IBM Security

Devi migliorare la tua strategia di difesa?

Cinque domande da porsi prima di passare a una soluzione SIEM

Quando si tratta di sicurezza, le soluzioni “fai da te” non bastano

I team di sicurezza informatica devono riuscire a proteggere la propria organizzazione da attacchi cibernetici nel rispetto dei requisiti interni e di compliance, quali ISO 27001 (Organizzazione internazionale per la normazione), PCI DSS (Payment Card Industry Data Security Standard) e GDPR (General Data Protection Regulations). Questo non è un compito semplice. Affidandosi a un semplice log manager oppure a fogli di calcolo elementari per il salvataggio e la ricerca nei log, si corre il pericolo di ignorare incidenti critici. Con attacchi sempre più pericolosi e normative in continua evoluzione, gli strumenti elementari sono semplicemente inadeguati. É arrivato il momento di passare al sistema SIEM (Security Information and Event Management).

Esamineremo cinque domande fondamentali per aiutarti a individuare la migliore soluzione per la tua organizzazione.

Le soluzioni SIEM moderne non si limitano alla raccolta automatica, all'attività di parsing e alla normalizzazione dei log. Applicano correlazioni e analytics avanzati per rilevare automaticamente eventuali minacce, valutarne la gravità e filtrare i dati rilevanti per allertare l'utente della presenza di eventi critici. Si avvalgono di funzioni di automazione e intelligence integrate per consentirti di avere protezione e, contemporaneamente, avere il tempo necessario da dedicare ad attività di ripristino e risoluzione dei problemi.

> **I team che si occupano di sicurezza informatica vedono *200,000* eventi di sicurezza ogni giorno.**

Cos’è un moderno SIEM?

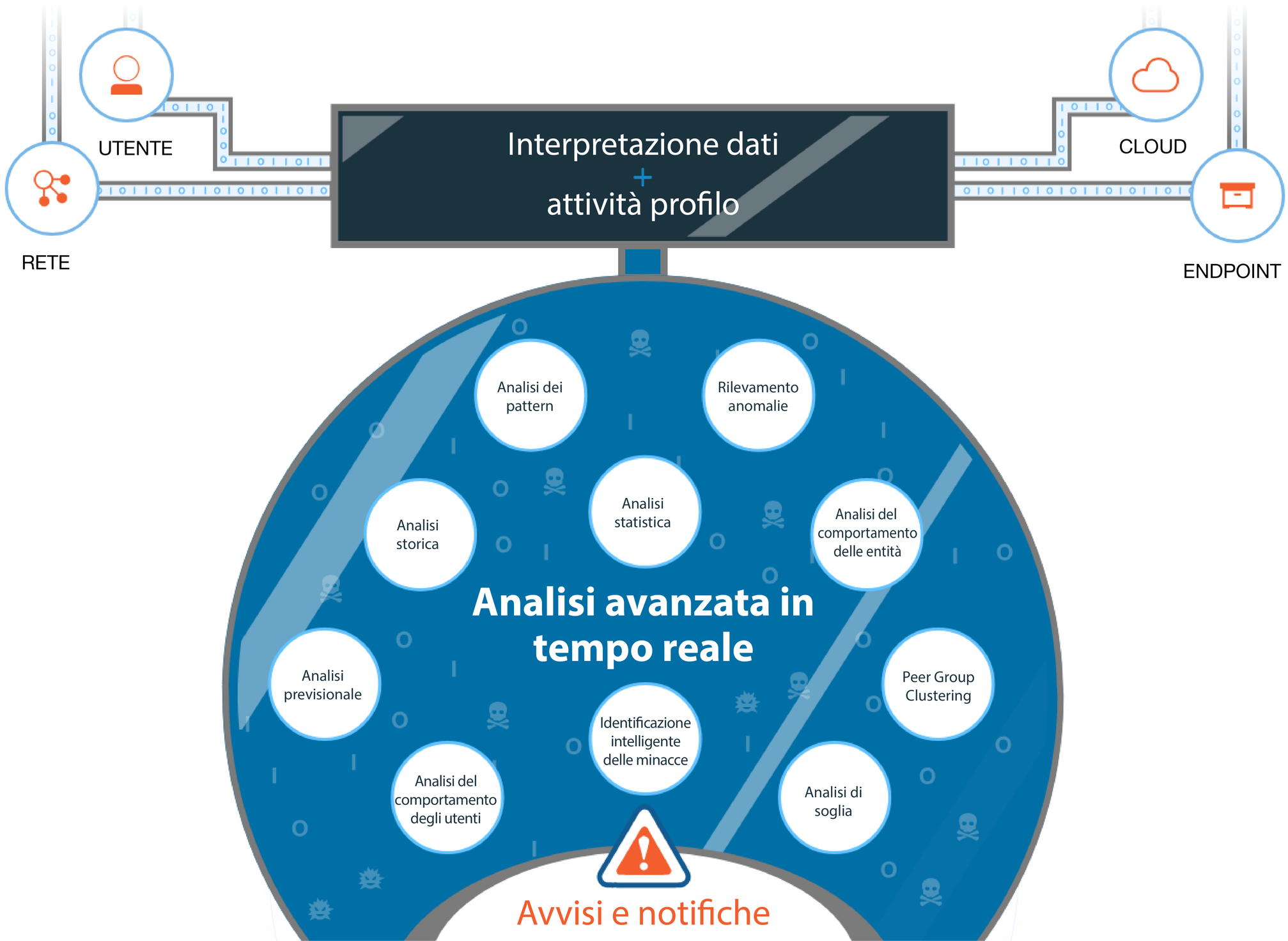
1

Riesci a stare al passo con tutti i tuoi dati relativi alla sicurezza, in tempo reale?

Affidandosi ai fogli di calcolo per la ricerca e la gestione dei log si rischia di ignorare eventuali cambiamenti in tempo reale, per non menzionare il tempo e le risorse impiegate a gestire il sistema. Un moderno sistema SIEM centralizzato non si limita ad automatizzare le attività di raccolta, la normalizzazione e le analisi dei log, ma fornisce anche dati per interpretare insight relativi al network e i log in modo dettagliato.

Le informazioni sul flusso di rete permettono individuare gli autori di attacchi informatici

Oltre ai log di sistema, i sistemi SIEM moderni analizzano i flussi di rete, i dati degli endpoint, l'utilizzo del cloud e i comportamenti dell'utente. Tenendo in considerazione i dati relativi a tutte queste attività è possibile capire esattamente cosa sta avvenendo nel proprio ambiente informatico, capire cosa è normale e utilizzarlo come riferimento per identificare automaticamente deviazioni che possono segnalare eventuali minacce.



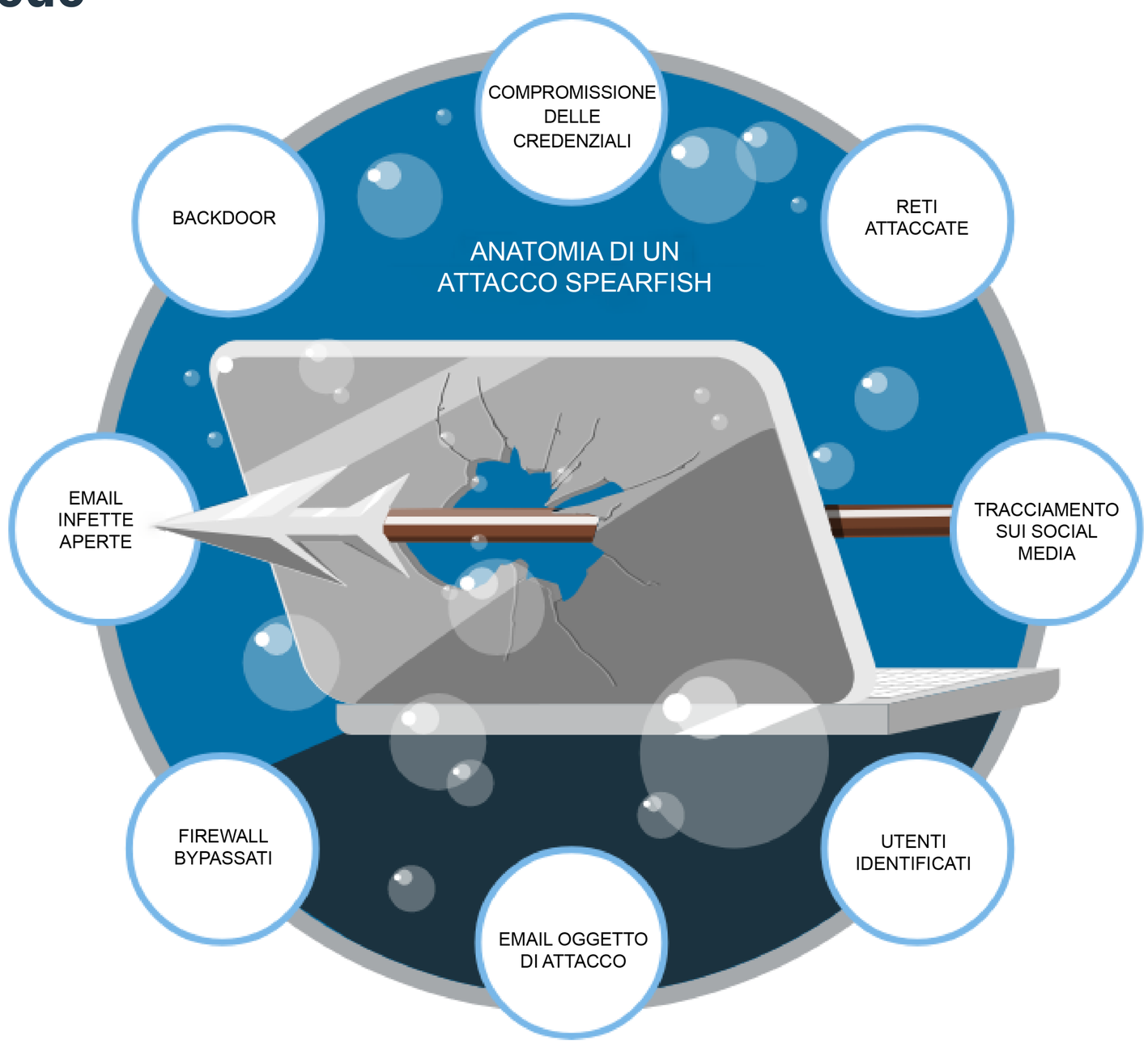
2

Il mio programma per la sicurezza informatica tiene in considerazione il fattore umano?

Potrebbe capitare che un utente faccia clic su un link dannoso senza rendersene conto. In altri casi, un dipendente potrebbe addirittura decidere di tradire la vostra azienda. La vostra soluzione tiene conto del fattore umano?

La maggior parte degli attacchi è effettuata da personale interno, in modo accidentale o volontario.

Gli utenti con intenzioni dannose seguono comportamenti diversi dagli altri. Riuscire a individuare queste eccezioni può aiutare a prevenire danni. Per far questo è necessario determinare il livello di normale attività dei propri utenti e utilizzare questi dati come riferimento per individuare le anomalie che possono segnalare eventuali minacce. Le tecniche di analisi del comportamento degli utenti che sfruttano le capacità di apprendimento automatico possono essere preziose nell'individuazione delle anomalie in tutti i sistemi dell'azienda. Nell'ambito di un sistema SIEM, le attività anomale vengono individuate e la priorità viene data agli utenti ad alto rischio in grado di causare il maggior danno.



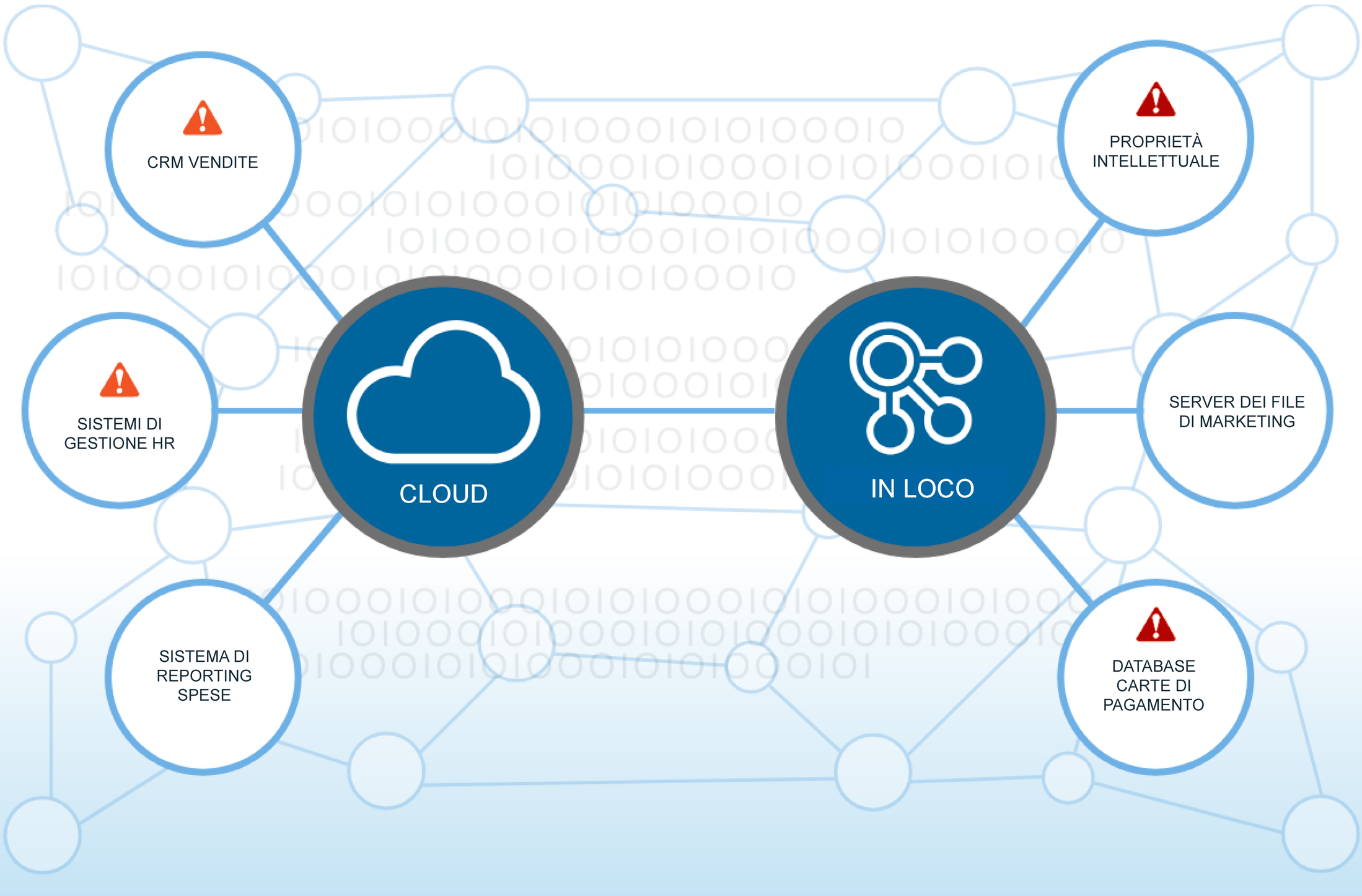
3

Può aiutarti a dare priorità agli attacchi che minacciano i dati e gli asset più importanti?

Il file server utilizzato dal reparto marketing e il database nell'ambiente PCI (Payment Card Industry) comportano livelli di rischio molto diversi se compromessi. È fondamentale poter contare su un sistema in grado di interpretare correttamente il valore dei tuoi asset, di dare automaticamente la priorità alle minacce in base al rischio aziendale e di segnalare i pericoli quando necessario.

> *Una buona soluzione per la sicurezza informatica deve riuscire a interpretare la rete correttamente. Deve dare la possibilità di definire i tuoi asset, i segmenti di rete e i servizi cloud più sensibili e utilizzare analytics per personalizzare gli alert in base ai rischi del tuo ambiente specifico.*

“ Per individuare una violazione della sicurezza servono in media *191* giorni. Altri *66* giorni sono necessari per contenerla.



4

Il tuo sistema automatizza i processi per aumentare la tua produttività?

Vista la mancanza di professionisti rispetto alla domanda di mercato, la maggior parte dei team di sicurezza informatica soffre di carenza di personale. Una buona soluzione SIEM mette a disposizione funzioni di intelligenza artificiale e automazione per contribuire a eliminare i processi manuali. I sistemi SIEM moderni sono in grado di aumentare la produttività senza la necessità di aumentare il personale.

> *La soluzione SIEM ideale aiuta ad automatizzare i processi di rilevamento, assegnazione delle priorità e investigazione. Deve essere in grado di offrire modalità di integrazione predefinite con sistemi di risposta agli incidenti e gestione dei problemi che accelerano i processi di contenimento, risoluzione e ripristino.*

> ***Il 70%* dei professionisti della sicurezza informatica dichiara che le carenze nelle competenze del personale hanno influito negativamente sulla loro organizzazione.**

> **Entro il 2020, il numero delle posizioni aperte nel settore della sicurezza informatica salirà a *1,5 milioni,* rispetto a *1 milione* di posti di lavoro disponibili 2 anni fa.**

5

Quanto è facile iniziare e integrare il sistema nel tuo ambiente?

Scopri quali metodi di implementazione sono supportati. Una buona soluzione SIEM dovrebbe offrire sufficiente flessibilità per adeguarsi alle tue esigenze, che si tratti di hardware, software o di soluzioni SaaS (Software as a Solution). Successivamente, prima di poter sfruttare le potenzialità del sistema SIEM, è necessario trasferire i dati. Chiedi se il sistema è compatibile con tutti i tuoi sistemi esistenti, inclusi gli asset on-premises, le applicazioni SaaS e gli ambienti cloud pubblici.

È importante considerare la semplicità di integrazione non solo in relazione alle sorgenti di log ma anche rispetto alle soluzioni complementari, come feed con informazioni sulle minacce, scanner per la vulnerabilità, strumenti di gestione delle risposte agli eventi e sistemi di gestione dei problemi, per citarne solo alcune. Un ecosistema aperto per app e integrazioni aiuta a rimanere aggiornati e a reagire velocemente all'evoluzione dei rischi e delle minacce. Maggiore il numero di integrazioni predefinite, minore il numero di ore lavorative necessarie per ottenere valore.

“ Le aziende utilizzano normalmente *75* prodotti di sicurezza per proteggere la propria rete che devono interagire insieme.

I criminali informatici si stanno facendo più furbi. E questo ci porta ad un'ulteriore domanda: sei pronto?

Le soluzioni SIEM moderne non si limitano alla gestione dei log e ai processi manuali. Con 200.000 minacce alla sicurezza giornaliere, la protezione deve essere immediata. Una buona soluzione SIEM dovrebbe essere in grado di rilevare una serie di minacce e di indicatori di minacce come attacchi di phishing, malware, furto d'identità, movimenti laterali ed estrapolazione dei dati, per fare solo alcuni esempi, e di segnalare il problema prima che si verifichino danni. Ma è importante ricordare questo: non tutte le soluzioni SIEM sono uguali.

Cerchi una soluzione che:

- Offre funzionalità di analytics sulla sicurezza avanzate per la rilevazione di una vasta gamma di minacce
- Assegna automaticamente la priorità alle minacce e agli alert, per individuare i dati che contano veramente
- Fornisce integrazioni predefinite con i tuoi sistemi
- Consolida i dati sulla sicurezza e le analisi in un'unica piattaforma e interfaccia
- Fornisce capacità di implementazione scalabile, dalle piccole alle più grandi realtà.
- È sufficientemente flessibile da supportare il metodo di deployment preferito, che si tratti di un sistema on-premise, SaaS o cloud pubblico.

Informazioni su IBM QRadar

La piattaforma IBM® QRadar Security Intelligence è una soluzione completa di security analytics che riunisce in un'unica piattaforma funzioni di gestione dei log, analytics avanzati, analisi del network, gestione delle vulnerabilità, analisi del comportamento degli utenti, threat intelligence e investigazioni delle minacce con funzioni di intelligenza artificiale; il tutto gestibile da un'unica interfaccia.

I componenti della soluzione sono completamente integrati per permettere ai clienti di iniziare in piccolo o in grande e di ampliare o ridimensionare la soluzione in base alle esigenze. Con oltre 500 integrazioni predefinite validate e regole pre-configurate, i clienti possono cominciare a utilizzare la soluzione velocemente e possono aggiungere con facilità nuove funzionalità attraverso IBM Security App Exchange.

Per ulteriori informazioni accedere al link: www.ibm.com/qradar.

Riferimenti

Investigazione delle minacce con Watson for Cyber Security, **IBM**

IBM X-Force 2016 Cyber Security Intelligence Index, **IBM**

Ponemon Institute: 2017 Cost of Data Breach Study: Global Overview, **IBM**

La carenza di competenze nella sicurezza informatica crea squilibri nelle assunzioni., **CSO**

Le posizioni aperte nel settore della sicurezza informatica saliranno a 1,5 milioni entro il 2021, **ISC**

La vera difesa: smettere di spendere, cominciare a consolidare, **CSO**

IBM Security

IBM Italia S.p.A
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato da IBM in qualsiasi momento. Non tutte le offerte sono disponibili in ogni paese in cui IBM opera.

Gli esempi di clienti citati hanno un puro scopo illustrativo. Le prestazioni effettive possono variare in base alle specifiche configurazioni e condizioni operative. È responsabilità dell'utente valutare e verificare il funzionamento di altri prodotti o programmi insieme a prodotti o programmi IBM. LE INFORMAZIONI PRESENTI IN QUESTO DOCUMENTO VENGONO FORNITE COSÌ COME SONO, SENZA ALCUNA GARANZIA, ESPRESSA O IMPLICITA, DI ALCUN TIPO, NEANCHE COMMERCIALE, INCLUDENDO TRA QUESTE ANCHE L'IDONEITÀ PER UN FINE PARTICOLARE O QUALSIASI VIOLAZIONE DI DIRITTI DI TERZI. I prodotti IBM sono garantiti secondo i termini e le condizioni dei contratti in base ai quali vengono forniti.

Riciclare

39015239-ITIT-00