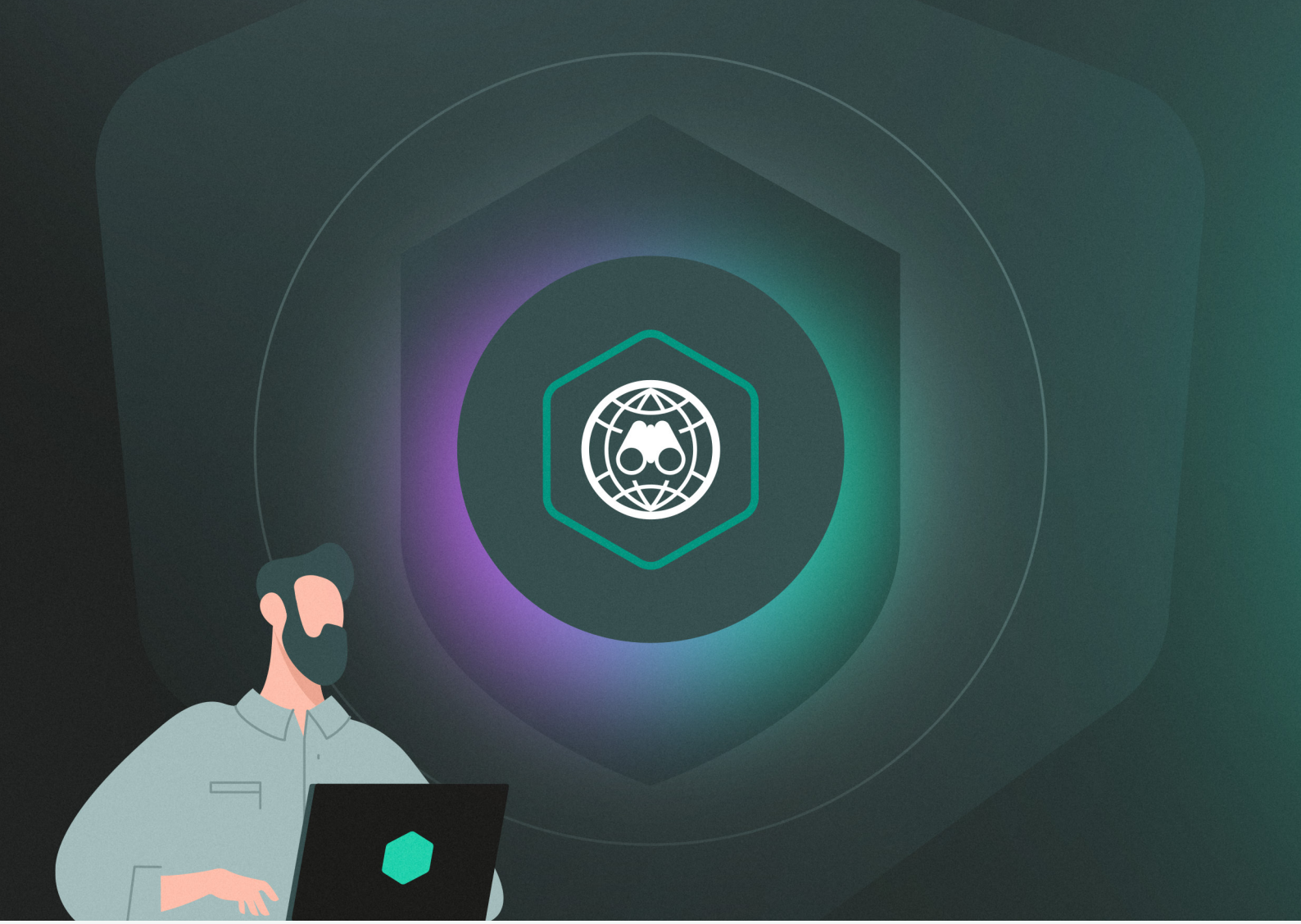

Kaspersky
Threat Intelligence

Valutazione delle fonti di Threat Intelligence

kaspersky BRING ON THE FUTURE

Maggiori informazioni su kaspersky.it
#bringonthefuture

Introduzione

Con una superficie di attacco sempre maggiore e una crescente complessità delle minacce, la semplice reazione a un incidente non è sufficiente. Ambienti sempre più complessi offrono molteplici opportunità per gli autori degli attacchi. Ogni settore e ogni organizzazione ha dati unici da proteggere e utilizza uno specifico set di applicazioni, tecnologie. Tutto questo introduce un numero enorme di variabili nei possibili metodi di esecuzione di un attacco, con nuove tecniche che emergono ogni giorno.

Negli ultimi due anni, abbiamo osservato confini sempre più labili tra i diversi tipi di minacce e i diversi tipi di autori delle minacce. I metodi e gli strumenti che in precedenza rappresentavano una minaccia per un numero limitato di organizzazioni si sono diffusi sul mercato più ampio. Un esempio a questo proposito è il dumping del codice da parte del gruppo Shadow Brokers, che ha reso disponibili exploit avanzati a gruppi di gruppi criminali che diversamente non avrebbero avuto accesso a codice sofisticato di questo tipo. Un chiaro esempio è rappresentato dalla comparsa sulla scena di campagne APT (Advanced Persistent Threat) di natura mirata incentrate non su attività di cyberspionaggio, ma sul furto di denaro, allo scopo di finanziare altre attività. E l'elenco potrebbe continuare.

È necessario un nuovo approccio

I metodi e gli strumenti che in precedenza rappresentavano una minaccia per un numero limitato di organizzazioni si sono diffusi sul mercato più ampio.

Dal momento che sempre più imprese restano vittime di attacchi avanzati e mirati, è chiaro che una difesa di successo richiede nuovi metodi. Per proteggersi, le aziende devono adottare un approccio proattivo, adattando costantemente i propri controlli di sicurezza all'ambiente delle minacce in continua evoluzione. L'unico modo per tenere il passo con questi cambiamenti è quello di creare un programma di Threat Intelligence efficace.

La Threat Intelligence è già diventata un componente chiave delle operazioni di sicurezza messe in atto da aziende di varie dimensioni in tutti i settori e aree geografiche. Disponibile in formati sia human-readable che machine-readable, la Threat Intelligence può supportare i team di sicurezza con informazioni significative durante tutto il ciclo di gestione degli incidenti e supportare il processo decisionale strategico (figura 1).

Tuttavia, la crescente domanda di Threat Intelligence esterna ha dato origine al proliferare di fornitori di questi servizi, ognuno dei quali offre una serie di soluzioni diverse. Un mercato ampio e competitivo con innumerevoli opzioni complesse può rendere la scelta della soluzione più adattabile alla vostra organizzazione estremamente confusa e frustrante.

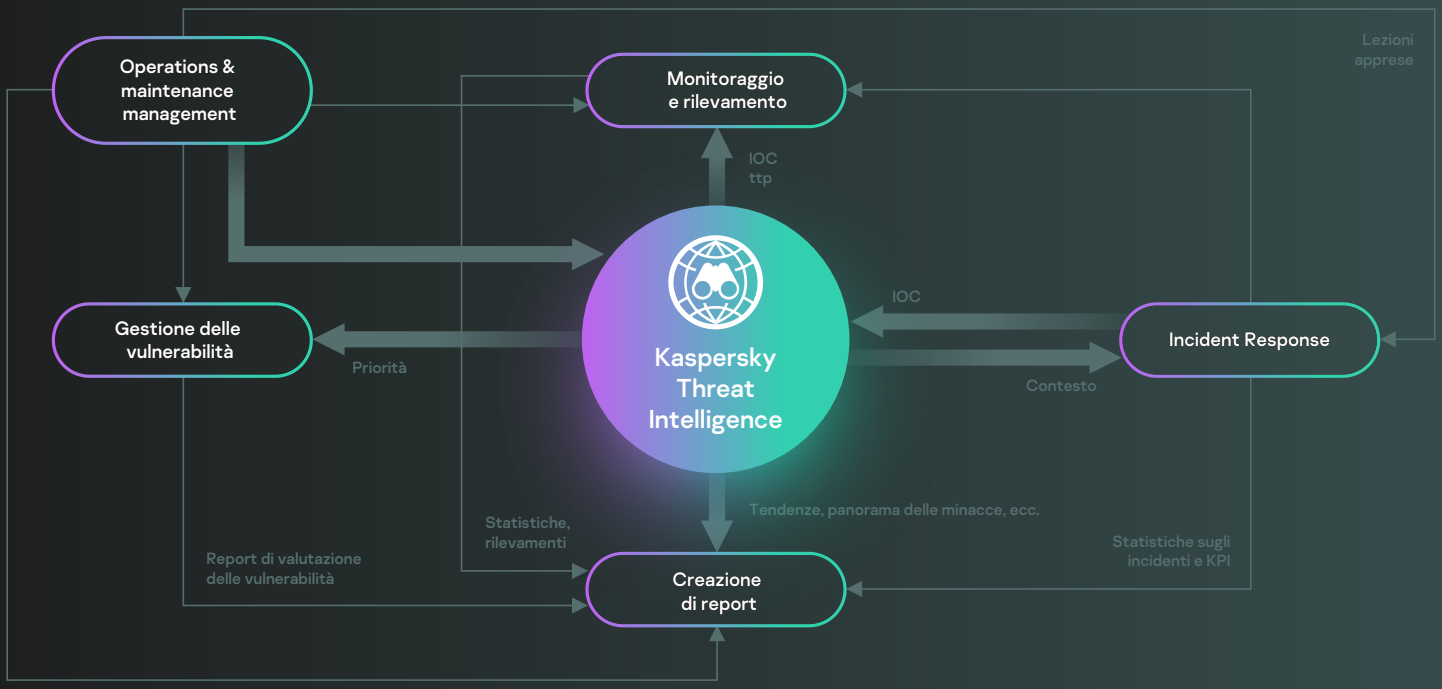

Figura 1

Operazioni di security basate su Threat Intelligence

Una Threat Intelligence che non è personalizzata per le specifiche esigenze della vostra attività può esacerbare la situazione. Oggi, in molte aziende, gli analisti della sicurezza trascorrono più di metà del proprio tempo a occuparsi dei falsi positivi, invece di eseguire ricerche delle minacce e rispondere in modo proattivo, con un significativo aumento dei tempi di rilevamento. Fornire informazioni irrilevanti o imprecise per le operazioni di sicurezza farà aumentare ulteriormente il numero di falsi allarmi e avrà un impatto notevolmente negativo sulle capacità di risposta e sulla sicurezza complessiva dell'azienda.

Dove trovare la migliore Intelligence...

Come si valutano le numerose fonti di Threat Intelligence, e come si identificano quelle più rilevanti per l'organizzazione e le si rendono operative in modo efficace? Come orientarsi tra le enormi quantità di inutile materiale marketing, in cui quasi tutti i fornitori sostengono di fornire le informazioni migliori?

Queste domande, per quanto valide, non sono sicuramente le prime che dovreste porvi. Attratte da messaggi allettanti e promesse altisonanti, molte organizzazioni credono che un vendor esterno possa fornire loro una sorta di visione a raggi-X, trascurando completamente il fatto che l'intelligence più preziosa si trova all'interno del perimetro delle proprie reti aziendali...

I dati provenienti da sistemi di rilevamento e prevenzione delle intrusioni, firewall, log delle applicazioni e log di altri controlli di sicurezza possono rivelare molto su ciò che sta accadendo all'interno della rete aziendale. Consentono di identificare modelli di attività dannose specifiche per l'organizzazione. Permettono di distinguere tra un normale comportamento dell'utente e della rete e di mantenere una registrazione delle attività di accesso ai dati.

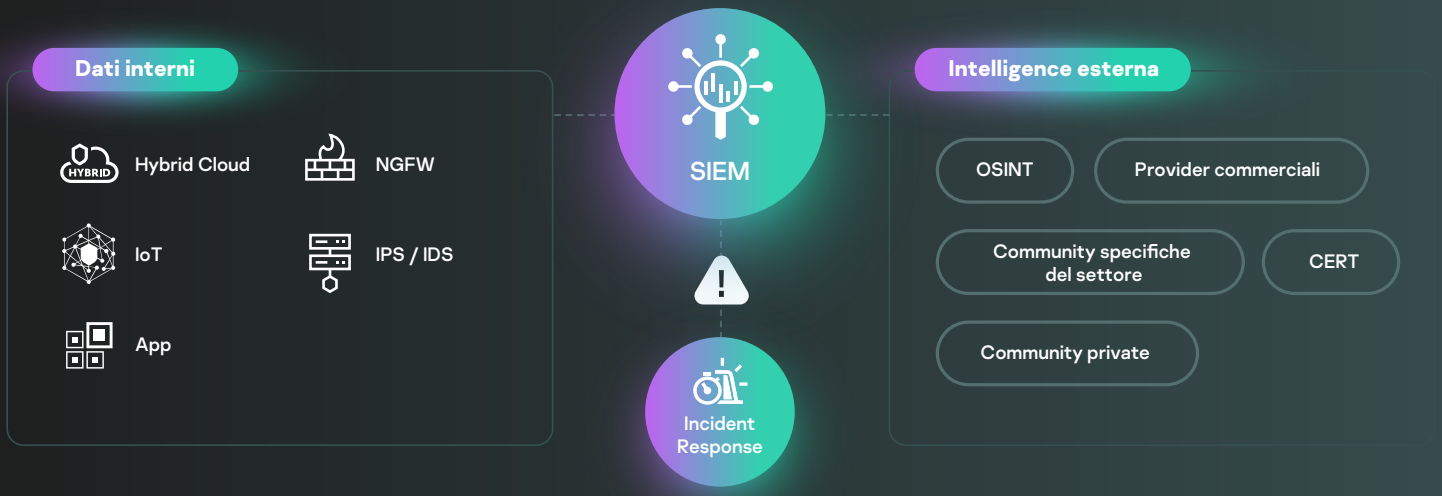

Figura 2

Threat Intelligence esterna pienamente operativa

Pensare come l'autore di un attacco

Per creare un efficace programma di Threat Intelligence, le aziende, incluse quelle che dispongono di un SOC (Security Operational Center), devono pensare come l'autore di un attacco, identificando e proteggendo gli obiettivi più probabili. Per ottenere un valore reale da un programma di Threat Intelligence, occorre una comprensione molto chiara delle risorse chiave, nonché dei set di dati e dei processi aziendali fondamentali per gli obiettivi dell'organizzazione. Identificare questi obiettivi consente alle aziende di stabilire intorno a loro dei punti di raccolta dati, per mappare i dati raccolti con le informazioni sulle minacce disponibili esternamente. Considerando le risorse limitate in genere disponibili per i reparti di sicurezza delle informazioni, la profilazione di un'intera organizzazione è un'impresa enorme. La soluzione consiste nell'adottare un approccio basato sul rischio, concentrandosi prima sugli obiettivi più sensibili.

Una volta definite e rese operative le fonti interne di Threat Intelligence, l'azienda può iniziare a pensare di aggiungere informazioni esterne nei flussi di lavoro esistenti.

È una questione di fiducia

Le fonti esterne di Threat Intelligence presentano vari livelli di attendibilità:

Le fonti aperte sono disponibili gratuitamente, ma spesso mancano di un contesto e restituiscono un numero significativo di falsi positivi

Le fonti commerciali di Threat Intelligence sono molto più affidabili, anche se l'acquisto per l'accesso alle informazioni può essere costoso

Una buona opzione per iniziare è l'accesso a community per la condivisione di informazioni specifiche di settore, come Financial Services Information Sharing and Analysis Center (FS-ISAC). Queste community forniscono informazioni estremamente preziose, anche se spesso sono protette ed è necessario iscriversi per ottenere l'accesso

Il principio guida per la scelta delle fonti esterne di Threat Intelligence dovrebbe essere la qualità rispetto alla quantità. Alcune organizzazioni potrebbero pensare che più fonti di Threat Intelligence riescono a integrare, maggiore sarà la visibilità che otterranno. Questo può essere vero in alcuni casi: ad esempio, quando si tratta di fonti altamente attendibili, incluse quelle commerciali, che forniscono informazioni su misura per il profilo di minaccia specifico dell'organizzazione. In caso contrario, esiste un rischio significativo di sovraccaricare le operazioni di sicurezza con informazioni irrilevanti.

La sovrapposizione delle informazioni fornite dai vendor di Threat Intelligence specializzati può essere molto piccola. Poiché le fonti di intelligence e i metodi di raccolta variano, le informazioni fornite da ciascun vendor saranno uniche per alcuni aspetti. Ad esempio, un vendor, essendo particolarmente presente in un'area specifica, fornirà maggiori dettagli sulle minacce provenienti da tale area, mentre un altro fornirà maggiori dettagli su specifici tipi di minacce. Di conseguenza, può essere utile ottenere l'accesso a entrambe le fonti: se usate insieme, possono aiutare a rivelare un quadro più ampio e guidare iniziative più efficaci di ricerca delle minacce e risposta agli incidenti. Occorre tuttavia tenere presente che questi tipi di fonti attendibili richiedono anche un'attenta valutazione preliminare per garantire che l'intelligence fornita sia appropriata per le specifiche esigenze e gli scenari di utilizzo dell'organizzazione, come operazioni di sicurezza, risposta agli incidenti, gestione dei rischi, gestione delle vulnerabilità, red teaming togliere o cambiare.

Aspetti da considerare durante la valutazione delle offerte di Threat Intelligence commerciali

Anche se non esistono ancora criteri comuni per valutare le varie offerte di Threat Intelligence commerciali, ecco alcuni elementi da tenere presente durante la valutazione:

Si presuppone che l'azienda disponga già di alcuni controlli di sicurezza, con processi associati definiti, e che ritenga importante utilizzare la Threat Intelligence con gli strumenti già utilizzati e conosciuti. Cercate quindi metodi di distribuzione, meccanismi di integrazione e formati che supportino una completa integrazione della Threat Intelligence nelle vostre operazioni di sicurezza esistenti

Cercate informazioni di intelligence di portata globale. Gli attacchi non hanno confini: un attacco che colpisce un'azienda in America Latina può essere lanciato dall'Europa e viceversa. Il vendor raccoglie informazioni a livello globale e riunisce attività apparentemente disgiunte in campagne coerenti? Questo tipo di intelligence vi aiuterà a prendere le misure appropriate

Il contesto crea l'intelligence dai dati. Gli indicatori di minacce senza contesto non hanno alcun valore: dovreste cercare provider che vi aiutino a rispondere alla domanda "perché questo è importante?". Il contesto delle relazioni (ad esempio, i domini associati agli indirizzi IP o agli URL rilevati da cui è stato scaricato un file specifico) fornisce un valore aggiunto, rendendo più efficienti le indagini sugli incidenti e supportando una migliore "definizione dell'ambito" degli incidenti, attraverso l'identificazione degli indicatori di compromissione correlati acquisiti nella rete

Se siete alla ricerca di contenuti maggiormente strategici per supportare la pianificazione della sicurezza a lungo termine, come:

- Informazioni generali sulle tendenze degli attacchi
- Tecniche e metodi utilizzati dagli autori degli attacchi
- Motivazioni
- Attribuzioni,

cercate un provider di Threat Intelligence con una comprovata esperienza nell'individuazione e nelle indagini sulle minacce complesse nella vostra area geografica o nel vostro settore. Anche la capacità del provider di adattare le proprie capacità di ricerca alle specifiche della vostra azienda è fondamentale

Conclusione

In Kaspersky ci siamo concentrati sulla ricerca sulle minacce per oltre due decenni. Con la possibilità di estrapolare petabyte di dati sulle minacce, tecnologie di machine learning avanzate e un pool di esperti unico al mondo, lavoriamo per supportarvi con la più recente tecnologia di Threat Intelligence proveniente da tutto il mondo, al fine di garantire la sicurezza anche contro gli attacchi informatici precedentemente passati inosservati.

Kaspersky Threat Intelligence

Per saperne di più

www.kaspersky.it