Stel een aangepast DLP-beleid in om geformatteerde en niet-geformatteerde socialezekerheidsnummers te detecteren

Inhoud

Inleiding

Dit document beschrijft hoe u een aangepast DLP-beleid kunt instellen om geformatteerde en niet-geformatteerde socialezekerheidsnummers (SSN) op de Cisco Email Security Appliance (ESA) te detecteren.

Stel een aangepast DLP-beleid in om geformatteerde en niet-geformatteerde socialezekerheidsnummers te detecteren

Door het ontwerp van de DLP-scanmachine worden alleen geformatteerde socialezekerheidsnummers gedetecteerd. Dit is het gevolg van het hoge aantal valse positieven veroorzaakt door 9-cijferige getallen in gegevens die door verschillende industrieën worden gebruikt. Zo zijn de ABA-routingnummers voor banken bijvoorbeeld 9-cijfers en zullen deze geactiveerd worden tijdens het scannen voor een niet-geformatteerd socialezekerheidsnummer. Als zodanig wordt u aangeraden om niet te scannen op niet-geformatteerde socialezekerheidsnummers, tenzij dit strikt noodzakelijk is voor uw organisatie. Als het vereist is dat uw organisatie scant voor niet-geformatteerde Sociale Veiligheidsnummers, kunt u een aangepast DLP beleid creëren door de stappen te volgen die in de onderstaande oplossing worden geleverd.

AsyncOS biedt de optie om uw eigen beleid vanaf nul te creëren met behulp van classificators die door RSA of uw organisatie zijn ontwikkeld. Deze optie wordt als geavanceerd beschouwd en dient alleen in de zeldzame gevallen te worden gebruikt wanneer de vooraf gedefinieerde beleidssjablonen niet voldoen aan de unieke vereisten van uw netwerkomgeving.

Een aangepast beleid maken

1. Vanuit de GUI: **Mail Policy > DLP Policy Manager**.
2. Klik op het **DLP-beleid toevoegen...** -toets.
3. Selecteer **Aangepast beleid** onder in het scherm en klik op **Toevoegen** naast Aangepast beleid.
4. Voer een DLP-beleidsnaam in. Bijvoorbeeld: *Aangepast beleid van SSN*.

Een Classifier maken

Het creëren van aangepaste classificatoren geeft u grote flexibiliteit over de gescande criteria in de DLP-motor. We zullen dit in ons voordeel gebruiken om te scannen op zowel geformatteerd SSN als niet-geformatteerd SSN.

1. Selecteer in de vervolgkeuzelijst Content Matching Classifier **een Classifier maken** en klik op de knop **Add**.
2. Voer een overeenkomende Classifier-naam in. Bijvoorbeeld: *N Alle formaten.*
3. Stel onder het gedeelte Regels de uitrollijst in van woorden of zinnen naar **entiteit**.
4. Selecteer de entiteit: **US Social Security Number, opgemaakt**.
5. Klik op **Regel toevoegen**.
6. Selecteer nogmaals **Entiteit**.
7. Selecteer de entiteit: **US Social Security Number, ongeformatteerd**.
8. Klik op **Inzenden**.

Instellingen ernst instellen

De volgende instellingen zijn een goed startpunt, maar ze zijn slechts een richtlijn om u te helpen en het kan zijn dat er instellingen voor een calibratie of alternatieve configuratie nodig zijn, afhankelijk van de behoeften van uw organisatie.

- **Ernstige kritieke instellingen**
  Actie toegepast op berichten: **Quarantine**
  Encryptie inschakelen (gecontroleerd)
  Encryptieregel: **Gebruik altijd een berichtencryptie**
  Encryptieprofiel (selecteer uw geconfigureerde encryptieprofiel in de vervolgkeuzelijst)
  Onderwerp versleuteld bericht: **$ subject**
- **Instellingen hoge prioriteit**
  Actie toegepast op berichten: **leveren**
  Encryptie inschakelen (gecontroleerd)
  Encryptieregel: **Gebruik altijd een berichtencryptie**
  Encryptieprofiel (selecteer uw geconfigureerde encryptieprofiel in de vervolgkeuzelijst)
  Onderwerp versleuteld bericht: **$ subject**
- **Instellingen gemiddelde ernst**
  Actie toegepast op berichten: *leveren*
  Encryptie inschakelen (gecontroleerd)
  Encryptieregel: **Alleen berichtencryptie gebruiken als TLS mislukt**

Encryptieprofiel (selecteer uw geconfigureerde encryptieprofiel in de vervolgkeuzelijst)
Onderwerp versleuteld bericht: **$ subject**

- **Instellingen lage ernst**
  Actie toegepast op berichten: **leveren**
  Encryptie inschakelen (ongecontroleerd)

De schaal van de ernst instellen

Opnieuw zijn de volgende instellingen een goed startpunt, maar ze zijn slechts een richtlijn om u te helpen en kunnen enige calibratie of alternatieve configuratie instellingen nodig hebben die zijn gebaseerd op de behoeften van uw organisaties.

1. Klik rechts van het schema van de ernst van de schaal op **Schaal bewerken**.
2. Schuif de eerste hendel tot IGNORE = 0.
3. Schuif de tweede hendel tot LOW = 1 tot 9.
4. Schuif de derde handgreep tot MEDIUM = 10 tot 50.
5. Schuif de vierde hendel tot HOOG = 60 tot 89.
6. Als u dit correct hebt ingesteld, wordt CRITICAL automatisch ingesteld op 90 tot 100.
7. Klik op **Gereed** als het programma klaar is.

Wijzigingen indienen en beloven

Klik op de knop **Indienen om** de aanmaak van dit beleid te voltooien. Klik de knop **Wijzigingen** aan **het** woord in de rechterbovenhoek van de GUI aan. U wordt naar het scherm Ongecommitteerde Veranderingen gebracht, klik op **Commit Veranderingen**. Indien geslaagd dient u **geen wijzigingen** te zien in de rechterbovenhoek van de GUI.

Eindstappen

U moet nu het DLP-beleid voor een vertrekkend postbeleid **per e-mail** inschakelen**.>Uitgaande postbeleidsmaatregelen**. Voor testen buiten de productie kunt u een aangepast uitgaand beleid maken met uzelf als zender aangewezen en het DLP-beleid voor dit testbeleid mogelijk maken.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems