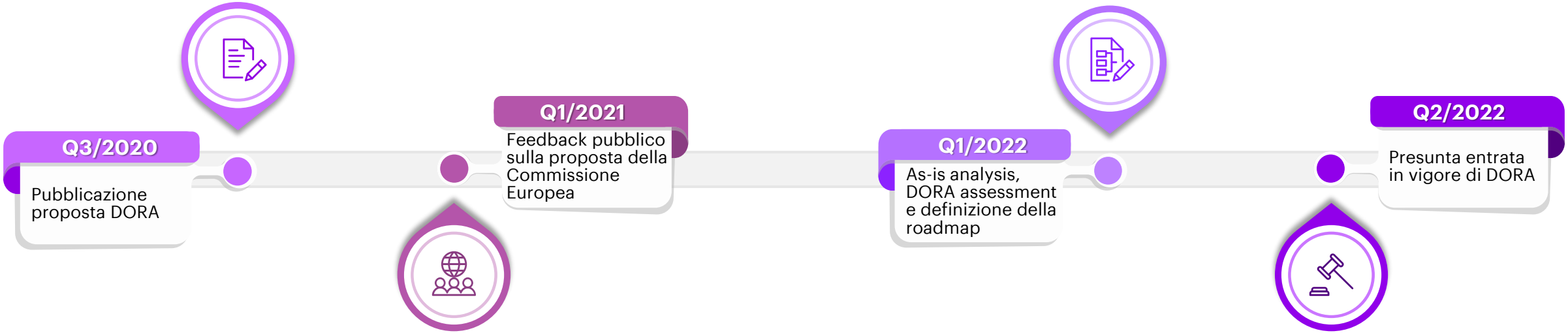
Esecuzione periodica di test di resilienza operativa avanzati

ICT Third-Party Management

Gestione attiva del rischio legato alle Terze Parti

Reporting alle Autorità

Il rispetto del regolamento sarà garantito dalle rispettive Authorities locali



Elementi distintivi per attuare DORA

1 Secure Cloud Express

Consente una rapida valutazione delle **vulnerabilità relative alle tecnologie in cloud** con **piano** per la **mitigazione del rischio**, combinando tecnologie leader di mercato e strumenti *cloud-native*.

Il servizio è applicabile **a tutte le organizzazioni,** indipendentemente dal livello di adozione delle tecnologie cloud, in accordo con i **principali framework** di controllo adottando strumenti non intrusivi.

Attraverso un approccio **cloud-native**, basato sui principi **DevSecOps**, forniamo un **servizio di assessment cross provider** oltre che gli strumenti necessari per indirizzare le vulnerabilità emerse.

2 Third Party Risk Management

Prevede l'automazione del processo di gestione e di **monitoraggio** delle **terze parti**, al fine di:

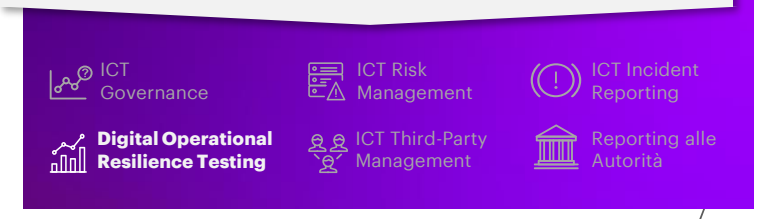
- **Migliorare l'efficienza dei processi** garantendo al contempo la conformità e mitigando i rischi
- **Garantire una miglior visibilità dell'intero processo di valutazione** in termini di gestione e controllo dei dati, in relazione, anche, a possibili richieste di audit
- **Far fronte efficacemente a richieste di aggregazione** e reporting dei dati in relazione ai rischi afferenti la gestione delle terze parti

3 Threat Intelligence-based Ethical Red Teaming (Tiber)

Consente di supportare i clienti nell'adozione del **framework TIBER**, con l'obiettivo di:

- **Analizzare il panorama delle minacce** e la relativa **esposizione**, il profilo di rischio e l'impatto sulla continuità/resilienza operativa
- **Migliorare la resilienza operativa** e la *security posture*
- **Prepararsi alla conduzione dell'esercizio TIBER** secondo i criteri definiti dall' ESA, attraverso un'attività di simulazione

Accenture è leader nell'esecuzione delle attività **TIBER** ed è certificata CREST/CBEST.



Accenture è l'azienda più grande al mondo che fornisce servizi di Cybersecurity

+8.000 professionisti nel mondo

+1.500 clienti serviti globalmente

+20 anni di esperienza nella sicurezza informatica

> L'**Italia è la prima practice a livello mondiale** per numero di talenti.

> Abbiamo un **Cyber Fusion Center** a **Napoli** per l'erogazione di **servizi gestiti di sicurezza** che si inserisce in un network globale di centri di innovazione.

Grazie!

Marco Valsecchi
Managing Director, Accenture Security

marco.valsecchi@accenture.com

www.accenture.com/stateofcyber