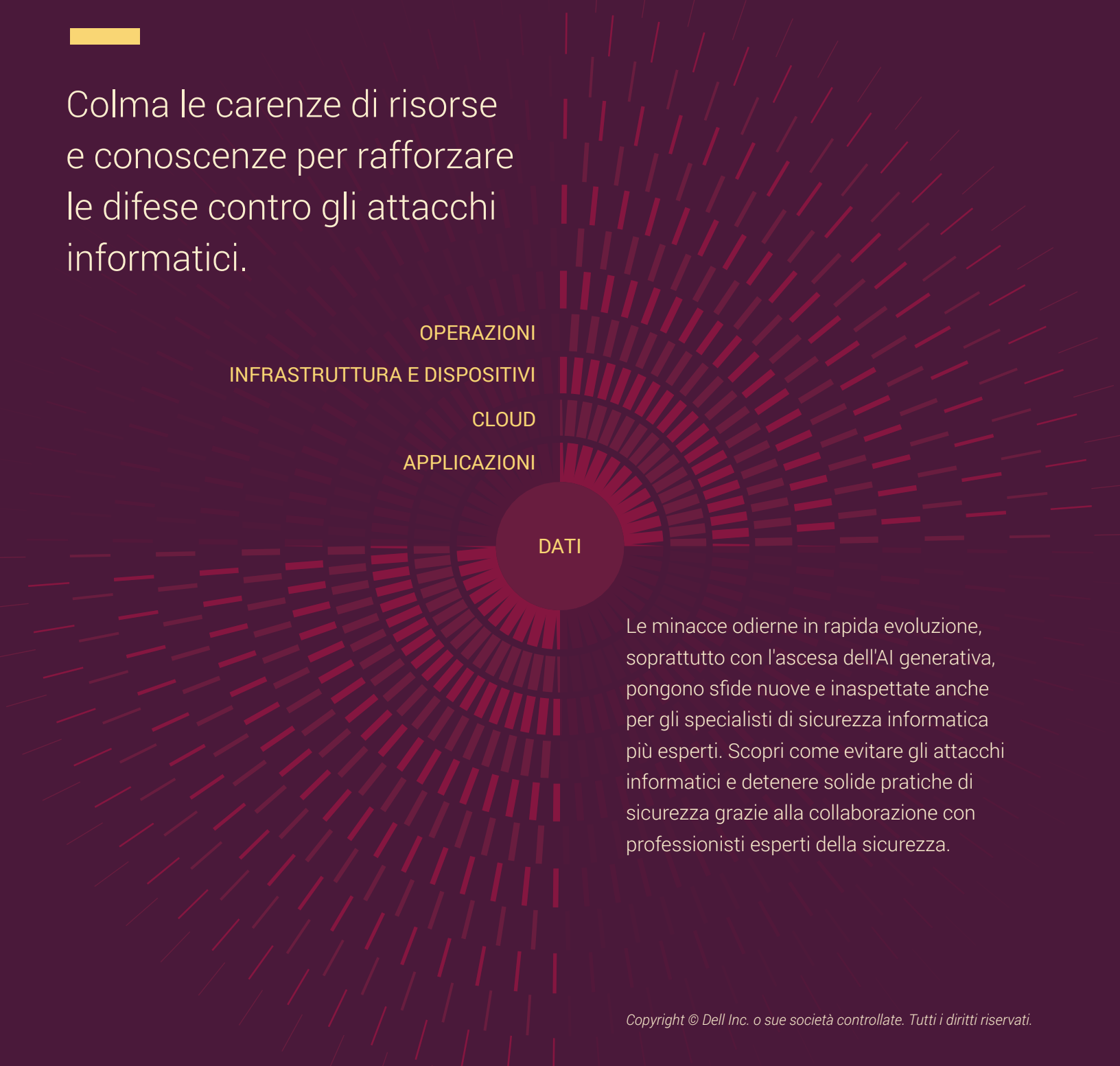
DELL Technologies

Migliorare la sicurezza informatica e la maturità Zero Trust.

Colma le carenze di risorse e conoscenze per rafforzare le difese contro gli attacchi informatici.



Le minacce odierne in rapida evoluzione, soprattutto con l'ascesa dell'AI generativa, pongono sfide nuove e inaspettate anche per gli specialisti di sicurezza informatica più esperti. Scopri come evitare gli attacchi informatici e detenere solide pratiche di sicurezza grazie alla collaborazione con professionisti esperti della sicurezza.

Le minacce informatiche sono come un'invasione di formiche

Ti liberi della prima e ne arriva subito un'altra.

In un mondo sempre più interconnesso, in cui le organizzazioni si affidano molto alle infrastrutture digitali e i dati sono diventati un bene di vasta portata, è meglio presumere che un aggressore esperto abbia già violato l'ambiente IT.

Per fortuna abbiamo a disposizione partner esperti specializzati nell'incontro tra tecnologia e sicurezza informatica.

Dell Technologies apporta soluzioni innovative e competenze preziose, non sempre disponibili internamente, utili per conoscere il panorama delle minacce in continua evoluzione.

- Sicurezza hardware e software
- Informazioni approfondite sui rischi emergenti
- Comprensione delle tecniche di attacco avanzate
- AIOps per rispondere alle minacce in rapida evoluzione
- Nuove strategie di sicurezza e best practice

Metti in campo difese su più livelli per migliorare costantemente le pratiche di sicurezza e adotta l'approccio Zero Trust.

Dell Technologies è partner per la sicurezza informatica e offre Professional Services completi, soluzioni hardware e software e un ecosistema di partner solido che limita le possibilità di attacco, individua le vulnerabilità e le riduce al minimo e ti supporta nel ripristinare rapidamente le operazioni di business.

Riduzione della superficie di attacco →

Rilevamento e risposta alle minacce informatiche →

Ripristino rapido dopo un attacco →

Edge **Core** **Multicloud**

Professional Services

Ecosistema di partner aziendali e tecnologici **Supply chain sicura**

DELL Technologies

Riduzione della superficie di attacco

Potenzia le difese e diventa un bersaglio più difficile da colpire limitando le vie d'accesso preferite dai criminali informatici.

Per rafforzare il profilo di sicurezza è necessario individuare e ridurre al minimo le vulnerabilità e i punti di ingresso che compromettono applicazioni, sistemi o reti in vari ambienti, tra cui l'edge, il core e il cloud.

IDENTIFICA le vulnerabilità

- Vulnerabilità del software
- Configurazioni errate
- Meccanismi di autenticazione deboli
- Sistemi sprovvisti di patch
- Privilegi utente eccessivi
- Porte di rete aperte
- Scarsa sicurezza fisica

IMPLEMENTA misure preventive

- Collaborazione con fornitori sicuri
- Applicazione della segmentazione di rete completa
- Isolamento dei dati critici
- Rigorosi controlli degli accessi
- Aggiornamento e patch a sistemi e applicazioni
- Individuazione e risoluzione delle vulnerabilità con l'AI, oltre a valutazioni e test periodici

Adozione dell'approccio Zero Trust

Con l'architettura Zero Trust, l'organizzazione diffida in automatico di tutto ciò che si trova al suo interno o all'esterno. Quindi, procede a verificare tutto quello che tenta di connettersi ai sistemi prima di concedergli l'accesso. Questo modello è istituito e prescritto dal Dipartimento della Difesa degli Stati Uniti e include **7 pilastri correlati** che sviluppano in modo sistematico la maturità.

1. Fiducia degli utenti
2. Affidabilità dei dispositivi
3. Fiducia nei dati
4. Applicazioni e carichi di lavoro
5. Rete e ambienti
6. Visibilità e analisi
7. Automazione e orchestration

DELL Technologies

Riduzione della superficie di attacco

Identifica i punti deboli che compromettono i sistemi prima che si verifichino problemi.

La sicurezza informatica è un percorso costante, non una meta singola. Verifiche periodiche, test di penetrazione e valutazioni delle vulnerabilità, con il supporto di un partner per i servizi di sicurezza esperto, sono utili per identificare le carenze e colmarle, riducendo i rischi.

Procedure sicure della supply chain	La sicurezza entra in gioco prima di quanto immagini. Crea una base affidabile avvalendoti di dispositivi e infrastrutture progettati, realizzati e forniti con supply chain e ciclo di vita per lo sviluppo sicuri, nonché modellazione rigorosa delle minacce.
Sicurezza integrata	Lavora con dispositivi e infrastrutture dotati di sicurezza integrata e basata sull'hardware, progettata per individuare e contrastare gli attacchi prima che provochino danni.
Applicazione di patch e aggiornamenti regolari	Risolvi le vulnerabilità note e riduci al minimo i rischi di utilizzo mantenendo aggiornate le applicazioni, il firmware e i sistemi operativi con le più recenti patch di sicurezza.
Privilegi minimi	Limita gli account utente e di sistema concedendo i diritti di accesso minimi necessari per l'esecuzione delle loro attività. Questo approccio limita l'impatto potenziale dell'accesso non autorizzato da parte degli aggressori.
Segmentazione della rete	Isola gli asset critici per limitare l'accesso alla rete utilizzando la segmentazione di rete moderna per i dati critici, i gruppi aziendali e le applicazioni. La segmentazione contiene gli attacchi impedendo il movimento laterale.
Sicurezza delle applicazioni	Implementa pratiche di codifica sicure, conduci regolarmente test di sicurezza, esamina periodicamente il codice e utilizza firewall per le applicazioni web allo scopo di facilitare la protezione dagli attacchi comuni a livello di applicazione e ridurre la superficie di attacco delle applicazioni web.
Professional Services e partnership	Collabora con fornitori di servizi di sicurezza informatica e costituisci partnership con partner aziendali e tecnologici per usufruire di competenze e soluzioni non sempre disponibili internamente.
Sensibilizzazione e formazione degli utenti	Prevedi attività di formazione per dipendenti e utenti affinché riconoscano e segnalino potenziali minacce alla sicurezza, tentativi di phishing e tattiche di social engineering. In questo modo riduci al minimo i rischi che sfruttano le vulnerabilità umane.

DELL Technologies

Rilevamento e risposta alle minacce informatiche

Le prassi di sicurezza di vecchio stampo sono come l'Internet Dial-up, troppo lente e inefficaci nella realtà esigente di oggi.

Per contrastare le minacce informatiche sofisticate, è necessario disporre di un vero e proprio asso nella manica per la sicurezza, come AI e ML, da integrare nelle applicazioni e nelle metodologie che identificano gli elementi noti e quelli sconosciuti, per poi rispondergli.

Implementa potenti sistemi di rilevamento e di prevenzione delle intrusioni

Sfrutta l'AI e l'ML per rilevare le anomalie

Predisponi il monitoraggio in tempo reale del traffico di rete e del comportamento degli utenti

Migliora la resilienza collaborando con Professional Services esperti per acquisire competenze specializzate.

In qualità di partner tecnologico esperto, Dell Technologies ti supporta per definire protocolli proattivi di risposta agli incidenti e relativo ripristino, che delineano ruoli e responsabilità e garantiscono comunicazione e coordinamento ottimali tra i componenti.

Migliora la capacità di rilevare e rispondere in modo proattivo alle minacce informatiche utilizzando strumenti avanzati come:

- Threat Intelligence
- Risposta agli incidenti
- Gestione delle informazioni e degli eventi di sicurezza
- Protezione degli endpoint
- Analisi comportamentale

Favorisci il ripristino rapido ed efficiente e riduci al minimo la perdita di dati con:

- Piano di risposta agli incidenti e collaborazione ben definiti
- Backup regolari di dati e sistemi critici
- Soluzioni di storage off-site sicure e crittografia dei dati

DELL Technologies

Rilevamento e risposta alle minacce informatiche

Resta in guardia e intervieni rapidamente.

Rilevare e rispondere alle minacce informatiche significa restare all'erta e prepararsi allo scenario peggiore. Predisponi un piano di risposta e ripristino in costante aggiornamento, provando regolarmente ad applicarlo, in modo che l'intera organizzazione sappia come limitare gli effetti degli attacchi. Si tratta di un processo continuo e iterativo che richiede una combinazione di tecnologie, personale qualificato, processi ben definiti e collaborazione tra team.

Monitoraggio continuo	Strumenti di sicurezza come i sistemi di rilevamento delle intrusioni, i sistemi di prevenzione delle intrusioni, l'analisi dei registri e la Threat Intelligence sono utili per individuare segni di accessi non autorizzati, intrusioni, infezioni da malware e violazioni dei dati.
Rilevamento delle minacce	Analizza i dati sfruttando l'AI e il ML per individuare schemi, anomalie e indicatori di compromissione, possibili indici della presenza di una minaccia. I vantaggi includono il riconoscimento delle firme di attacco note e dei comportamenti devianti.
Avvisi e notifiche	Predisponi avvisi tempestivi per avviare prontamente indagini e interventi. Attiva avvisi e notifiche bolla in superficie per azioni rapide con sicurezza integrata. Alimenta la telemetria a livello di dispositivo, al di sopra del sistema operativo, per accelerare il rilevamento delle minacce e mobilitare il personale addetto alla sicurezza o un Centro operativo di sicurezza (SOC) quando si rilevano potenziali minacce o incidenti.
Risposta agli incidenti	Avvia un piano di risposta per analizzare e mitigare gli incidenti di sicurezza confermati. Il piano prevede il contenimento dell'impatto, l'identificazione della root cause e l'implementazione delle azioni necessarie per ripristinare i sistemi ed evitare ulteriori danni.
Analisi forense	Conduci l'analisi dettagliata degli incidenti per comprendere la metodologia di attacco, determinare la portata della violazione, individuare i sistemi o i dati interessati e raccogliere prove per scovare le carenze di sicurezza e colmarle.
Correzione e ripristino	Adotta misure per correggere le vulnerabilità, applicare patch ai sistemi, rimuovere malware e implementare misure di sicurezza potenziate per evitare incidenti simili. Ripristina allo stato normale i sistemi e i dati colpiti dall'attacco per completare il processo di ripristino.

DELL Technologies

Ripristino dagli attacchi informatici

Schiaccia l'acceleratore e torna subito in pista con il tuo business.

La cyber-resilienza è necessaria nel mondo odierno basato sui dati ed è richiesta sia dai clienti che dai partner. Per assicurarne il successo, sono necessari più livelli di protezione, che garantiscono la salvaguardia e l'isolamento dei dati critici, in modo da ripristinarli rapidamente e in tutta sicurezza dopo un attacco. Valuta la tua cyber-resilienza ›

- Intervieni per attenuare i danni causati dagli attacchi informatici
- Ricostituisci i servizi e i dispositivi compromessi o interrotti
- Analizza l'incidente per evitare attacchi futuri
- Rispetta gli SLA aziendali e riporta le operazioni alla normalità

Predisponi una strategia di sicurezza informatica completa affinché la tua organizzazione effettui il ripristino in modo efficace ed efficiente.

Il ripristino dopo un attacco informatico richiede sforzi coordinati che coinvolgono team IT, professionisti della sicurezza informatica, responsabili della gestione e, in alcuni casi, esperti esterni. La chiave per il ripristino è il rapido ritorno alla normalità dei sistemi e delle operazioni, traendo al contempo informazioni dall'incidente per ridurre le interruzioni e il downtime, ripristinare i servizi e l'integrità dei dati, ridurre al minimo l'impatto finanziario e relativo all'immagine dell'organizzazione e rafforzare la sicurezza informatica per evitare attacchi simili in futuro.

- Valuta l'impatto dell'attacco sulle operazioni aziendali
- Dai priorità ai servizi critici
- Implementa sistemi per la protezione dei dati
- Comunica eventuali progressi relativi all'incidente e al ripristino
- Sviluppa un piano e garantisci la continuità esercitandoti ad applicarlo il più possibile

DELL Technologies

Ripristino dagli attacchi informatici

Torna operativo riattivando sistemi, reti e dati dopo un incidente.

Predisporre una strategia di cyber-resilienza implica integrare persone, processi e tecnologie in un framework olistico che protegge l'intera organizzazione.

Contenimento degli incidenti

Il primo passo è isolare e contenere l'impatto dell'attacco informatico. Per questo è necessario disconnettere dalla rete i sistemi colpiti, disabilitare gli account compromessi e implementare misure per evitare ulteriori danni o l'espansione dell'attacco.

Ripristino dei sistemi o dei dispositivi

Una volta contenuto l'incidente, le reti e i sistemi colpiti sono ripristinati a uno stato pulito e sicuro. È possibile che ciò comporti la ricostituzione dei sistemi compromessi, la reinstallazione dei software, l'applicazione di patch di sicurezza e l'esecuzione di aggiornamenti. In alcuni casi, l'automazione e il self-healing svolgono un ruolo significativo nel ripristinare lo stato di operatività.

Ripristino dei dati

È necessario ripristinare i dati che sono stati, eventualmente, compromessi, crittografati o eliminati durante l'attacco. È possibile effettuarne il ripristino dai backup o ricorrere a tecniche specifiche apposite per recuperare i file persi o crittografati.

Analisi forense

Dopo un attacco è fondamentale comprendere come si è verificata la violazione, quali vulnerabilità sono state sfruttate e quali misure occorre attuare per evitare attacchi simili. Sistemi come la Gestione delle informazioni e degli eventi di sicurezza (Security Information and Event Management, SIEM) e funzionalità come il confronto tra BIOS esterni all'host forniscono informazioni utili.

Valutazione della risposta agli incidenti

Dopo il ripristino è essenziale valutare il processo di risposta agli incidenti e individuare gli aspetti da migliorare. Le informazioni apprese dall'attacco sono utili per migliorare le procedure di sicurezza, aggiornare i piani di risposta agli incidenti e fornire migliore protezione contro gli incidenti futuri.

Professional Services e partnership

I fornitori di servizi di sicurezza informatica e i partner tecnologici mettono a disposizione competenze e risorse preziose utili alla tua organizzazione per effettuare il ripristino. Offrono supporto con attività come l'analisi forense, la determinazione della frequenza delle violazioni e la proposta di misure per prevenire gli incidenti futuri.

DELL Technologies

Estensione della sicurezza informatica agli ambienti edge e cloud

Con la diffusione delle reti dal core all'edge fino al cloud, gli ambienti sono diventati un punto cruciale delle vulnerabilità.

Nel potenziamento della strategia di sicurezza informatica, l'organizzazione dovrebbe estendere i principi di Zero Trust all'edge e al cloud per garantire rigorosi controlli degli accessi, autenticazione continua, oltre a visibilità e controllo completi sul traffico di rete. Con l'evolversi della gamma di minacce è fondamentale implementare le funzionalità dell'AI come prima linea di difesa. Inoltre, la strategia è completa solo se gli ambienti core di rete e cloud dispongono di misure di sicurezza, come la segmentazione della rete, la crittografia e il monitoraggio continuo.

Adozione di un approccio olistico con i Professional Services per la sicurezza informatica.

Collegare varie soluzioni di sicurezza è una sfida. Collaborare con i Professional Services specializzati nella sicurezza dell'edge, del core e del cloud ti garantisce le competenze necessarie per attuare misure efficaci che proteggano l'organizzazione sotto ogni aspetto.

Edge

Definisci più livelli di sicurezza nell'edge, nella rete e all'interno di hardware e software.

Core

Allinea l'infrastruttura all'approccio Zero Trust tramite l'AI, l'ML e l'automazione.

Multicloud

Proteggi qualsiasi carico di lavoro in ogni ambiente, inclusi public cloud, container e carichi di lavoro nativi per il cloud.

DELL Technologies

AI generativa: un'arma a doppio taglio per la sicurezza informatica

L'AI di nuova generazione ci conduce rapidamente verso il miglioramento della sicurezza, ma anche verso nuovi rischi.

L'AI generativa, prossima evoluzione dell'AI, prevede sistemi in grado di comprendere, imparare, adattare e implementare le conoscenze in una serie di attività.

Da un lato, promette un miglioramento di rilevamento delle minacce e risposta, funzionalità predittive ed efficienza operativa. Dall'altro, pone nuove sfide che richiedono strategie di sicurezza informatica in evoluzione, capaci di affrontare i rischi attraverso misure di sicurezza efficaci, monitoraggio costante, aggiornamenti e applicazione di patch periodici e un approccio in continua evoluzione alla riservatezza dei dati e all'etica.

Protezione delle organizzazioni con l'AI generativa

Sbloccando nuove possibilità di protezione delle organizzazioni, l'AI generativa è diventata un alleato fondamentale nella sicurezza informatica.

- Rilevamento delle minacce e risposta più efficaci.
- Previsione delle minacce future o identificazione delle potenziali vulnerabilità.
- Automatizzazione del rilevamento delle minacce ed efficienza.
- Analisi forense per individuare rapidamente schemi, anomalie e indicatori di compromissione.
- Formazione personalizzata per la sensibilizzazione alla sicurezza.
- Scalabilità delle operazioni di sicurezza con accesso più rapido a informazioni più approfondite.

Protezione dei sistemi di AI generativa

Sebbene l'AI generativa offra notevoli vantaggi in termini di sicurezza, in assenza di protezioni adeguate le sue funzionalità sono soggette ad applicazioni malevole.

- Garantisci la riservatezza e l'integrità dei dati.
- Mitiga gli attacchi avversari progettati per ingannare i sistemi di AI che provocano malfunzionamenti.
- Rileva gli usi impropri del sistema derivanti dall'AI malevola e intervieni.
- Verifica e mitiga i problemi etici e i preconcetti.
- Implementa controlli degli accessi efficaci per i sistemi di AI.
- Proteggi e ripristina in modo sicuro i modelli linguistici di grandi dimensioni.

La sicurezza informatica moderna dovrebbe essere intelligente, scalabile e automatizzata

Dell Technologies ti offre il proprio supporto per mettere in campo una sicurezza completa che ti protegga dalle minacce informatiche in evoluzione. Con l'avanzamento della tecnologia, il nostro approccio alla sicurezza informatica resta un passo avanti, sfruttando la potenza dell'AI e del ML per proteggere le infrastrutture digitali e preservare la fiducia nel mondo digitale. Indipendentemente dal punto in cui ti trovi nel percorso della sicurezza informatica, lavoriamo con te per andare oltre la semplice protezione dell'organizzazione, con azioni utili a garantirti agilità e resilienza.

DELL Technologies

Dell.com/SecuritySolutions

Richiedi di essere contattato

Apri una chat con un consulente per la sicurezza

Chiama il numero 1-800-433-2393