使用DLP监控AWS S3和Azure存储中的敏感数据泄露

目录

简介

本文档介绍如何使用防数据丢失(DLP)监控AWS S3和Azure存储中的敏感数据泄露。

概述

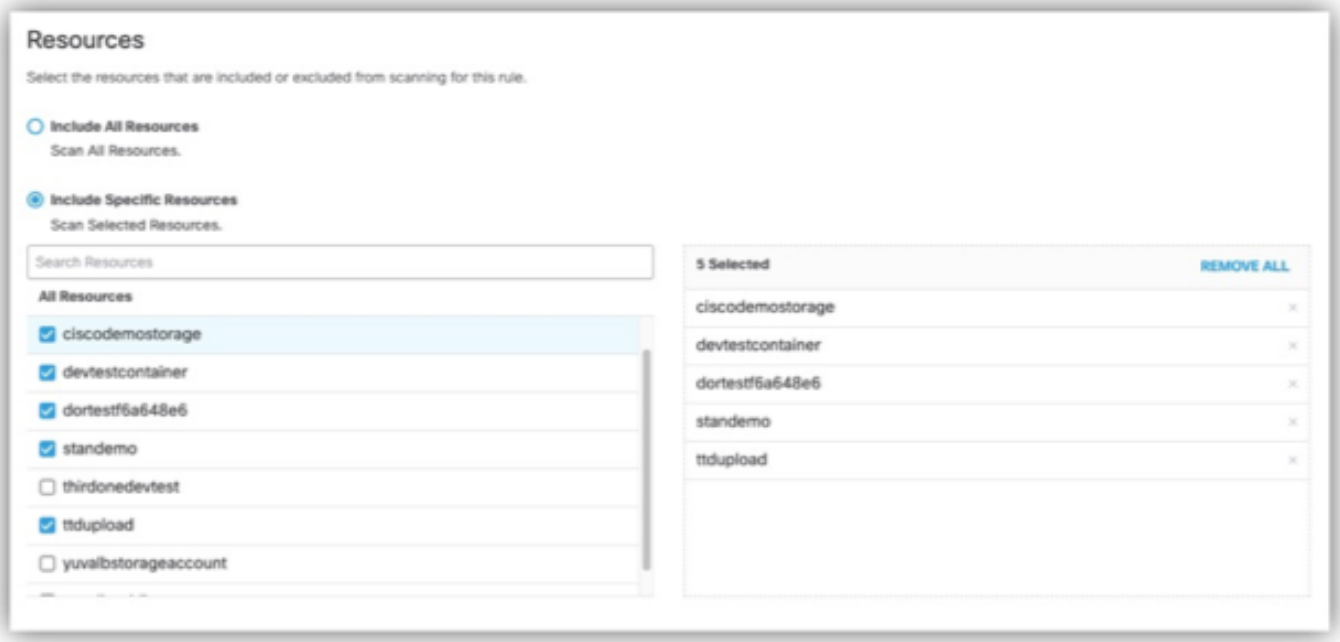
借助适用于AWS S3和Azure存储的新连接器，您现在可以在云环境中扫描敏感数据泄露。这些功能可帮助您发现并监控暴露的凭证（如API密钥、机密和令牌）以及敏感数据，包括可能暴露于公共Web的个人识别信息(PII)、财务记录和医疗保健信息。

在AWS S3和Azure文件存储中扫描哪些内容？

- AWS S3:
  DLP对预先存在的敏感数据执行初始发现扫描，并对新文件或更新文件执行持续监控。可以通过在DLP规则中选择要扫描的S3存储段。

- Azure文件存储：
  DLP支持新文件或更新文件的初始发现和持续监控。你可以选择要在DLP规则内扫描的特定Azure容器。

您可以通过选择精确的AWS S3存储桶或Azure容器来定制DLP扫描，以满足您的需求和优先级。



AWS和Azure支持的响应操作

目前，仅支持监控作为AWS S3和Azure存储的响应操作。自动补救操作（如文件删除或隔离）不可用。此方法可避免中断任务关键型IaaS环境的风险，同时仍允许您有效地监控敏感数据的泄露。

查找AWS S3 Buckets和Azure Storage Blob以进行手动补救

为协助手动修复，DLP报告包含详细信息：

- 报告显示实际的S3存储桶或blob名称，便于在AWS或Azure控制台中搜索。
- 每个DLP违规事件都会提供资源名称、目标URL以及资源ID（如果可用）。
- 使用此信息在AWS S3存储桶和Azure存储Blob中高效地定位和处理DLP违规。

相关资源

有关详细指导，请参阅Umbrella文档：

- 为AWS租户启用SaaS API数据丢失保护
- 为Azure租户启用SaaS API数据丢失保护
- 将SaaS API规则添加到防数据丢失策略
- 防数据丢失报告

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。