

"Cyber Risk: la bomba a orologeria dentro ogni boardroom"

deda.tech

Luca Bechelli | Direttivo Clusit, *Clusit*

Filippo Angelo Romeo | Head of Cybersecurity & GRC Advisory, *Deda Tech*

Relatori



LUCA BECHELLI

COMITATO DIRETTIVO



PARTNER @P4I – GRUPPO DIGITAL360



FILIPPO ANGELO ROMEO

HEAD OF CYBERSECURITY & GRC ADVISORY

DEDA TECH – GRUPPO DEDAGROUP

deda.tech

Scenario

Enisa Threat Landscape 2025

Fonte: <https://enisa.europa.eu/publications/enisa-threat-landscape-2025>

Fig. 1 - Most identified initial infection vector.

Source: ENISA dataset

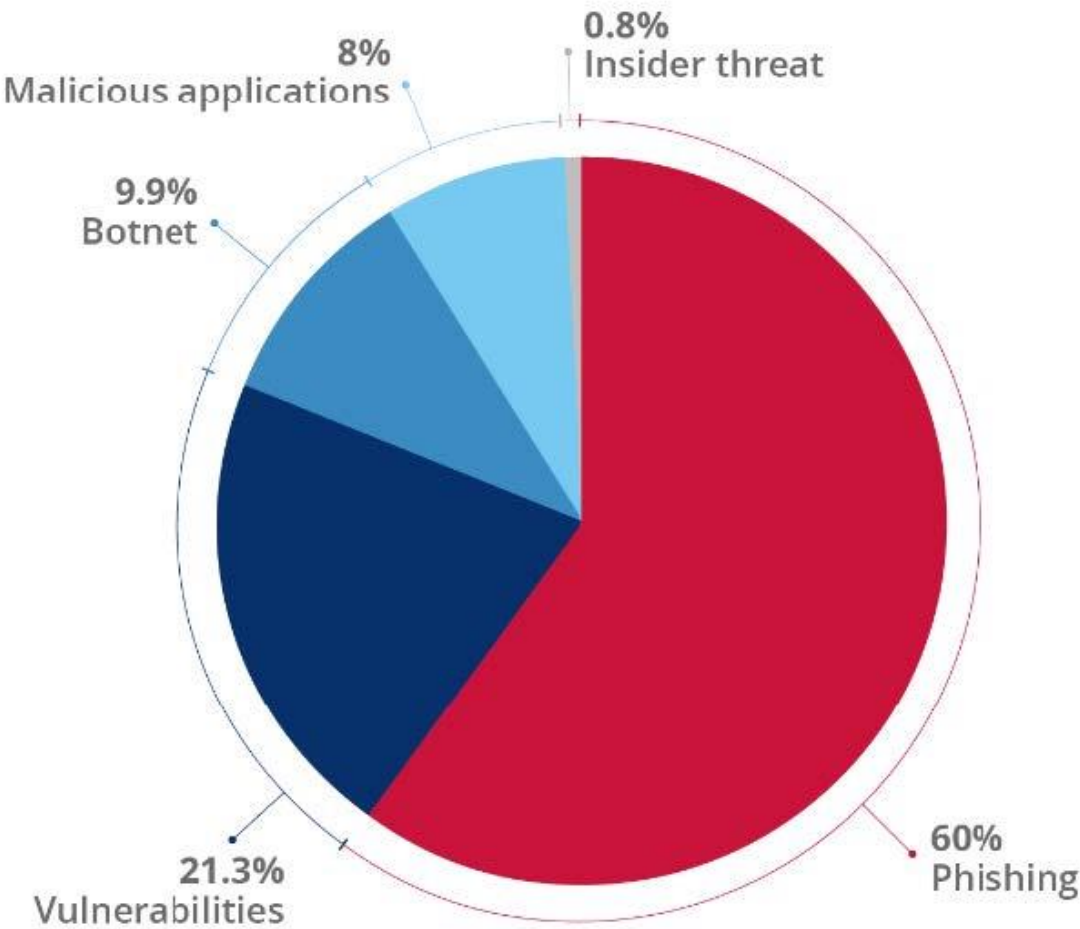


Fig. 2 - Distribution of incident types.

Source: ENISA dataset

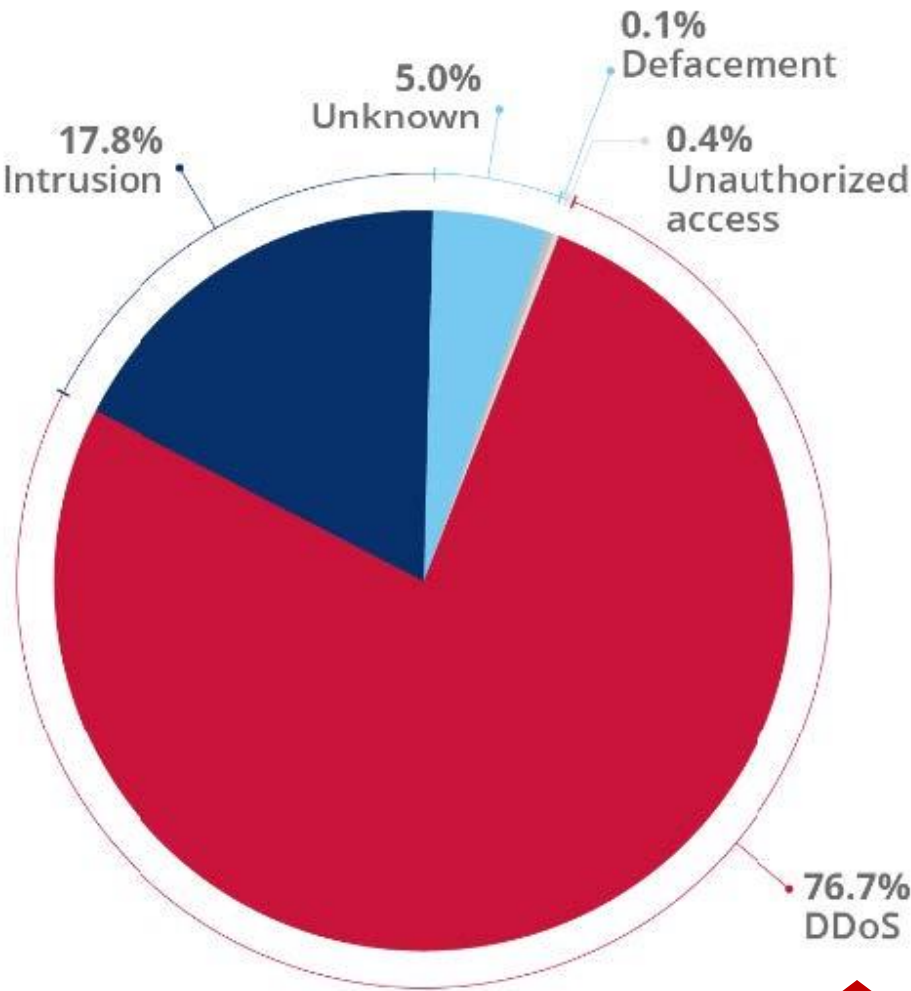
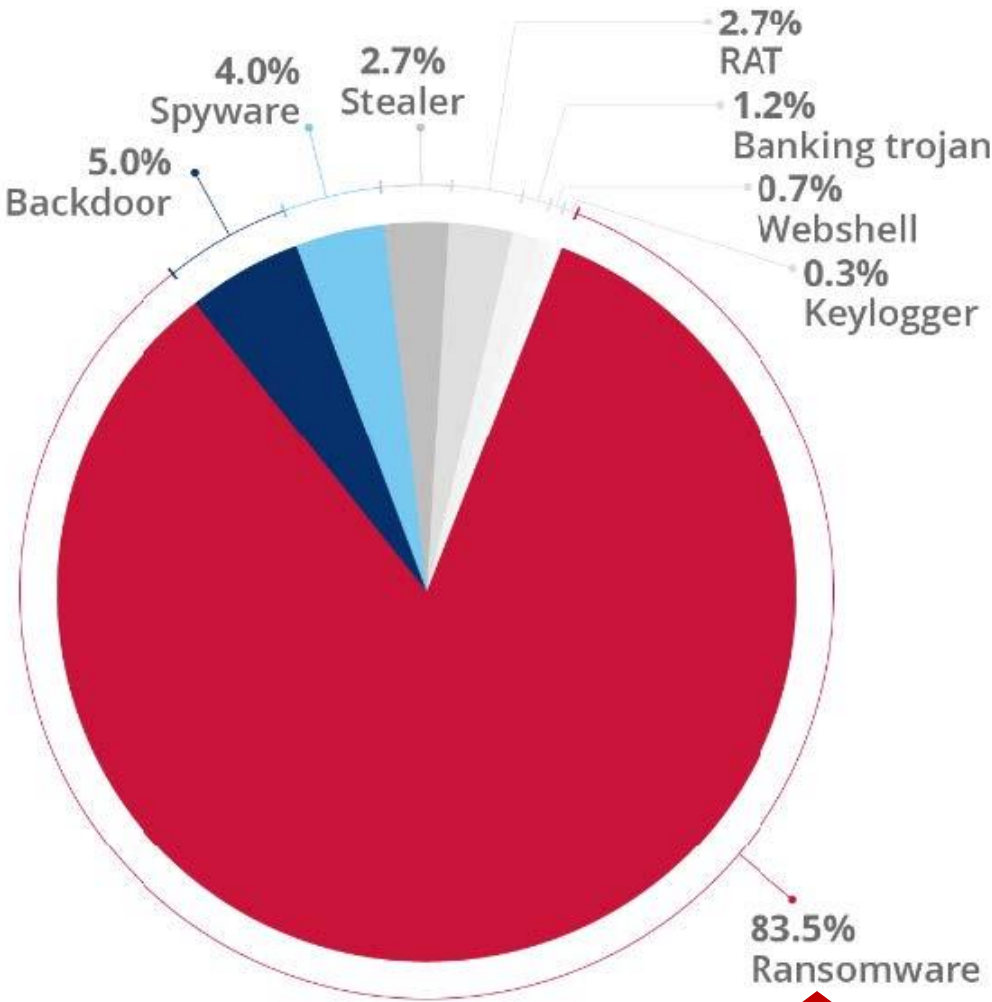


Fig. 3 - Distribution of identified malicious codes.

Source: ENISA dataset



Enisa Threat Landscape 2025 - 2

Fonte: <https://enisa.europa.eu/publications/enisa-threat-landscape-2025>

Fig. 4 - Outcome of identified intrusions.
Source: ENISA dataset

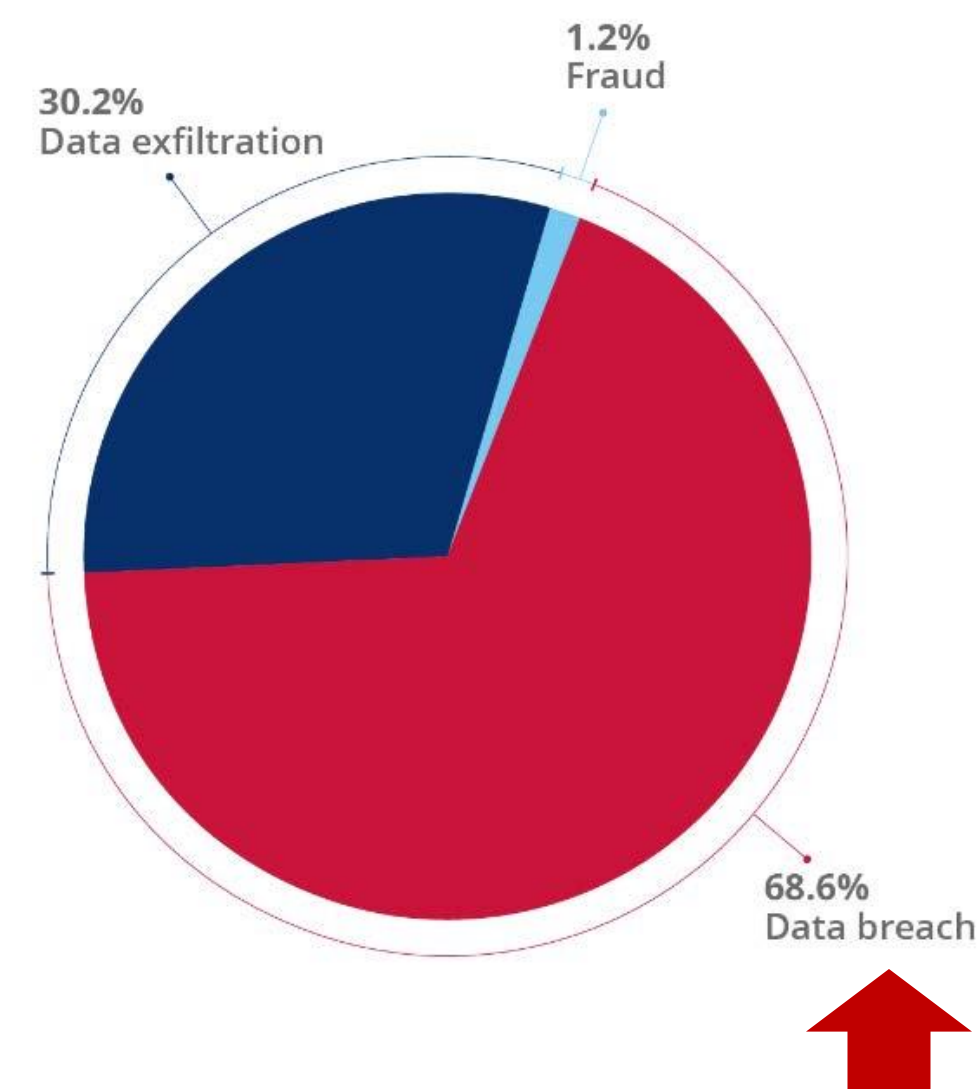


Fig. 5 - Distribution of threats.
Source: ENISA dataset

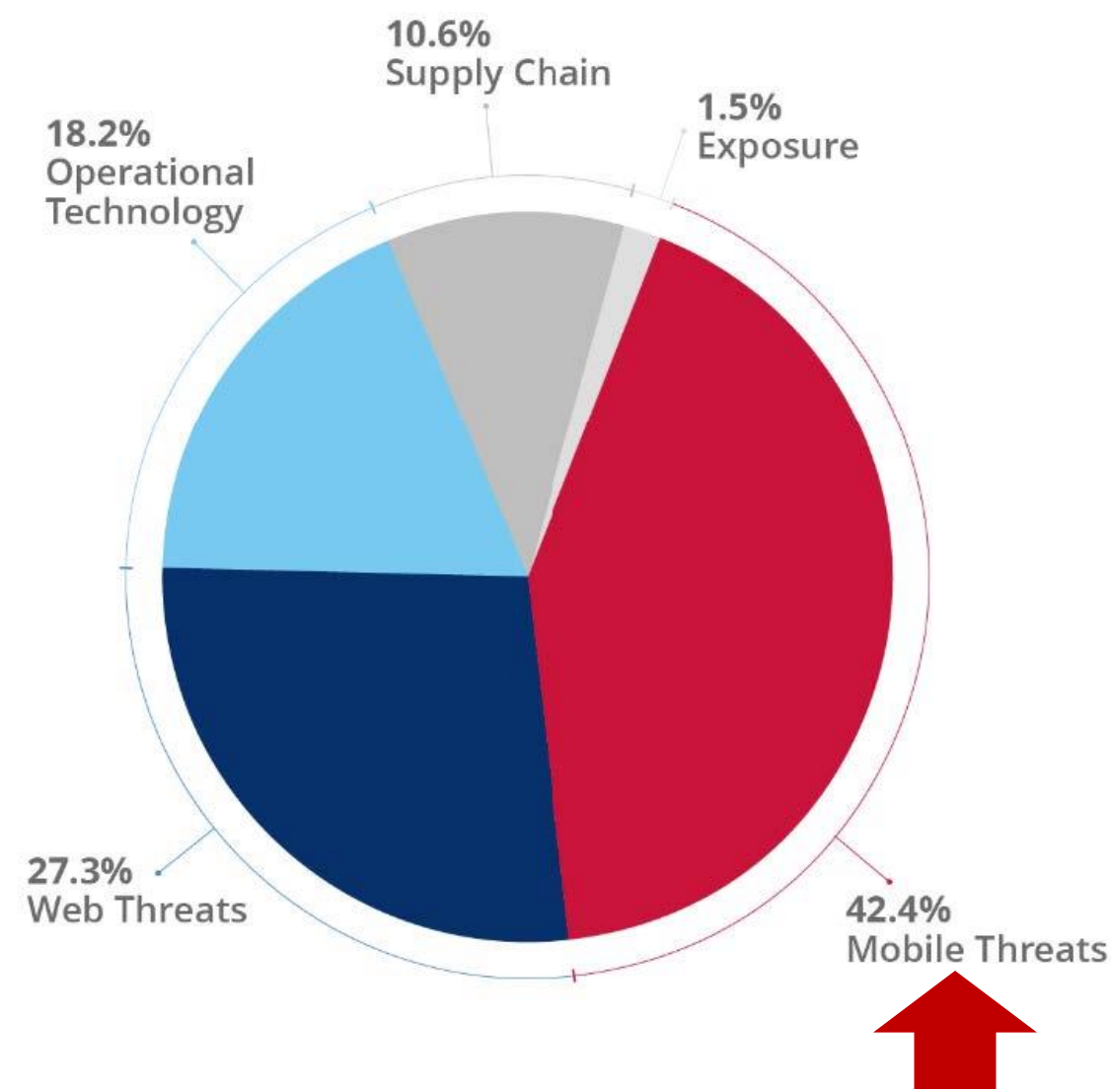
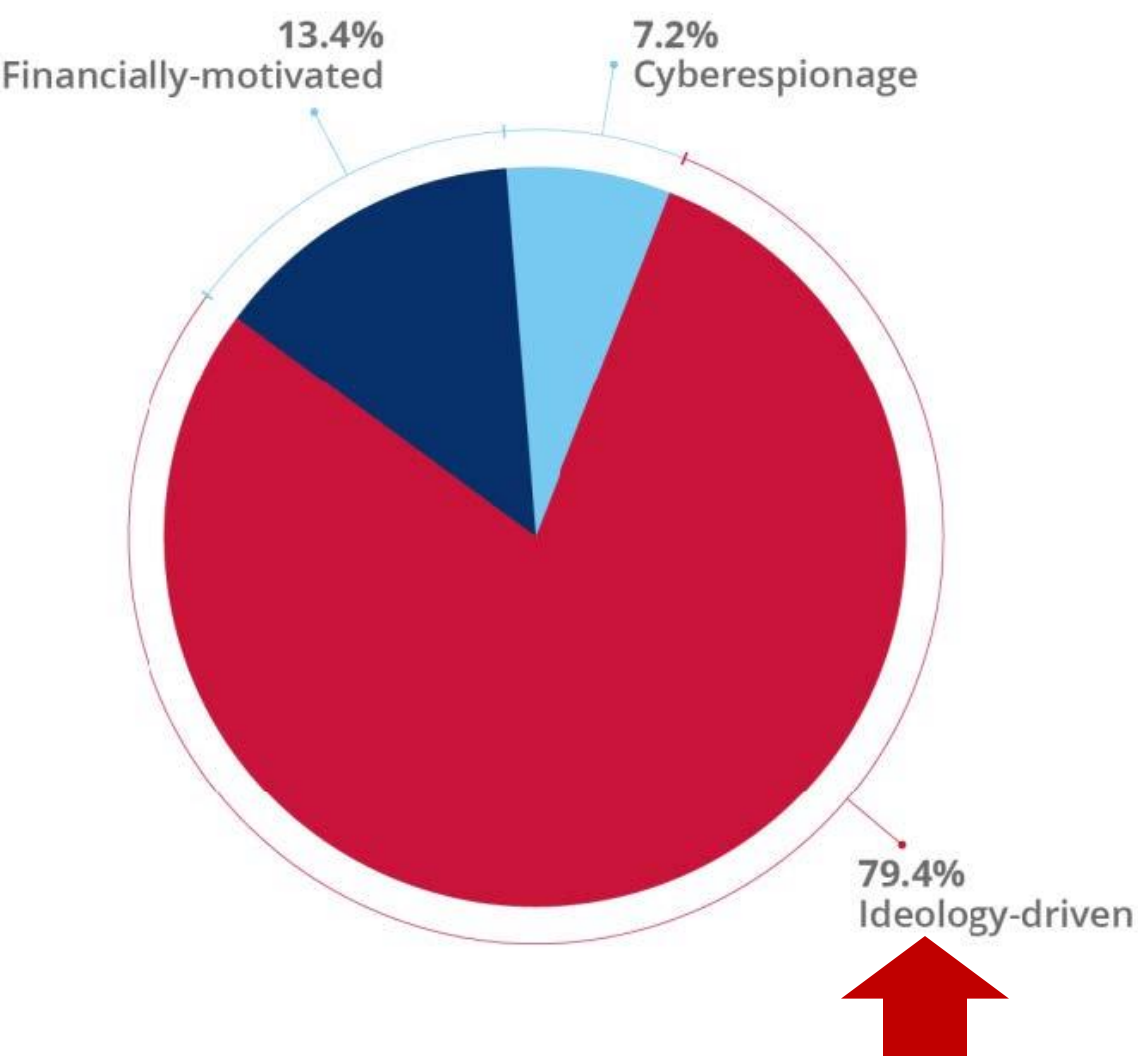


Fig. 6 - Distribution of assessed objectives.
Source: ENISA dataset



Minacce informatiche: convergenza di complessità e sofisticazione

Tipo di Minaccia	Vettore Primario	Fattore Abilitante Avversario	Settori più Colpiti (UE)	Statistica Chiave
Social Engineering potenziato da AI	Phishing / Vishing	Generative AI, Deepfake, Modelli Jailbroken	Pubblica Amministrazione, Trasporti, Finanza	>80% delle attività di social engineering è potenziato da AI
Ransomware	Sfruttamento di Vulnerabilità, Phishing	Ransomware-as-a-Service (RaaS), Tattiche di Doppia Estorsione	Manifatturiero, Servizi Digitali, Pubblica Amministrazione	La minaccia con il maggiore impatto nell'UE
Spionaggio/Sabotaggio di Matrice Statale	APT, Sfruttamento di Zero-Day	"Faketivism", Compromissione della Supply Chain	Pubblica Amministrazione, Manifatturiero, Telecomunicazioni	Intensificazione delle campagne a lungo termine contro l'infrastruttura UE
Compromissione della Supply Chain	Fornitori Terzi, Vulnerabilità Software	Mancanza di Visibilità, Disuguaglianza competenziale	Tutti i settori, con impatto a cascata	Il 54% delle grandi organizzazioni lo considera il maggiore ostacolo alla resilienza

Convergenza IT/OT/AI: la superficie di attacco estesa

IT – OT: Silos con missioni e paradigmi di sicurezza divergenti

Attributo	Ambiente IT	Ambiente OT
Priorità Primaria	Riservatezza, Integrità, Disponibilità (CIA)	Sicurezza Fisica (Safety), Disponibilità, Integrità
Ciclo di Vita del Sistema	3-5 anni	15-25+ anni
Patching/Aggiornamenti	Frequenti, spesso automatizzati	Rari, pianificati con mesi di anticipo, spesso impossibili
Architettura di Rete	Dinamica, connessa a Internet	Statica, storicamente isolata ("air-gapped")
Impatto del Downtime	Perdita di dati, danno finanziario e reputazionale	Rischio per la vita umana, danno ambientale, guasto catastrofico
Rischio Dominante	Furto di informazioni, frode finanziaria	Interruzione dei processi fisici, sabotaggio

Convergenza IT/OT/AI: la superficie di attacco estesa

AI Offensiva: Tattiche, Tecniche e Procedure Avversarie (TTP)

- Social Engineering iper-realistico: Deep Fake;
- Scalabilità e evasione automatizzata degli attacchi;
- attacchi di AI/ML avversari;

Obblighi normativi

NIS2 e **DORA** rappresentano la risposta ponderata e strutturata del legislatore europeo alla nuova realtà di rischio sistemico.

Sono il **diretto risultato dell'analisi di attacchi su larga scala** che hanno dimostrato la fragilità delle nostre infrastrutture digitali e l'interdipendenza critica tra settori economici.

La recente determinazione di ACN in merito al riferimento CSIRT dimostra ulteriormente la necessità per le Aziende di **implementare un approccio strutturato alla cybersicurezza**.

Il Paradigma classico della strategia di cybersicurezza è adeguato?

Il Paradigma di protezione classico si fonda **sull'obiettivo primario di prevenire** gli attacchi.

È usata una logica perimetrale: creare una barriera robusta tra un "**interno**" fidato (la rete aziendale) e un "**esterno**" ostile (Internet).

Il successo, in questo modello, è misurato in modo binario: **l'assenza di incidenti di sicurezza**, il che presuppone che il perimetro sia definibile, controllabile e difendibile al 100%.

Gli investimenti sono quindi proiettati ad aumentare le dimensioni della barriera, sovrapponendo perlopiù **strati di tecnologie**.

Il Paradigma attuale della strategia di cybersicurezza è adeguato?

Il perimetro attuale è «liquido» (cloud, lavoro da remoto, ecc.)

Dunque non è definibile, controllabile e difendibile al 100%

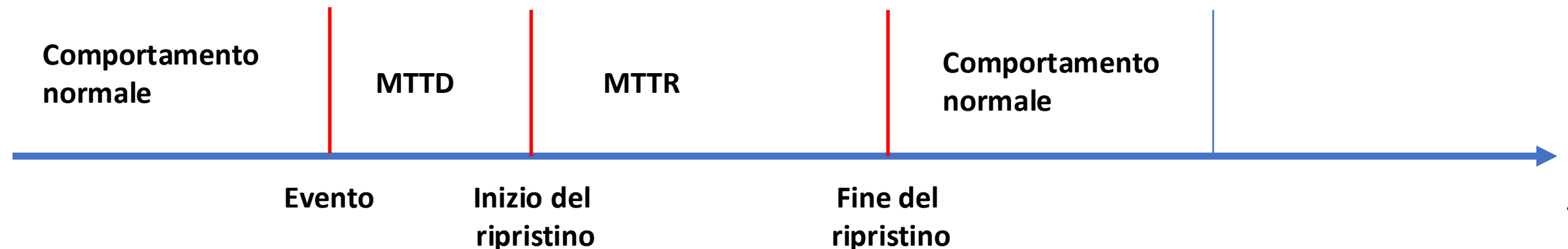
**Il Paradigma attuale della strategia di
cybersicurezza non è adeguato!**

Il nuovo Paradigma: la Resilienza

*La resilienza è la capacità di un'organizzazione di **prepararsi, resistere, adattarsi e riprendersi** rapidamente da un incidente di cybersicurezza, garantendo la continuità operativa aziendale.*

Le metriche di successo di un piano di continuità operativa cambiano decisamente, infatti si misurano:

- la riduzione del tempo medio di rilevamento (Mean Time to Detect - MTTD) e del tempo medio di risposta (Mean Time to Respond - MTTR);
- la rapidità e l'efficacia della ripresa
- la minimizzazione dell'impatto finanziario e operativo dell'incidente.



Il nuovo Paradigma: la Resilienza - 2

Caratteristica	Paradigma di Protezione	Paradigma di Resilienza
Presupposto Fondamentale	È possibile prevenire tutte le intrusioni.	Le violazioni sono inevitabili ("assume-breach").
Obiettivo Primario	Impedire l'accesso non autorizzato.	Garantire la continuità operativa durante e dopo un attacco.
Metriche di Successo	Assenza di incidenti; numero di attacchi bloccati.	Tempo di rilevamento (MTTD); tempo di ripristino (MTTR); impatto sul business.
Focus degli Investimenti	Prevenzione perimetrale (firewall, antivirus, IPS).	Portafoglio bilanciato: governo, protezione, rilevamento, risposta, ripristino.
Approccio Culturale	La sicurezza è un problema del dipartimento IT.	La sicurezza è una responsabilità di business condivisa.
Tecnologie Chiave	Firewall, VPN, Antivirus, Web Application Firewall.	EDR/XDR, SIEM/SOAR, Threat Intelligence, Piani di Disaster Recovery.

La strategia di cybersicurezza adattiva: un framework operativo per la resilienza nell'era delle minacce evolute

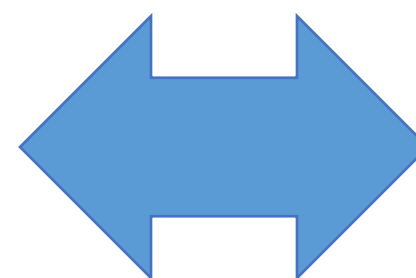
La strategia di cybersicurezza adattiva

Governance integrata: Allineare la strategia di cybersicurezza agli obiettivi di business, alla gestione del rischio d'impresa e agli adempimenti normativi.

Resilienza architetturale: Implementare un'architettura Zero Trust, che elimina la fiducia implicita e applica controlli granulari per limitare drasticamente il movimento laterale degli aggressori all'interno della rete.

Difesa continua: Abbandonare il concetto di "risposta agli incidenti" (*incident response*) in favore di una "risposta continua" (*continuous response*), monitorando e analizzando costantemente l'ambiente per individuare anomalie e segnali di compromissione.

Comportamento proattivo: Sfruttare l'IA e il machine learning non solo per difendersi dalle minacce potenziate dall'IA, ma anche per anticipare i vettori di attacco, dare priorità alle vulnerabilità più critiche e automatizzare le risposte a velocità macchina.



Prepararsi

Resistere

Adattarsi

Riprendersi

La strategia di cybersicurezza adattiva - 2

Gestione delle minacce focalizzata sul rilevamento di minacce sconosciute ed emergenti

Valutazione del rischio continua e in tempo reale

Approccio alla fiducia dinamico in base al comportamento e al contesto in tempo reale

Applicazione dei principi Zero Trust

Postura di sicurezza con evoluzione dinamica

Deda Tech Cybersecurity Consulting

Proteggiamo il valore creato dalle organizzazioni

Strategy & Transformation

Aiutiamo le Aziende nella definizione della strategia più adeguata a mantenere la cybersecurity posture allineata alle esigenze di business

Governance & Compliance

Supportiamo il governo della cybersecurity attraverso piani di sviluppo che rendono la conformità un fattore competitivo abilitante

Technical Implementation

Offriamo capacità e visione per l'adozione di tecnologie

Operation

Siamo al fianco delle Aziende durante tutte le fasi di gestione della cybersicurezza



Deda Tech Cybersecurity Consulting

Proteggiamo il valore creato dalle organizzazioni

Valutazione continua dei
Requisiti di Sicurezza



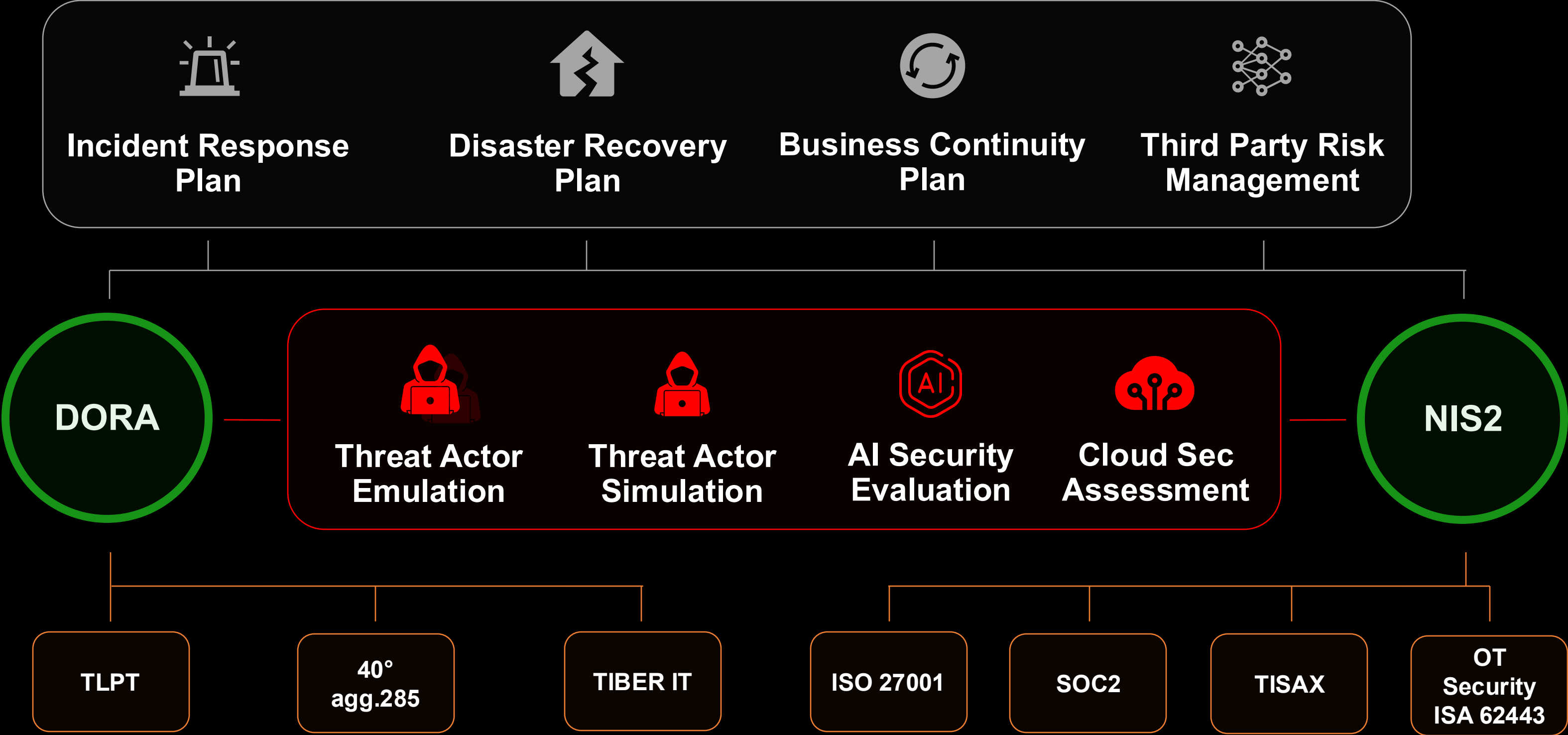
Comprensione
delle esigenze



Approccio multidisciplinare
al Security by Design



GRC Advisory & Offensive - Service Portfolio



Q&A

Vieni a trovarci al nostro stand!

 www.dedatech.com | info@dedagroup.it