Realtime DLP-problemen oplossen met Cisco Secure Access

Inhoud

inleiding

In dit document worden de stappen beschreven voor het oplossen van problemen met Inline of Realtime Data Loss Prevention (DLP) binnen de Secure Web Gateway (SWG)-omgeving.

Voorwaarden en waarschuwingen

- HTTPS-inspectie: Zorg ervoor dat HTTPS-inspectie is ingeschakeld. DLP kan geen gecodeerd verkeer scannen. Zorg ervoor dat de website wordt gedecodeerd met Cisco Secure Access Root CA of aangepaste CA.
- QUIC-protocol: Schakel het QUIC-protocol in alle browsers uit. QUIC maakt gebruik van UDP, die de SWG omzeilt en DLP-scanning voorkomt.
- IPv6: Schakel IPv6 uit als het verkeer de SWG niet raakt, omdat de functionaliteit voor dubbele stapels bypasses moet veroorzaken.
- Beveiligingsbeleid: Zorg ervoor dat de toegangsregel "Toestaan – Beveiliging overschrijven" of "Isolatie" niet is ingeschakeld.

Overzicht

Inline DLP is een uitgebreide scanfunctie van de SWG. Het controleert of blokkeert het uploaden van gevoelige, vertrouwelijke of persoonlijk identificeerbare gegevens in bestanden die zijn geüpload via de SWG-proxy. Klanten maken gegevensclassificaties met behulp van door Cisco gedefinieerde identificatoren (bijvoorbeeld creditcards of sofinummers) of aangepaste zoekwoorden. Deze classificaties worden toegepast op DLP-beleid dat is toegewezen aan specifieke identiteiten en bestemmingen. De DLP-engine scant alleen HTTP POST-, PUT- en PATCH-methoden.

Algemene controlelijst voor probleemoplossing

Als DLP-detectie niet optreedt, controleert u de onderstaande stappen:

- Connectiviteit: Bevestig dat de client de SWG gebruikt door naar http://policy.test.sse.cisco.com te gaan. Controleer of het juiste SWG-datacenter is toegepast en het testresultaat "protected by Secure Access" (beveiligd door beveiligde toegang) weergeeft.
- Decodering: Zorg ervoor dat SSL-decodering is ingeschakeld in het beveiligingsprofiel. Controleer of er geen selectieve decodering of niet-decoderen lijst uitsluitingen.
- Traffic Steering: Zorg ervoor dat er geen externe domeinomleiding is geconfigureerd in Internet Settings.
- Identiteit: Als DLP-beleid afhankelijk is van Active Directory-groepen, bevestigt u dat de gebruiker lid is van de juiste groep.
- Toepassingsinstellingen: Zorg ervoor dat de compatibiliteitsinstellingen voor Office 365 Bypass of M365 zijn uitgeschakeld als een Microsoft-domein wordt gebruikt voor DLP.
- Activiteit zoeken: gebruik Rapportage > Activiteit zoeken om ervoor te zorgen dat de volledige URL zichtbaar is (gedecodeerd) en de verwachte identiteit is gekoppeld aan het verkeer. Controleer Rapportage > Preventie van gegevensverlies om te controleren of de monitor- of blokactiviteit is geregistreerd.
- Beleidsconfiguratie: controleer of het DLP-beleid is geconfigureerd voor de juiste identiteit en doeltoepassing.
- Testen: gebruik een bekende goede bestemming (bijvoorbeeld pastebin.com of dlptest.com) en een bekende goede teststring uit de Cisco-documentatie.
- Ondersteuningsgegevens: Verzamel een HAR-bestand van de gebruiker om te controleren of het verkeer door de SWG wordt geleid en controleer op SWG-headers.

Problemen met vals negatieven oplossen

Als DLP actief is, maar een specifieke classificator niet kan worden geactiveerd, onderzoekt u de volgende gebieden:

Classifiers, bestanden en tekenreeksen

- Bestandsstatus: Zorg ervoor dat het bestand niet is gecodeerd of niet kan worden gescand. Test met een eenvoudig tekstbestand.
- Drempelwaarden: Controleer de instellingen Drempel en nabijheid in Beleid > Gegevensclassificatie. De classifier kan een hoger aantal hits of nabijheid van een aangepaste string vereisen.
- Regex Patterns: Gebruik een online tool (bijvoorbeeld regexr.com) om patronen te visualiseren. Vereenvoudig het patroon om een kleiner deel van de snaar te vangen en geleidelijk uit te breiden.

Bestandslabels

- Compatibiliteit: detectie van bestandslabels werkt niet voor Confluence of JIRA.
- Metagegevens: Documenteigenschappen openen in een Microsoft-toepassing. De waarde moet exact overeenkomen met het label Umbrella File; dit is hoofdlettergevoelig.
- Codering: labeldetectie werkt niet voor bestanden die met een wachtwoord zijn beveiligd of gecodeerd.

Websites en bestemmingen

- Ondersteunde toepassingen: bekijk de lijst met ondersteunde toepassingen. Voor niet-ondersteunde apps of "Alle bestemmingen" worden alleen specifieke mime-typen gescand.
- Toepassingen doorgelicht: Toepassingen doorgelicht (bijvoorbeeld dlptest.com) worden uitgebreider gescand. Willekeurige websites mogen alleen worden gescand op bestandsovertredingen.
- Bestandsnamen: Het systeem zoekt alleen naar bestandsnamen voor bepaalde doorgelichte toepassingen.

Problemen oplossen met fout-positieven

Als DLP-inhoud onverwacht overeenkomt, controleert u de classificatienaam en de DLP-regel in Rapportage > Preventie van gegevensverlies. Als de detectie legitiem maar ongewenst is, past u de instellingen Drempelwaarden of Nabijheid aan om het beleid te verfijnen.

Ondersteuning voor desktoptoepassingen

Ondersteuning voor desktop-gebaseerde toepassingen (bijvoorbeeld Outlook, Teams of Google Workspace) wordt op basis van best effort geleverd. De effectiviteit hangt af van het berichtformaat dat wordt gebruikt tijdens het uploaden van bestanden, dat kan verschillen tussen webgebaseerde en desktopversies. Voor niet-doorgelichte toepassingen is er geen garantie dat het uploaden van bestanden wordt ondersteund.

DLP Classifier Gotchas

- Creditcardnummers: Het Luhn-algoritme wordt gebruikt voor validatie. Test alleen met geldige creditcardnummers.
- Persoonsnamen: vereist 2-3 woorden en elk woord moet met een hoofdletter worden geschreven.
- Naamcombinaties: Er is een scheidingstekenreeks vereist tussen de naam en andere gegevens (bijvoorbeeld "Viagra - John Smith" komt overeen, maar "Viagra John Smith" niet).
- Geboortedatum: Moet in de buurt zijn van een trefwoord of koptekst zoals "dob" of "geboortedatum".
- Aanstootgevende inhoud: Bepaalde uitzonderingsstrings voorkomen dat deze classifier wordt afgevuurd als de tekst lijkt op een boek of rapport.
- Postcode: Moet zich in de buurt van specifieke locatie-gerelateerde zoekwoorden bevinden.

Exacte gegevensuitwisseling (EDM)

Voordat u EDM onderzoekt, moet u bevestigen dat het algemene DLP-scannen functioneel is. Controleer voor EDM-specifieke problemen of het veld "Laatste bewerking" actueel is in het dashboard en controleer de uitvoer van het indexeringsgereedschap.

Opdrachtgebruik:

Voer het indexeringsgereedschap uit met de optie `-d` om een bloeifilterbestand (.blm) te genereren. Deze opdracht wordt gebruikt om de EDM-index te valideren en om vast te stellen waarom records moeten worden overgeslagen. De `d`-vlag instrueert de tool om het diagnostische bloomfilterbestand uit te voeren, dat moet worden gedeeld met ondersteuning, samen met een voorbeeldbestand of HAR / webontwikkelaarstoolgegevens.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.