



# ACCSIA

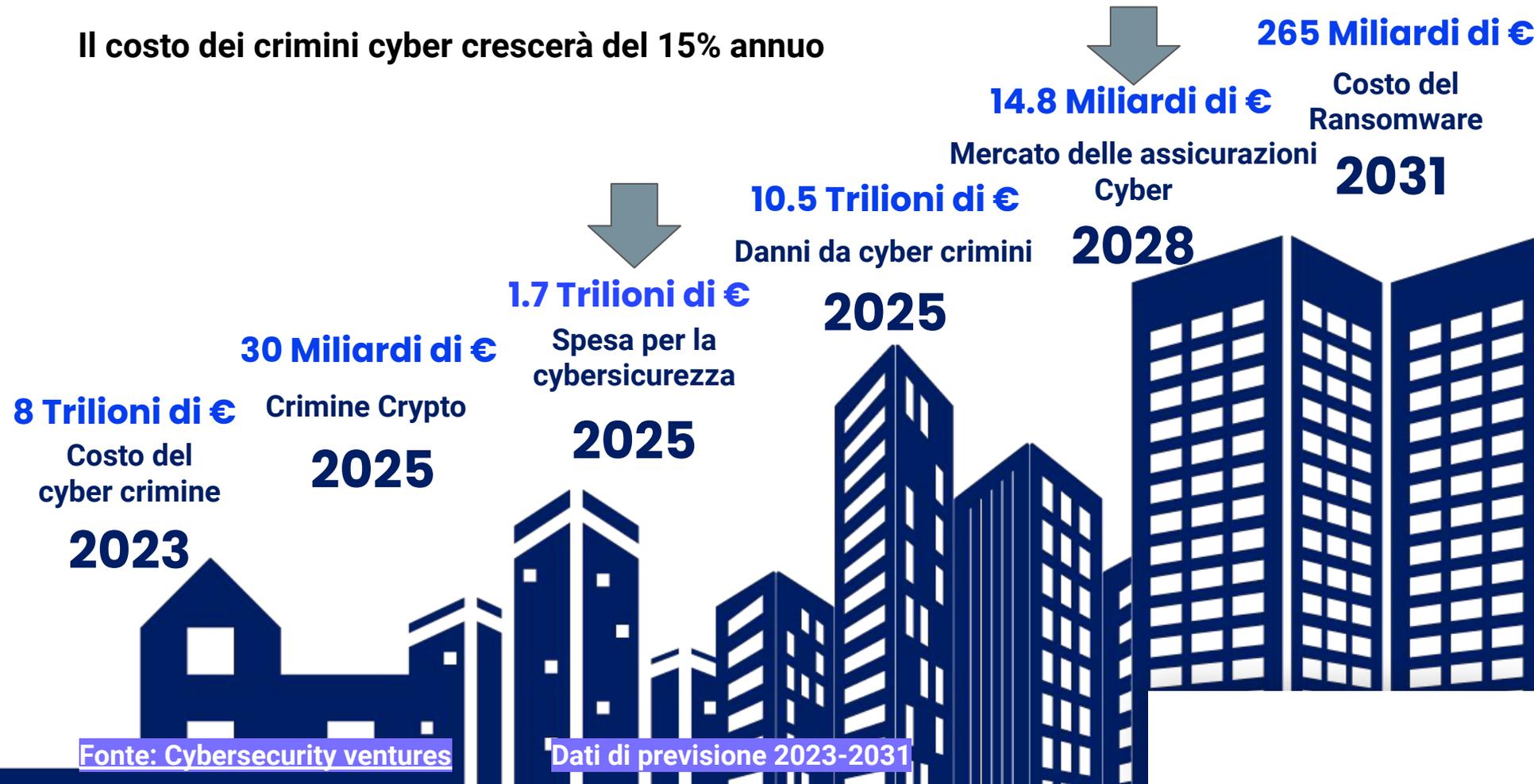
**XDR PLUS**

**Sviluppato in Europa**



# I Crimini Informatici Sono un Problema Globale

Il costo dei crimini cyber crescerà del 15% annuo



265 Miliardi di €

Costo del Ransomware

2031

14.8 Miliardi di €

Mercato delle assicurazioni Cyber

2028

Danni da cyber crimini

10.5 Trilioni di €

2025

1.7 Trilioni di €

Spesa per la cybersicurezza

2025

30 Miliardi di €

Crimine Crypto

2025

8 Trilioni di €

Costo del cyber crimine

2023

Fonte: Cybersecurity ventures

Dati di previsione 2023-2031

# I Cybercriminali a Piede Libero Danneggiano le Imprese

Giorno 0



50

100

150

200

Giorno 243



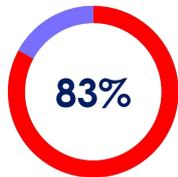
300

Giorno 327



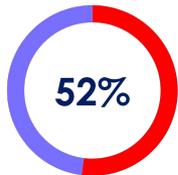
Costo medio di  
dati rubati o  
compromessi

4  
Milioni  
di €



83%

83% delle organizzazioni hanno subito incursioni



52%

52% dei problemi di sicurezza dei dati sono causati da attacchi volontari

# Opportunità: le Soluzioni di Cybersicurezza Attuali Non Sono Efficaci



**Le dimensioni del problema sono enormi**

I dipendenti lavorano da qualsiasi parte del mondo e i loro dispositivi accedono ai dati aziendali dal cloud, **al di fuori dei comuni protocolli di sicurezza.**



**I veri esperti sono pochi e troppo indaffarati**

Il lavoro degli impiegati dedicati alla cybersicurezza non è mai stato così impegnativo: ogni soluzione puntualmente richiede una gestione separata e competenze specifiche per il suo funzionamento. Tale complessità ha **inciso pesantemente sulla produttività dei team cyber.**



**Le soluzioni si focalizzano solo sui "rimedi" post-attacco**

**La maggior parte delle soluzioni informatiche si concentra sulla reazione a crimini già avvenuti.** I team di cybersicurezza si trovano a dover gestire la confusione tra i tanti avvisi di rischio, cercando di tenere il passo con gli attacchi informatici (veri o presunti) rilevati.



**Soluzioni tardive e poco efficaci**

Anche i prodotti XDR più avanzati sono unicamente reattivi: ciò significa che devono essere rilevati codice o attività dannosi all'interno dei sistemi, prima che essi si attivino. **Spesso è troppo tardi per fermare i danni dell'attacco.**

# Cos'è ACSIA XDR Plus?



**ACSIA XDR Plus™** è una soluzione basata su piattaforma XDR (extended detection & response), alla quale aggiunge elementi unici come una cyber difesa **Predittiva & Proattiva**.

**ACSIA – Automated Cyber Security Intelligence Applications**



# ACZIA XDR Plus Anticipa i Cyber Criminali ed Impedisce Attacchi alla Tua Azienda.

## Pensa Come il Nemico

ACZIA XDR Plus monitora i sistemi IT della tua azienda, le reti, gli utilizzatori ed il perimetro. È ricettivo alle minime avvisaglie di un potenziale attacco cyber.



## Difende da Azioni Precedenti un Attacco

ACZIA XDR Plus individua la pianificazione e la preparazione di un attacco informatico, fermandolo già durante le fasi di ricognizione e raccolta di informazioni.



## Scopre & Blocca Visitatori Sospetti

ACZIA XDR Plus ferma i cyber criminali, anticipandoli. Blocca infatti chiunque analizzi la vostra infrastruttura con intenzioni malevole.



## Semplifica le Azioni di Risposta

I colleghi del reparto cyber son sotto pressione? La nostra soluzione combina le funzionalità di molteplici programmi, semplificando le contromisure ad avvisi di pericolo.



## Mantiene al Sicuro l'Azienda

ACZIA XDR Plus permette di mantenere alte le difese e liberare risorse preziose, risponde automaticamente alle minacce e ottimizza l'impiego del team.



Le soluzioni XDR della concorrenza son solo reattive. ACZIA XDR Plus è diverso: offre infatti soluzioni proattive che prevengono i rischi derivanti dallo spionaggio e raccolta informazioni da parte dei cyber criminali, ancora prima che attacchino.

# ACSIA XDR Plus Blocca un Attacco nella Fase Chiave – Ovvero Prima che Avvenga

## XDR Predittivo



- Blocca reti anonime
- Blocca file .exe
- Blocca URL sospette
- Blocca “command & control”
- Blocca indirizzi IP sospetti

## XDR Proattivo



- Anti sorveglianza
- Blocca le azioni di raccolta informazioni
- Previene la scansione porte
- Ferma la scansione di vulnerabilità
- Identifica e blocca le attività criminali antecedenti un attacco

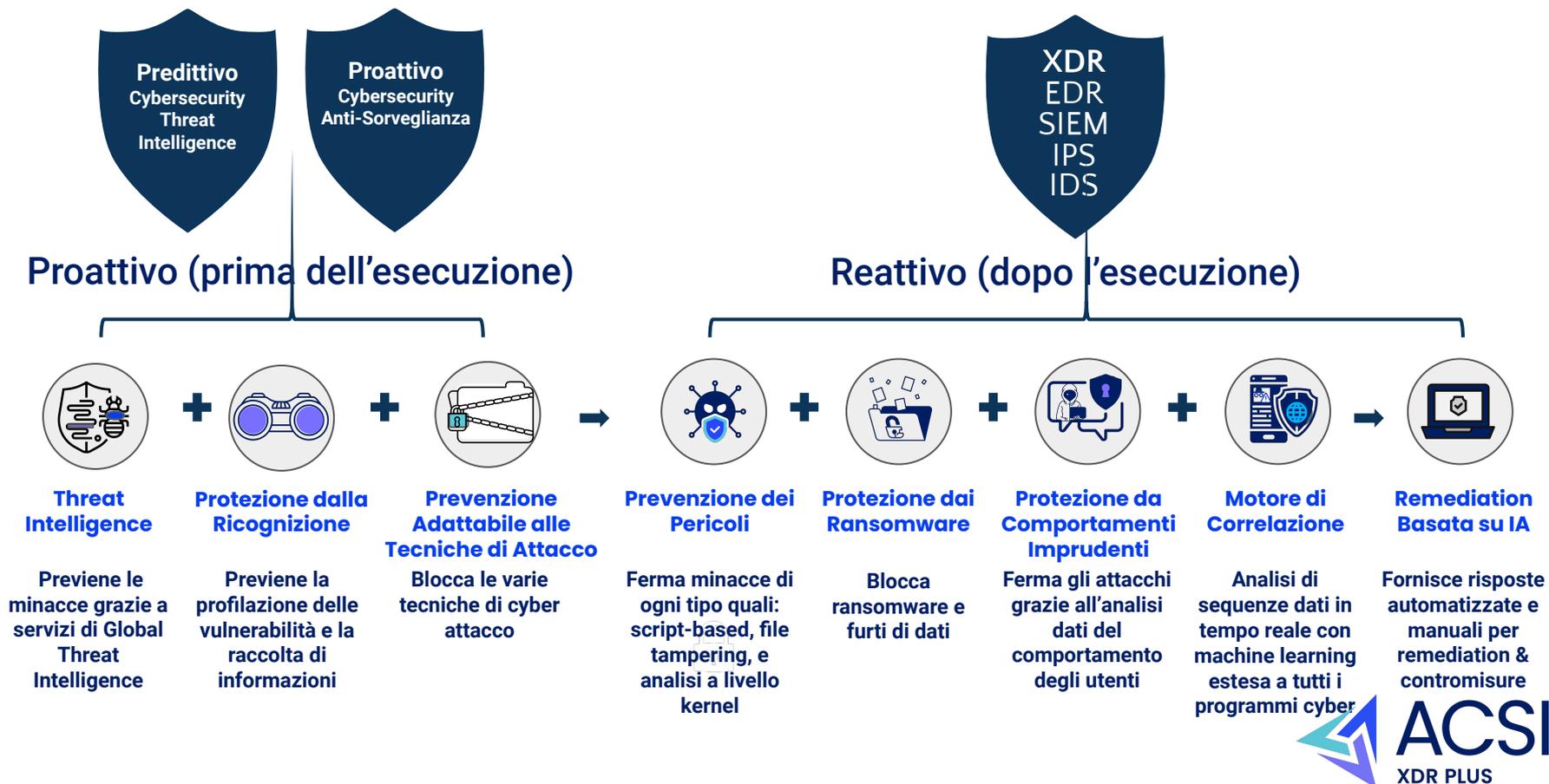
## XDR Reattivo



- EDR, IDS, IPS & SIEM centralizzati
- Correlazione in tempo reale di tutti i log
- Monitoraggio a livello Kernel
- Account Compromise & User Profiler
- Rileva comportamenti anomali

La tecnologia pre attacco di ACSIA XDR Plus previene gli attacchi informatici, bloccando le attività di ricognizione e raccolta informazioni, che rappresentano la fase iniziale di una minaccia cyber, che può poi risultare in un attacco.

# ACZIA XDR Plus – Difesa Predittiva, Proattiva & Reattiva



# ACZIA XDR Plus - un Cacciatore di Minacce Predittivo

**ACZIA XDR Plus è unico** - il nostro programma blocca in maniera predittiva gli attacchi prima che avvengano, potendo rilevare tutte le fonti che li consentono, come:

**Indirizzi IP  
Sospetti**



**Traffico che  
Utilizza Reti  
Anonime**



**Fonti di  
Malware**



**URL Pericolosi e  
Sospetti**



La cyber sicurezza è solitamente gestita da vari programmi non sincronizzati, causando un elevato numero di falsi positivi: essi provocano confusione e stress, dovuti ai tanti avvisi di falso pericolo, per i colleghi del team cyber. Le soluzioni abituali rappresentano quindi un inefficiente utilizzo delle risorse IT ed una fonte di logorio e perdita di motivazione per il personale.

**“ Se i criminali informatici non possono trovarti, non possono attaccarti. ”**

Solo ACSIA XDR Plus fornisce **correlazione di eventi in tempo reale su tutti i domini** per:



**Nascondere la tua infrastruttura ai cyber criminali**



**Fermare ricognizione e raccolta informazioni**



**Utilizzare capacità di rilevamento a tutti i livelli per prevenire gli attacchi**



**Consentire il rilevamento XDR multi livello per tutti gli ambienti**

# ACCSIA XDR Plus Agisce Anche in Fase Reattiva, Dopo un Attacco

## Prevenzione di Situazioni Rischiose

Ferma minacce di ogni tipo quali: script-based, file tampering, e analisi a livello kernel



## Protezione dai Ransomware

Blocca ransomware e furti di dati



## Protezione da Comportamenti Imprudenti

Ferma gli attacchi grazie all'analisi dati del comportamento degli utenti



## Motore di Correlazione

Analisi di sequenze dati in tempo reale con machine learning estesa a tutti i programmi cyber



## Remediation Basata su IA

Fornisce risposte automatizzate e manuali per la remediation, così da facilitare la controffensiva del tuo team



Impiegando un approccio combinato, ACSA XDR Plus farà il lavoro più pesante in termini di analisi e monitoraggio della cyber sicurezza, profilazione e difesa da ogni rischio, onde garantire un elevato livello di automazione, efficacia ed efficienza.

# ACSIA XDR Plus – Una Soluzione Unica per Semplificare la Cyber Difesa

La nostra piattaforma previene gli attacchi informatici pensando come il nemico, bloccando azioni e minacce conosciute e utilizzando la threat intelligence per sventare potenziali cyber attacchi prima che avvengano, coprendo e sventando fino al 98% delle potenziali minacce in anticipo.

**Cyber Difesa  
Predittiva &  
Raccolta  
Informazioni**



90%

**Cyber Difesa  
Proattiva**



98%

**Cyber Difesa  
Reattiva**



2%

**Risposta Rapida a  
Minacce  
Informatiche**





**Grazie**

**Sviluppato in Europa**