



# RAFFORZARE LA STRATEGIA DI SICUREZZA INFORMATICA DEI DATI IN TRE FASI



CHAMPION  
GUIDE

EBOOK

# SOMMARIO

- 3** Introduzione
- 4** Fase 1: assumere il controllo dei dati
- 6** Fase 2: condurre la ricerca proattiva delle minacce su tutti i dati
- 7** Fase 3: promuovere la collaborazione con il team dati
- 9** Conclusione: un programma di sicurezza informatica di successo richiede una strategia legata ai dati moderna
- 10** Informazioni su Snowflake

# INTRODUZIONE

## Le organizzazioni di sicurezza possono sfruttare gli investimenti nella piattaforma dati esistente per affrontare meglio le minacce e ridurre i rischi per l'azienda.

È possibile risolvere con un migliore accesso ai dati una contraddizione del valore di miliardi di dollari nel settore della cybersecurity? Secondo **Gartner**<sup>®</sup>, nel 2021 sono stati spesi in tutto il mondo 150,4 miliardi di dollari per tecnologie e servizi di sicurezza e gestione dei rischi delle informazioni. Solo 15 anni fa, la spesa era di soli 3,5 miliardi di dollari, secondo quanto riportato da **Cybersecurity Ventures**. Eppure, le violazioni della sicurezza informatica hanno raggiunto livelli record e la posta in gioco non è mai stata così alta. **IBM** stima che oggi una singola violazione dei dati sia arrivata a costare alle organizzazioni, in media, 4,2 milioni di dollari, la cifra più alta mai raggiunta nei 17 anni in cui IBM ha segnalato episodi di violazione dei dati.

Questa contraddizione tra investimenti ed esito è il risultato della crescente asimmetria tra gli autori delle minacce e i team di difesa informatica. Gli autori delle minacce si sono rapidamente adattati alle tendenze aziendali, come l'infrastruttura cloud dinamica, le supply chain con software interconnessi e una forza lavoro che opera in gran parte al di fuori del perimetro dell'ufficio. Approfittano della portata e della complessità dei loro target per ottenere l'accesso e rimangono inosservati fino a quando non raggiungono i loro scopi. I team di sicurezza, nel frattempo, cercano perlopiù di comprendere il nuovo ambiente aziendale e il panorama delle minacce utilizzando soluzioni obsolete.

Mentre chi si occupa di difesa informatica rimaneva indietro nella corsa alla messa in sicurezza delle aziende, altri reparti si evolvevano grazie all'innovazione nel moderno stack di dati. Di conseguenza, è emersa l'opportunità per gli addetti ai sistemi di difesa di scavalcare i loro avversari trattando la sicurezza informatica come un problema di dati. Le organizzazioni di sicurezza informatica di successo saranno quelle che riusciranno a mobilitare i dati senza vincoli di fonti o tempo e sfruttando appieno le ultime funzionalità di piattaforme dati e analytics.

Il cuore di questa nuova strategia è un data lake di sicurezza centralizzato, reso possibile da una moderna cloud data platform. Un data lake di sicurezza consente alle organizzazioni di eliminare i tradizionali limiti di visibilità e costi legati alla quantità di dati che è possibile caricare, archiviare e conservare, e per quanto tempo. È fondamentale anche il supporto per i linguaggi di analisi standard, come SQL e Python, per abilitare la collaborazione tra analisti della sicurezza come esperti in materia, analisti di dati per il reporting self-service e data scientist per i modelli comportamentali e il machine learning. Inoltre, i controlli di accesso granulari e la condivisione sicura dei dati, che abilitano la collaborazione all'interno di un'organizzazione, tra aziende del settore e con provider di dati esterni, sono tutti aspetti critici dei moderni data lake di sicurezza.

Nelle pagine seguenti, descriveremo le tre fasi di una transizione di successo a una strategia di sicurezza informatica data-driven.

# FASE 1: ASSUMERE IL CONTROLLO DEI DATI

Controllo dei dati significa libertà: libertà di caricare e conservare tutti i dati desiderati, libertà di analizzare i data set recenti e storici e libertà di scegliere quali soluzioni di sicurezza supportano la missione di proteggere la propria azienda.

## LA SFIDA: GLI STRUMENTI SIEM TRADIZIONALI LIMITANO LA LIBERTÀ E IL CONTROLLO DEI DATI

La maggior parte dei team di sicurezza utilizza una soluzione SIEM per il rilevamento delle minacce e la risposta agli incidenti. Il SIEM è la fonte di verità per il programma di sicurezza. Tuttavia, i SIEM legacy sono integrati verticalmente e richiedono l'uso dei database proprietari incorporati. Non sorprende che questi strumenti non siano riusciti a tenere il passo con le prestazioni e la scalabilità delle cloud data platform generaliste e operino come uno stack di dati indipendente per la sicurezza informatica, separato dal resto dell'azienda.

Di conseguenza, i team addetti alla sicurezza devono confrontarsi con analisi rudimentali e silos di dati frammentati. Talvolta si possono ricercare alcuni dati di sicurezza, ma non è possibile combinarli facilmente con dati contestuali, come dati aziendali o qualsiasi altra informazione che fornisca ai team di sicurezza un contesto più ampio riguardo a una potenziale minaccia. I dati di sicurezza da soli non sono sufficienti per poter valutare in modo approfondito le potenziali minacce.

Inoltre, gli elevati costi di licenza degli strumenti SIEM tradizionali costringono gli utenti a memorizzare altrove un numero sempre maggiore di dati relativi alla sicurezza, soprattutto in bucket cloud che risolvono solo il problema dello storage. Questo approccio introduce processi complicati e oneri aggiuntivi quando i data set devono essere integrati per l'analisi, allunga i tempi di risposta durante una violazione e inoltre non supporta i casi d'uso chiave, come la ricerca proattiva e il lavoro di intelligence sulle minacce. Le sfide legate alla governance dei dati aggravano la proliferazione incontrollata dei dati sotto forma di livelli di storage autogestiti.



## LA SOLUZIONE: UN DATA LAKE DI SICUREZZA CENTRALIZZATO BASATO SU CLOUD

Un moderno data lake di sicurezza è un archivio in cui i log e altri data set vengono memorizzati in un sistema di archiviazione in cloud economico e quasi illimitato, in cui possono essere analizzati rapidamente. I moderni data lake sono progettati per fornire un accesso centralizzato e sicuro ai dati di un'organizzazione. Centralizzando i dati relativi alla sicurezza in un'unica piattaforma, si possono ottenere tanti vantaggi immediati, tra cui:

- **La possibilità di caricare e conservare petabyte di log degli eventi a costi contenuti**
- **L'opportunità di integrare i dati di sicurezza con i dati aziendali e delle applicazioni per contestualizzare e quindi automatizzare le operazioni di sicurezza**
- **La libertà di condurre indagini senza sapere in anticipo quali siano i record di dati attinenti o senza dover recuperare dati storici da vecchi archivi**
- **La possibilità di controllare quali fornitori hanno accesso a quali data set**
- **La flessibilità necessaria per migrare le soluzioni di sicurezza senza dover spostare i dati raccolti**

Un moderno data lake di sicurezza può consentire a utenti di tutta l'azienda di accedere alla stessa unica fonte di riferimento per più casi d'uso di cybersecurity: rilevamento e risposta alle minacce, gestione delle vulnerabilità, automazione della conformità e reporting dei rischi al consiglio di amministrazione.

Oltre a promuovere e accelerare le iniziative relative ai programmi di sicurezza, un moderno data lake di sicurezza può generare risparmi di costi ed efficienza del budget. Uno storage economico con compressione a riposo implica una riduzione dei costi di archiviazione. Ancora più significativa è la potenza di elaborazione elastica e quasi infinita delle principali cloud data platform che elimina la necessità di sovradimensionare le risorse. Le piattaforme che combinano l'elaborazione elastica con il pricing a consumo consentono ai clienti di pagare solo le risorse di cui hanno bisogno, quando ne hanno bisogno. Nel contesto della sicurezza informatica, in cui spesso è necessaria una minima potenza di elaborazione, ma talvolta ne serve molta, questo modello libera il budget di sicurezza per altri usi.

L'implementazione di un moderno data lake di sicurezza basato sul cloud può rivelarsi rivoluzionaria per un'organizzazione. Ospitando i dati in un'unica piattaforma, i team di sicurezza hanno l'opportunità di semplificare lo stack tecnologico, consolidare diversi archivi di dati e attivare l'analisi avanzata per più casi d'uso. Le funzioni di governance e il controllo centralizzato costituiscono una barriera di protezione, mentre le opportunità di collaborazione sui dati consentono ai team di sicurezza operanti di lavoro di portare a termine con successo iniziative di importanza critica per molti anni a venire.



# FASE 2: CONDURRE LA RICERCA PROATTIVA DELLE MINACCE SU TUTTI I DATI

Con un panorama delle minacce in rapida evoluzione, le aziende dipendono sempre più da terze parti nella loro supply chain e nell'infrastruttura basata su SaaS. Per mitigare il rischio per le aziende, è necessario adottare una posizione di "presunta violazione". Purtroppo, la maggior parte dei team di sicurezza sceglie un approccio "guscio duro, cuore morbido" per cui le minacce che superano i sistemi di difesa iniziali possono persistere per mesi all'interno dell'ambiente. Questo pericoloso status quo è in gran parte il risultato delle limitazioni imposte dalle soluzioni SIEM legacy.

## LA SFIDA: GLI INVESTIGATORI DELLE MINACCE NON HANNO ACCESSO AI DATI E ALLE ANALISI DI CUI HANNO BISOGNO

Mentre il rilevamento delle minacce di base può essere eseguito in tempo reale man mano che vengono raccolti i registri degli eventi, i rilevamenti avanzati e la ricerca proattiva delle minacce richiedono la combinazione di data set con origini e intervalli di tempo differenti. Gli autori delle minacce, soprattutto una volta che sono riusciti a penetrare nell'ambiente, hanno un grande vantaggio e molti luoghi per nascondersi. Questo è ciò che rende gli investigatori delle minacce così potenzialmente preziosi per i programmi di sicurezza aziendali.

Purtroppo, la ricerca proattiva delle minacce non può avere successo se non è possibile rispondere a determinate domande. Quando i dati sono separati e isolati in diversi sistemi di origine, bloccati in un cold storage o persi a causa delle politiche di conservazione aziendali, gli investigatori delle minacce non possono utilizzarli. Gli investigatori delle minacce rimangono bloccati anche quando le loro query richiedono ore, quando le loro ricerche restituiscono criptici errori di "memoria esaurita" o hanno conflitti di risorse con altri team.

Infine, la maggior parte dei prodotti di sicurezza legacy limita le query ai linguaggi di ricerca proprietari o alle tecniche grep/regex rudimentali. Questo introduce una curva di apprendimento per i nuovi membri del team e impedisce agli investigatori delle minacce di esprimere correttamente le loro ipotesi come codice.

## LA SOLUZIONE: OFFRIRE AGLI INVESTIGATORI DELLE MINACCE UNA CLOUD DATA PLATFORM CHE SUPPORTA L'ANALISI SU LARGA SCALA

Un'architettura dati costruita sul cloud che si basa su un data lake di sicurezza e riesce a smantellare i silos di dati è fondamentale per consentire la ricerca proattiva delle minacce. Una volta stabilita un'architettura di questo tipo, gli analisti della sicurezza possono iniziare rapidamente a individuare le minacce latenti tramite tecniche di analisi universali standard. Con un motore di query sufficientemente performante, gli investigatori delle minacce possono lavorare su dati raccolti nel giro di mesi o addirittura anni dell'ordine dei petabyte.

Anche gli addetti alle operazioni di sicurezza meno esperti possono collaborare con i data analyst aziendali. Sebbene i data analyst non sarebbero mai in grado di ricercare proattivamente le minacce in un ambiente di sicurezza altamente specializzato, sono abili nel trasformare la logica aziendale in linguaggio SQL all'interno della piattaforma dati aziendale, come vedremo in seguito.

Gli ulteriori vantaggi della ricerca delle minacce derivano dall'uso di cloud data platform che offrono un data marketplace con prodotti di intelligence sulle minacce. I data marketplace basati sulla moderna tecnologia di data sharing possono consentire ai fornitori di intelligence sulle minacce e agli istituti di ricerca di pubblicare indicatori di compromissione (IOC) e altri prodotti di intelligence per un consumo quasi istantaneo. I team addetti alla sicurezza che utilizzano i feed di intelligence in questo modo sono in grado di applicare automaticamente IOC aggiornati ai dati di log. Gli investigatori delle minacce e gli strumenti di automazione possono così individuare in maniera affidabile gli utenti malevoli senza dover integrare API o ricercare manualmente gli indicatori in un portale.

Questo approccio potenzia la ricerca proattiva delle minacce dimostrando la grande opportunità rappresentata dall'allineamento della cybersicurezza alla strategia legata ai dati dell'intera azienda: con l'emergere di nuove capacità e metodologie di analisi dei dati, gli addetti ai sistemi di difesa accorceranno sempre di più il vantaggio degli utenti malevoli.

# FASE 3: PROMUOVERE LA COLLABORAZIONE CON IL TEAM DATI

Nella maggior parte delle aziende, il team dati è il gruppo che cresce più rapidamente. Data analyst, data engineer e data scientist sono ruoli fondamentali per il marketing, il dipartimento finanziario e altre funzioni dell'organizzazione. Oggi, i responsabili della sicurezza stanno mettendo in atto tecnologie e processi che consentono di rilevare le minacce e ridurre i rischi grazie alla collaborazione tra i team addetti alla sicurezza e i team dati.

## LA SFIDA: I TEAM DI SICUREZZA DEDICANO TROPPO TEMPO A OPERAZIONI NON CORRELATE ALLA SICUREZZA, COME LA RACCOLTA DEI DATI E IL REPORTING

Se un team è oberato di lavoro nell'intento di stare al passo con gli autori degli attacchi, non deve perdere tempo su qualcosa che non richiede le sue competenze specifiche. Aniché smistare gli avvisi o analizzare le minacce, molti team di sicurezza dedicano gran parte del tempo alla ricerca di dati, all'aggiornamento di fogli di calcolo o al ripristino di cluster utilizzati per la ricerca.

La sicurezza svolge, inoltre, un ruolo importante nelle certificazioni e nei controlli che le aziende devono eseguire per poter vendere i loro prodotti ai clienti. Questo può diventare un grosso onere quando comporta riunioni fiume tra i team di sicurezza informatica e le parti interessate dei settori conformità, IT, DevOps e la leadership aziendale.

Dopo trent'anni e due approcci molto diversi all'abilitazione di un'analisi dei dati efficace è nata la moderna piattaforma dati, che riunisce la potenza del data warehouse tradizionale, la flessibilità delle soluzioni per i big data e l'elasticità del cloud a una frazione del costo delle soluzioni precedenti.



## LA SOLUZIONE: CREARE UNA PARTNERSHIP TRA ANALISTI DELLA SICUREZZA E PROFESSIONISTI DEI DATI PERCHÉ PROTEGGANO INSIEME L'AZIENDA

Osserviamo i diversi modi in cui gli esperti di sicurezza impiegano il proprio tempo. Quali attività non richiedono le loro competenze specializzate? Tra queste attività, quali sono quelle principalmente dedicate alla preparazione, all'analisi o al reporting dei dati? È importante coinvolgere i colleghi responsabili della gestione dei dati in un confronto aperto su queste aree di collaborazione.

Ad esempio, la raccolta dei record delle risorse umane per l'arricchimento durante il rilevamento e la risposta è un'attività di pipeline dati meglio eseguita dai data engineer. Per i data analyst è semplice valutare l'applicazione delle patch di sicurezza rispetto alle prestazioni previste dagli SLA. Inoltre, avendo a disposizione i log delle attività, i data scientist possono facilmente identificare i trasferimenti di file insoliti.

L'integrazione dei dati di sicurezza con il resto dell'organizzazione crea la base della collaborazione tra i team di sicurezza e i professionisti che si occupano di dati. Questa collaborazione può migliorare notevolmente la capacità di un'organizzazione di ottenere analytics di sicurezza altamente affidabili, utilizzando al meglio i talenti esistenti all'interno dell'azienda.

I report BI (Business Intelligence) self-service possono risultare un ottimo modo per eliminare le riunioni ed evitare il coinvolgimento degli addetti alla sicurezza nei processi aziendali di routine. Ad esempio, un tipico programma di gestione delle patch può coinvolgere i tecnici addetti alla sicurezza, che valuteranno i risultati in termini di rischio di vulnerabilità, e gli analisti della conformità, che definiranno le priorità per la risoluzione dei problemi emersi. Tale prioritizzazione potrebbe basarsi sulla sede del problema (ambiente di produzione customer-facing o sandbox interno) e sul tempo trascorso dall'individuazione iniziale. Queste considerazioni sono il frutto di strutture di conformità a cui l'azienda deve attenersi per continuare a fornire il servizio ai clienti.

I dashboard interattivi che applicano logica aziendale e data set contestuali ai problemi di sicurezza in modo automatizzato e tempestivo possono consentire di correggere i problemi senza necessità di partecipare a riunioni. Gli aggiornamenti dello stato vengono eliminati quando una persona autorizzata visualizza lo stato più recente nello strumento BI aziendale. I data analyst se ne occupano regolarmente per altri reparti, il che consente di avviare la trasformazione digitale nell'organizzazione di sicurezza.

Questo approccio trasforma la sicurezza informatica da una pratica compartimentata e reattiva in una più ampia forma di collaborazione per risolvere i problemi con soluzioni basate sui dati.

# CONCLUSIONE: UN PROGRAMMA DI SICUREZZA INFORMATICA DI SUCCESSO RICHIEDE UNA STRATEGIA LEGATA AI DATI MODERNA

Abbiamo descritto tre fasi comprovate per portare la strategia di sicurezza informatica dei dati a un livello superiore. Questa strategia è essenziale per proteggere dalle minacce informatiche un'organizzazione moderna e basata sul cloud.

Per avere successo, gli analisti della sicurezza hanno bisogno di un moderno data lake di sicurezza, che utilizzi una cloud data platform e sia offerto come servizio per poter accedere rapidamente ai dati rilevanti in una posizione centrale. Ciò vale tanto per le grandi imprese globali quanto per le startup in rapida evoluzione. Anche un solo evento di violazione potrebbe distruggere qualsiasi tipo di organizzazione.

Ricorda che i team di sicurezza informatica non devono più lavorare da soli, senza le competenze e gli strumenti per i dati oggi presenti praticamente in tutte le aziende. I responsabili della sicurezza possono gettare le basi per consentire al proprio team di sfruttare le competenze di altre parti dell'organizzazione e concentrarsi quindi sugli aspetti della sicurezza informatica che nessun altro può gestire.

Seguendo i tre passaggi descritti in questo ebook, potrai passare da una gestione reattiva della sicurezza informatica al progressivo supporto di approcci proattivi, come l'investigazione delle minacce e il reporting self-service. Nel corso del tempo, con un approccio data-driven la tua organizzazione di sicurezza informatica potrà raggiungere il suo pieno potenziale e tradurre gli investimenti nella sicurezza in maggiore tranquillità per la tua azienda e i suoi clienti.





# INFORMAZIONI SU SNOWFLAKE

Snowflake permette a ogni organizzazione di mobilitare i propri dati grazie al Data Cloud. I clienti utilizzano il Data Cloud per unificare i dati contenuti nei silos, esplorare e condividere i dati in totale sicurezza, potenziare le applicazioni basate sui dati, ed eseguire diversi workload di AI/ML e analitici. Ovunque siano i dati o gli utenti, Snowflake offre un'esperienza sui dati unica che si estende a più cloud e aree geografiche. Migliaia di clienti di ogni settore, tra cui 590 della classifica 2022 Forbes Global 2000 (G2K) al 30 aprile 2023, utilizzano il Data Cloud di Snowflake per far crescere le loro aziende. Scopri di più su [snowflake.com](https://www.snowflake.com)



© 2022 Snowflake Inc. Tutti i diritti riservati. Snowflake, il logo Snowflake e tutti gli altri nomi di prodotti, funzioni e servizi Snowflake menzionati nel presente documento sono marchi o marchi registrati di Snowflake Inc. negli Stati Uniti e in altri Paesi. Tutti gli altri nomi di marchi o loghi menzionati o usati nel presente documento sono a puro scopo identificativo e possono essere marchi registrati dei rispettivi proprietari. Snowflake non può essere associato, sponsorizzato o sostenuto da tali proprietari.

---

## NOTE

<sup>1</sup> Secondo Gartner, la spesa per la sicurezza e la gestione dei rischi a livello mondiale supererà i 150 miliardi di dollari nel 2021

<sup>2</sup> La spesa globale per la sicurezza informatica supererà 1,75 trilioni di dollari nel periodo 2021-2025