Fehlerbehebung bei DLP-Problemen mit Cisco Secure Access in Echtzeit

Inhalt

Einführung

In diesem Dokument werden die Schritte zur Fehlerbehebung bei Inline- oder Echtzeit-DLP-Problemen (Data Loss Prevention) in der SWG-Umgebung (Secure Web Gateway) beschrieben.

Voraussetzungen und Warnungen

- HTTPS-Inspektion: Stellen Sie sicher, dass die HTTPS-Überprüfung aktiviert ist. SvD kann verschlüsselten Datenverkehr nicht scannen. Stellen Sie sicher, dass die Website mit der Cisco Secure Access Root-Zertifizierungsstelle oder einer benutzerdefinierten Zertifizierungsstelle entschlüsselt wird.
- QUIC-Protokoll: Deaktivieren des QUIC-Protokolls in allen Browsern. QUIC verwendet UDP, wodurch die SWG umgangen und DLP-Scans verhindert werden.
- IPv6: Deaktivieren Sie IPv6, wenn der Datenverkehr die SWG nicht erreicht, da die Dual-Stack-Funktion Umgehungen verursachen muss.
- Sicherheitsrichtlinie: Stellen Sie sicher, dass für die Zugriffsregel "Zulassen - Sicherheit außer Kraft setzen" oder "Isolierung" nicht aktiviert ist.

Überblick

Inline-SvD ist eine erweiterte Scan-Funktion der SWG. Es überwacht oder blockiert den Upload sensibler, vertraulicher oder persönlich identifizierbarer Daten in Dateien, die über den SWG-Proxy hochgeladen werden. Kunden erstellen Datenklassifizierungen mithilfe von von von Cisco definierten IDs (z. B. Kreditkarten- oder Sozialversicherungsnummern) oder benutzerdefinierten Schlüsselwörtern. Diese Klassifizierungen werden auf SvD-Policys angewendet, die bestimmten Identitäten und Zielen zugewiesen sind. Die DLP-Engine überprüft nur die Methoden HTTP POST, PUT und PATCH.

Allgemeine Checkliste zur Fehlerbehebung

Wenn keine SvD-Erkennung auftritt, überprüfen Sie die folgenden Schritte:

- Konnektivität: Vergewissern Sie sich unter http://policy.test.sse.cisco.com, dass der Kunde die SWG verwendet. Überprüfen Sie, ob das richtige SWG-Rechenzentrum angewendet wurde und das Testergebnis "protected by Secure Access" (durch sicheren Zugriff geschützt) anzeigt.
- Entschlüsselung: Stellen Sie sicher, dass die SSL-Verschlüsselung im Sicherheitsprofil aktiviert ist. Vergewissern Sie sich, dass keine Ausschlüsse für die selektive Entschlüsselung oder die Liste "Nicht entschlüsseln" vorliegen.
- Verkehrssteuerung: Stellen Sie sicher, dass in den Interneteinstellungen keine externe Domänenumgehung konfiguriert ist.
- Identität: Wenn SvD-Policys auf Active Directory-Gruppen basieren, stellen Sie sicher, dass der Benutzer Mitglied der richtigen Gruppe ist.
- Anwendungseinstellungen: Stellen Sie sicher, dass die Office 365-Bypass- oder M365-Kompatibilitätseinstellungen deaktiviert sind, wenn eine Microsoft-Domäne für SvD verwendet wird.
- Aktivitätssuche: Verwenden Sie Reporting > Activity Search, um sicherzustellen, dass die vollständige URL sichtbar (entschlüsselt) ist und die erwartete Identität mit dem Datenverkehr verknüpft ist. Aktivieren Sie Reporting > Data Loss Prevention, um zu bestätigen, ob Überwachungs- oder Blockierungsaktivitäten protokolliert werden.
- Richtlinienkonfiguration: Überprüfen Sie, ob die SvD-Policy für die richtige Identität und Zielanwendung konfiguriert ist.
- Tests: Verwenden Sie ein zweifelsfrei funktionierendes Ziel (z. B. pastebin.com oder dlptest.com) und eine zweifelsfrei funktionierende Beispieltestzeichenfolge aus der Cisco Dokumentation.
- Support-Daten: Holen Sie eine HAR-Datei vom Benutzer ein, um zu überprüfen, ob der Datenverkehr durch die SWG geleitet wird, und suchen Sie nach SWG-Headern.

Fehlerbehebung bei Fehlalarmen

Wenn der SvD aktiv ist, aber keine bestimmte Klassifizierung ausgelöst wird, untersuchen Sie die folgenden Bereiche:

Klassifizierungen, Dateien und Zeichenfolgen

- Dateistatus: Stellen Sie sicher, dass die Datei nicht verschlüsselt oder nicht gescannt werden kann. Mit einer einfachen Textdatei testen.
- Grenzwerte: Überprüfen Sie die Einstellungen für Grenzwert und Nähe unter Richtlinie > Datenklassifizierung. Die Klassifizierung kann eine höhere Anzahl von Treffern oder die Nähe zu einer benutzerdefinierten Zeichenfolge erfordern.
- Reguläre Muster: Verwenden Sie ein Online-Tool (z. B. regexr.com), um Muster zu visualisieren. Vereinfachen Sie das Muster, um einen kleineren Teil der Zeichenkette zu fangen und allmählich zu erweitern.

Dateibezeichnungen

- Kompatibilität: Die Erkennung von Dateibezeichnungen funktioniert nicht für Confluence oder JIRA.
- Metadaten: Öffnen von Dokumenteigenschaften in einer Microsoft-Anwendung. Der Wert muss genau mit der Umbrella File-Bezeichnung übereinstimmen. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden.
- Verschlüsselung: Die Labelerkennung funktioniert nicht für kennwortgeschützte oder verschlüsselte Dateien.

Websites und Ziele

- Unterstützte Anwendungen: Überprüfen Sie die Liste der unterstützten Anwendungen. Bei nicht unterstützten Apps oder "Alle Ziele" werden nur bestimmte MIME-Typen gescannt.
- Geprüfte Anwendungen: Geprüfte Anwendungen (z. B. dlptest.com) werden umfassender gescannt. Zufällige Websites dürfen nur auf Dateiverletzungen überprüft werden.
- Dateinamen: Das System sucht nur nach Dateinamen für bestimmte geprüfte Anwendungen.

Fehlerbehebung bei Fehlalarmen

Wenn SvD den Inhalt unerwartet erfüllt, überprüfen Sie den Klassifizierungsnamen und die SvD-

Regel in Reporting > Data Loss Prevention. Wenn die Erkennung legitim, aber unerwünscht ist, passen Sie die Einstellungen für "Thresholds" oder "Proximity" an, um die Richtlinie zu verfeinern.

Desktop-Anwendungsunterstützung

Desktop-basierte Anwendungen (z. B. Outlook, Teams oder Google Workspace) werden nach bestem Bemühen unterstützt. Die Effektivität hängt vom Nachrichtenformat ab, das beim Hochladen von Dateien verwendet wird. Dieses kann sich zwischen Web- und Desktop-Versionen unterscheiden. Für nicht geprüfte Anwendungen gibt es keine Garantie, dass Datei-Uploads unterstützt werden.

DLP-Klassifizierung Gotchas

- Kreditkartennummern: Zur Validierung wird der Luhn-Algorithmus verwendet. Führen Sie den Test nur mit gültigen Kreditkartennummern durch.
- Personennamen: Benötigt 2-3 Wörter und jedes Wort muss großgeschrieben werden.
- Namenskombinationen: Zwischen dem Namen und anderen Daten ist eine Trennzeichenfolge erforderlich (beispielsweise stimmt "Viagra - John Smith" überein, "Viagra John Smith" jedoch nicht).
- Geburtsdatum: Muss sich in der Nähe eines Schlüsselworts oder Headers befinden, z. B. "dob" oder "Geburtsdatum".
- Unangenehme Inhalte: Bestimmte Ausnahmezeichenfolgen verhindern, dass diese Klassifizierung ausgelöst wird, wenn der Text einem Buch oder Bericht ähnelt.
- Postleitzahl: Muss sich in der Nähe bestimmter standortbezogener Schlüsselwörter befinden.

Genaue Datenzuordnung (EDM)

Bevor Sie EDM untersuchen, stellen Sie sicher, dass der allgemeine DLP-Scan funktioniert. Prüfen Sie bei EDM-spezifischen Problemen, ob das Feld "Last Edit" (Letzte Bearbeitung) im Dashboard aktuell ist, und überprüfen Sie die Ausgabe des Indextools.

Befehlsverwendung:

Führen Sie das Indexierungstool mit der Option `-d` aus, um eine Blütenfilterdatei (.blm) zu generieren. Mit diesem Befehl wird der EDM-Index validiert, und es wird eine Fehlerbehebung durchgeführt, warum Datensätze übersprungen werden müssen. Das `-d`-Flag weist das Tool an, die diagnostische Bloom-Filterdatei auszugeben, die zusammen mit einer Beispieldatei oder

HAR/Web-Entwicklerwerkzeugdaten an den Support weitergegeben werden soll.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.