CYBEROO

LA CYBER SECURITY È UN PROCESSO, NON UN PRODOTTO.

CYBEROO

SOMMARIO

L'IMPORTANZA DELLA CYBER SECURITY

PERCHÉ DOVRESTI PROTEGGERE I DATI SENSIBILI E LA CONTINUITÀ OPERATIVA DELLA TUA AZIENDA

LASCERESTI IL TUO CELLULARE IN MANO A UNO SCONOSCIUTO?

La tua privacy è importante. Per questo esistono sistemi di sicurezza in grado di proteggerla e tutelarla. Il cellulare, uno strumento di uso quotidiano, è allo stesso tempo una delle fonti di informazioni più importanti e dettagliate sulla tua vita privata, e proprio per questo è reso inaccessibile dai sistemi di protezione più innovativi e sofisticati: dal codice alfanumerico, all'impronta digitale, fino al riconoscimento facciale. Alzi la mano chi non fa uso di almeno una di queste tecnologie.

E I TUOI DATI AZIENDALI? SONO PROTETTI A SUFFICIENZA?

Non adottare sistemi efficienti di Cyber Security in azienda è esattamente come lasciare il proprio cellulare, privo di ogni protezione, in mano a degli sconosciuti. I tuoi dati sensibili sono più accessibili di quanto tu possa immaginare. Ogni giorno la tua azienda fa affidamento a sistemi informatici per gestire le proprie finanze, archiviare documenti riservati, organizzare i contatti, inviare e-mail e aggiornare il proprio sito web, pensando che semplici firewall e software antivirus possano preservarli dalle minacce esterne. Ma i tempi in cui questi sistemi di protezione erano efficaci sono finiti.
Secondo Clusit, in Italia si registra un attacco informatico **ogni 39 secondi**, mentre il numero complessivo delle violazioni di dati sul web è **quasi raddoppiato** negli ultimi 4 anni. Le tecniche di hackeraggio sono diventate **sempre più sofisticate** e impercettibili: in media, trascorrono **120 giorni** prima che un'organizzazione si accorga di una violazione dei dati e il 60% delle aziende non è in grado di scoprire la fonte di un attacco **entro i 12 mesi successivi**.

E se non ti sembra abbastanza preoccupante, ti sarà utile sapere che, secondo il rapporto *Cost of Data Breach* (IBM, 2020), **il costo medio di una violazione è di 3,32milioni di euro** (circa 123 euro per ogni record rubato).

CHE COSA FANNO GLI HACKER CON I TUOI DATI AZIENDALI?

La criminalità informatica si sta industrializzando ed è in grado di offrire garanzie e servizi al pari di un'organizzazione legalizzata: dallo sviluppo del prodotto, al supporto tecnico, fino ai servizi personalizzati. Proprio perché consente di avere accesso a dati riservati con facilità e riservatezza, negli ultimi anni la clientela del cyber crime

sta crescendo esponenzialmente, in tutti i settori. Il suo compito è quello di impossessarsi, per poi rivendere, nuove tecnologie, informazioni sensibili e piani strategici delle aziende per offrire ai loro acquirenti un vantaggio sui concorrenti. Tra i mezzi più utilizzati dal cyber crime ci sono i **ransomware**, i virus che sequestrano il contenuto del tuo hard disk paralizzando la tua azienda per giorni e impedendo qualsiasi operatività, o il **cryptomining**, software pirata che sfrutta la potenza del tuo computer per coniare criptovalute, o, ancora, il **phishing**, una truffa perpetrata a nome della tua azienda per carpire informazioni riservate ai tuoi clienti.

COSA POTREBBE SCOPRIRE IL TUO COMPETITOR, SE ENTRASSE IN POSSESSO DEI DATI RISERVATI DELLA TUA AZIENDA?

Ti diamo **quattro motivi** per cui dovresti dotarti di un sistema di Cyber Security:

1 PER ESSERE CONFORME ALLA LEGGE SULLA CYBER SECURITY

La stesura di un Incident Reponse Plan (IRP), il piano di intervento nel caso di incidenti informatici, è stato reso obbligatorio dalle disposizioni di legge in materia di sicurezza informatica e protezione dei dati, prima fra tutte l'ormai nota GDPR (General Data Protection Regulation). Oltre alle norme più generali, esistono anche standard specifici a cui aziende e organizzazioni operanti in precisi settori devono conformarsi. Ma attenzione: utilizzare sistemi di difesa solo per essere conformi alle normative non è sufficiente per garantire una reale protezione dal cyber crime. La legge, infatti, richiede solo le misure minime e indispensabili per la sicurezza aziendale.

2 PERCHÉ SE NON PROTEGGI I TUOI DATI, METTERAI A RISCHIO ANCHE QUELLI DELLA TUA FILIERA

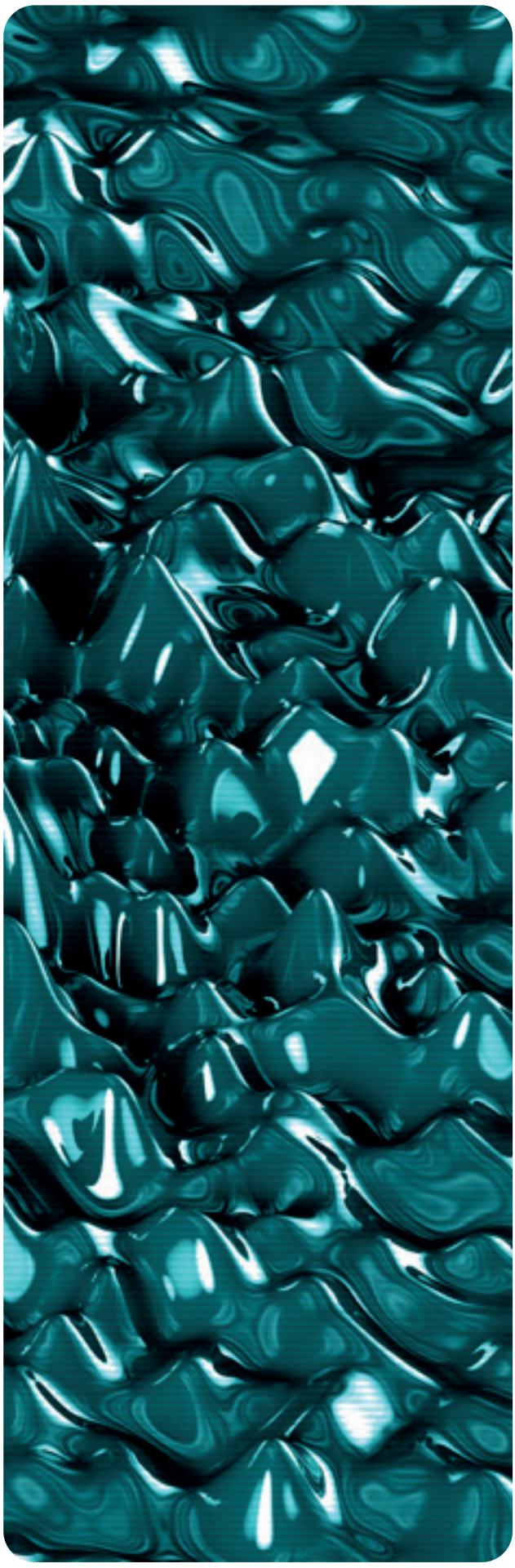
La sicurezza della tua azienda è direttamente legata a quella di tutta la filiera. Partner, clienti, fornitori, dipendenti, formano un grande network che diventa facilmente attaccabile se anche un solo elemento della catena non dovesse essere sufficientemente protetto dagli attacchi sul web. I sistemi informatici della tua rete di business non sono compartimenti stagni ma porte di accesso ai dati di ogni organizzazione che la compone. L'80% delle aziende che hanno subìto una violazione, ha visto compromettere anche le informazioni riservate dei suoi clienti.

3 PER ASSICURARTI LA CONTINUITÀ OPERATIVA E PROTEGGERTI DA INGENTI PERDITE FINANZIARIE

Immagina di dover dire ai tuoi clienti che non puoi gestire la loro richiesta per settimane, o addirittura per mesi, perché il tuo sito e-commerce è stato hackerato, non puoi accedere alla mail e il tuo gestionale è criptato. Una violazione della sicurezza influirebbe non solo sul fatturato, ma anche sulla reputazione dell'azienda. Che cosa potrebbe pensare un potenziale cliente se scoprisse che il sistema di protezione della tua azienda è vulnerabile e che i suoi dati potrebbero essere messi a rischio?

4 PER PRESERVARE LA TUA POSIZIONE STRATEGICA SUL MERCATO

Ci sono segreti aziendali che non possono essere rivelati: la gestione finanziaria, negoziazioni riservate, esclusivi processi di produzione...sono informazioni



top secret ma, purtroppo, facilmente accessibili per il cyber crime. Proteggere la rete informatica significa, prima di tutto, proteggere il business e tutelare il lavoro di anni dal rischio che finisca nelle mani sbagliate.

NON AVER SUBÌTO ATTACCHI NON È SINONIMO DI AVERE UN SISTEMA DI SICUREZZA STRUTTURATO ED EFFICACE.

E nemmeno essere una piccola impresa. Verrebbe spontaneo pensare che il cyber crime sia abbia più interesse a rubare i dati alle grandi enterprise. Niente di più sbagliato: le statistiche dimostrano che il 52% delle violazioni informatiche è rivolto alle PMI, proprio perché sono le prime ad ignorare l'importanza di un efficace sistema di protezione dati, o perché ritengono di avere un budget troppo limitato per poter investire nella cyber security.

NON CONFONDERE LA CONFORMITÀ CON LA SICUREZZA

Essere conforme ad un determinato standard di sicurezza non comporta necessariamente che la tua rete sia **inattaccabile**. Il tuo sistema informatico potrebbe comunque essere **vulnerabile** agli attacchi e quindi facilmente compromettibile.

QUAL È LA NORMATIVA CHE REGOLA LA PROTEZIONE DEI DATI SENSIBILI?

Direttiva Polizia (n. 2016/680)

La Direttiva Polizia mira a garantire lo scambio dei dati personali tra le autorità all'interno dell'UE.

Direttiva NIS (n. 2016/1148)

La Direttiva NIS – Network and Information Security – persegue l'obiettivo di stabilire quali siano le misure necessarie a conseguire un livello comune ed elevato di sicurezza della rete dei sistemi informativi, rafforzando la cooperazione a livello locale e in ambito UE.

Regolamento eIDAS (n. 2014/910)

Il Regolamento europeo eIDAS – per l'identificazione elettronica e le transazioni elettroniche nel mercato interno – ha lo scopo di disciplinare la firma elettronica, i trasferimenti di denaro e altri tipi di transazione nel mercato unico europeo.

Direttiva PSD2 (n. 1025/23669

La Direttiva europea PSD2 – sui pagamenti digitali – è volta a delineare le regole sulla trasparenza delle condizioni e sui requisiti informativi dei servizi di pagamento, e a definire diritti e obblighi di utenti e prestatori.

Regolamento sui dati non personali (n. 2017/1807)

Il Regolamento sui dati non personali garantisce la libera circolazione transfrontaliera dei dati relativi alle imprese.

Cybersecurity Act (n. 2019/881)

L'Atto mira a rafforzare la posizione dell'ENISA – l'Agenzia dell'UE per la Cyber Security – e ad introdurre un sistema europeo di certificazione della sicurezza informativa dei prodotti e dei servizi digitali.

LA SICUREZZA NON È UN PRODOTTO

PERCHÉ NON DOVRESTI ACCONTENTARTI DI SOLUZIONI STANDARD E "FAI DA TE"

Se pensi che l'ultimo antivirus che hai acquistato, pagandolo un occhio della testa, e installato su tutti i computer aziendali sia sufficiente per difendere i tuoi dati dal cyber crime, sei fuori strada. Ti gioverà sapere, infatti, che il **93% dei sistemi informatici violati** è solitamente "protetto" da un software antivirus di quelli più diffusi in commercio.

LA SICUREZZA NON È UN PRODOTTO MA UN PROCESSO

che avviene in fasi definite e coinvolge tutte le aree dell'azienda attraverso un **progetto ampio e integrato**. Una strategia di cyber security può ridurre il numero di attacchi che vanno a buon fine, diminuire i tempi di risoluzione dei problemi e limitare i danni derivanti dalla perdita dei dati o da interruzioni del servizio, ma può farlo in maniera efficace solo se **delegata a specialisti** in grado di elaborare un progetto strutturato e di implementarlo con costanza.

Il tuo comparto IT possiede le competenze, la verticalità, l'esperienza e la prospettiva olistica indispensabili per costruire una strategia efficace? Ma soprattutto, dispone del tempo necessario per monitorare i sistemi di cyber security 24 H e 7 giorni su 7 per intervenire tempestivamente in caso di minaccia? Se la risposta è no, dovresti iniziare a pensare di rivolgerti ad una società specializzata.

5 MOTIVI PER DELEGARE AD ALTRI LA TUA SICUREZZA INFORMATICA

Sul mercato esistono software di ogni tipo, per tutte le tasche e per ogni tipo di organizzazione, che garantiscono la piena protezione dei sistemi informatici aziendali. Ma un fornitore può assicurarti quello che i più comuni tool non saranno mai in grado di offrire:

1. **ASSISTENZA H 24, 365 GIORNI ALL'ANNO (LO SAI CHE IL 76% DEGLI ATTACCHI AVVIENE NEL WEEKEND E DI NOTTE?)**
2. **SOLUZIONI CUSTOMIZZATE SULLA BASE DELLE TUE NECESSITÀ**

3 **MONITORAGGIO, AGGIORNAMENTO E IMPLEMENTAZIONE CONTINUI DEI SISTEMI DI SICUREZZA**

4 **NOTIFICA IMMEDIATA IN CASO DI MINACCIA**

5 **UNA PREOCCUPAZIONE IN MENO PER IL TUO COMPARTO IT (E PIÙ TEMPO LIBERO)**

GLI STRUMENTI DI SICUREZZA SONO EFFICIENTI SOLO SE CONFIGURATI A DOVERE, INTEGRATI CON I SISTEMI AZIENDALI E MONITORATI DA PERSONALE COMPETENTE

Gli attacchi informatici crescono costantemente in complessità e raffinatezza, e chi perpetra l'attacco può rimanere dormiente per giorni prima di compiere la violazione: per mettere in atto un piano di sicurezza informatica servono, quindi, aggiornamento e studio continui e una vigilanza attenta e costante. Nonché la stesura di un Incident Response Plan personalizzato sulla base delle esigenze di ogni singola impresa. **Non esiste una strategia che vada bene per tutti**: un piano di cyber security deve integrarsi perfettamente con i sistemi informatici adottati in azienda e adattarsi alla strategia più ampia di gestione aziendale. Dal punto di vista pratico, l'ITP deve identificare una serie di incidenti tipo e prevedere un'azione per ognuno di essi, stabilendo procedure e strumenti per prevenire il problema o per risolverlo. Un piano ideale di sicurezza informatica, inoltre, dovrebbe prevedere un'ana-

lisi periodica dello stato del sistema per individuare eventuali falle nella sicurezza e punti di debolezza nel piano d'azione.

NON TI ABBIAMO ANCORA CONVINTO?

Allora considera questi tre punti:

1 LA SICUREZZA INFORMATICA NON È UN OPTIONAL

Essenzialmente per due ragioni: **i problemi finanziari** che possono derivare da una fuga di dati, e la **perdita di reputazione** che ne potrebbe conseguire. Il valore dei dati aziendali, siano essi di proprietà esclusiva dell'azienda o di proprietà di terzi, è inestimabile e la loro violazione può produrre danni ingenti al business, talvolta non risolvibili. Una protezione adeguata contro gli attacchi cibernetici ti consentirà di evitare **pesanti sanzioni e danni reputazionali**.

2 DEVI ASSICURARE PROTEZIONE AL TUO NETWORK

I tuoi clienti, partner, fornitori continuerebbero a rivolgerti a te se sapessero che la tua rete informatica è debole e può essere attaccata da un momento all'altro? Il business comporta un continuo scambio di informazioni, alcune delle quali **estremamente riservate**, e il digitale è diventato il veicolo principale di questo scambio. Ti fideresti di un servizio di home banking al quale tutti possono accedere senza credenziali, senza privacy e senza limiti?

3 AFFIDARTI A ESPERTI DI SICUREZZA TI DÀ MAGGIORI GARANZIE

Considera l'outsourcing di tutte le tue esigenze di Cyber Security: potrai risparmiare sui costi di lavoro, spostare la maggior parte delle responsabilità al di fuori dell'azienda, ed essere seguito tutto il giorno, tutti i giorni, da un team di specialisti dedicati. Cosa vuoi di più?

L'MDR (Managed Detection and Response) è un sevizio proattivo e avanzato che monitora, rileva, analizza e risponde ad attività dannose nella rete, o a qualsiasi altra violazione della sicurezza informatica, ed è interamente gestito da un fornitore di sicurezza.

Entro il 2025 il 50% delle mid-size company utilizzerà un MDR come unico provider di servizi di sicurezza.

Gartner - Market Guide for Managed Detection and Response Services (25 ottobre 2021)

Un MDR comprende molto di più di una semplice notifica di violazione.

1 RILEVAMENTO

Dei sistemi di Intelligenza Artificiale raccolgono un'ampia mole di dati dai software di protezione già installati nell'ecosistema aziendale . Dialogando con sistemi di Machine Learning, le Intelligenze Artificiali individuano la minaccia e attivano un alert che viene in-

dirizzato direttamente all'iSOC.

2 ANALISI

Identificata una minaccia e stabilito il suo grado di priorità, l'iSOC (intelligence Security Operation Center)ne esamina l'origine e la portata, valutando il suo eventuale impatto sulla rete.

3 RISPOSTA

Raccolte le informazioni necessarie, gli specialist mettono in guardia l'organizzazione del rischio di attacco, fornendole analisi causali, consigli sulla mitigazione e toolkit necessari a gestire la potenziale violazione.

"PUÒ BENISSIMO FARLO IL NOSTRO COMPARTO IT"

È una frase che ci sentiamo ripetere spesso. Ma il tuo comparto di IT è in possesso di questi requisiti?

IL TUO IT È DOTATO DI COMPETENZE VERTICALI SULLA CYBER SECURITY?

È una lacuna che spesso riscontriamo nelle organizzazioni con le quali lavoriamo, soprattutto in quelle di medie e piccole dimensioni. Perché il sistema di protezione sia efficace è necessario sia monitorato e implementato da un team specializzato, che possa dedicarsi alla ricerca delle minacce a tempo pieno: un'esigenza che può concretizzarsi, forse, nelle aziende più grandi dove risorse e budget non mancano, ma che è difficile da realizzare nelle organizzazioni più piccole e di medie dimensioni.

IL TUO IT È IN GRADO DI IMPLEMENTARE SOLUZIONI MDR?

Le soluzioni **MDR (Managed Detection and Response)** sono servizi avanzati molto complessi che si differenziano dai tradizionali sistemi di sicurezza informatica perché garantiscono una percentuale di efficacia maggiore ma richiedono competenze altamente qualificate (e spesso, ricercate) per essere impiegate al massimo delle loro potenzialità.

Gli MDR, sono servizi altamente evoluti che consentono di avere una panoramica a 360° dei pericoli che minacciano la tua azienda, ma presuppongono delle conoscenze di cyber security specialistiche e approfondite che i comparti IT normalmente non possiedono.

IL TUO IT DISPONE DEL TEMPO NECESSARIO PER GESTIRE LE MINACCE?

Un altro problema spesso sottovalutato dalle organizzazioni è quello dell'enorme mole di avvisi che i comparti IT ricevono regolarmente dai sistemi di sicurezza. Molti di questi alert richiedono un'analisi approfondita prima di essere archiviati come "falsi allarmi" perché potrebbero celare minacce non immediatamente identificabili o fare parte di un attacco molto più ampio. La cyber security, inoltre, richiede un monitoraggio continuativo, h24 e 7 giorni su 7, che spesso gli IT non sono in grado di garantire per mancanza di tempo e di risorse. Ecco perché avere un team dedicato alla Cyber Security è fondamentale per assicurare una copertura completa ed efficace dagli attacchi informatici.

Insomma, gli specialisti della Cyber Security sono in grado di gestire minacce avanzate che il comparto IT non ha le giuste competenze per affrontare, con costo inferiore a quello che l'azienda dovrebbe investire per creare un proprio team di sicurezza specializzato.

CYBEROO

IL CUSTODE DELLA TUA PRIVACY AZIENDALE

Se hai letto fino a qui vuol dire che hai preso finalmente sul serio il tema della sicurezza della tua rete informatica aziendale e che probabilmente stai cercando uno specialista a cui rivolgerti.

Mi chiamo **Cyberoo** e **sono quello che cerchi.**

Sono una PMI innovativa specializzata in cyber security per le imprese. Sono la prima azienda del settore a essere quotata a Piazza Affari, più precisamente su su Euronext Growth Milan (ex AIM Italia), il mercato della Borsa Italiana dedicato alle PMI ad alto potenziale di crescita. Mi occupo di sicurezza informatica a 360°, intesa non solo come protezione dei sistemi informatici dagli attacchi esterni, ma anche come realizzazione di una vera e propria strategia in grado di difendere, monitorare e gestire le informazioni dell'ecosistema IT.

Per svolgere il mio lavoro, mi avvalgo di oltre 60 specialisti della Cyber Security, altamente qualificati, che effettuano attività di ethical haketing.
Nel tempo, ho rafforzato le mie competenze distintive investendo in abilità tecnologiche che supportino l'analisi dei dati e dei comportamenti (Intelligenza Artificiale, Machine Learning, Deep Learning e Big Data).

Nel 2017 è nato il cuore pulsante delle attività di cyber security: Cyberoo LAB, un network di i-SOC (intelligence Security Operation Center) proprietari con il compito di creare soluzioni intelligenti e competitive a supporto della sicurezza delle aziende e della loro continuità operativa.

PERCHÉ DOVRESTI SCEGLIERMI?

1 Sono attiva 24 ore su 24, 7 giorni su 7, 365 giorni all'anno per proteggere i tuoi dati. Monitoro costantemente minacce e anomalie nella tua rete informatica tramite avanzati strumenti di detection e processi automatizzati. Sono sempre pronta per intervenire e per bloccare qualsiasi tipo di violazione.

2 Non vendo un prodotto, ma offro un servizio totalmente personalizzato che soddisfi le tue esigenze specifiche e si integri con i tuoi sistemi. Con me, non devi ripensare alla tua struttura.

3 Tutto quello che faccio, lo faccio con passione, qualità e trasparenza, sia sui tempi che sulle aspettative. Inoltre, mi baso sull'esperienza che mi consente di comprendere le esigenze di chi lavora e di affrontare ogni sfida con competenza e tempestività.

QUALI SOLUZIONI POSSO OFFRIRTI?

CYBER SECURITY SUITE

La mia Cyber Security Suite è un servizio MDR che si compone di due diverse soluzioni: CYPEER e CSI.

CYPEER: è un servizio basato su una piattaforma di Detection intelligente che si occupa del monitoraggio della rete informatica **verso il suo interno.** Raccoglie informazioni sugli eventi che si svolgono entro il perimetro di sicurezza informatica aziendale e li confronta con i dati raccolti dai sistemi di protezione tradizionali come Firewalls, Filtri Antispam, Antivirus, ecc.
Cypeer può attivare remediation automatiche a fronte di allarmi specifici. È proprio nella remediation che si distinguono le due modalità del servizio: Cypeer Pure e Cypeer Sonic.

CSI (Cyber Security Intelligence):
effettua l'azione di monitoraggio **verso l'esterno**, navigando nel Deep & Dark Web e individuando potenziali minacce afferenti all'azienda prima che altri segnali la rendano evidente. La soluzione è completamente implementata in un **Cloud** localizzato in Italia.

Queste due soluzioni forniscono una **panoramica completa** dello scenario di sicurezza della rete aziendale e abilitano interventi di tipo mirato e preventivo.

I-SOC TEAM

La Cyber Security Suite, inoltre, si integra al **monitoraggio continuativo** da parte di un **i-SOC team** (intelligence - Security Operation Center): una squadra di **oltre 60 esperti** qualificati dislocati in Italia e all'estero che si occupano dell'analisi dei dati e della gestione delle segnalazioni provenienti da CYPEER e CSI, senza interruzioni, per offrirti un servizio sempre attivo e un pronto intervento in caso di minaccia. Sia CYPEER che CSI sono sistemi che forniscono alert dettagliati e puntuali, ma l'operato del team consente una valutazione delle notifiche più raffinata di un qualsiasi tool super-tecnologico.
L'i-SOC è il baricentro di tutte le operazioni di cyber security, il luogo in cui persone e tecnologia si integrano per difenderti ogni giorno.

Con la Cyber Security Suite avrai:

1 UN SERVIZIO ATTIVO 24/7

Copertura completa e continuativa, a un costo minore di quello che richiederebbe la formazione di un team e di un framework interno.

2 IL MONITORAGGIO DEL DEEP & DARK WEB

Analisi e raccolta dati dal Deep & Dark Web da parte di un team di esperti, al fine di proteggere la sicurezza digitale sia interna che esterna all'azienda.

3 IL RILEVAMENTO DI DATA BREACH E DI FRODI

Identificazione di violazioni della sicurezza informatica e intervento immediato in caso di fuoriuscita di dati e credenziali aziendali.

RISPOSTA AGLI INCIDENTI INFORMATICI

Il rischio zero non esiste, gli incidenti informatici avvengono. È fondamentale essere in grado di salvaguardare l'azienda da eventuali danni alla rete e al brand.

Incident Response è un servizio di risposta agli incidenti informatici, disponibile **24 ore su 24, 7 giorni su 7, 365 giorni all'anno**, per contrastare gli attacchi informatici critici in modo rapido ed efficace.

Nel momento in cui si verificano incidenti informatici come databreach o ransomware, il team di Incident Response si attiva per **individuare e isolare gli attaccanti, e contenere la minaccia.**
Si tratta di un team di specialisti dell'Offensive Security a tua disposizione per definire il perimetro dell'incidente, analizzare il vettore d'attacco, gli impatti e le compromissioni. A seguito delle analisi sulla minaccia e il canale di attacco, si propone un piano di risposta che include il dettaglio delle attività per limitare il danno **ed eradicare la causa, evitando una possibile cronicità dell'evento.**

REPRESENTATIVE VENDOR NELLA GARTNER MARKET GUIDE FOR MANAGED DETECTION AND RESPONSE SERVICES

La “Market Guide for **Managed Detection & Response (MDR) Services 2021**” di Gartner Inc., la più importante e autorevole ricerca internazionale sui servizi gestiti di sicurezza informatica, ha **riconosciuto Cyberoo**, come parte del ristretto novero dei “**representative vendor**” delle nuove frontiere della cybersecurity.

Per Gartner, Cyberoo e le due soluzioni MDR (l’innovativa Cyber Security Suite, con i servizi CYPEER e CSI) rispecchiano quindi perfettamente tutti i requisiti tecnici necessari per erogare questo tipo di servizio, al pari di poche altre aziende vendor internazionali, per lo più statunitensi.

La “Market Guide for Managed Detection & Response Services 2021” di Gartner Inc. è disponibile sul sito dell’azienda:

Notes: Market Guide for Managed Detection and Response Services, Published 25 October 2021 By Pete Shoard, Craig Lawson, Mitchell Schneider, John Collins, Mark Wah, Andrew Davies.

SEGUICI SU:

Linkedin

https://www.linkedin.com/company/cyberoo

Twitter

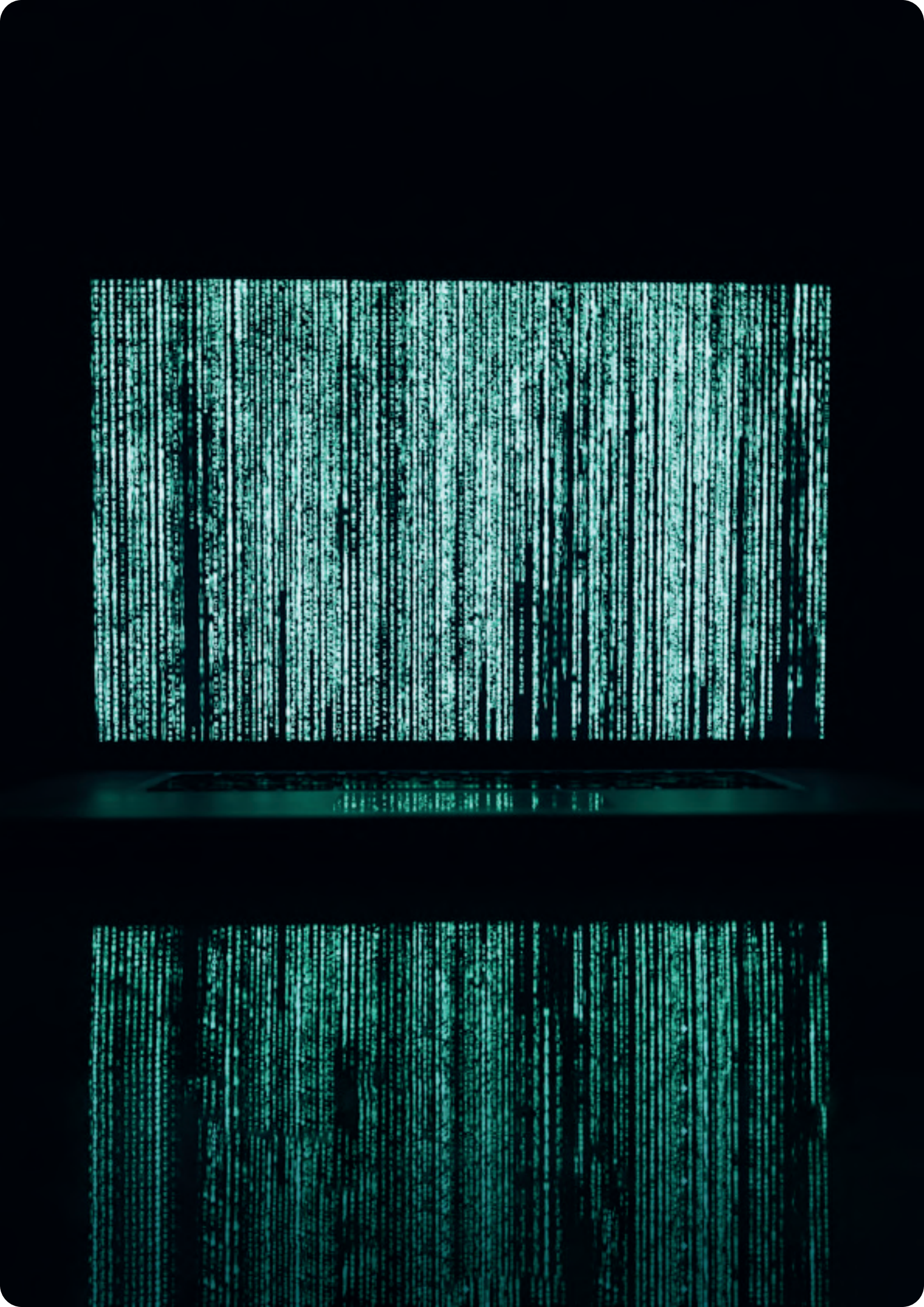
https://twitter.com/CYBEROO_ITALIA

Blog

https://blog.cyberoo.com/

Podcast

https://www.radioit.it/cyberoo-podcast/



CASE STUDIES

HO LAVORATO PER...

Tutte le brochure che si rispettino si concludono con qualche case study, ma non questa.
Posso dirti che sono attiva nei settori dell'energia, della moda, dell'automotive e del tech, ma non citerò i nomi delle aziende che si sono affidate ai miei sistemi di cyber security, perché conosco l'importanza di tutelare e preservare i dati sensibili dal rischio che cadano nelle mani sbagliate.
Da sempre, metto la riservatezza dei miei clienti al primo posto e mi adopero per costruire caveau sofisticati e inattaccabili in cui nascondere i loro dati più segreti.

Proprio per questo, porto avanti fino allo stremo l'ideale di un hacketing etico e di una rete finalmente libera dalle minacce, e combatto ogni giorno per perseguirlo.

CONTATTI

Reggio Emilia
via Brigata Reggio, 37 – 42124
Tel. 0522.388111