Guida Sulle Competenze di Cybersecurity di Insight

Insight

Introduzione

La sicurezza informatica è più importante che mai per aziende di tutte le dimensioni, in quanto la frequenza e la sofisticatezza delle minacce informatiche aumentano. Le violazioni dI sicurezza informatica possono avere conseguenze devastanti, tra cui perdite finanziarie, responsabilità legali, danni reputazionali per il brand e perdita di fiducia da parte dei clienti.

Proteggere la tua azienda dalle minacce informatiche non è solo una questione di conformità o una buona prassi; è essenziale per proteggere le tue operazioni e garantire la continutià del business. Investire in solide misure di sicurezza informatica è un investimento nella resilienza e nel successo futuro della tua azienda. Implementando strategie di sicurezza informatica efficaci, è possibile mitigare i rischi, rilevare e rispondere tempestivamente alle minacce e costruire una solida difesa contro gli attacchi informatici.

La sicurezza informatica non è solo una necessità; è un imperativo strategico per le aziende che cercano di prosperare in un ambiente sicuro e resiliente.

Noi di Insight comprendiamo la necessità di un approccio completo alla sicurezza.

L'approccio di Insight alla sicurezza informatica

La sicurezza informatica è complicata e richiede un approccio "all-hands-on-deck" da parte degli utenti finali, dei team di sicurezza e dello strumento. Ecco perché adottiamo un approccio olistico alla cybersecurity, sia in ambito tecnologico che in ambito di integrazione, attraverso metodi ripetibili e processi collaudati che producono risultati positivi. I nostri esperti ti guideranno dall'inizio alla fine, migliorando l'efficienza, l'efficacia e l'allineamento strategico.

Il modello olistico di Insight

L'approccio di Insight alla sicurezza informatica

Disponiamo di competenze tecniche complete nelle seguenti cinque aree tecnologiche:

- Endpoint
- Applicazioni
- Cloud
- Reti, Datacenter e IoT
- Data-Centric

ma, in qualità di leading solution integrator, sappiamo che l'eccellenza tecnica in questi settori non è sufficiente. La sicurezza deve essere affrontata in modo olistico, assicurando che tutti gli ambiti della sicurezza siano integrati e coordinati. Ciò avviene tramite l'applicazione di:

- Governance e compliance
- Identità e accessi
- Rilevamento e risposta alle minacce
- Fattori umani

Le falle di collegamento tra i vari ambiti delle tecnologie spesso sono caratterizzate da un valore aggiunto, che contribuisce a migliorare il livello complessivo di protezione in maniera economicamente vantaggiosa.

Possiamo aiutarti a:

- Migliorare la cybersecurity
- Identificare e mitigare i rischi
- Ridurre la complessità minimizzando le sovrapposizioni.
- Ottimizzare le operazioni di sicurezza
- Assicurare che i controlli di sicurezza apportino valore aggiunto e migliorino il ritorno sulle spese.

I pilastri della tecnologia

Endpoint

Sono finiti i giorni in cui in un'azienda si utilizzava un solo dispositivo per utente; è più che probabile che i dipendenti utilizzino più dispositivi. Gli endpoint svolgono un ruolo fondamentale nella sicurezza informatica per le organizzazioni, poiché possono risultare punti di ingresso per minacce e vulnerabilità informatiche. Le sfide legate alla protezione degli endpoint sono cresciute a causa della proliferazione dei dispositivi, degli ambienti di lavoro da remoto e della crescente sofisticatezza degli attacchi informatici che prendono di mira gli endpoint.

Le sfide più comuni includono: visibilità degli endpoint, gestione delle vulnerabilità, protezione dei dati e controllo delle applicazioni.

Questi dispositivi devono essere gestiti, il loro stato di sicurezza monitorato e aggiornato e le difese per bloccare malware ed exploit devono essere distribuite e mantenute. Le nostre Endpoint Security Solutions si concentrano sul processo di protezione di endpoint quali notebook, desktop, server e dispositivi mobile utilizzati per accedere alle reti e ai dati dell'azienda.

Possiamo aiutarti a:

- Ottieni visibilità sull'intero ambiente endpoint, a livello di dispositivo e applicazione.
- Rileva e rispondi alle minacce informatiche in tempo reale.
- Proteggi i dati sensibili sui dispositivi dall'accesso non autorizzato.
- Prevenzione delle infezioni da malware e degli attacchi informatici agli endpoint.
- Ottieni visibilità sulle attività degli endpoint per un monitoraggio efficace.
- Dispositivi sicuri per ambienti di lavoro remoti.

Applicazioni

Con le minacce informatiche in continua evoluzione, le organizzazioni devono affrontare sfide significative. Ciò è ulteriormente aggravato dal fatto che la complessità delle applicazioni moderne sta aumentando sempre più, con numerose componenti interconnesse e integrazioni di terze parti, con conseguente superficie di attacco sempre più ampia. Gli hacker e i malintenzionati sono alla continua ricerca di nuove tecniche per sfruttare le vulnerabilità delle applicazioni.

Tutte le organizzazioni utilizzano applicazioni che richiedono patch per rimanere al passo con le vulnerabilità, sia sugli endpoint degli utenti che sull'infrastruttura dei server. Molte organizzazioni creeranno anche le proprie applicazioni tramite low/no code o tramite sviluppo tradizionale o DevOps. L'integrazione di sicurezza e privacy "by design" nel ciclo di vita dello sviluppo software è fondamentale per queste organizzazioni.

In Insight, il nostro team esperto di security advisor può aiutarti a ridurre i rischi legati alle tue applicazioni. Ti aiuteremo a rimanere aggiornato con la gestione delle vulnerabilità e delle patch per le tue applicazioni standard, oltre a fornire penetration test per qualsiasi applicazione web creata internamente.

ffidatevi a Insight per affrontare in modo diretto le problematiche legate alla protezione delle applicazioni, assicurandoti una protezione efficace e la massima tranquillità.

Possiamo aiutarti a:

- Gestire il tuo parco applicazioni per rimanere al passo con il ciclo delle vulnerabilità e delle patch.
- Integrare i controlli di sicurezza nei tuoi processi DevOps senza compromettere la velocità di sviluppo.
- Rilevare e correggere le minacce, riducendo i costi di gestione.

Cloud

Il cloud computing offre una scalabilità e un'efficacia senza eguali, ma presenta anche notevoli problematiche di sicurezza informatica. Le aziende hanno la necessità di proteggere i propri dati sensibili da accessi non autorizzati, violazioni e falle, nel pieno rispetto dei regolamenti e salvaguardando l'immagine aziendale.

È necessario adottare un approccio proattivo e basato sul rischio, collaborando con i provider di servizi cloud per stabilire un framework di protezione solido.

Gli esperti in cloud e security di Insight hanno anni di esperienza nella creazione, protezione e gestione di ambienti multicloud per organizzazioni di qualsiasi dimensione e complessità. Ti aiuteremo a strutturare un framework di sicurezza completo con monitoraggio proattivo, in modo che tu possa concentrarti esclusivamente sul tuo business.

Possiamo aiutarti a:

- Ottienere visibilità sull'ambiente multicloud.
- Proteggere i carichi di lavoro, indipendentemente da dove vengano creati.
- Monitorare e mantenere la conformità ai framework di sicurezza.

Data center, rete e IoT

Nel mondo odierno, sempre più connesso, si assiste a una rapida espansione del panorama digitale, creando una complessa rete di tecnologie che ha aperto le porte a un aumento delle minacce informatiche, dei casi di violazione dei dati e degli accessi non autorizzati.

Al giorno d'oggi, occorre un approccio a livelli multipli per implementare le difese di sicurezza e la resilienza nelle aziende. Una combinazione di firewall, cifratura, controlli di accesso e controlli di sicurezza regolari sono solo l'inizio. È necessario essere costantemente all'avanguardia con sistemi avanzati di rilevamento delle minacce e analisi di esperti per essere proattivi nell'identificare e mitigare i potenziali rischi.

Adottiamo un approccio consulenziale per risolvere le tue sfide di sicurezza dei datacenter, delle reti e dell'IoT. Avendo una conoscenza approfondita del business, della tecnologia e della protezione, creiamo la soluzione giusta per la tua azienda, partendo dalla progettazione e pianificazione, per arrivare alla realizzazione e alla gestione dei servizi. I nostri esperti di IT security sono in grado di aiutarti ad affrontare la complessità delle tecnologie richieste per creare e gestire soluzioni di cybersecurity efficaci, riducendo al minimo le sovrapposizioni e garantendo una difesa informatica economicamente vantaggiosa.

Ti aiutiamo con:

- Maggiore visibilità su architetture ibride complesse
- Maggiore continuità operativa.
- Controlli di sicurezza che funzioneranno sia nelle reti on-premise che in quelle cloud.
- Protezione dei dati dall'origine alla destinazione.

Data-Centric

Sebbene i professionisti della sicurezza dedichino molto tempo alla protezione delle applicazioni e delle infrastrutture di molte organizzazioni, la risorsa critica che devono proteggere sono i dati. Che si tratti di informazioni sui dipendenti, ordini dei clienti, cifre di produzione o proprietà intellettuale, sono i dati che si muovono all'interno della tua azienda ad aggiungere probabilmente più valore per i tuoi clienti finali e per la tua azienda.

Un buon punto di partenza per una strategia olistica di IT security è la gestione dei dati, per cui è necessario partire da un approccio incentrato sui dati, coinvolgendo gli interlocutori commerciali, non la tecnologia.

Ci concentriamo sulla protezione dei dati stessi, anziché limitarci a proteggere i sistemi o le reti che li archiviano e li trasmettono. Ti aiutiamo a rimanere un passo avanti e a proteggere in modo efficace le risorse più preziose della tua organizzazione: i suoi dati.

Ti aiutiamo con:

- Rilevamento dei dati sensibili e obsoleti.
- Classificazione dei dati per garantire l'applicazione della giusta quantità di controllo.
- Rispetto delle norme sulla protezione dei dati.
- Verificabilità dell'utilizzo dei dati.

Domini di integrazione

Governance e compliance

Governance, rischio e conformità sono componenti essenziali della sicurezza informatica per le aziende, che comprendono policy, procedure e meccanismi per gestire i rischi di cybersecurity e garantire la conformità ai requisiti normativi come il GDPR e la NIS2. Le organizzazioni si trovano ad affrontare sfide nella creazione di strutture di governance efficaci, nell'identificazione e nella valutazione dei rischi per la sicurezza informatica e nell'implementazione di controlli robusti per mitigare le minacce.

Pratiche GRC efficaci stabiliscono ruoli chiari, semplificano i processi e mitigano i rischi informatici. Una strategia efficace consente di migliorare la propria maturità nella gestione della cybersecurity, ridurre le responsabilità legali e finanziarie, migliorare la fiducia dei tuoi clienti e rispettare la conformità alle normative. Insight si assicura che la cybersecurity supporti le esigenze dell'azienda, e non le vincoli. Utilizzare quadri di riferimento per valutare il rischio, calcolare il costo di tale rischio e determinare dove collocare i controlli per ottenere i migliori risultati, garantendo al contempo che i controlli selezionati svolgano il loro lavoro in modo efficace.

Forniamo supporto per:

- Valutazione dei rischi
- Definizione di controlli più efficaci
- Sviluppo di politiche e processi
- Consulenza di esperti integrati a tutti i livelli

- **NIS / NIS2**
- **DORA**
- **EU AI act**
- **ISO27001**
- **Cyber Essentials/+**
- **CIS18**
- **NIST CSF**
- **PCI-DSS**

Identità e accesso

La gestione delle identità e degli accessi è un aspetto cruciale della sicurezza informatica per le aziende, che comprende i processi e le tecnologie utilizzati per gestire e proteggere le identità digitali e controllare l'accesso alle risorse. Le organizzazioni devono affrontare sfide nel garantire pratiche sicure ed efficienti di gestione delle identità e degli accessi, come la gestione delle identità degli utenti su più sistemi, l'applicazione dei controlli di accesso con privilegi minimi e la prevenzione degli accessi non autorizzati.

Per essere efficaci, le aziende necessitano di una soluzione di gestione delle identità e degli accessi integrata nei loro pilastri tecnologici, per fornire una soluzione informatica solida e completa.

Il team di esperti in sicurezza informatica di Insight ti aiuta concentrandosi sull'identificazione e sulla mitigazione delle aree di rischio e poi supportandoti nella creazione di soluzioni convenienti che soddisfino i requisiti delle policy e dei processi della tua organizzazione. Con l'approccio di Insight su misura per la tua attività, otterrai maggiore sicurezza, rischi ridotti e maggiore efficienza.

Possiamo raggiungere questo obiettivo attraverso:

- Assistenza nel percorso verso l'approccio Zero Trust
- Adozione di un approccio basato sul business per quanto riguarda l'accesso a dati e applicazioni
- Garanzia che le persone giuste abbiano accesso alle tue applicazioni e ai tuoi dati.

Rilevamento e risposta alle minacce

Il rilevamento e la risposta alle minacce sono componenti fondamentali di una solida strategia di sicurezza informatica per le aziende. Le organizzazioni devono affrontare innumerevoli sfide nell'identificazione e nella mitigazione delle minacce informatiche, tra cui la natura in continua evoluzione degli attacchi, la complessità degli ambienti IT e la carenza di professionisti qualificati in sicurezza informatica. Un rilevamento efficace delle minacce richiede monitoraggio in tempo reale, analisi degli eventi di sicurezza e una rapida risposta agli incidenti per ridurre al minimo l'impatto delle violazioni della sicurezza.

Gli esperti di sicurezza di Insight possono aiutarti ad adottare un approccio multilivello alle soluzioni di rilevamento e risposta alle minacce in tutti i domini tecnologici della tua azienda.

Le nostre soluzioni si basano su strumenti e tecnologie all'avanguardia, oltre che sulle nostre competenze tecniche, per individuare e mitigare i rischi prima che possano causare seri danni alla tua azienda. Insight utilizza tecnologie quali SIEM e XDR, supportate da analisti della sicurezza, per riunire le enormi quantità di dati generati dai tuoi strumenti di sicurezza, per prendere decisioni intelligenti sulle minacce e sulle risposte nell'intera azienda.

Possiamo aiutarti con:

- Identificazione precoce delle minacce
- Riduzione dei rischi all'interno della rete
- Condivisione di informazioni utili sulle minacce
- Automazione della difesa contro le minacce

Fattori umani

Anche se le infrastrutture, gli strumenti e i controlli di sicurezza vengono costantemente migliorati e si investe in tali attività, le violazioni continuano a verificarsi e non sono facili da identificare e risolvere. Esistono molti controlli di sicurezza specializzati per diversi tipi di minacce, dagli attacchi agli endpoint agli attacchi alle supply chain, ma quando si esamina come si sono verificati questi attacchi, i tre motivi principali sono:

- **Password**
- **Phishing**
- **Patching**

I team IT possono utilizzare la tecnologia per contribuire a ridurre le possibilità di violazioni, ma gli utenti finali avranno sempre un ruolo nel supportare la sicurezza di un'organizzazione. Spesso i team IT si concentrano sulla tecnologia e talvolta sul processo, per poi dimenticare il lato umano, quando è questo a determinare il fallimento o il successo di un progetto.

Con Insight i tuoi dipendenti possono diventare una prima linea di difesa impenetrabile contro le minacce informatiche. Adottando un approccio incentrato sull'uomo, possiamo aiutarti ad affrontare le vulnerabilità direttamente, rafforzando il tuo livello di sicurezza e riducendo al minimo i rischi.

Ti aiuteremo a:

- Migliorare la consapevolezza della sicurezza informatica degli utenti finali.
- Fornire formazione agli sviluppatori su come codificare tenendo conto della sicurezza.
- Assicurarti che gli amministratori dispongano delle competenze necessarie per rilevare e rispondere a un attacco informatico.
- Ridurre i rischi di attacco.
- Risparmia sui costi evitando violazioni dei dati.

Managed Security

L'aspettativa delle sfide di sicurezza è inarrestabile, con organizzazioni che si trovano ad affrontare un aumento sempre maggiore di minacce informatiche, dai sofisticati tentativi di hacking agli attacchi di ransomware insidiosi. Le aziende devono rispettare severi requisiti normativi, proteggere i dati di natura sensibile e mantenersi un passo avanti rispetto ai rischi di sicurezza informatica in continua evoluzione. Le soluzioni di sicurezza forniscono numerosi avvisi e alert, ma sapere su quali agire con urgenza è la chiave per prevenire danni maggiori alla tua azienda.

La combinazione di queste sfide crea la necessità di fornire soluzioni di sicurezza informatica complete e proattive per proteggere le aziende dalle minacce diverse e sofisticate che devono affrontare quotidianamente. La preparazione e la resilienza alla sicurezza informatica sono di fondamentale importanza per tutelare la continuità e il successo di qualsiasi azienda moderna.

È qui che Insight può aiutarti: il nostro team di esperti di sicurezza è disponibile 24/7, supportandoti nel potenziare la tua sicurezza informatica con monitoraggio, rilevamento e risposta proattive delle minacce, avendo accesso a tecnologie all'avanguardia.

Il nostro Security Operations Centre (SOC) offre due servizi gestiti, che forniscono capacità avanzate di rilevamento, indagine e risposta alle minacce:

- **Managed Endpoint Detection and Response (MEDR)** Adatta a computer portatili, desktop e dispositivi portatili.
- **Managed Extended Detection and Response (MXDR)** L'unione di log e feed provenienti da una vasta gamma di fonti offre capacità di rivelazione più efficaci per il tuo ambiente.

Grazie alla combinazione di tecnologie quali IA, threat intelligence e analisi, il nostro team di esperti di analisi della protezione è in grado di individuare e rispondere in tempo reale alle minacce presenti nel tuo ambiente.

Questo è possibile grazie a:

- Gestione proattiva degli aggiornamenti
- Analisi di esperti e incident response.
- Accesso a tecnologie di protezione all'avanguardia.
- Guida alla strategia di sicurezza e alla roadmap.
- Modello scalabile e conveniente

Come funziona

Ti aiuteremo a elaborare strategie, implementare e gestire soluzioni di sicurezza IT pronte per il futuro.

Assessment

- Ti aiutiamo a ottenere l'accreditamento secondo i quadri normativi del settore come ISO27001 o NIS2
- Esaminiamo i controlli di sicurezza esistenti e identifichiamo i rischi residui
- Ti aiutiamo a creare una roadmap prioritaria per raggiungere il livello di sicurezza desiderato

Plan & Design

- Ti assistiamo nella traduzione delle sfide aziendali in progetti di sicurezza
- Ti supportiamo e guidiamo nella selezione di fornitori, prodotti e servizi appropriati
- Envisioning workshop e progettazione tecnica

Build & Implement

- Trasformiamo i piani in realtà, passando dalla progettazione a controlli di sicurezza completamente costruiti e documentati
- Insight considera ogni progetto nel contesto della roadmap complessiva
- Collaboriamo con i tuoi team interni per la gestione o la transizione ai Managed Services di Insight

Security Operations Management

- I nostri servizi di supporto mantengono i controlli di sicurezza al meglio delle loro capacità
- Forniamo Managed Services in cui Insight si assume la responsabilità dei controlli di sicurezza

I nostri partner tecnologici di sicurezza

La modernizzazione IT è un lavoro di squadra. Uniamo le capacità di oltre 6.000 partner e fornitori di software, hardware e cloud con l'esperienza del nostro team sotto un unico tetto per creare soluzioni best-in-class che accelerano il tuo percorso di trasformazione.

Lavoriamo direttamente con aziende leader nel settore IT, in modo che i nostri clienti possano beneficiare di:

- Un unico punto di contatto per accedere ai prodotti e alle soluzioni tecnologiche più recenti.
- Un ecosistema di team collaborativi e altamente qualificati per attrezzare e gestire l'ambiente IT.
- Prezzi competitivi e negoziazione semplificata dei contratti.
- Soluzioni indipendenti, costruite su misura per le necessità specifiche dei nostri clienti.

Microsoft · cisco · aws · Google · paloalto NETWORKS · KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD. · FORTINET

Perché collaborare con Insight?

La sicurezza informatica è complicata e richiede un approccio “all-hands-on-deck” da parte degli utenti finali, dei team di sicurezza e dello strumento. Ecco perché abbiamo sviluppato metodi replicabili e processi collaudati che producono risultati di successo. I nostri esperti ti guideranno dall’inizio alla fine, migliorando l’efficienza, l’efficacia e l’allineamento strategico.

Abbiamo a disposizione:

Oltre 20 anni di conoscenza ed esperienza in tema di security

Partnership consolidate con i migliori fornitori

Approccio indipendente per trovare soluzioni in linea con le necessità dei clienti.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Gold Microsoft Partner

Microsoft

Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Fasi successive

Contatta Insight per migliorare la tua strategia di sicurezza informatica e le operazioni quotidiane. Con l'aumento delle minacce alla sicurezza informatica, proteggere la tua azienda è fondamentale per il successo del tuo business. Il nostro approccio completo migliora la sicurezza informatica, identifica e mitiga i rischi, semplifica le operazioni, ottimizza i controlli di sicurezza, massimizzando al contempo gli investimenti. Affidatevi ai metodi collaudati e alla guida degli esperti di Insight per rafforzare le difese di cybersecurity e promuovere la resilienza e la crescita aziendale.

- **it.insight.com**
- **02 21080210**