Guida all'acquisto dei servizi di Managed Security

Insight

Introduzione

Tutti, dai CEO e dai membri dei consigli di amministrazione ai singoli individui nella loro vita privata, riconoscono l'importanza della sicurezza informatica. È raro che passi un giorno senza imbattersi in una notizia riguardante un importante' azienda che ha subito una violazione della sicurezza o che ha affrontato un incidente di phishing via e-mail. Internet è fondamentale per gran parte della nostra vita personale e lavorativa, ma la sua natura globale ci espone anche a una serie di rischi globali.

Se il "costo della criminalità informatica" fosse una nazione, nel 2024 sarebbe stata la terza economia più grande al mondo, dietro solo agli Stati Uniti e alla Cina, con 9.000 miliardi di dollari[1].

Viviamo in un'epoca di incertezza geopolitica e di guerre ibride. I conflitti non sono più limitati al campo di battaglia: gli Stati nazionali e gli attori ad essi collegati sfruttano regolarmente le interruzioni del nostro mondo digitale per perseguire i loro obiettivi nel mondo reale. I gruppi della criminalità organizzata hanno puntato sulla tecnologia e si sono resi conto che è possibile fare grandi fortune tramite attacchi ransomware, purtroppo con scarse possibilità di essere assicurati alla giustizia.

In circa il 45% dei casi di quest'anno, i pirati informatici hanno esfiltrato i dati entro un giorno dalla compromissione[2].

L'ambiente normativo non è mai stato così rigoroso: l'Unione Europea ha introdotto leggi come NIS 2 e DORA che obbligano le organizzazioni a migliorare la loro sicurezza informatica.

Con organizzazioni che operano in un ambiente complesso, strette tra un panorama di minacce in peggioramento e requisiti normativi sempre più rigidi, ci auguriamo che questa guida aiuti a chiarire alcuni termini tecnici e fornisca un aiuto pratico su come orientare la propria organizzazione in questi tempi turbolenti.

Per gli incidenti non correlati all'estorsione nel 2022 e nel 2023, il tempo medio per l'esfiltrazione dei dati è rimasto costantemente inferiore a un giorno, il che significa che i difensori devono reagire a un attacco ransom in meno di 24 ore[3].

I rischi di non fare nulla

Non investire in solide misure di sicurezza informatica può avere gravi conseguenze:

- **Perdita finanziaria:** le violazioni dei dati e gli attacchi ransomware possono comportare multe, spese legali e perdita di profitti.
- **Danni alla reputazione:** un incidente di sicurezza può erodere la fiducia nei clienti e negli stakeholder.
- **Tempi di inattività operativa:** gli attacchi informatici spesso interrompono i processi aziendali, causando ritardi e perdita di produttività.
- **Sanzioni normative:** la mancata conformità a quadri normativi come NIS2 o GDPR può comportare sanzioni significative.

Se da un lato è chiaro che un investimento insufficiente nella sicurezza comporta rischi evidenti, dall'altro un investimento eccessivo nella sicurezza o un investimento nelle aree sbagliate è negativo per le aziende. Troppa sicurezza può frustrare i dipendenti e i clienti, per non parlare del costo opportunità di utilizzare quel budget per far crescere l'azienda.

La sicurezza è sempre un gioco di equilibri, con l'obiettivo di ottenere un livello di sicurezza "sufficiente" senza causare altri impatti sull'azienda.

Comprendere le basi

Esiste un'incredibile gamma di acronimi utilizzati dal settore: il marketing dei fornitori di software contribuisce notevolmente alla confusione. Vale la pena conoscere e comprendere alcuni dei più comuni, in modo da poter essere sicuri di parlare la stessa lingua con fornitori e partner.

Tecnologia

- **Endpoint Detection and Response (EDR):** si concentra sull'identificazione e sulla risposta alle minacce sui singoli endpoint (laptop, server, dispositivi mobili) fornendo dati forensi dettagliati e strumenti di correzione.
- **Network Detection and Response (NDR):** è un approccio alla sicurezza informatica che utilizza analisi avanzate, machine learning e rilevamento comportamentale per monitorare il traffico di rete in tempo reale, identificare anomalie o minacce e fornire Insight utilizzabili per mitigare i rischi e migliorare i tempi di risposta.
- **Extended Detection and Response (XDR):** va oltre gli endpoint, integrando dati provenienti da più fonti (rete, e-mail, cloud) per un rilevamento delle minacce e un contesto più ampi.
- **Security Information and Event Management (SIEM):** raccoglie e analizza i log provenienti da tutta l'organizzazione per identificare le attività sospette. Ottimo per la conformità e la centralizzazione dei dati.
- **Ingestion dei dati:** un'automobile è inutile senza il giusto tipo di carburante, e il SIEM è lo stesso. Deve essere alimentato con i log delle risorse IT esistenti e la quantità di log ingeriti avrà un impatto sul costo della soluzione. Solitamente misurata in gigabyte al giorno o in eventi al secondo. (EPS).
- **Security orchestration, Automation, and Response (SOAR):** si riferisce a un set di strumenti e processi che consentono ai team di sicurezza di semplificare e automatizzare i flussi di lavoro di rilevamento, indagine e risposta alle minacce. Integrando sistemi di sicurezza disparati e automatizzando le attività ripetitive, SOAR migliora l'efficienza, riduce i tempi di risposta e consente agli analisti di concentrarsi su attività di maggior valore.

Persone e processi:

- **Managed Detection and Response (MDR):** servizi di sicurezza esternalizzati che combinano tecnologia (spesso SIEM o XDR) con un team di esperti che si occupano di rilevamento, indagine e risposta.
- **Security Operations Centre (SOC):** un team o una struttura centralizzata responsabile del monitoraggio e della risposta agli incidenti di sicurezza, sia interni che gestiti da un fornitore.

Come funzionano tutti insieme?

Un servizio di sicurezza gestito è composto da persone, processi e tecnologia. La tecnologia è fondamentale per poter raccogliere tutti i dati necessari per fornire informazioni alle persone che gestiscono il servizio. Un requisito minimo assoluto è uno strumento EDR che fornisca dati su ciò che accade a livello di endpoint. Molti vendor stanno passando dall'EDR all'XDR, che include molto più dei soli dati sugli endpoint, per fornire una visione più ampia dell'intera organizzazione.

Gli strumenti XDR sono ottimi per rilevare gli incidenti "all'istante", ma di solito hanno una visione più a breve termine del mondo. Molte organizzazioni scelgono di potenziare l'XDR con una soluzione SIEM, che conserva i dati di log grezzi per un periodo di tempo prolungato, in genere un minimo di 90 giorni, ma all'occorrenza anche per molti anni. Se la tua organizzazione ha bisogno di allinearsi ai requisiti di conformità, un SIEM potrebbe essere una necessità.

Le persone e gli elementi di processo di solito provengono dal fornitore di servizi gestiti. Se hai già investito in questa tecnologia, avrai bisogno di un partner che sia esperto in quella tecnologia e che abbia maturato esperienza, regole e rilevamenti basati su quel vendor, in modo che possa offrire immediatamente valore. Se non hai ancora investito nella tecnologia, molti partner saranno lieti di suggerirti una soluzione.

Se hai deciso di affidarti ad un partner per la sicurezza gestita, assicurati di assicurati di fare un acquisto che porti un risultato. Se la tecnologia è di un leader di mercato comprovato, è ancora più importante scegliere un partner in base al servizio che offre e alla sua capacità di soddisfare le tue necessità di sicurezza. Concentrati su come collaborerete per migliorare la sicurezza e lascia che sia il partner a preoccuparsi della tecnologia.

SIEM contro XDR: Qual è la differenza?

Sebbene sia SIEM che XDR siano tecnologie fondamentali nella sicurezza informatica, servono a scopi diversi:

CARATTERISTICHE	SIEM	XDR
Funzioni fondamentali	Aggregazione e analisi dei log per la conformità e il rilevamento delle minacce.	Rilevamento unificato delle minacce su più vettori, con risposte automatizzate.
Modello di distribuzione	Solitamente richiede configurazione e manutenzione in-house.	Fornito come servizio completamente gestito o piattaforma software.
Campo di applicazione	Ampio e flessibile, supporta integrazioni personalizzate.	Ambito più ristretto ma integrazione più profonda tra gli strumenti supportati.
Casi d'uso	Ideale per le organizzazioni incentrate sulla conformità con competenze esistenti.	Ideale per le organizzazioni che cercano un rilevamento e una risposta semplificati e integrati.

Entrambi hanno i loro punti di forza. Molte organizzazioni combinano le funzionalità di conformità di un SIEM con il rilevamento avanzato delle minacce di XDR per coprire tutte le basi.

Il business case della sicurezza gestita

Un paio di decenni fa, molte organizzazioni non consideravano affatto la sicurezza. Con l'insorgere delle prime minacce informatiche, le organizzazioni hanno iniziato a investire in antivirus, firewall e altri controlli di ssicurezza di base. La "persona addetta alla sicurezza" gestiva questi controlli e le cose erano semplici. Tuttavia, l'aumento delle minacce ha comportato maggiori investimenti in nuovi controlli. Il "responsabile della sicurezza" diventa un team di sicurezza, in cui ogni membro ha un diverso set di competenze. La protezione dei dati, delle applicazioni, dell'infrastruttura, del cloud e dei sistemi di AI richiede una serie di competenze diverse e tutte queste diverse competenze devono essere gestite in modo coerente per garantire una copertura di sicurezza end-to-end.

Il costo e la complessità della gestione interna della sicurezza rappresentano un ostacolo all'ingresso per molti. L'alternativa è collaborare con un Managed Security Service Provider.

ASPETTO	SOC In-House	Partner MSSP
Costi	Elevati costi iniziali per infrastrutture, strumenti e noleggio.	Riduzione dei costi iniziali e dei costi di servizio continui grazie al pagamento di FTE frazionati.
Competenza:	Richiede l'assunzione e il mantenimento di professionisti altamente qualificati.	Accesso a un'ampia gamma di competenze senza la necessità di reclutamento.
Scalabilità	La scalabilità richiede ulteriori investimenti in risorse, personale e infrastrutture.	Facilmente scalabile con l'infrastruttura esistente del MSSP.
Copertura 24/7	Costosa e complessa da realizzare con il personale interno. Necessità di almeno 12 persone per coprire tutto il giorno.	Di solito incluso come parte del servizio.

ASPETTO	In-House SOC	MSSP Partner
Controllo	Controllo completo sulle operazioni SOC, sulle personalizzazioni e sulle priorità.	Controllo limitato, con una certa dipendenza dai processi e dalle priorità dell'MSSP.
Tempi di attuazione	Più lungo a causa dell'installazione, del noleggio e della configurazione.	Configurazione più rapida, poiché gli MSSP spesso hanno soluzioni e processi predefiniti.
Aggiornamenti della tecnologia	L'organizzazione ha la responsabilità di rimanere al passo con gli strumenti e le tecnologie.	Gli MSSP forniscono l'accesso agli strumenti e alle tecnologie più recenti come parte del servizio.
Conformità e governance	Piena responsabilità per il rispetto dei requisiti normativi e di conformità.	Gli MSSP forniscono solitamente servizi allineati ai requisiti di conformità, ma potrebbero non coprire le sfumature specifiche dell'organizzazione.
Dati di intelligence	Richiede la creazione o l'iscrizione a feed di intelligence sulle minacce in modo indipendente.	Accesso ai dati aggregati di intelligence sulle minacce provenienti da più clienti.
Personalizzazione	Altamente personalizzabile in base alle esigenze e ai flussi di lavoro specifici dell'organizzazione.	Le offerte standardizzate possono non essere pienamente in linea con i requisiti specifici.
Conoscenza del contesto aziendale	Forte comprensione della struttura organizzativa, delle priorità e del contesto.	Comprensione limitata dell'ambiente specifico dell'organizzazione.
Collaborazione interna	Allineamento più semplice delle operazioni SOC con i team IT e di sicurezza interni.	Richiede un maggiore coordinamento tra l'organizzazione e l'MSSP.

Quali sono i costi per la creazione di un team interno?

L'istituzione di un centro operativo di sicurezza (SOC) interno richiede un'attenta pianificazione finanziaria, poiché ci sono diversi fattori di costo da considerare:

1. Costi del personale

- **Analisti SOC:** supponiamo un minimo assoluto di due analisti per turno per mantenere la copertura 24/7, tenendo conto di malattia, ferie e prevenzione del burnout.
- **Esperti della sicurezza:** almeno due ingegneri dedicati per costruire, gestire e aggiornare gli strumenti SOC e l'infrastruttura.
- **Ruoli specializzati:** considera l'aggiunta di incident responder, threat hunter e un SOC manager per garantire che il team operi in modo efficace.
- **Formazione e certificazione:** formazione continua per mantenere il team aggiornato sull'evoluzione delle minacce, degli strumenti e dei requisiti di conformità.

2. Costi SIEM (Security Information and Event Management)

- **Costi di licensing e di abbonamento:** I costi sono spesso basati sul volume dei dati di log acquisiti.
- **Infrastruttura:** l'hosting del SIEM on-premise o nel cloud può comportare costi aggiuntivi per server, storage e larghezza di banda.
- **Alternative open source:** sebbene esistano piattaforme gratuite, possono richiedere investimenti sostanziali in personale qualificato o consulenza esterna per l'installazione, la manutenzione e la messa a punto.

3. Costi di intelligence sulle minacce

- **Abbonamenti:** accesso a pagamento ai feed di intelligence sulle minacce per arricchire i dati e contestualizzare gli avvisi.
- **Integrazione:** costi aggiuntivi per l'integrazione delle piattaforme di intelligence sulle minacce nell'ecosistema esistente.

4. Costi di Endpoint Detection and Response (EDR/XDR)

- **Licenze d'uso:** licenze per il rilevamento e la risposta alle minacce su endpoint, reti e altre risorse.
- **Costi di scalabilità:** scala dei costi basata sul numero di dispositivi o risorse monitorate.

5. Costi dell'infrastruttura

- **Hardware e software:** server, dispositivi di archiviazione e software per la raccolta, l'analisi e l'archiviazione dei log.
- **Ridondanza e Disaster Recovery:** sistemi di backup e piani di disaster recovery per le operazioni SOC.
- **Spazio disponibile:** spazio sicuro in ufficio o una sala operativa dedicata con controlli ambientali adeguati.

6. Strumenti di monitoraggio e rilevamento

- Strumenti per il monitoraggio del traffico di rete, l'analisi comportamentale e i sistemi di rilevamento delle intrusioni (IDS/IPS).
- Aggiornamenti e ottimizzazioni regolari per garantire l'efficacia contro le minacce in evoluzione.

7. Costi di risposta agli incidenti

- **Sviluppo del Playbook:** tempo e risorse per sviluppare processi e flussi di lavoro dettagliati di risposta agli incidenti.
- **Strumenti forensi:** strumenti specializzati per indagini approfondite su violazioni o attività sospette.

8. Costi legati alla conformità alle normative

- Garantire la conformità agli standard di settore (ad es. ISO27001, NIS2, PCI DSS) può richiedere ulteriori investimenti in strumenti, audit e competenze.
- Valutazioni e audit periodici per verificare la conformità.

9. Gestione delle vulnerabilità

- Strumenti per la scansione e la gestione delle vulnerabilità nell'intero panorama IT.
- Tempo o consulenza del personale per la gestione delle patch e le attività di ripristino.

10. Licensing per le piattaforme di sicurezza

- Costi di licensing aggiuntivi per DLP (Data Loss Prevention), strumenti di sicurezza cloud o firewall integrati con le operazioni SOC.

11. Costi di test e ottimizzazione

- **Test di penetrazione delle reti:** test regolari dei processi SOC e delle difese per identificare le lacune.
- **Esercizi Red Team / Blue Team:** esercitazioni di formazione per migliorare la prontezza del SOC e perfezionare l'incidentalità.

12. Integrazione con i sistemi IT esistenti

- Costi per l'integrazione degli strumenti SOC con i sistemi di gestione IT, come Active Directory, sistemi di ticketing e piattaforme ITSM.

13. Manutenzione e aggiornamenti continui

- Aggiornamenti software regolari, patch e regolazioni della configurazione.
- Sostituzione di hardware o software obsoleti nel tempo.

14. Consulenze e partnership di terze parti

- Costi a breve termine per consulenti specializzati per assistere nella configurazione iniziale o in attività complesse.
- Potenziali partnership con i fornitori per il supporto e la co gestione durante le prime fasi operative.

15. Costi nascosti e indiretti

- **Ottimizzare gli investimenti:** tempo significativo richiesto per la configurazione, la messa a punto e l'ottimizzazione del SOC prima della sua piena operatività.
- **Costi opportunità:** tempo e risorse sottratti ad altri progetti IT e di sicurezza.

Quali sono i costi di una partnership con un MSSP?

Poiché il fornitore ha già investito in tutte le voci di spesa sopra menzionate, pagherai una quota di questi costi, solitamente in base al tuo consumo. Il vantaggio per te è che non pagherai per un intero team che sarà sottoutilizzato, ma avrai accesso a un intero team quando sarà necessario.

I fornitori di servizi di sicurezza gestiti tipici addebiteranno un prezzo per un servizio in base a una combinazione dei seguenti fattori:

- **Numero di utenti:** ovviamente, più utenti ci sono - si presuppone che ci saranno più incidenti da gestire.
- **Numero di endpoint:** al giorno d'oggi, gli utenti spesso dispongono di più endpoint e anche i server sono fondamentali da monitorare.
- **Volume di dati di log:** alcune piccole organizzazioni generano molti dati, mentre altre grandi organizzazioni possono avere un'infrastruttura piuttosto semplice. Osservando la quantità di dati di log generati, gli MSSP possono ipotizzare il livello di risposta agli incidenti che sarà necessario.

Sebbene si conosca molto probabilmente il numero di utenti ed endpoint, a meno che non si disponga già di un SIEM o SOC, il volume dei dati di log potrebbe non essere noto. Un buon partner ti aiuterà a stimare questo costo in base alla quantità e alla tipologia di dispositivi presenti nella tua azienda; questo lavoro viene solitamente svolto gratuitamente come parte dell'impegno di prevendita.

Il fornitore può offrire un pagamento anticipato per coprire il lavoro di consulenza necessario per configurare il servizio, seguito da un canone mensile, oppure può combinare entrambi in un unico canone mensile. Idealmente, saranno in grado di lavorare con entrambi, a seconda delle tue preferenze.

La licenza della piattaforma SIEM stessa può comportare dei costi. Possono essere inclusi nel canone mensile o pagati separatamente a un provider SaaS come Microsoft o Cisco. Il partner deve indicare chiaramente se sono dovuti costi aggiuntivi a terzi e deve stimarli per fornire un prezzo totale.

SLA e reporting: la base del servizio

Un Service Level Agreement (SLA) definisce le aspettative, le responsabilità e le metriche di performance tra il cliente e il fornitore di managed security. Un solido SLA garantisce chiarezza, responsabilità e allineamento con le esigenze aziendali, ma non tutti gli SLA sono uguali.

- **Tempo medio di rilevamento:** quanto tempo trascorre tra il verificarsi di un incidente e il suo rilevamento da parte del SOC? Con le moderne piattaforme SIEM, il rilevamento dovrebbe avvenire quasi in tempo reale; tuttavia, il rilevamento di un incidente dipende dalla configurazione della piattaforma, dalle fonti di log acquisite e dalla qualità delle regole. È difficile confrontare direttamente gli SLA a questo livello.

- **Tempo medio di risposta:** una volta rilevato un incidente, quanto rapidamente reagisce il SOC? Sebbene questa misura sia spesso la più importante, non è così semplice come cercare il partner nel minor tempo possibile... (come vedrai nella sezione “Come si presenta un buon SLA”).

- **Tempo medio di correzione:** quanto tempo ci vuole tra la risposta e la risoluzione del problema. Esiste un’ampia gamma di tipi e complessità di incidenti, quindi anche questo numero è difficile da confrontare. Inoltre, alcune attività di correzione possono richiedere la risoluzione da parte del team IT interno o di terzi - gli MSSP escludono questi tempi da questo SLA.

Come si presenta un buon SLA

Un SLA ben elaborato bilancia prestazioni e praticità. Assicurati di avere:

- **Prioritizzazione basata sul rischio:** maggiore urgenza per incidenti critici e minore priorità per problematiche minori.

- **Metriche trasparenti:** definizioni chiare dei tempi di risposta e risoluzione con risultati misurabili.

- **Timeline realistiche:** a prima vista, un tempo di risposta di 5 minuti potrebbe sembrare migliore di un tempo di risposta di 30 minuti. Ma qual è il contenuto di una "risposta"? Vuoi davvero essere chiamato ogni notte alle 3 del mattino perché un partner sta dando priorità al suo SLA rispetto alla rimozione dei falsi positivi? Il partner viene pagato per eseguire il triage e confermare i veri positivi, non solo per inoltrare direttamente a te ogni allarme proveniente dal SIEM.

Gli SLA sono la base della fiducia tra te e il tuo provider. Un buon SLA non promette solo velocità, ma garantisce qualità, responsabilità e allineamento con gli obiettivi aziendali.

Reportistica

In genere si incontrano due tipi di report. Report “ad hoc” che vengono generati quando viene rilevato e notificato un incidente. Questi sono finalizzati alla comunicazione rapida di un problema, di solito qualcosa che richiede il tuo intervento o una notifica tempestiva.

Tuttavia, l’MSSP non deve essere coinvolto solo quando si verifica un problema. Dovrebbe esserci una cadenza regolare di riunioni, sia con gli stakeholder tecnici che aziendali, che trattano argomenti come:

- **Copertura delle origini dei log:** la qualità del servizio dipende dai log a cui ha accesso. Il provider utilizza un framework come MITRE ATT&CK per consigliare fonti di log aggiuntive che potrebbero aggiungere valore?
- **Prestazioni rispetto a SLA:** un’opportunità per esaminare le prestazioni del servizio rispetto agli SLA e, se necessario, implementare piani correttivi.
- **Revisione degli incidenti precedenti:** uno sguardo ad alcuni degli incidenti più gravi: cosa è andato bene e cosa potrebbe essere migliorato?
- **Una visione più ampia:** il mondo non è fermo, e la tua organizzazione cambierà nel tempo, così come il panorama delle minacce. Dovrebbe esserci un’opportunità regolare per informare il provider di eventuali cambiamenti aziendali (ad es. fusioni e acquisizioni) che potrebbero avere un impatto sul servizio, e per il provider di fornire indicazioni su nuove minacce e soluzioni.

Funzionalità da cercare in un partner di Managed Security

Automazione e AI:

Le minacce moderne richiedono rilevamento e risposta rapidi. I fornitori devono sfruttare l'automazione e l'AI per:

- Identificare le anomalie in tempo reale, riducendo la dipendenza dall'analisi manuale.
- Semplificare i flussi di lavoro di risposta agli incidenti, garantendo un contenimento rapido.
- Automatizzare azioni comuni come l'isolamento di un dispositivo o il blocco di un account compromesso. Ciò è particolarmente importante se si desidera che il partner possa intervenire per conto proprio al di fuori dell'orario di lavoro.

Intelligence sulle minacce:

I dati di intelligence sulle minacce ti aiutano a rimanere un passo avanti rispetto ai rischi in continua evoluzione. Cerca fornitori che:

- Mantengono aggiornati i feed delle minacce e li integrano nei loro servizi.
- Condividono informazioni sulle nuove tendenze di attacco rilevanti per il tuo settore.
- Utilizzano l'intelligenza per migliorare il rilevamento e dare priorità alle minacce critiche.

Threat hunting:

Il threat hunting proattivo garantisce che le minacce non rimangano inosservate. Valuta se il fornitore

- Offre attività di threat hunting regolari e manuali.
- Utilizza strumenti avanzati per identificare i rischi nascosti.
- Fornisce report dettagliati sui risultati e sulle fasi di mitigazione.

Misure di riparazione

Gli alert sono solo una parte dell'equazione: la correzione efficace è fondamentale. Assicurati che il fornitore:

- Offra una guida chiara sulle strategie di contenimento.
- Possieda capacità di consulenza per aiutarti ad agire su progetti più grandi per migliorare il livello di maturità della sicurezza.

Aspetti pratici

Certificazioni

Qualsiasi partner sarà in grado di mostrarti materiali di marketing interessanti, ma quale prova può fornire per supportare l'efficacia del suo servizio?

- Verifica la certificazione dei fornitori da fonti come MSSP Alert: www.msspalert.com/top-250

- Verifica se sono accreditati presso il fornitore scelto. Vuoi assicurarti che siano esperti nel loro set di strumenti e che il loro servizio sia stato verificato dal fornitore. Ciò significa anche che collaboreranno a stretto contatto con il fornitore per apportare miglioramenti e avranno un buon rapporto con il loro team di ingegneri.

- Verifica i quadri di conformità pertinenti che sono rilevanti nella tua regione o nel tuo settore. Certificazioni come Cyber Essentials+ e ISO27001 indicano che l'organizzazione prende sul serio la propria sicurezza e dovrebbe essere un requisito minimo per un fornitore di servizi di sicurezza.

Processo di Onboarding

Dovresti aspettarti che un buon partner ti guidi attraverso il processo di onboarding. La tabella che segue illustra le fasi principali del processo. Anche se il partner dovrebbe fare il lavoro pesante, è importante essere consapevoli di qualsiasi dipendenza dal personale, in modo da poterla pianificare..

Cosa?	Il tuo impegno
Scoping e scoperta: Per poter fornire una soluzione appropriata, il partner dovrà porre molte domande sulle tue aspirazioni per il servizio e sul tuo attuale stack tecnologico.	Dovresti coinvolgere diversi stakeholder per essere in grado di fornire una panoramica della composizione e delle dimensioni della tua azienda. Conoscere informazioni come il numero di dispositivi endpoint, la marca, il modello e la quantità di firewall, servizi cloud e altre risorse ti aiuterà a garantire che la progettazione sia adatta alle tue esigenze.
Piattaforma di sviluppo: Se è necessaria l'implementazione di uno strumento SIEM, o se l'XDR deve essere implementato in tutta l'azienda, dovrai essere coinvolto in questo processo per ridurre al minimo le interruzioni per gli utenti.	Il team IT potrebbe dover fornire l'accesso all'ambiente cloud per consentire al partner di implementare il SIEM. Si consiglia di collaborare con il partner per creare un piano congiunto su come e quando distribuire gli agenti endpoint.
Personalizzazione: Ogni buon partner avrà un set di regole predefinite che funzionano per rilevare gli incidenti per la maggior parte delle organizzazioni. Tuttavia, se hai esigenze di personalizzazione specifiche, dovrai collaborare con il partner per garantire che tali requisiti vengano recepiti.	Se sono presenti regole esistenti in un sistema legacy che devono essere riscritte, fornirle può portare a un onboarding più rapido che iniziare da zero. Se questi sono nuovi requisiti, documentarli in linguaggio naturale può aiutare a comunicare le tue necessità al partner.
Supporto iniziale: Una volta che il servizio entrerà in funzione, ci sarà un periodo di ulteriore messa a punto per ridurre i falsi positivi e adattare il sistema al tuo ambiente specifico.	Il team IT e il partner dovranno collaborare a stretto contatto. Anche se molti incidenti saranno facili da classificare come falsi positivi o veri positivi, il partner vorrà lavorare con te sulla "zona grigia" per garantire che gli articoli della knowledge base possano essere scritti e le regole personalizzate per garantire che i falsi positivi siano ridotti al minimo durante il funzionamento.
Operazioni in tempo reale: Una volta completato il supporto iniziale, la soluzione passerà allo stato stazionario. Il lavoro di personalizzazione del partner non si ferma a questo punto, ma dovrebbe rallentare notevolmente quando l'attenzione si sposta sul rilevamento degli incidenti.	Sarà necessario fornire una mappa dei contatti per indicare chi deve essere informato quando si verifca un incidente di sicurezza. Potrebbe trattarsi di un unico elenco di distribuzione per le organizzazioni più piccole, ma potrebbe presentare complessità aggiuntive, come percorsi di escalation diversi durante o fuori dall'orario lavorativo, oppure gruppi di risoluzione specifici per problemi con determinate tecnologie. Ciò potrebbe anche includere terze parti a cui hai esternalizzato alcune operazioni.

Servizi a valore aggiunto

Sebbene la tua preoccupazione principale nella ricerca di un fornitore di Managed Security sarà quella di aiutarti a rilevare e risolvere gli incidenti di sicurezza, spesso ci sono altri servizi che si adattano naturalmente a un fornitore di Managed Security. Vale la pena considerare se qualcuno di questi potrebbe esserti utile e potrebbe essere incluso nello stesso pacchetto. Spesso è vantaggioso avere più servizi forniti dallo stesso partner, in quanto avranno una visibilità più ampia della sicurezza e potranno spesso prendere decisioni più informate.

La gestione delle vulnerabilità è un complemento naturale di un SOC, che identifica, valuta e dà priorità in modo proattivo alle falle di sicurezza nell'ambiente digitale di un'organizzazione. Integrando questo servizio, le organizzazioni beneficiano di un monitoraggio continuo delle vulnerabilità e di piani di correzione attuabili che si allineano alle capacità di rilevamento delle minacce del SOC. Ciò ne riduce di sfruttamento chiudendo le falle di sicurezza prima che gli aggressori possano approfittarne.

Digital Risk Protection Services (DRPS) offrono un'ulteriore aggiunta strategica, estendendo la portata del SOC oltre la rete aziendale nel panorama digitale più ampio. Il DRPS monitora le minacce in ambienti esterni come il dark web, i social media e i sistemi rivolti all'esterno. Identificando furti di identità, fughe di credenziali o dati sensibili esposti, le organizzazioni possono ricevere avvisi tempestivi su potenziali minacce, consentendo al SOC di rispondere rapidamente e mitigare i rischi.

Per le organizzazioni che affrontano minacce o violazioni attive, l'abbinamento di **Digital Forensics and Incident Response (DFIR)** con Managed Security garantisce un rapido contenimento e un'analisi dettagliata post-incidente. I team DFIR possono sfruttare la telemetria e i registri del SOC per indagare sulle cause principali, determinare l'entità della violazione e consigliare le fasi di ripristino. Questo approccio olistico consente alle aziende di rispondere in modo deciso, acquisendo al contempo informazioni utili per prevenire il ripetersi di situazioni problematiche. L'unione di questi servizi crea una soluzione di sicurezza end-to-end fluida, che offre alle organizzazioni sicurezza sia nella prevenzione che nella resilienza.

Fasi successive

Le minacce alla sicurezza informatica sono in aumento e i costi derivanti dall'inazione sono elevati. Non aspettare che si verifichi questa una violazione; contatta Insight, un MSSP di prim'ordine, e scopri come i nostri servizi di sicurezza gestita possono essere il modo più conveniente per aiutarti a proteggere la tua azienda.

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

[1] source: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[3] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report