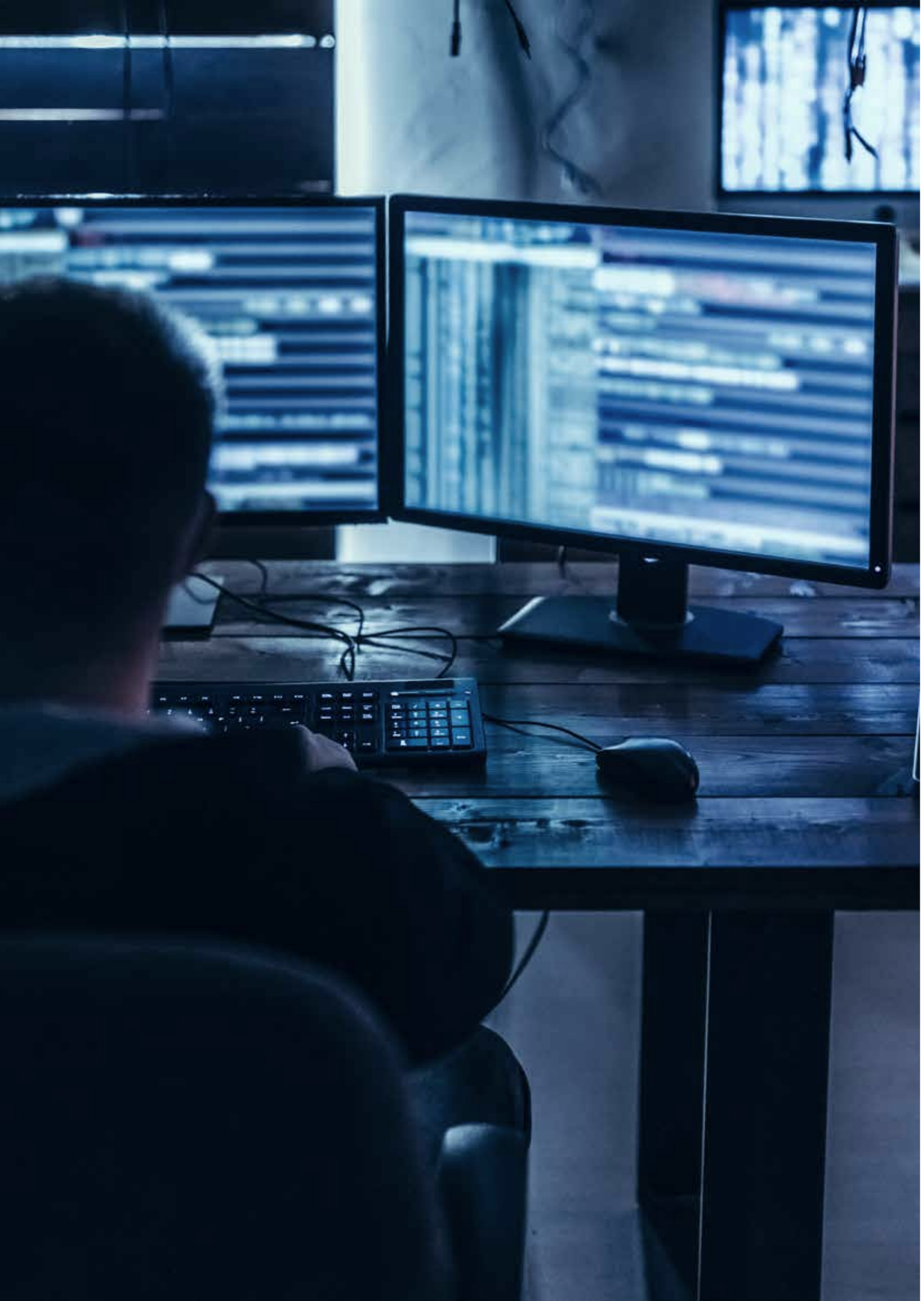
PAPER 2024

CONNECTING TECH & BUSINESS

Il nuovo ruolo chiave del SOC moderno



Introduzione

Nel settembre del 2010, il vice-segretario della Difesa statunitense William J. Lynn III ha pubblicamente qualificato il cyber-space come il quinto dominio della conflittualità dopo terra, mare, aria e spazio. Questo dominio è caratterizzato dalla crescente evoluzione dei sistemi digitali e dalla velocità con cui questi interagiscono. I rischi emergenti di sicurezza oggi non sono legati solamente al contesto aziendale ma sono estesi a tutta la società, come ampiamente documentato e dimostrato dagli episodi ormai quotidiani di pirateria informatica.
Si rende quindi necessario reagire tempestivamente per arginare o addirittura annullare ogni tentativo doloso di accesso ai dati e alle infrastrutture.
Tentativi che, se portati a termine, producono impatti sempre più complessi da gestire per il business.

In un periodo storico in cui siamo sempre più connessi, la sicurezza del cyber-spazio non può essere messa in secondo piano. Con tempistiche sempre più urgenti, oggi è quindi fondamentale ricorrere a soluzioni più agili, efficaci e moderne.
Eppure, questa stessa agilità abilitata dall'impiego delle nuove tecnologie digitali porta con sè nuovi livelli di complessità nella cybersecurity. Per questo è necessario adeguare sia i sistemi di protezione che quelli di monitoraggio delle minacce, integrandoli e governandoli in modo da rendere il proprio Security Operations Center il centro nevralgico che anticipa, gestisce, reagisce e soprattutto non subisce passivamente le sempre più articolate criticità e minacce del cyber-spazio.

Cyber-attacchi

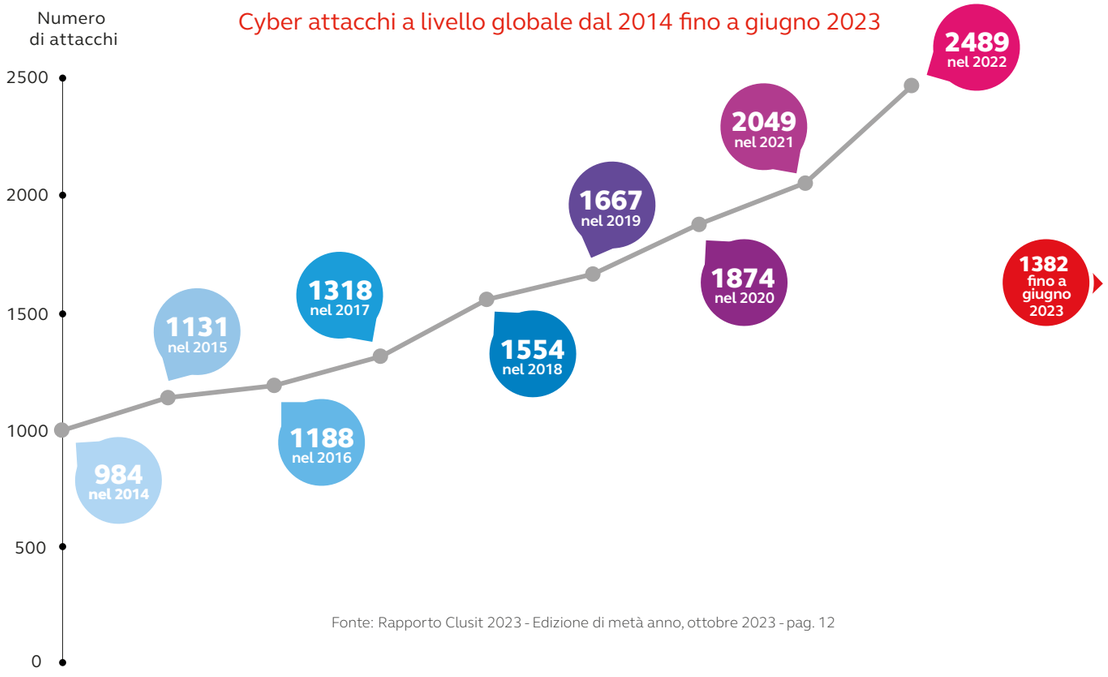
I costi e gli impatti per le organizzazioni

I temi della cybersecurity e gli impatti del cybercrimine nei diversi settori di industria possono essere illustrati analizzando i dati che caratterizzano gli attacchi nell'anno 2022 e nel primo semestre del 2023. Secondo il CLUSIT, il 2022 si è distinto per essere l'anno peggiore a livello globale; nel mondo sono stati registrati 2.489 incidenti gravi, rispetto ai 984 del 2014, che corrisponde a un aumento del 153%.

Il Rapporto Clusit di ottobre 2023 contiene dati relativi al primo semestre del 2023.

Il primo semestre del 2023 conferma questo trend, registrando 1.382 incidenti gravi, pari ad un aumento dell'86% rispetto allo stesso periodo del 2014. Questo incremento si verifica anche sulla media mensile degli attacchi: **nei primi sei mesi del 2023 in Italia sono stati registrati in media 230 attacchi al mese**, corrispondenti a circa **8 episodi giornalieri**.

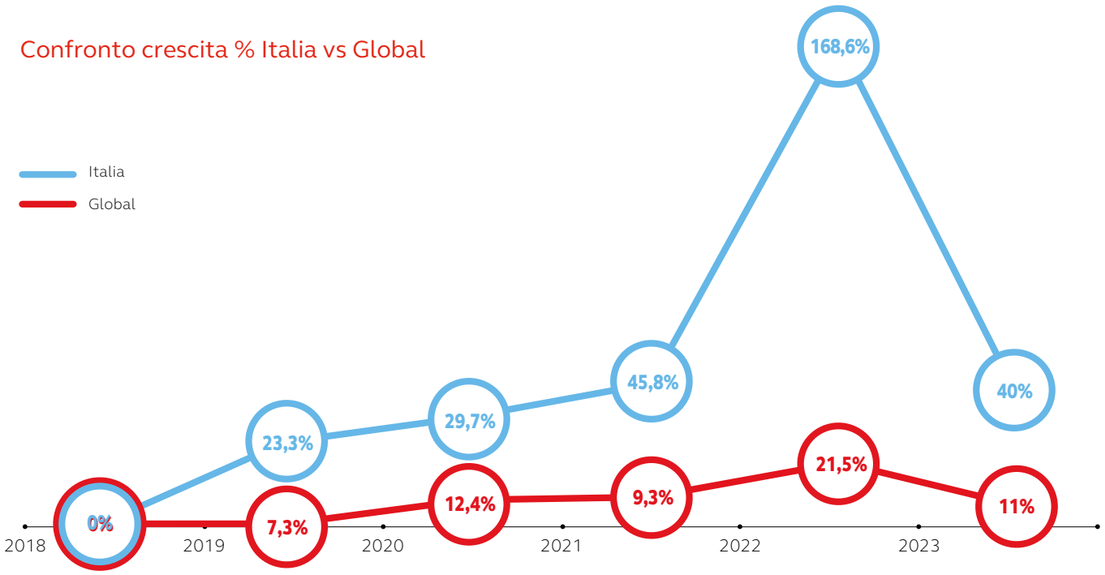
Cyber attacchi a livello globale dal 2014 fino a giugno 2023



Fonte: Rapporto Clusit 2023 - Edizione di metà anno, ottobre 2023 - pag. 12

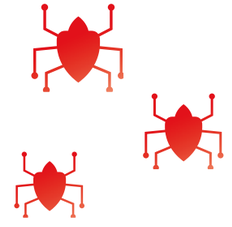
Questo tipo di incidenti, inoltre, non ha una natura comune: la maggioranza è legata a cyber attacchi isolati, mentre il resto spazia dallo spionaggio e sabotaggio aziendale all'hacktivism. Analizzando il contesto relativo all'Italia, i dati non sono confortanti: il 7,6% degli attacchi avvenuti nel 2022 a livello globale ha avuto come obiettivo un'organizzazione o un'istituzione italiana, un aumento del 168% rispetto ai dati del 2021. Purtroppo nel'83% dei casi questi eventi hanno anche causato danni concreti e significativi alle organizzazioni attaccate.

Confronto crescita % Italia vs Global



Fonte: Rapporto Clusit 2023 - Edizione di metà anno, ottobre 2023 - pag. 29

Al netto del numero di attacchi, per comprendere a fondo il fenomeno è necessario analizzare anche i settori di industria colpiti dai cyber criminali, come analizzato nel report X-Force Threat Intelligence Index.



Percentuali di attacchi per settore, 2018-2022

SETTORE	2018	2019	2020	2021	2022
Produzione manufatturiera	10%	8%	17,7%	23,2%	24,8%
Finanza e assicurazioni	19%	17%	23%	22,4%	18%
Servizi professionali, aziendali e per il consumatore	12%	19%	8,7%	12,7%	14,6%
Energia	6%	6%	11,1%	8,2%	10,7%
Commercio al dettaglio e all'ingrosso	11%	16%	10,2%	7,3%	8,7%
Istruzione	6%	8%	4%	2,8%	7,3%
Sanità	6%	3%	6,6%	5,1%	5,8%
Pubblica amministrazione	8%	8%	7,9%	2,8%	4,8%
Trasporti	13%	13%	5,1%	4%	3,8%
Media e telecomunicazioni	8%	10%	5,7%	2,50%	0,5%

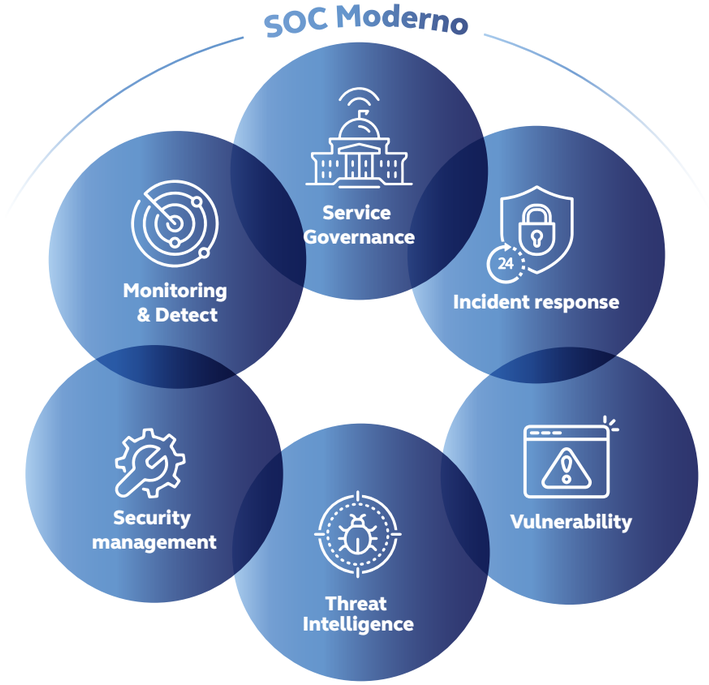
Fonte: IBM Security X-Force Threat Intelligence Index 2023 - pag. 42

In questo contesto è evidente che nessuna azienda, in qualunque settore, sia esente dai rischi cyber: per poter convivere con questa realtà, è importante per ogni organizzazione, intraprendere azioni che possano prevenire o gestire qualsiasi tentativo di attacco, con l'obiettivo di salvaguardare la continuità dei servizi offerti a clienti e cittadini e tutelando, quindi, gli interessi sia dell'azienda che della Nazione.

La centralità del Security Operations Center

Nel panorama attuale, con l'incremento esponenziale del livello di digitalizzazione delle organizzazioni anche grazie all'adozione di soluzioni in cloud e l'implementazione di nuove tecnologie, diventa sempre più importante proteggere tutte le risorse digitali di un'organizzazione: i dati, le applicazioni e più in generale i servizi accessibili dal cyber space.
Questo patrimonio è ciò che va protetto e costantemente monitorato.

Una delle modalità per riuscire in questo intento risiede nella creazione di Security Operations Center: un insieme di processi e tecnologie che può essere gestito internamente all'organizzazione o affidato ad un'azienda esterna e specializzata denominata Managed Security Service Provider (MSSP).
Per molti anni il compito principale dei Security Operations Center (SOC) è stato quello di collezionare dati, eventi e log dei sistemi, con l'obiettivo di identificare anomalie utili ad evidenziare possibili intrusioni ed attacchi. I SOC focalizzavano la loro funzione principalmente nell'attività di monitoring.
Con il progressivo incremento degli attacchi oggi un SOC moderno non può limitare la sua azione nell'attività di monitoring ma – per poter essere efficace – deve necessariamente supportare l'organizzazione nella reazione tempestiva di risposta (respond) a qualsiasi attacco o incidente.
L'azione di risposta può avvenire per mezzo del personale che opera nel SOC o anche attraverso azioni svolte da sistemi che si attivano in modo automatico, a partire dall'identificazione di specifici scenari di attacco. Queste nuove modalità di reazione, risultano molto più efficaci e consentono di contenere e isolare le minacce di cyber attacchi.
Un'ulteriore funzione del Security Operation Center, denominata Threat Intelligence, riguarda l'analisi delle minacce di cyber security. Lo studio delle tecniche di attacco usate dai cybercriminali e la conoscenza dei sistemi di azione di malware, consentono al personale che opera nel SOC di attivare meccanismi in grado di intercettare attacchi cyber e ridurre, se non scongiurare, gli impatti all'interno dell'ambiente organizzativo.
Infine un SOC moderno deve essere in grado di sensibilizzare l'organizzazione, attraverso attività di comunicazione e reporting sia nei confronti del personale ma soprattutto verso le figure apicali dell'azienda, con l'obiettivo di poterle supportare nei processi decisionali legati alla protezione degli asset aziendali.
In sintesi un SOC moderno, considerando i rapidi progressi dei processi di digitalizzazione e la complessità delle nuove tecnologie adottate dalle aziende, deve poter operare su un'elevata mole di dati: non soltanto i log di sicurezza dei sistemi digitali ma anche tutte le azioni svolte sugli asset da proteggere.
La sfida è quindi quella di riuscire ad applicare soluzioni in grado di analizzare in modalità real time un elevata quantità di dati e applicare, sulla base di scenari di attacco, regole di risposta automatizzate in grado di preservare la continuità operativa, l'integrità e la riservatezza dei dati dell'organizzazione.

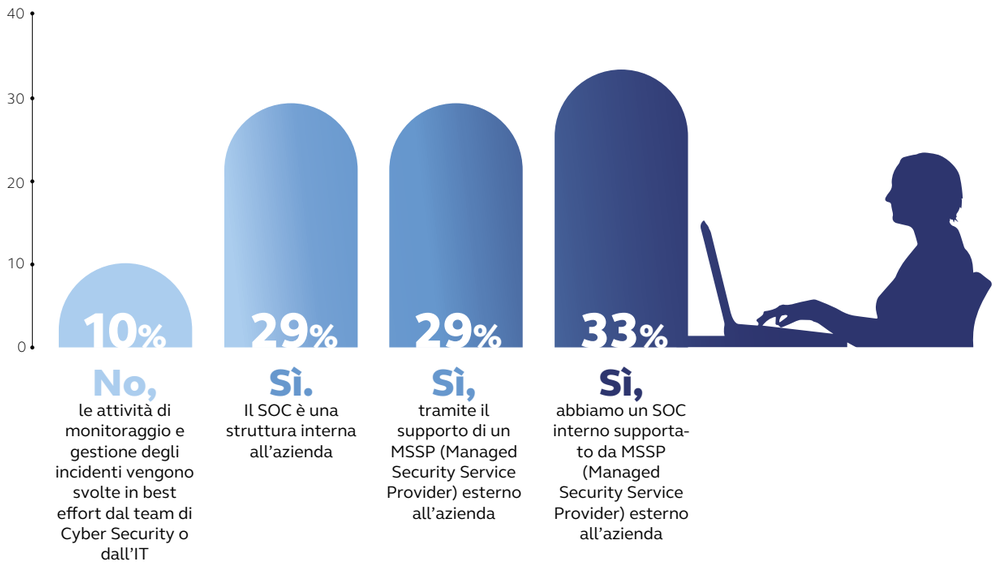


Innovare i Security Operations Center

Le sfide nel settore della cybersecurity sono in costante aumento. Per poter fronteggiare le nuove minacce provenienti dal cybercrime è necessario adottare nuovi approcci, nuove professionalità e nuove tecnologie: una delle poche certezze che non cambia in questo settore è l'importanza del fattore tempo. L'incremento dell'uso di infrastrutture cloud rende più complesse le operazioni demandate ai Security Operations Center.

La presenza di un SOC all'interno delle organizzazioni, se ieri era una scelta riservata a poche aziende, sta diventando una costante.
L'indagine condotta dall'Osservatorio BIP in collaborazione con il Centro di Eccellenza BIP CyberSec* rileva che solo il 10% delle aziende intervistate non è dotata di un SOC, ma svolge attività di monitoring e gestione di incidenti cyber in best effort.

1 La tua organizzazione è dotata di un Security Operations Center?



La complessità nel gestire i dati

La crescente difficoltà nella gestione delle soluzioni in cloud è documentata anche da Cloud Security Alliance: oltre il 50% delle aziende riconosce un grado di complessità maggiore circa la gestione della sicurezza degli ambienti cloud rispetto a infrastrutture on-premise. Uno dei motivi di tale complessità risiede nella mole di dati che è necessario raccogliere per poter intercettare anomalie e malfunzionamenti tipici delle prime fasi di un attacco. La gestione di un volume più elevato di dati comporta sia un aumento considerevole dei costi, sia una complessità operativa non sempre indirizzabile attraverso azioni manuali del personale specializzato che opera nel SOC.
Il problema legato all'ottimizzazione e gestione dei dati è presente anche nel contesto delle soluzioni di Endpoint Detection and Response (EDR), cioè le soluzioni dedicate alla rilevazione e gestione di anomalie ed attacchi su desktop, laptop, smartphone e server dell'azienda. Tutti questi device generano una quantità di dati che va processata in tempi brevi: tempi che non si conciliano con le attività di un SOC tradizionale. Quest'ultimo aspetto è correlato ad alcune questioni che di fatto rendono poco adattabile l'impostazione che sino ad ora ha caratterizzato i SOC. Ad oggi numerosi provider sono sbilanciati su una funzione piuttosto che un'altra. Ne consegue che il SOC non viene valorizzato appieno. Altro punto d'attenzione è legato alla migrazione verso il cloud delle aziende: al classico SIEM per la raccolta degli eventi di sicurezza va affiancata una soluzione tecnologica che possa tenere il passo della nuova complessità e velocità di reazione rischiesta, allo scopo di evitare dispendio di tempo prezioso che viene 'bruciato' per effettuare operazioni manuali e che invece potrebbero essere automatizzate. Ben cinque organizzazioni su dieci, pur essendo dotate di un SOC e di una serie di playbook definiti, demandano l'esecuzione manuale di questi ultimi ad analisti SOC e a strutture di supporto, 'spendendo' del tempo prezioso nella gestione degli incident. Tempo che il 19% delle organizzazioni invece 'guadagna' con azioni automatizzate sulla struttura.

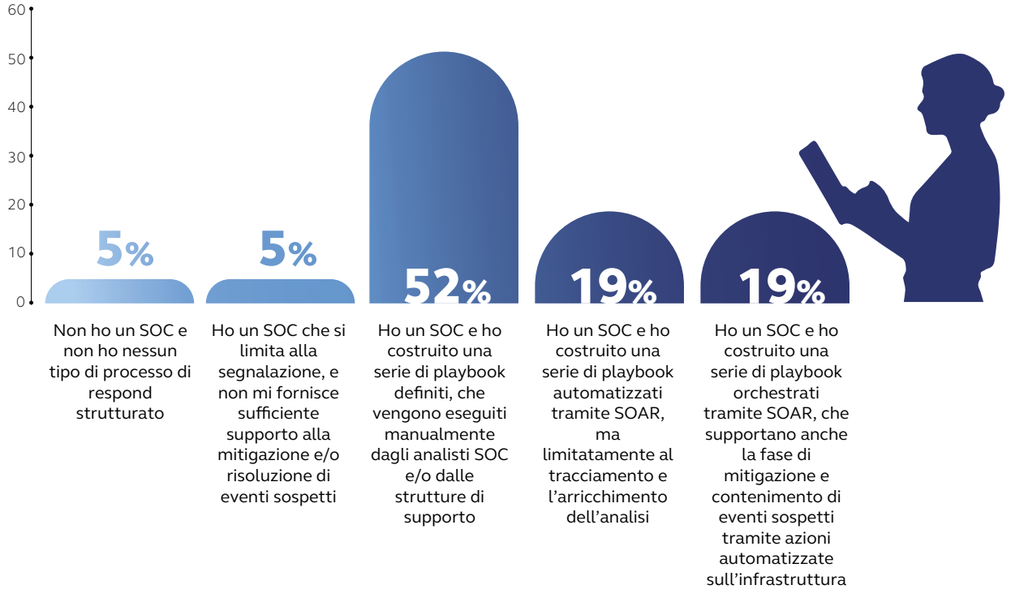
A trarre in inganno non deve essere la dimensione dell'azienda: riuscire a proteggere gli asset digitali dell'azienda è oggi una sfida che abbracciano tutte le tipologie di organizzazioni, dalla piccola impresa alla grande enterprise.
Una delle motivazioni connesse alla complessità della azione

A trarre in inganno non deve essere la dimensione dell'azienda: riuscire a proteggere gli asset digitali dell'azienda è oggi una sfida che abbracciano tutte le tipologie di organizzazioni, dalla piccola impresa alla grande enterprise.

di protezione risiede nella rivoluzione digitale avvenuta durante la pandemia: tante aziende hanno dovuto attivare in emergenza ambienti digitali per poter continuare ad operare da remoto durante il lock-down. Il tutto, senza avere il tempo di progettare le contromisure necessarie a proteggere tali infrastrutture e soluzioni digitali.
Una delle scelte che si adotta per gestire l'enorme quantità di informazioni generata dagli EDR e dalle altre soluzioni di detection è quella di omettere la raccolta di alcuni dati a favore di un set limitato e sintetico per facilitare il funzionamento dei SOC: questa scelta ha un esito in realtà negativo, in quanto rende i SOC sostanzialmente ciechi, aumentando il grado di vulnerabilità dell'azienda. Le criticità non sono relative solo alle organizzazioni che gestiscono internamente il proprio SOC: altre problematiche, di natura lievemente differente, si estendono anche a chi ne demanda a terze parti la gestione.
In un'indagine condotta da IDG Connect risulta che il 51% delle aziende ritiene che il proprio SOC (sia esso interno o affidato ad un MSSP), non garantisce il grado di sicurezza richiesto.

In riferimento al processo di respond di eventi sospetti quali di queste affermazioni si applicano al tuo SOC:

2



In riferimento al processo di respond di eventi sospetti quali di queste affermazioni si applicano al tuo SOC:

3

Gli eventi sospetti sono valutati soltanto rispetto alle vulnerabilità tecnologiche e non in base al potenziale impatto sul business

I processi e gli strumenti a supporto permettono al SOC di contestualizzare l'evento sospetto e gestirne la priorità in funzione del potenziale impatto sul business

Una delle ragioni di questa insoddisfazione riguarda la modalità con cui molti provider operano. Numerosi MSSP lavorano in modo tradizionale, impiegando team di esperti e soluzioni di raccolta e monitoraggio degli eventi di sicurezza (SIEM) che agiscono attraverso azioni manuali.
Al classico SIEM per la raccolta degli eventi di sicurezza andrebbe invece affiancata una soluzione tecnologica di automazione, basata anche su algoritmi di intelligenza artificiale, che possa tenere il passo della nuova complessità e velocità di reazione richiesta. Anche per evitare che analisti esperti impieghino il loro tempo prezioso nell'effettuare operazioni manuali e ripetitive.

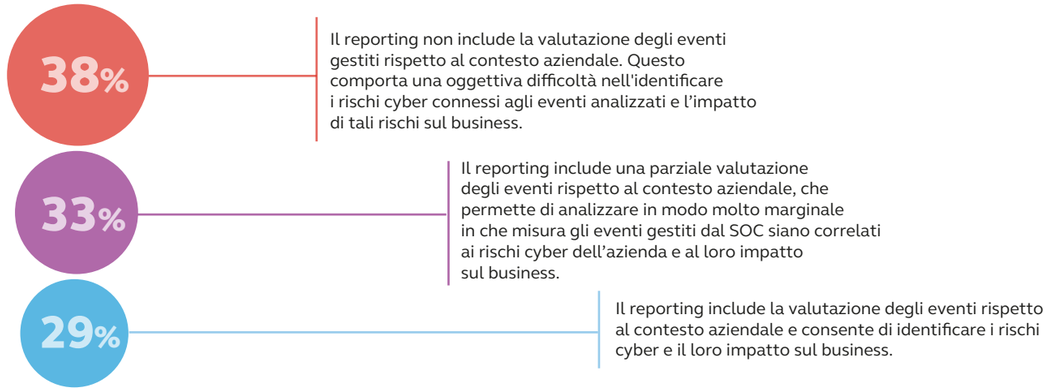
Dalla nostra analisi emerge che 5 organizzazioni su 10, pur essendo dotate di un SOC e di una serie di azioni di risposta (playbook) definite, demandano l'esecuzione manuale di queste azioni ad analisti SOC o a un MSSP esterno. Soltanto il 19% delle organizzazioni riesce a impiegare soluzioni di automazione di nuova generazione. In questi casi, gli analisti possono dedicare il proprio tempo, prima impiegato in azioni manuali, ad attività di intelligence e di threat hunting: operazioni che consentono all'organizzazione di poter prevedere, con meno incognite, un potenziale evento dannoso.

Un'altra importante attività, delegata al personale che opera all'interno dei SOC, riguarda la contestualizzazione degli eventi di sicurezza sulla base del loro impatto sull'azienda.

Il 57%
delle organizzazioni riesce infatti a gestire gli eventi in base all'impatto sul business e non esclusivamente in base alla vulnerabilità tecnologica.

In riferimento alla fase di reporting effettuata dal team che gestisce il SOC, quali di queste affermazioni si applicano al tuo contesto:

4



Un attacco cyber può colpire infrastrutture digitali poco rilevanti rispetto al business dell'organizzazione. O al contrario, può mettere a repentaglio la sopravvivenza della azienda stessa se colpisce processi, asset o sistemi fondamentali per garantirne la corretta funzionalità operativa. Ci riferiamo, ad esempio, ad attacchi che potrebbero colpire sistemi industriali, compromettendo la catena produttiva di una azienda manifatturiera. In questo caso, il danno non sarebbe soltanto economico ma reputazionale con gravi conseguenze su entrambi i fronti.
Analizzare gli impatti sul business dell'organizzazione durante le fasi di detection dell'attacco, è quindi fondamentale per attribuire la corretta priorità di intervento e delle azioni di escalation.
Il 57% delle organizzazioni intervistate nella nostra survey adotta questo metodo e afferma di riuscire a gestire gli eventi in base all'impatto sul business e non esclusivamente in base alla valutazione della minaccia tecnologica.

La correlazione tra episodio critico e impatto sul business emerge anche al momento del reporting: sviluppando in modo più efficace la reportistica, è possibile avere un quadro più aderente alle necessità del business e non solo meramente legato agli aspetti tecnologici. A cogliere questa sfida, però, sono solo 4 organizzazioni su 10, le quali producono report e analisi facendo emergere gli effetti sul business degli eventi critici.

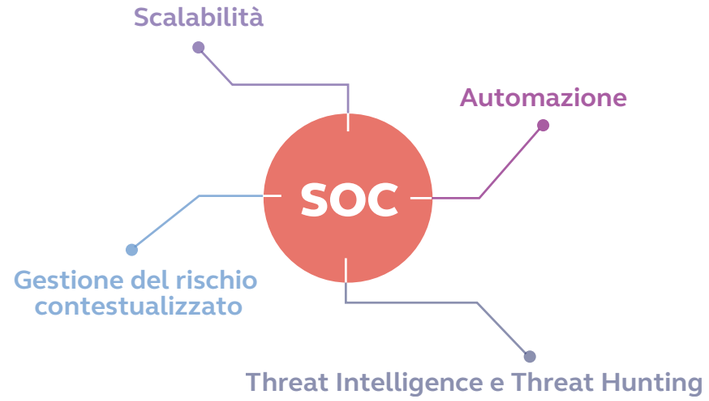
Un SOC connesso con il business

Per poter costruire un SOC moderno, è opportuno ricorrere ad una soluzione composta da un SIEM in cloud, che garantisce agilità nella raccolta e nel monitoraggio di una grande mole di eventi di sicurezza.

Alla scalabilità del SIEM in cloud va affiancata l'automazione dei processi di risposta garantita dai sistemi SOAR, i quali permettono al personale specializzato del SOC di concentrarsi solo in azioni di threat intelligence e threat-hunting, andando quindi a migliorare le caratteristiche di prevenzione e mitigazione necessarie per proteggere l'organizzazione.
La riduzione delle azioni manuali a vantaggio di quelle automatizzate consente quindi di valorizzare il ruolo del personale che opera all'interno del SOC: professionisti che conoscono la tecnologia, il panorama globale delle minacce cyber e il contesto di business in cui operano.

In conclusione, l'aderenza tra il business e gli aspetti di sicurezza si rivela centrale per poter interpretare al meglio gli eventi nel momento stesso in cui accadono e le ripercussioni che gli stessi hanno nel breve e nel lungo termine.

Automazione, scalabilità, ricerca, expertise, contestualizzazione dei rischi: sono le caratteristiche fondamentali su cui costruire processi e sistemi di sicurezza moderni, come i Security Operations Center.



In conclusione, l'aderenza tra il business e gli aspetti di sicurezza si rivela centrale per poter interpretare al meglio gli eventi nel momento stesso in cui accadono e le ripercussioni che gli stessi hanno nel breve e nel lungo termine.

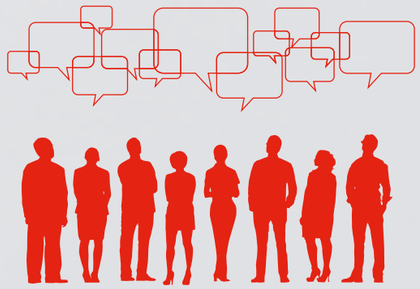
*Nota Metodologica

L'indagine è stata condotta dall'Osservatorio BIP Content Factory in collaborazione con il Centro di Eccellenza Bip CyberSec. Lo studio verte sull'organizzazione, sui processi e sulle tecnologie del Security Operations (SOC) nelle aziende e in particolar modo le capacità di identificare e rispondere in modo rapido ed efficace agli attacchi informatici che l'organizzazione potrebbe subire.

Il questionario è stato compilato da organizzazioni operati nei settori Energy, Transport, Banking, IT, Mercato Finanziario, Telecomunicazioni, PA, Manifacturing, Media & Entertainment. Il documento è stato distribuito in forma digitale, garantendo l'anonimato degli output.

I risultati sono stati sintetizzati su base percentuale, assumendo come denominatore il numero complessivo dei rispondenti. Il denominatore è mutato solo in alcuni casi e di conseguenza le percentuali sono state ricavate tramite calcolo ponderato.

Nello specifico tale casistica è occorsa in quesiti in cui era opportuno analizzare l'incidenza di eventi data una specifica condizione evidenziata nel corso del questionario.



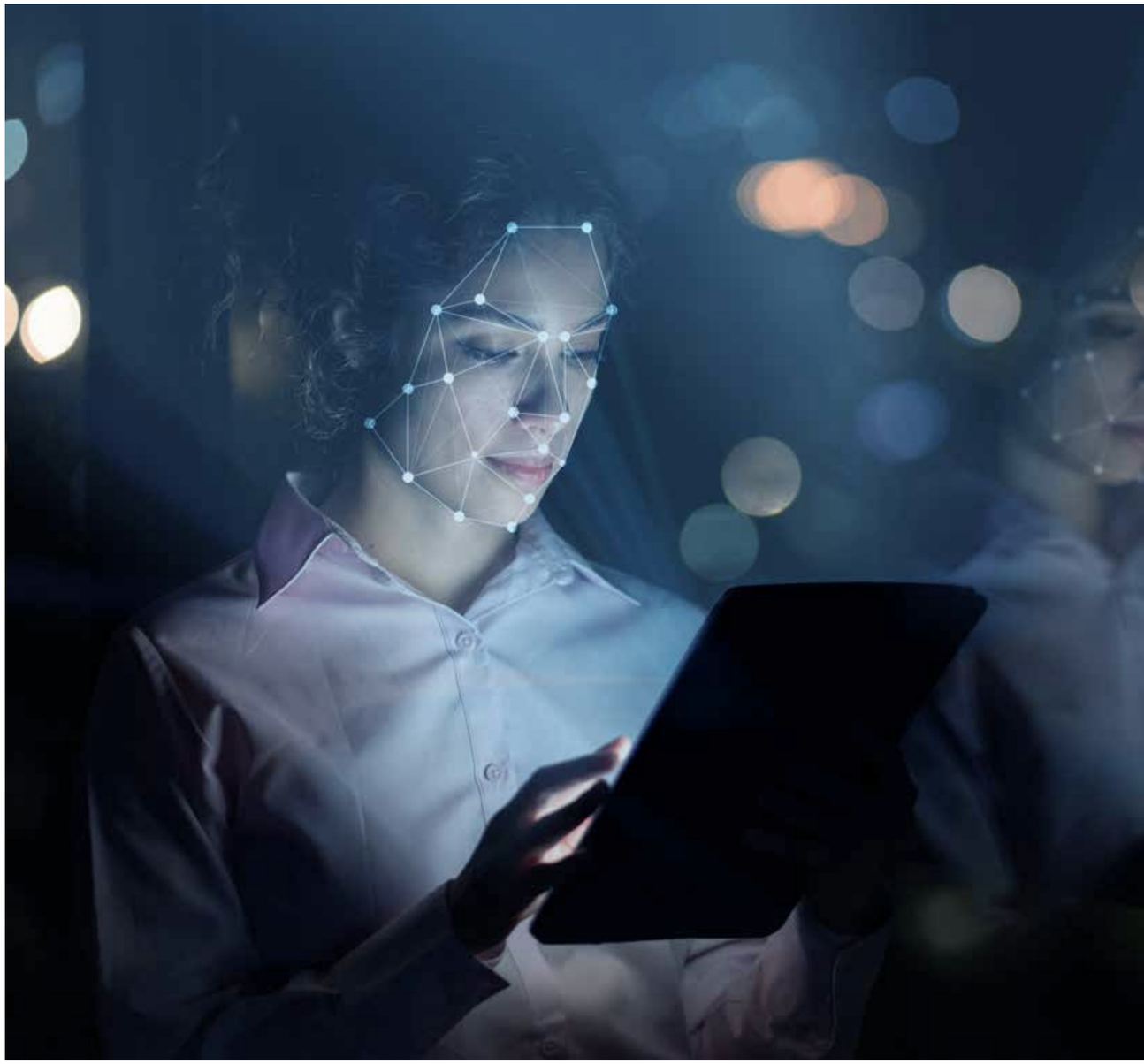
Takeaway

Il tema della cybersicurezza non va contemplato come un costo o un mero adempimento alle normative. Si tratta invece di un'opportunità per le organizzazioni in termini di vantaggio competitivo. Il vantaggio competitivo si compone della rinnovata e rafforzata resilienza informatica derivante da una strategia di cybersicurezza solida e al passo con il panorama tecnologico esistente.

La resilienza informatica ha una ricaduta sulla business continuity: evitare il verificarsi degli attacchi è qualcosa di pressoché impossibile, ma saperli gestire in tempi rapidi ed essere adattivi nei confronti delle minacce cyber è un elemento che costituisce vantaggio e preserva le attività in corso.

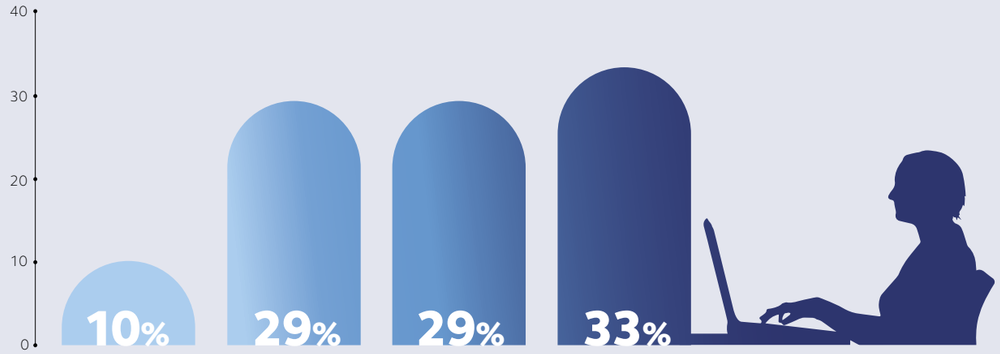
Tale vantaggio può diventare concreto solo gestendo il fattore tempo in maniera ottimale, approntando metodologie e protocolli che vengono prodotti di pari passo all'aggiornamento tecnologico costante.

A questa sfida le organizzazioni possono rispondere con la costituzione di un SOC moderno, il quale combina un SIEM scalabile con relativi vantaggi in termini di costi e tempi, un SOAR che automatizzi i processi di risposta agli eventi e un team che ha il suo principale punto di forza nella capacità di integrazione e interpretazione tra quanto accade sul versante tecnologico interno ed esterno al contesto aziendale e per contestualizzarne gli impatti di sul business e sull'organizzazione. Ciò, in sintesi, è un SOC moderno che non solo si auto-alimenta ma produce valore tangibile per il top management e per tutti i gradi dell'organizzazione.



Addendum

1 La tua organizzazione è dotata di un Security Operations Center?



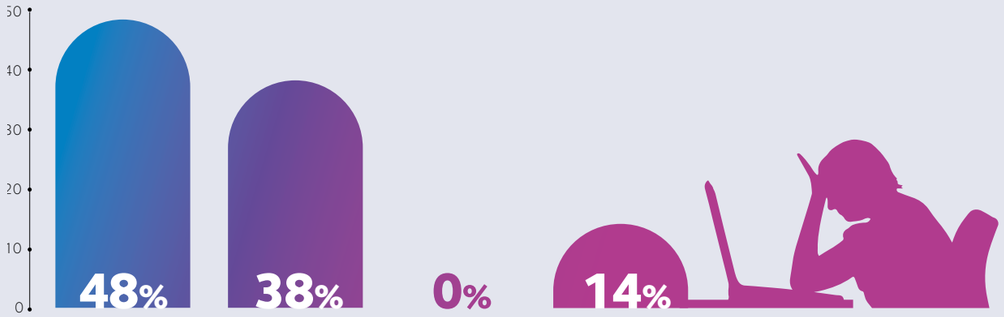
No, le attività di monitoraggio e gestione degli incidenti vengono svolte in best effort dal team di Cyber Security o dall'IT

Sì. Il SOC è una struttura interna all'azienda

Sì, tramite il supporto di un MSSP (Managed Security Service Provider) esterno all'azienda

Sì, abbiamo un SOC interno supportato da MSSP (Managed Security Service Provider) esterno all'azienda

2 Nel corso degli ultimi 18 mesi hai subito incidenti di sicurezza di una certa gravità?



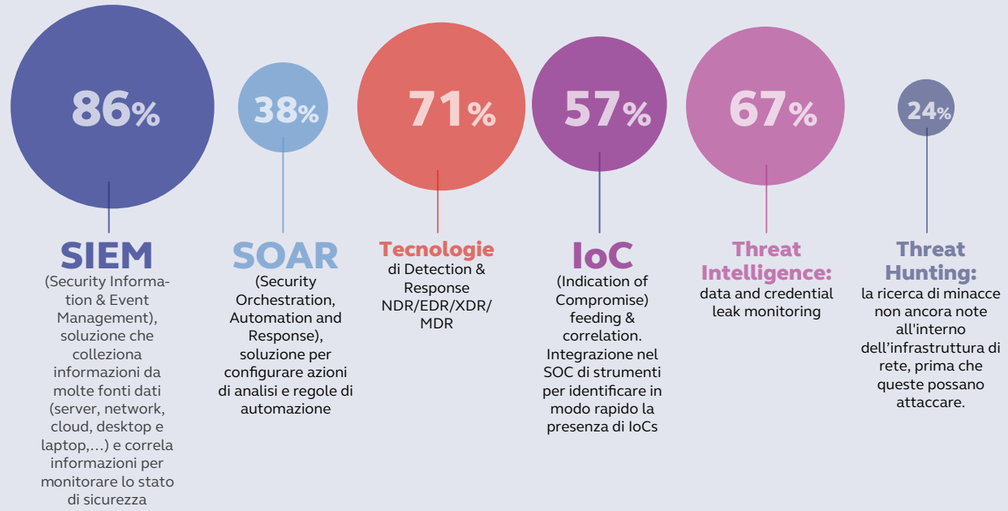
No

Sì, ma il SOC è stato in grado di identificare per tempo l'evento e minimizzarne gli impatti

Sì, l'evento non è stato identificato dal SOC e/o segnalato con ritardo e non abbiamo avuto quindi modo di contenere gli impatti

Sì, purtroppo l'evento è stato intercettato ma non gestito in maniera opportuna

3 Indicare quali di queste soluzioni e/o servizi sono componenti del servizio



SIEM (Security Information & Event Management), soluzione che colleziona informazioni da molte fonti dati (server, network, cloud, desktop e laptop,...) e correla informazioni per monitorare lo stato di sicurezza

SOAR (Security Orchestration, Automation and Response), soluzione per configurare azioni di analisi e regole di automazione

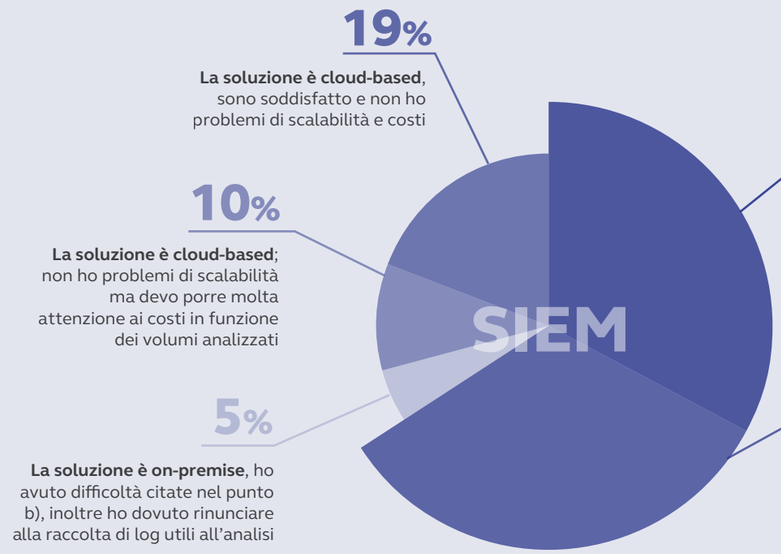
Tecnologie di Detection & Response NDR/EDR/XDR/MDR

IoC (Indication of Compromise) feeding & correlation. Integrazione nel SOC di strumenti per identificare in modo rapido la presenza di IoCs

Threat Intelligence: data and credential leak monitoring

Threat Hunting: la ricerca di minacce non ancora note all'interno dell'infrastruttura di rete, prima che queste possano attaccare.

4 In riferimento alla soluzione SIEM indicare quali di queste affermazioni si applica al tuo contesto:



19% **La soluzione è cloud-based**, sono soddisfatto e non ho problemi di scalabilità e costi

10% **La soluzione è cloud-based**; non ho problemi di scalabilità ma devo porre molta attenzione ai costi in funzione dei volumi analizzati

5% **La soluzione è on-premise**, ho avuto difficoltà citate nel punto b), inoltre ho dovuto rinunciare alla raccolta di log utili all'analisi

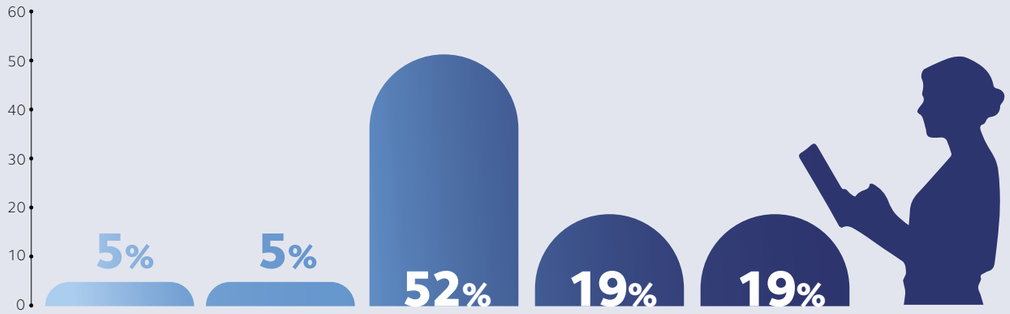
33% **La soluzione è on-premise** e sono pienamente soddisfatto della scelta e delle prestazioni

33% **La soluzione è on-premise**, ma ho vissuto difficoltà legate alla scalabilità del sistema al crescere dei volumi monitorati, anche da un punto di vista economico (allocazione risorse e/o costi di licenza della soluzione)

Addendum

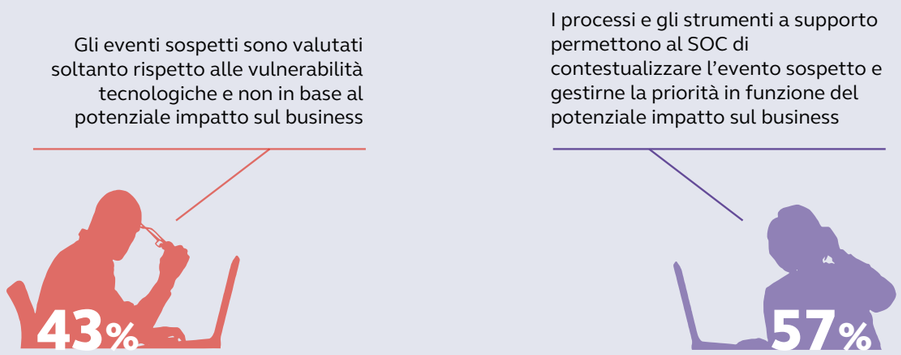
In riferimento al processo di respond di eventi sospetti quali di queste affermazioni si applicano al tuo SOC:

5



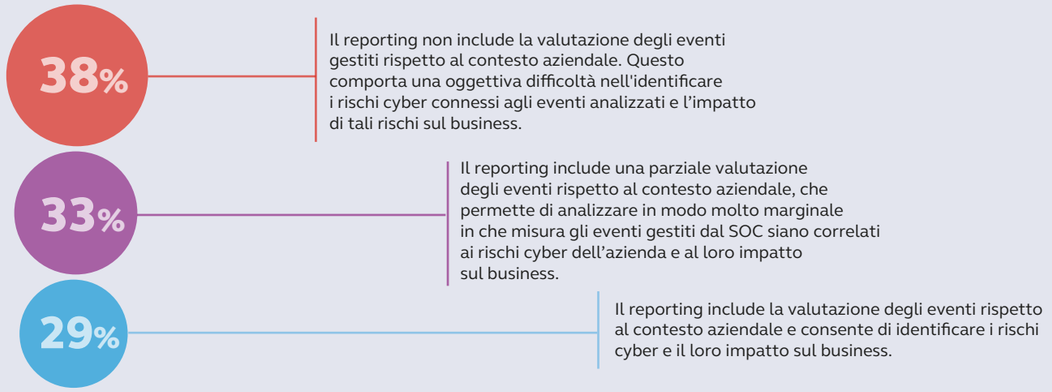
In riferimento al processo di respond di eventi sospetti quali di queste affermazioni si applicano al tuo SOC:

6



In riferimento alla fase di reporting effettuata dal team che gestisce il SOC, quali di queste affermazioni si applicano al tuo contesto:

7



BIP CyberSec è il Centro di Eccellenza di BIP Group specializzato in cybersecurity. Il viaggio di CyberSec inizia nel 2013, da un team di professionisti senior all'avanguardia che desiderano costruire una realtà in grado di avere un impatto reale nella gestione e nella protezione dei rischi informatici, anticipando quanto la sicurezza informatica sarebbe presto diventata un problema fondamentale per le aziende di tutto il mondo.

Oggi, CyberSec è un centro di eccellenza globale: oltre 350 professionisti altamente qualificati che operano in diversi settori (Telco, Energy & Utilities, Finance, Manufacturing, Pubbliche Amministrazioni) in più di 13 paesi (tra i quali Italia, Spagna, UK, USA, Brasile, Colombia, UAE) occupandosi di Strategia per la Sicurezza, Gestione del Rischio, identificazione e implementazione di soluzioni innovative di cybersecurity, Cyber Defense e Security Operations.

Abbiamo nel nostro portfolio 3 prodotti proprietari che seguono diversi obiettivi: l'analisi del rischio con Cyber Risk DIVE, la compliance in tema di data protection e privacy per aziende pubbliche e private con Privacy DIVE e la difesa degli asset critici nel settore industriale con xDefense.

Nel 2023 abbiamo inoltre dato vita al Re@ck Security Center, il Security Operation Center 24x7 adaptive, agile & automated per la gestione delle minacce informatiche.

AUTORI

Centro di Eccellenza
BIP CyberSec

Team Creative & Production BIP

HERE TO DARE

Bip è la società di consulenza
internazionale del XXI secolo.
Liberi da un retaggio tecnologico
che ci avrebbe costretto
ad imporre prodotti complessi
e competenze di cui nessuno
ha più bisogno.
Liberi da una tradizione
professionale abituata a separare
la strategia dall'esecuzione.
Liberi da un modello culturale
che chiedeva di fare di più e più
a lungo, mentre noi vogliamo
fare meglio e prima.
Liberi di osare