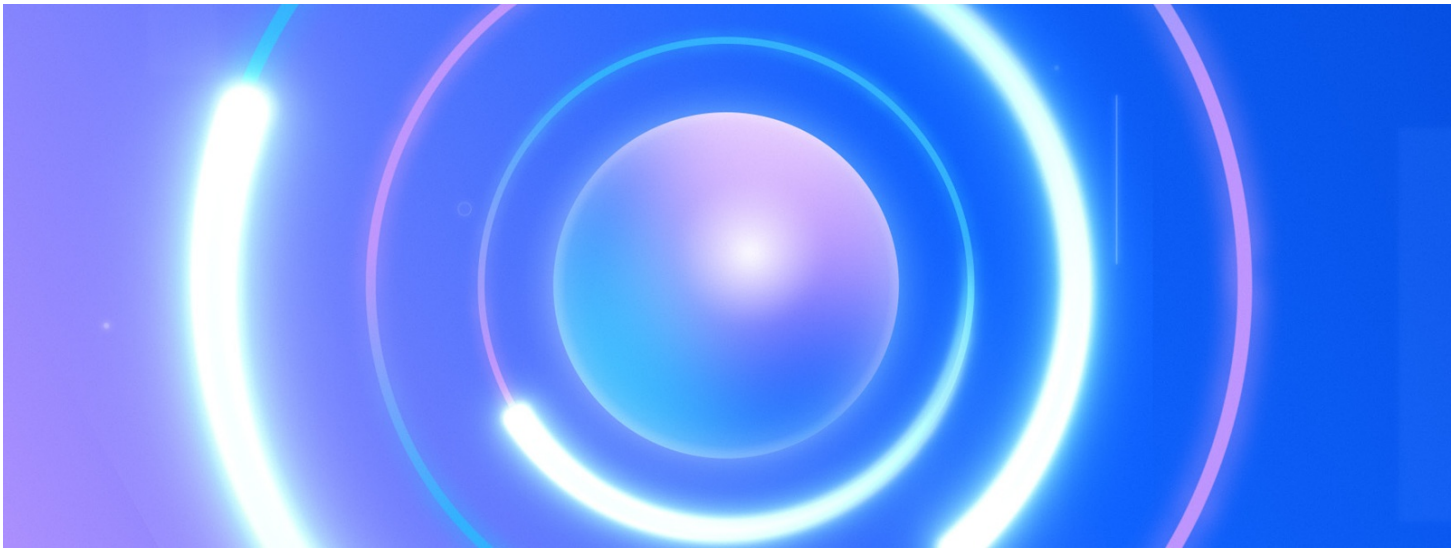
Comunicati stampa

# Nuovo studio IBM rileva che nella cybersecurity gli addetti alle attività di Incident Response hanno uno spiccato senso del dovere

**Il 77% degli intervistati afferma di aver intrapreso questa professione per senso di protezione verso gli altri**

**L'81% dichiara di dedicare la maggior parte delle proprie energie nella gestione degli attacchi ransomware**



**CAMBRIDGE, Mass.,3 ottobre 2022** - IBM Security ha annunciato i risultati di un sondaggio globale che esamina il ruolo critico degli addetti alla risposta agli incidenti di sicurezza informatica in un momento in cui il mondo fisico e digitale convergono sempre di più. Lo studio, pubblicato durante il National Cybersecurity Awareness Month, ha rilevato che i *cyber responder* intervistati, cioè gli addetti chiamati a fronteggiare in prima linea gli attacchi informatici, sono principalmente mossi da un forte senso del dovere nel proteggere gli altri; una responsabilità che è sempre più messa in discussione dall'aumento di attacchi distruttivi, dalla proliferazione di attacchi ransomware alla recente ascesa di wiper malware.

Le organizzazioni essenziali per l'economia globale, come quelle che operano nelle supply chain e nella logistica, sono diventate gli obiettivi primari dei più recenti e famosi attacchi. Nel 2021 IBM Security X-Force ha rilevato che gli attacchi informatici contro aziende energetiche sono quadruplicati rispetto all'anno precedente, mentre le imprese manifatturiere hanno riscontrato più attacchi ransomware di qualsiasi altro settore. Poiché gli attacchi informatici minacciano i servizi essenziali per le nostre esigenze quotidiane, gli addetti alle attività di Incident Response in questi settori devono far fronte a una maggiore pressione per difendere il fronte digitale. Infatti, l'81% degli intervistati ha dichiarato che l'aumento del ransomware ha esacerbato le energie psicologiche associate agli incidenti di sicurezza informatica.

Lo studio globale, sponsorizzato da IBM Security e condotto in 10 mercati da Morning Consult, ha riguardato 1.100 cyber responder. I risultati rivelano le tendenze e le sfide che gli addetti all'Incident Response devono affrontare a causa del loro tipo di professione. Alcuni punti salienti sono:

- **Il senso del servizio -** Oltre un terzo degli addetti alla risposta agli incidenti è stato spinto dal senso di responsabilità nel proteggere e aiutare gli altri e le aziende. Per quasi l'80% degli intervistati, questo è stato uno dei motivi principali che li ha attratti verso l'IR.

- **Combattere su più fronti -** Con il crescere degli attacchi informatici negli ultimi anni, il 68% degli intervistati ha affermato che è piuttosto frequente essere incaricati di rispondere a due o più incidenti contemporaneamente.

- **Impatto sulla vita quotidiana –** L'elevato impegno richiesto a chi si occupa di sicurezza informatica influisce anche sulla vita personale dei cyber responder, con il 67% che sperimenta stress o ansia nella propria vita quotidiana. L'insonnia, il burnout e l'impatto sulla vita sociale o sulle relazioni sono gli effetti citati dagli intervistati. Nonostante queste difficoltà, la stragrande maggioranza ha riconosciuto di disporre di un solido sistema di sostegno.

**Un campo di battaglia squilibrato**

Negli ultimi anni, non solo gli attacchi informatici sono diventati più dirompenti, ma il loro volume è aumentato. X-Force ha osservato un aumento di quasi il 25% nel numero di incidenti di sicurezza informatica in cui i team di IR sono stati impegnati dal 2020 al 2021. Inoltre, la ricerca di Check Point Software Technologies indica nel 2021 un aumento del 50% negli attacchi di rete settimanali rispetto al 2020. Mentre il settore è chiamato a rispondere a un crescente numero di attacchi informatici, il numero di professionisti della sicurezza specificamente formati e qualificati per rispondere agli incidenti informatici è purtroppo limitato.

Di conseguenza, mentre molti team di IR sono costretti a gestire più fronti di attacco, alcune aziende potrebbero non avere le risorse necessarie per mitigare e recuperare dagli attacchi. Lo studio IBM ha rilevato che il 68% degli intervistati ritiene che capiti comunemente di rispondere simultaneamente a due o più incidenti di sicurezza informatica. Tra gli intervistati, il 34% ha dichiarato che la durata media di un impegno IR è stata di 4-6 settimane, mentre un quarto ha citato la prima settimana come il periodo di coinvolgimento più stressante o impegnativo. Durante questo periodo circa un terzo degli intervistati lavora in media più di 12 ore al giorno.

**Istituzione di un solido sistema di supporto**

Poiché gli addetti alla risposta agli incidenti si fanno carico della pressione e di un elevato numero di richieste associate alla risposta informatica, la stragrande maggioranza degli intervistati ha riconosciuto di disporre di un solido sistema di supporto. In particolare, la maggior parte ritiene che il loro management abbia una forte comprensione delle attività che l'IR comporta e il 95% afferma di ricevere dai propri manager la struttura di supporto necessaria per avere successo. L'84% afferma di avere un

accesso adeguato alle risorse di supporto necessarie, con molti intervistati (64%) che cercano assistenza psicologica a supporto per la salute mentale a causa della natura impegnativa dell'IR.

Le aziende possono supportare ulteriormente gli addetti alla risposta agli incidenti, siano essi Blue Team interni o i team IR esterni coinvolti in caso di crisi informatica, dando priorità alla preparazione informatica e creando piani e playbook personalizzati in base al loro ambiente e alle loro risorse. Questo può consentire di fornire una risposta più agile e rapida nei primi momenti di un incidente e ad alleviare la pressione sull'azienda.

A tal fine, è importante conoscere la postura di sicurezza della propria infrastruttura. Le aziende possono effettuare dei test per comprendere il proprio stato di preparazione tramite esercizi di simulazione, non solo per avere un'idea di come i propri team reagiranno sotto attacco, ma per favorire l'integrazione  e la comunicazione tra i diversi team coinvolti durante un incidente informatico.

Risorse aggiuntive

- Lo studio completo di IBM Security sugli Incident Responder.
- Il blog di Security Intelligence sugli addetti alla risposta agli incidenti che difendono il fronte digitale
- Per iscriversi al webinar sulla risposta agli incidenti di IBM Security X-Force, "Tales from the Digital Frontlines", che si terrà mercoledì 12 ottobre alle 13:00 ET, utilizza questo link
- Partecipa all'evento "Technology in action: Let's innovate Threat Management with Ecosystem" che si terrà il 13 ottobre presso IBM Studios Milano e in livestreaming, che tratterà la gestione dell'intero ciclo di vita delle minacce, dalla threat intelligence al rilevamento, fino alla risposta all'incidente e al ripristino dell'operatività. Questo il link per l'iscrizione.

**Informazioni su IBM Security**

IBM Security offre uno dei portfolio di prodotti e servizi per la sicurezza aziendale tra i più avanzati e integrati del mercato. Il portfolio, supportato dalla ricerca di IBM Security X-Force®, consente alle aziende di gestire in modo efficiente i rischi e di difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni e servizi di sicurezza più grandi del mondo, monitora oltre 150 miliardi di eventi al giorno in più di 130 paesi e ha ottenuto più di 10.000 brevetti di cybersecurity in tutto il mondo. Per ulteriori informazioni, consulta www.ibm.com/security, segui @IBMSecurity su Twitter o visita il blog IBM Security Intelligence.

Per maggiori informazioni:
**Claudia Ruffini**, *IBM Communications Leader, Italia*
email: cla@it.ibm.com.
tel. : +39 335 6325093