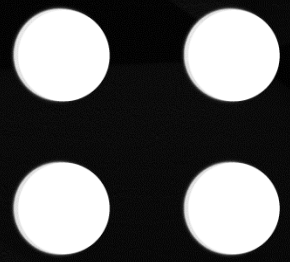


CYBEROO

SECURE SOUL

“The crisis you have to worry about most is the one you don’t see coming.”

Il panorama degli attacchi informatici era già grave alla fine del 2019. L’urgenza però di doversi adattare ad una situazione imprevedibile a priori come quella del COVID-19 ha obbligato milioni di persone a lavorare da casa, peggiorando ulteriormente la problematica cyber security.

“When you are out of control, someone is ready to take over.”

È facile immaginarsi in un panorama dove il dominio cyber delle aziende si estende ad ambiti che sono ben lontani dalle mura aziendali e dai sistemi IT direttamente controllati dalle aziende, che gli attacchi informatici proliferino.

Il Caso	Dipendenti	Fatturato (M€)	Settore	Danno
EasyJet, attacco hacker. A rischio i dati di 9 milioni di utenti della compagnia	15000+	6300	Trasporto	Databreach
Attacco hacker alla Bonfiglioli. "Chiesto riscatto di 2,4 milioni"	1000+	500	Manifattura	Fermo
Tecnimont truffata, la mail del capo era falsa: persi 17 milioni di dollari	1000+	2100	Chimico	Bonifico
Geox sotto attacco informatico: azienda paralizzata con richiesta di riscatto	500+	600	Moda	Fermo
Irpiniambiente sotto attacco hacker.	500+	50	Servizi	Fermo
Cantine Ferrari nel mirino degli hacker Sotto attacco informatico e «isolate» per due giorni	150+	500	Food	Fermo

Fonte: notizie pubbliche online

STATISTICS

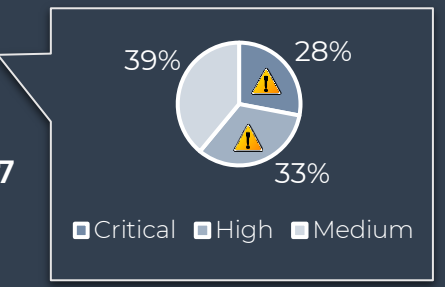
77%
delle aziende non ha un piano di Incident Response

32%
del personale IT, ignora attacchi a causa dei falsi positivi

48%
degli attacchi ha successo a causa dell'impreparazione del personale aziendale

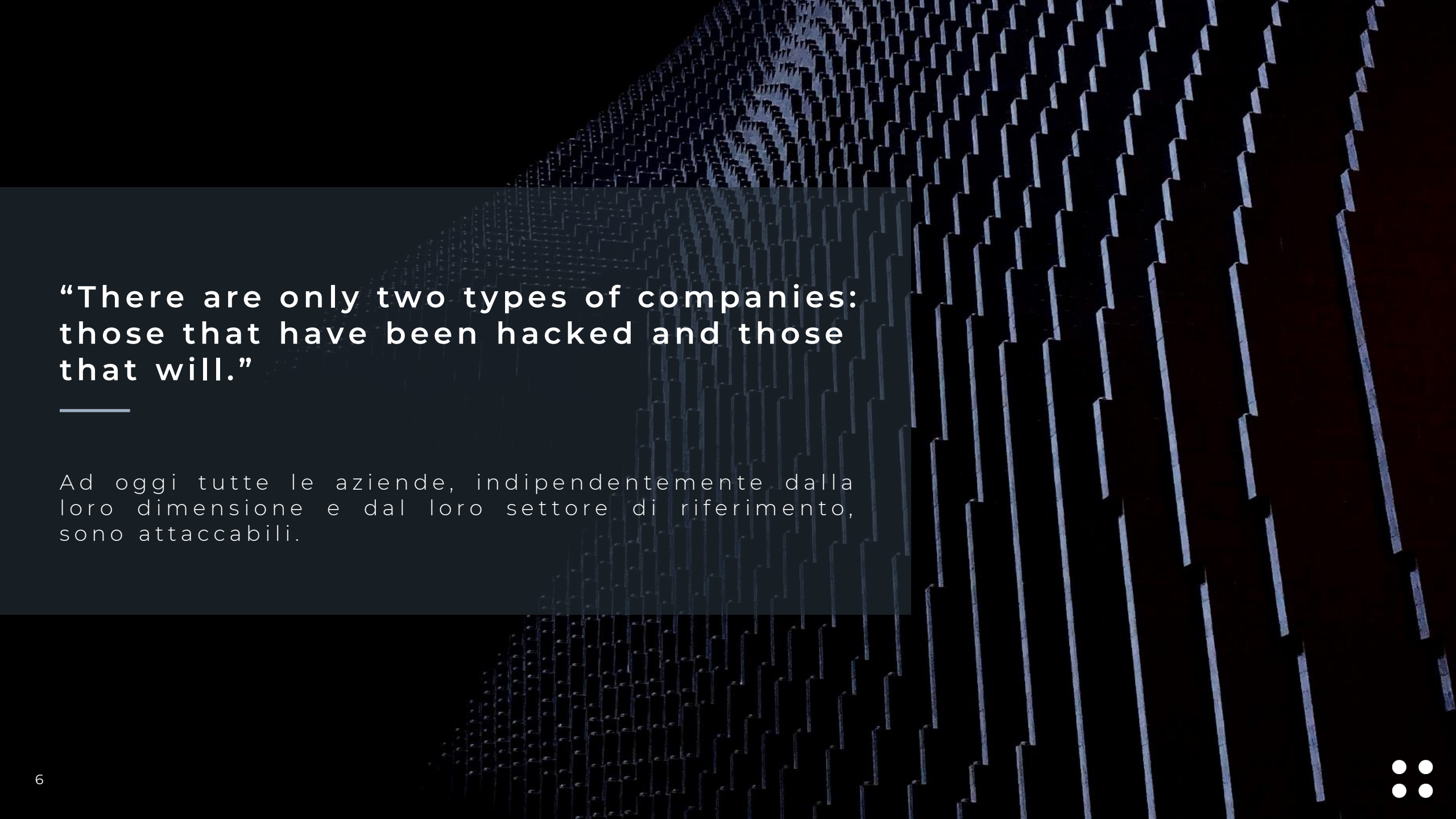
NUMERO ATTACCHI

2019-17 YoY +38%



Secondo le stime Clusit, **il numero di attacchi gravi*** alla sicurezza informatica in Italia **è quasi raddoppiato nel corso di soli 4 anni**.

* definiti come quegli attacchi capaci di portare danni finanziari o d'immagine oltre il milione di Euro. Fonte: Symantec, PhoenixNap, IBM & Clusit



“There are only two types of companies: those that have been hacked and those that will.”

Ad oggi tutte le aziende, indipendentemente dalla loro dimensione e dal loro settore di riferimento, sono attaccabili.

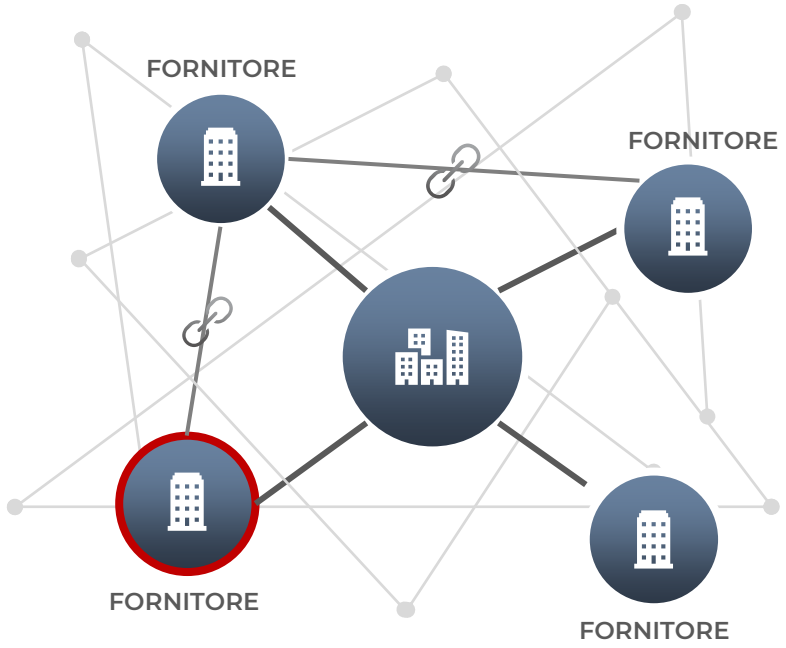
CYBER CRIME TARGET

ENTERPRISE

Un’azienda di grandi dimensioni ha un **valore considerevole** per il cybercrime, che tramite tecniche avanzate può **attestarsi anche per mesi all’interno della rete** al fine di raggiungere l’obbiettivo.

PMI

Le aziende di piccole dimensioni, a causa dei minori investimenti in sicurezza, hanno un **rapporto costo/beneficio molto più basso** e per questo sono un target “facile”.



Non preoccuparsi della propria sicurezza significa
IMPATTARE TUTTA LA FILIERA

La gestione del rischio è fondamentale per ogni dimensione aziendale ed è un
FATTORE CRITICO DI SUCCESSO

PERDITA

DIRETTA

Fermo produttivo

Investigazione

Notifica in caso di data breach

Perdita di dati

Riscatto ed estorsione

39s

Tempo che intercorre tra un attacco e l'altro, ogni giorno.

283gg

Tempo medio per identificare un breach in Italia.

135€

Costo medio per record perso in Italia.

24.577

Records in media di un breach in Italia.

INDIRETTA

Perdita di reputazione

Perdita di opportunità

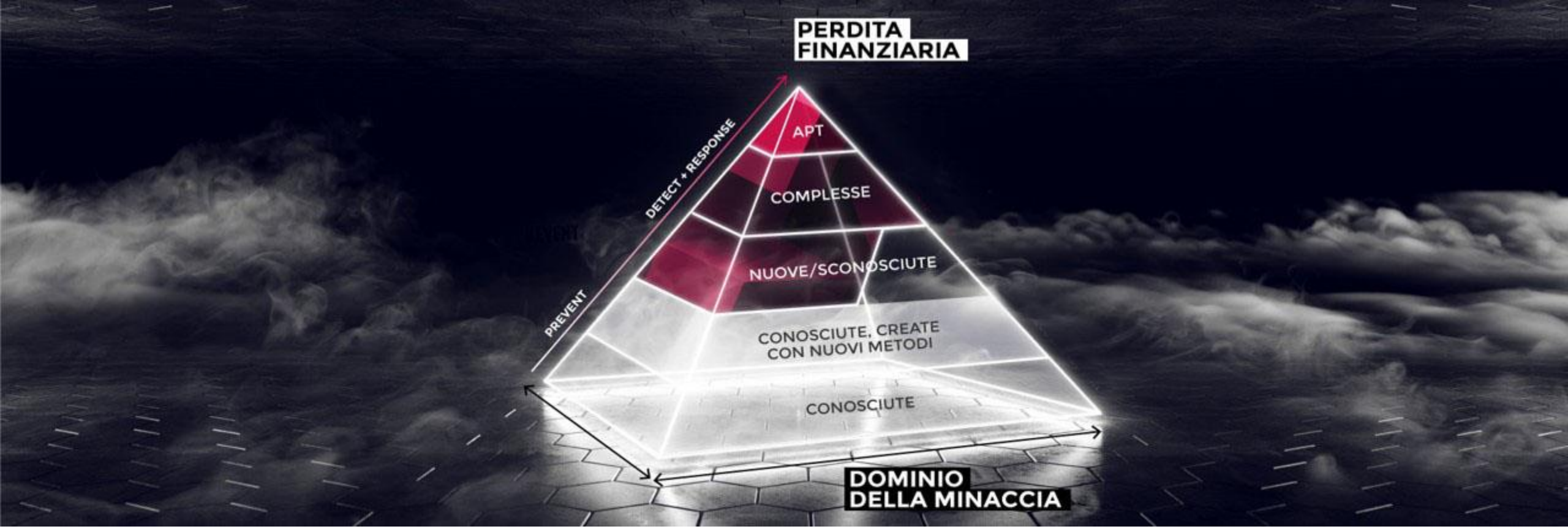
Perdita di linee di business

Spese legali

Violazione della privacy

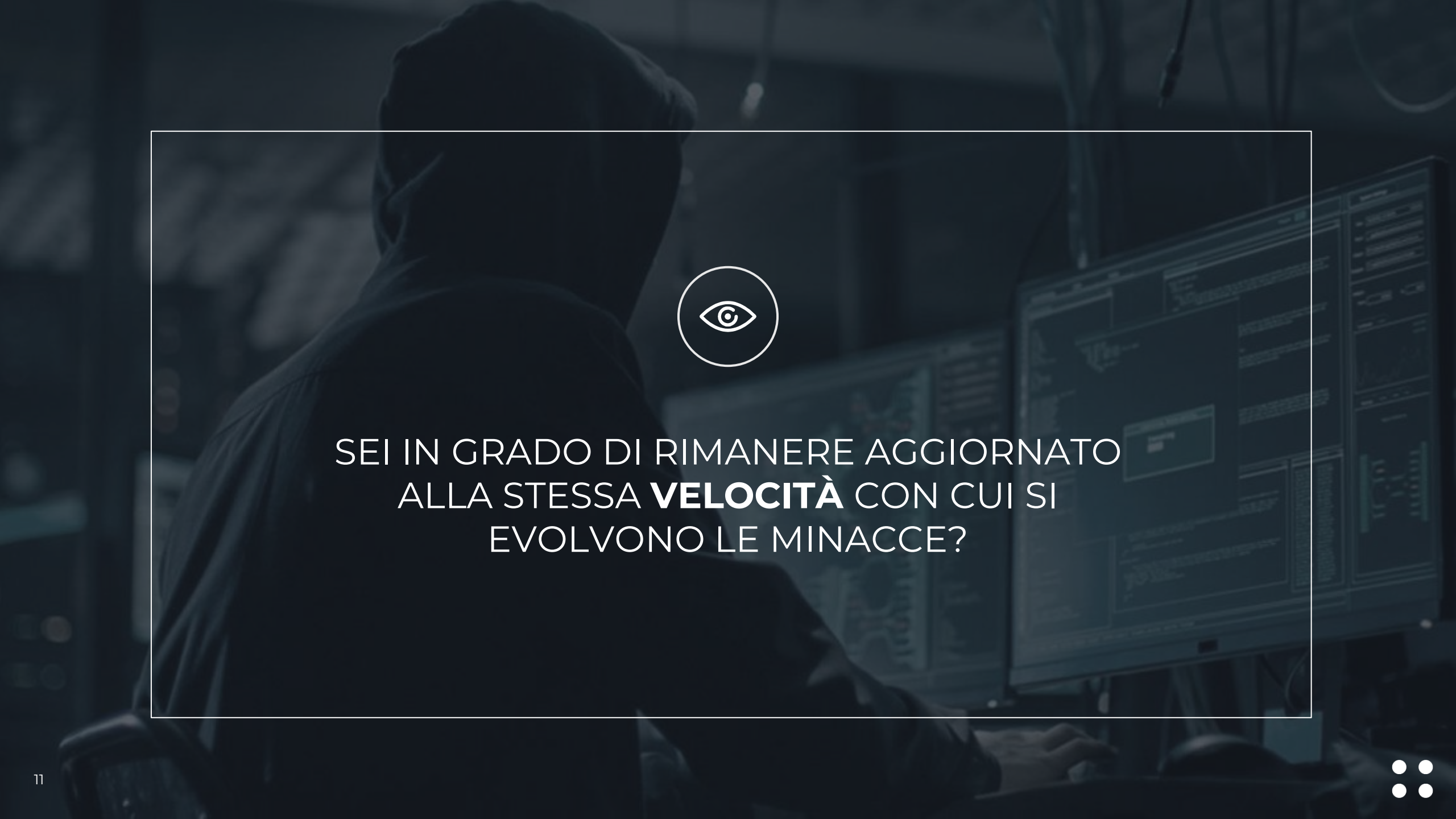
Furto di proprietà intellettuale

“Many things in life can be safely ignored but ignoring Cybersecurity Safe Practices is an open invitation for disaster.”



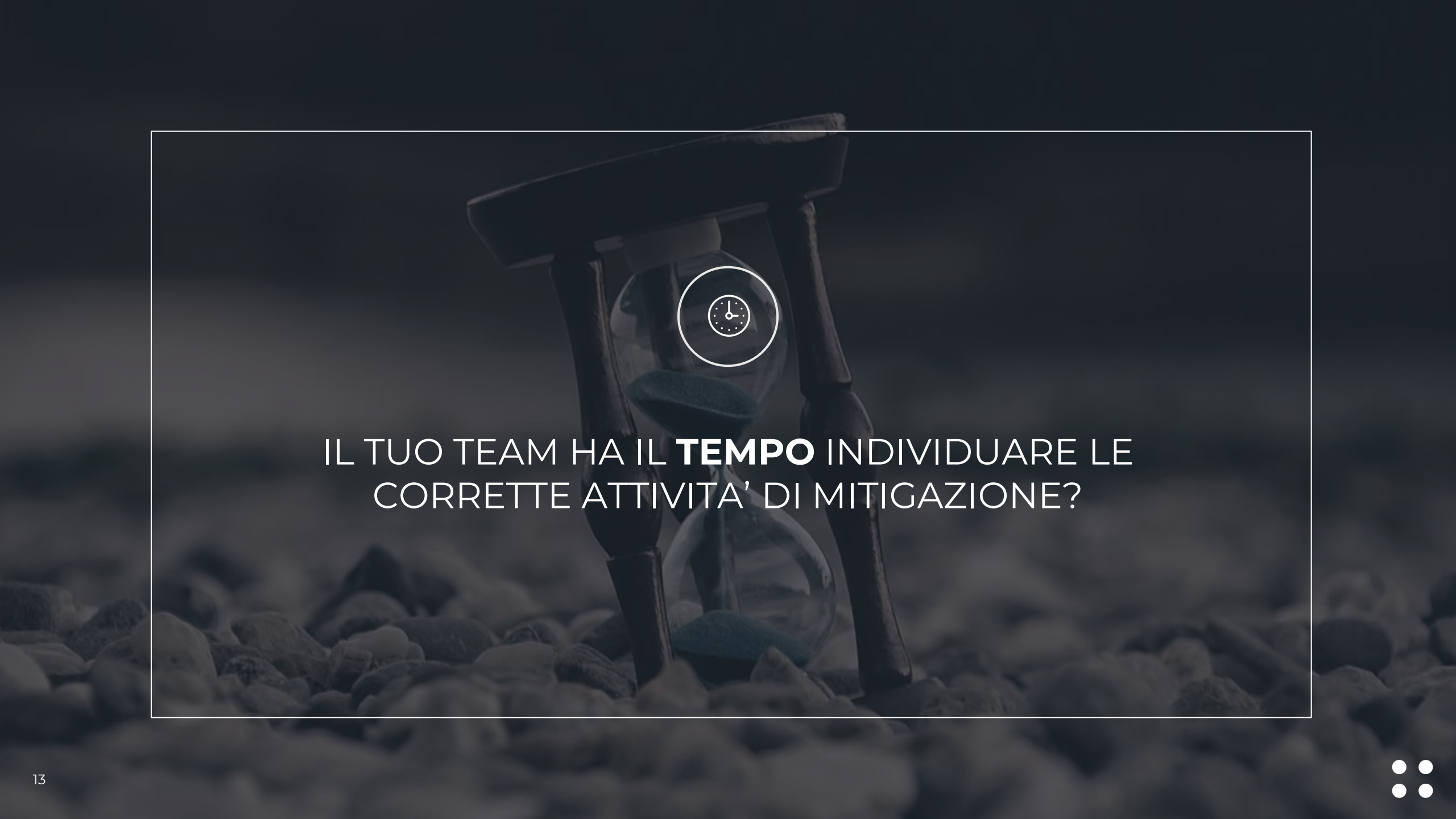
DOMINIO DELLA MINACCIA

Con l'aumentare della complessità e del livello di estraneità della minaccia risulta necessario essere protetti da una soluzione che oltre a prevenire l'attacco conosciuto con strumenti verticali, sia in grado di **correlare le informazioni, rilevare e rispondere ad attacchi sconosciuti altrimenti invisibili 24/7/365**.



SEI IN GRADO DI RIMANERE AGGIORNATO ALLA STESSA **VELOCITÀ** CON CUI SI EVOLVONO LE MINACCE?

POSSIEDI LE **RISORSE** PER GESTIRE TEMPESTIVAMENTE UN INCIDENTE DI SICUREZZA?



IL TUO TEAM HA IL **TEMPO** INDIVIDUARE LE CORRETTE ATTIVITA' DI MITIGAZIONE?

HAI **COMPETENZE** VERTICALI SULLA CYBER SECURITY PER ANALIZZARE I DATI DEI TUOI SISTEMI?


DON'T PANIC

PENSIAMO NOI ALLA SICUREZZA DEI TUOI DATI 24/7

MINACCE INTERNE

Integriamo e monitoriamo tutti i sistemi e i servizi esistenti all'interno del tuo ecosistema IT aziendale.

MINACCE ESTERNE

I nostri hacker etici si attestano nel mondo del deep e dark web per difenderti dalle minacce.

MONITORAGGIO

Avanzati strumenti di detection dotati di intelligenza artificiale e processi automatizzati.

I-SOC

Un team di cybersecurity specialist pronto a reagire in near real time a qualsiasi problematica.

Defence for ITALY

Questo il nome dell'iniziativa di solidarietà nata nel nostro headquarter di Reggio Emilia, che rende disponibili i servizi di cyber security, Cypeer, CSI, Admin Log & File Integrity.

- GRATUITÀ DEI SERVIZI PER I PRIMI TRE MESI
- SCONTO DEL 5% SUL PREZZO DI LISTINO* AL TERMINE DEI TRE MESI GRATUITI
- PAGAMENTO A 120 GG FM SULLA FATTURAZIONE TRIMESTRALE, ANZICHÉ 90 GG

*Il listino prezzi dei servizi di Cyber Security dipende dalla dimensione aziendale calcolata sul numero di server fisici e virtuali e sul numero di end user che compongono l'ecosistema IT aziendale.

CYBER SECURITY SUITE

IL NOSTRO SERVIZIO DI MANAGED DETECTION AND RESPONSE (MDR) 24/7/365

DETECTION

INTELLIGENZA ARTIFICIALE
MACHINE LEARNING
CORRELAZIONE

ANALYSIS

I-SOC TEAM
24/7/365

RESPONSE

ALERT E REMEDIATION
AL CLIENTE
24/7/365

CYBER SECURITY SUITE

LE TECNOLOGIE SU CUI BASIAMO IL NOSTRO SERVIZIO MDR

Una sola piattaforma. Milioni di informazioni.

CYBER SECURITY SUITE

CYPEER

Extended Detection & Response

Gestiamo la tua sicurezza interna

CSI

Threat Intelligence

Ti proteggiamo dalle minacce esterne

CYPEER

Un sistema evoluto XDR che raccoglie e correla tutte le informazioni e log provenienti da applicativi di sicurezza già presenti all'interno dell'ecosistema del cliente e non solo.
Grazie all'intelligenza artificiale il sistema è in grado di individuare attacchi e problematiche latenti non altrimenti visibili, che notifica immediatamente al nostro i-SOC 24/7/365 eliminando quasi la totalità dei falsi positivi.
Il nostro team di Cyber Security Specialist prende poi in carico le segnalazioni che il sistema segnala e individua tutte le attività di remediation e si affianca al cliente per metterle in opera.

All'interno della **dashboard cliente** è possibile visualizzare la correlazione dei dati provenienti da svariati sistemi di sicurezza aziendali, quali:

- Web Filtering
- Antispam
- Security agent
- Firewall
- Threat Hunting
- IDS/HIDS
- DHCP
- Antivirus

CYBER SECURITY INTELLIGENCE (CSI)

Soluzione basata su OPEN SOURCE INTELLIGENCE che consiste nella raccolta e analisi di dati provenienti dal deep e dark web al fine di proteggere la sicurezza digitale interna ed esterna del cliente.

CYBEROO dispone di un team di Cyber Security formato anche da Hacker Etici attestati nel mondo del deep e dark web, aventi accesso a fonti di informazioni non accessibili ad altri.
La maggior parte di questi dati si trova su forum in lingua cirillica, poiché molti hacker sono di origini russe. È anche per questo motivo che CYBEROO ha fondato un Hub a Kiev.

- Sistema di identificazione dei Data Breach per verificare la fuoriuscita di credenziali aziendali;
- Domain checker che verifica la presenza di domini clone, utilizzati per frodi;
- Controllo degli allegati malevoli;
- Monitoraggio informazioni utenti VIP del cliente (AD, Direttore, Amministratori, etc.);
- Analisi Clean/Dark/Deep web per l'analisi delle informazioni con possibili impatti sul cliente;
- Notifica delle nuove vulnerabilità.

VANTAGGI

CSI

CONTROLLA LE ATTIVITÀ DEL DEEP E DARK WEB

- Up to date con le nuove minacce provenienti da deep e dark web
- Proattività e prevenzione nella gestione delle vulnerabilità
- Eliminazione dei falsi positivi
- Competitività
- SOC 24/7/365
- Remediation

CY

SISTEMA DI RILEVAMENTO E RISPOSTA AGLI ATTACCHI AVANZATI

- Visibilità dei servizi di security in un'unica dashboard
- Dashboard semplice e user-friendly
- Eliminazione di zone d'ombra dei servizi di security
- Proattività nella gestione delle minacce
- Eliminazione dei falsi positivi
- Competitività
- SOC 24/7/365
- Automatic Remediation

TITAAN

LOG DEGLI AMMINISTRATORI DI SISTEMA

1

È un **software as a service** sviluppato per **soddisfare i requisiti GDPR** per la gestione dei Log di Amministratore di sistema.

2

Monitora tutti gli eventi che si registrano sulle singole macchine, identificando l'azione e lo user che lo scatena.

3

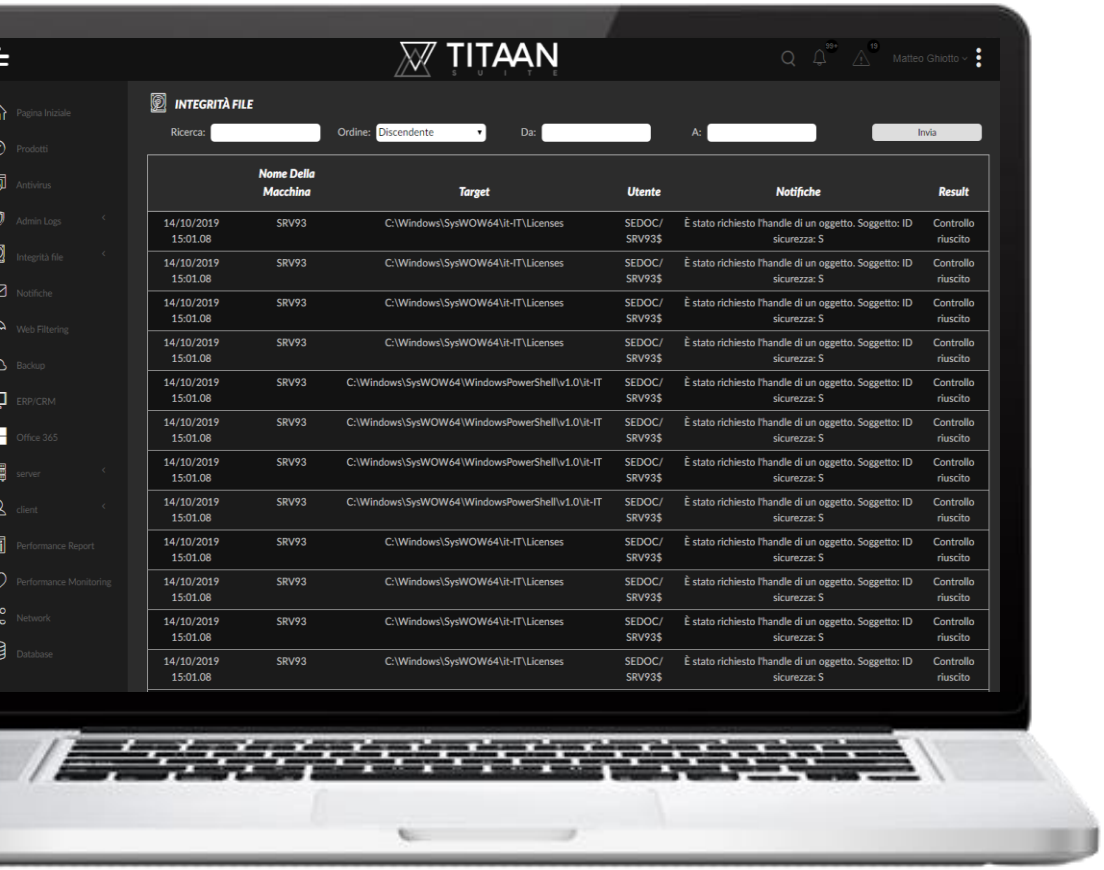
Identifica eventi che si verificano su **Active Directory**: **modifiche** e **assegnazioni** su utenti e gruppi; nuovi amministratori; modifiche delle Policy.

4

È possibile agganciarlo all'**Intelligenza Artificiale** per verificare che il comportamento dell'utente sia usuale.

TITAAN

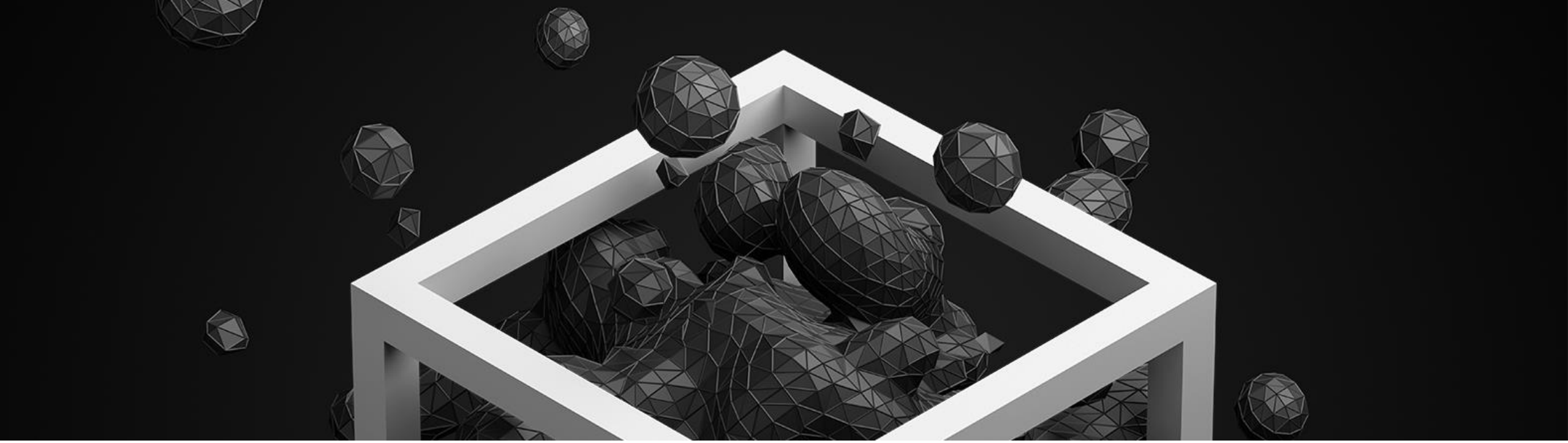
FILE INTEGRITY



1. Il modulo «Integrità File» risponde all' esigenza di capire **cosa avviene in un File Server**.
2. Dato un determinato path di sistema, fornisce **dettagli e storia del file** (chi, quando e con che programmi ha modificato o effettuato attività sul file).
3. È possibile inserire degli **alert sul comportamento anomalo** dell'utente.
4. È possibile agganciarlo all'**Intelligenza Artificiale** per verificare che il comportamento dell'utente sia usuale.

Cybercrime is among the greatest threat to every person and company in the world.

Be a step ahead.



WE ARE CYBEROO

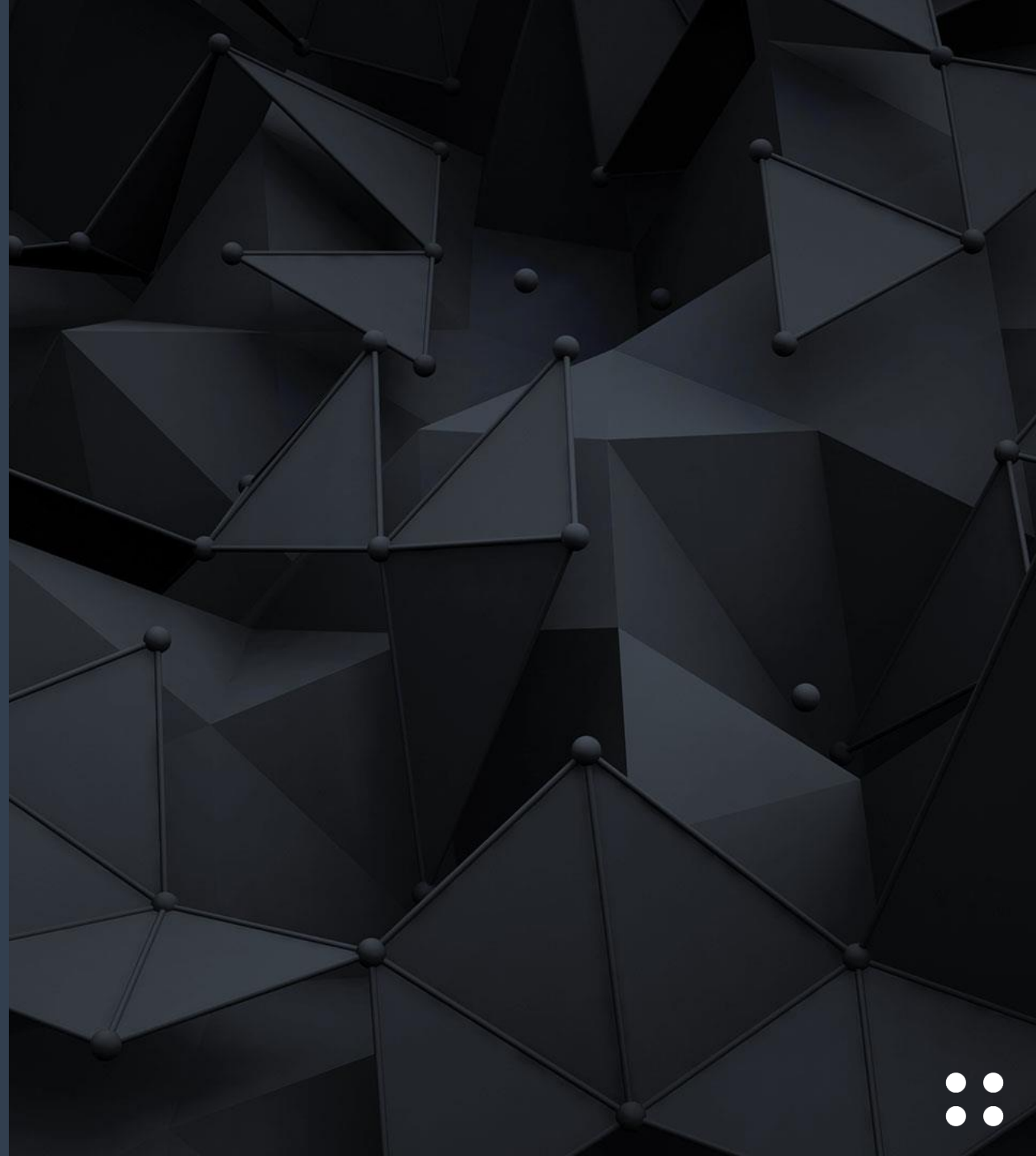
WE ARE DISRUPTIVE. WE ARE EXPERT. WE ARE TRUSTY.

CYBEROO combina l'apprendimento artificiale con l'intelligenza umana dei migliori professionisti sul mercato per garantire sicurezza, continuità e resilienza ai tuoi investimenti. Ci impegniamo nella creazione di una strategia per proteggere, monitorare e gestire il valore inestimabile delle tue informazioni. Gestiamo e semplifichiamo la tua complessità.

CYBEROO AT A GLANCE

- 1° società nel settore della Cyber Security ad essere quotata in Borsa Italiana su listino AIM
- PMI innovativa
- Oltre 600 Clienti
- 5 sedi in EMEA
- Oltre 100 dipendenti altamente qualificati
- 3 soluzioni proprietarie e certificate

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
DNV·GL
ISO/IEC 27001



PARTNERS

TECNOLOGIA

Gartner

elastic

Lenovo

freedcamp

CONTACTS

Address

CYBEROO S.p.A.
Via Brigata Reggio 37,
Reggio Emilia, 42124

Phone & Email

0522.385011
0522.382041
info@cyberoo.com
www.cyberoo.com