Fehlerbehebung: Datenblockierung für Echtzeit-SvD-Formulare für alle Ziele

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Konfiguration einer DLP-Regel (Data Loss Protection) in Echtzeit zum Blockieren aller Formulardaten beschrieben.

Hintergrundinformationen

Wenn eine DLP-Regel in Echtzeit so konfiguriert wird, dass alle Formulardaten blockiert werden, besteht das Risiko, dass sowohl tatsächliche als auch falsche Positiva zu unbeabsichtigten Folgen für Cloud-Anwendungen führen. Diese Folgen können sich auf den erfolgreichen Betrieb von Cloud-Anwendungen auswirken und können dazu führen, dass Benutzer die Anmeldeseite nicht nutzen können. In diesem Artikel werden diese Risiken hervorgehoben und Schritte zur Fehlerbehebung erläutert, um mögliche Probleme zu beheben.

Fehlerbehebung

Bei Problemen mit der Blockierung aller Formulardaten in Echtzeit-DLP-Regeln können die folgenden Schritte bei der Fehlerbehebung und Problemlösung helfen:

1. Daten-IDs verfeinern: Dieser Schritt sorgt für ein Gleichgewicht zwischen der effektiven Blockierung vertraulicher Daten und dem unterbrechungsfreien Durchlassen legitimer Formulardaten.

    - Überprüfen Sie die Details zu gesperrten SvD-Ereignissen über den Bericht Data Loss Prevention (Reporting > Additional Reports > Data Loss Prevention), um die spezifischen Datenkennungen zu identifizieren, die die SvD-Regel auslösen.

    - Erwägen Sie, die Datenkennungen durch Anpassung der Toleranzwerte oder Hinzufügen von Proximity-Begriffen zu verfeinern, um Fehlalarme zu reduzieren, während die Übereinstimmung nach Bedarf erhalten bleibt.

2. Blockierte URLs ausschließen: Durch das Ausschließen von URLs können Sie sicherstellen, dass Anmeldeseiten und andere wichtige Komponenten Ihrer Anwendungen von der Regel

zum Blockieren des SvD nicht betroffen sind.

- Analysieren Sie das Aktivitätsprotokoll über die Aktivitätssuche (Berichte > Kernberichte > Aktivitätssuche) und die SvD-Ereignisdetails, um die URLs zu identifizieren, die blockiert werden.
- Fügen Sie diese URLs einer unter "Select Destination Lists and Applications for Exclusion" (Ziellisten und Anwendungen für Ausschluss auswählen) konfigurierten Zielliste hinzu.

3. Ändern des SvD-Regelverhaltens - Wenn die Probleme weiterhin bestehen und die unbeabsichtigten Folgen die Vorteile der Blockierung aller Formulardaten überwiegen, müssen Sie das Verhalten des SvD ändern, um den Scannen von Formulardaten zu beenden. Das Verhalten kann durch Auswahl von "Datei-Uploads und Formulardaten von geprüften Anwendungen" geändert werden.

Schlussfolgerung

Beim Konfigurieren einer DLP-Regel in Echtzeit zum Blockieren aller Formulardaten ist es wichtig, sich der Risiken bewusst zu sein, die mit unbeabsichtigten Folgen verbunden sind. Diese Risiken können sich auf den reibungslosen Betrieb von Cloud-Anwendungen auswirken und auch die Nutzung der Anmeldeseite beeinträchtigen. Nutzen Sie die in diesem Leitfaden beschriebenen Schritte zur Fehlerbehebung, um diese Risiken zu minimieren und den erfolgreichen Betrieb Ihrer Cloud-Anwendungen sicherzustellen, ohne die Datensicherheit zu beeinträchtigen.

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.