Imposta criteri di prevenzione della perdita dei dati personalizzati per rilevare i numeri di previdenza sociale formattati e non formattati

Sommario

Introduzione

In questo documento viene descritto come impostare criteri di prevenzione della perdita dei dati personalizzati per rilevare numeri di previdenza sociale (SSN) formattati e non formattati su Cisco Email Security Appliance (ESA).

Imposta criteri di prevenzione della perdita dei dati personalizzati per rilevare i numeri di previdenza sociale formattati e non formattati

In base alla progettazione, il motore di scansione DLP rileva solo i numeri di previdenza sociale formattati. Ciò è dovuto all'elevato livello di falsi positivi causati da numeri a 9 cifre contenuti nei dati utilizzati da varie industrie. I numeri di registrazione ABA della banca, ad esempio, sono a 9 cifre e vengono attivati quando si cerca un codice fiscale non formattato. Di conseguenza, è consigliabile evitare la ricerca di numeri di previdenza sociale non formattati, a meno che non sia strettamente richiesto dall'organizzazione. Se è necessario che l'organizzazione esegua la ricerca di numeri di previdenza sociale non formattati, è possibile creare criteri di prevenzione della perdita dei dati personalizzati eseguendo la procedura indicata nella soluzione seguente.

AsyncOS offre la possibilità di creare criteri personalizzati da zero utilizzando classificatori sviluppati da RSA o dall'organizzazione. Questa opzione è considerata avanzata e deve essere utilizzata solo nei rari casi in cui i modelli di criteri predefiniti non soddisfano i requisiti specifici dell'ambiente di rete.

Creare un criterio personalizzato

1. Dalla GUI: **Mail Policies > DLP Policy Manager**.
2. Fare clic su **Aggiungi criteri di prevenzione della perdita dei dati...** pulsante.
3. Selezionare **Criterio personalizzato** nella parte inferiore della schermata e fare clic su **Aggiungi** accanto a Criterio personalizzato.
4. Immettere il nome di un criterio di prevenzione della perdita dei dati. Ad esempio: *Criterio personalizzato SSN*.

Creare un classificatore

La creazione di classificatori personalizzati offre una grande flessibilità rispetto ai criteri digitalizzati nel motore DLP. Questa funzionalità verrà utilizzata per la ricerca di SSN formattati e non formattati.

1. Dall'elenco a discesa Classificatore corrispondenza contenuto, selezionare **Crea classificatore** e fare clic sul pulsante **Aggiungi**.
2. Immettere il nome di un classificatore di corrispondenza contenuto. Ad esempio: *Tutti i formati SSN.*
3. Nella sezione Regole impostare l'elenco a discesa Parole o Frasi su **Entità**.
4. Selezionare l'entità: **Codice fiscale USA, formattato**.
5. Fare clic su **Aggiungi regola**.
6. Selezionare nuovamente **Entità**.
7. Selezionare l'entità: **Numero previdenza sociale USA, non formattato**.
8. Fare clic su **Invia**.

Impostazione delle impostazioni di gravità

Le seguenti impostazioni rappresentano un buon punto di partenza, ma rappresentano solo una linea guida per l'utente e potrebbero richiedere alcune impostazioni di calibrazione o di configurazione alternative in base alle esigenze dell'organizzazione.

- **Impostazioni gravità critica**
  Azione applicata ai messaggi: **Quarantena**
  Abilita crittografia (selezionata)
  Regola di crittografia: **Usa sempre crittografia messaggi**
  Profilo crittografia (selezionare il profilo di crittografia configurato dall'elenco a discesa)
  Oggetto messaggio crittografato: **$oggetto**
- **Impostazioni alta gravità**
  Azione applicata ai messaggi: **Consegna**
  Abilita crittografia (selezionata)
  Regola di crittografia: **Usa sempre crittografia messaggi**
  Profilo crittografia (selezionare il profilo di crittografia configurato dall'elenco a discesa)
  Oggetto messaggio crittografato: **$oggetto**
- **Impostazioni gravità media**
  Azione applicata ai messaggi: *Consegna*
  Abilita crittografia (selezionata)

Regola di crittografia: **Usa crittografia messaggi solo se TLS non riesce**
Profilo crittografia (selezionare il profilo di crittografia configurato dall'elenco a discesa)
Oggetto messaggio crittografato: **$oggetto**

- **Impostazioni bassa gravità**
  Azione applicata ai messaggi: **Consegna**
  Abilita crittografia (deselezionata)

Impostazione della scala di gravità

Anche in questo caso, le seguenti impostazioni rappresentano un buon punto di partenza, ma sono semplicemente una linea guida per l'utente e potrebbero richiedere alcune impostazioni di calibrazione o di configurazione alternative in base alle esigenze dell'organizzazione.

1. A destra del diagramma della scala di gravità fare clic su **Modifica scala**.
2. Far scorrere la prima maniglia fino a quando IGNORE = 0.
3. Far scorrere la seconda maniglia fino a quando LOW = da 1 a 9.
4. Far scorrere la terza maniglia fino a quando MEDIUM = da 10 a 50.
5. Far scorrere la quarta maniglia fino a quando HIGH = da 60 a 89.
6. Se l'impostazione è corretta, il valore CRITICAL verrà impostato automaticamente su un valore compreso tra 90 e 100.
7. Al termine, fate clic su **Fatto (Done)**.

Invia e conferma modifiche

Per completare la creazione del criterio, fare clic sul pulsante **Invia**. Fare clic sul pulsante **Commit Changes** nell'angolo superiore destro dell'interfaccia utente. Verrà visualizzata la schermata Modifiche di cui non è stato eseguito il commit. Fare clic su **Commit modifiche**. In caso di esito positivo, nell'angolo superiore destro della GUI **non** dovrebbe essere visualizzata **alcuna modifica** in **sospeso**.

Operazioni finali

Ènecessario abilitare i criteri di prevenzione della perdita dei dati per un criterio di posta in uscita in **Criteri posta ->Criteri posta in uscita**. Per il test al di fuori della produzione è possibile creare un criterio personalizzato in uscita con se stessi designati come mittente e abilitare i criteri di prevenzione della perdita dei dati in questo criterio di test.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems