

# Ripristino dagli attacchi informatici

Ripristina l'operatività in modo efficace ed efficiente dopo gli incidenti.

## Una strategia completa per il ripristino della sicurezza comprende

L'attenuazione dell'impatto dell'attacco



La ricostruzione dei servizi e dei dispositivi compromessi



Il ripristino delle operazioni



L'analisi e l'acquisizione di informazioni utili dall'incidente

## Operazioni per l'avanzamento della sicurezza informatica

### 1 Contenimento dell'incidente

Disconnetti dalla rete i sistemi colpiti dall'attacco, disabilita gli account compromessi e impedisce ulteriori danni.

### 2 Ripristino del sistema o dei dispositivi

Ricostituisci i sistemi compromessi, reinstalla il software, applica patch di sicurezza ed esegui gli aggiornamenti.

### 3 Ripristino dei dati

Ripristina i dati dai backup oppure applica tecniche specifiche per il ripristino dei dati, in modo da recuperare i file persi o criptati.

### 4 Analisi forense

Esamina le modalità di attacco e le vulnerabilità sfruttate per evitare incidenti futuri.

### 5 Valutazione della risposta agli incidenti

Una volta effettuato il ripristino, valutane il processo per individuare gli aspetti da migliorare.

### 6 Utilizzo dell'AI/ML

Accelera il ripristino individuando rapidamente i sistemi e i dati colpiti dall'attacco e automatizza il processo di ripristino dai backup.

Il ripristino dopo un attacco informatico richiede sforzi di gruppo.

### Professional Services e partnership

I partner per la sicurezza informatica offrono competenze e risorse preziose:

- Analisi forense
- Individuazione dell'origine della violazione
- Misure per scongiurare incidenti futuri

Scopri di più sull'implementazione di una strategia di sicurezza informatica completa.

[Esplora l'eBook](#) →