REPORT SULLA MISURAZIONE DELL'EFFICACIA DEI CONTROLLI

Introduzione

Il rischio delineato prevede che insider malintenzionati possano modificare le configurazioni per compromettere la confidenzialità, l'integrità e la disponibilità dei servizi aziendali, con conseguenze potenzialmente gravi come incidenti di sicurezza, divulgazione di dati, manipolazione e disservizi. Questi eventi possono avere impatti significativi sulla produttività, sulla reputazione aziendale, sui costi di risposta e recupero, e sulla posizione competitiva dell'organizzazione.

Questo report si concentra sul rischio specifico legato alla manipolazione intenzionale delle configurazioni dei dispositivi di sicurezza di rete, come firewall (FW), sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS), da parte di utenti autorizzati.

Scelta dei KRI

Per affrontare il rischio legato agli insider malintenzionati, è stata implementata una strategia di monitoraggio basata su indicatori chiave di rischio (KRI). Questi KRI sono suddivisi in due categorie principali: lead indicators (indicatori preventivi) e lag indicators (indicatori di risultato).

I lead KRI aiutano a identificare segnali precoci di potenziali minacce, consentendo interventi tempestivi, mentre i lag KRI forniscono una valutazione delle conseguenze di incidenti già verificatisi, aiutando a misurare l'efficacia delle misure di sicurezza esistenti.

I KRI individuati per questo scenario sono i seguenti:

Lead KRI:

- **Numero di tentativi di accesso falliti ai dispositivi di sicurezza:** Un aumento può indicare tentativi di accesso non autorizzato imminente.
- **Numero di accessi amministrativi fuori dall'orario di lavoro:** Potrebbe segnalare attività sospette che potrebbero portare a un attacco.

Lag KRI:

- **Tempo medio di rilevazione e risposta agli incidenti di sicurezza:** Misura il tempo impiegato per identificare e rispondere agli incidenti dopo che si sono verificati.
- **Numero di modifiche alle policy di sicurezza senza autorizzazione preventiva:** Controlla le modifiche alle policy di sicurezza che sono state effettuate precedentemente senza previa autorizzazione.

ID	Nome	Descrizione	Metrica	Tipo
KRI-1				Lead
KRI-2	Numero di tentativi di accesso falliti ai dispositivi di sicurezza	Monitorare il numero di tentativi falliti ai dispositivi di sicurezza	Numero di tentativi di accesso falliti	Lead
KRI-3	Numero di accessi amministrativi fuori dall'orario di lavoro	Monitorare il numero di accessi amministrativi fuori dall’orario di lavoro	Numero di accessi amministartivi fuori orario	Lead
KRI-4	Tempo medio di rilevazione degli incidenti di sicurezza	Calcolare una stima del tempo medio di rilevazione degli incidenti basandosi su report storici	Tempo medio necessario per rilevare gli incidenti	Lag

ID	Nome	Descrizione	Metrica	Tipo
KRI-5	Numero di modifiche alle policy di sicurezza senza autorizzazione preventiva	Controllare le modifiche alle policy di sicurezza apportate e verificarne l'autorizzazione	Numero di modifiche effettuate senza autorizzazione	Lag