

Utiliser les attributs d'application dans le rapport de découverte d'application Umbrella

Table des matières

[Introduction](#)

[Aperçu](#)

[Comment déterminer si les informations d'attributs sont mises à jour ?](#)

[Comment puis-je accéder à cette fonctionnalité ?](#)

[Additional Information](#)

Introduction

Ce document décrit comment utiliser la fonctionnalité Attributs d'application dans le Rapport de découverte des applications Cisco Umbrella.

Aperçu

La [fonctionnalité Attributs d'application du rapport Cisco Umbrella App Discovery Report](#) facilite l'évaluation des risques.

Les attributs d'application élargissent considérablement les informations contextuelles fournies par Cisco Umbrella pour chaque application identifiée, ce qui permet aux clients Cisco Umbrella de prendre des décisions stratégiques éclairées en fonction de leurs besoins.

Risk Details		Identities (34)		Attributes (38)		
Categories	Attribute	Value	Created	Updated	Provides GDPR information Discloses the ways in which personal data is collected, processed, stored, and used in compliance with the General Data Protection Regulation (GDPR).	
Compliance	Provides GDPR information	Yes https://www.cisc...	Apr 23, 2023	Apr 23, 2023		
Vulnerabilities	PCI_DSS	Yes	Aug 12, 2016	Jun 10, 2022		
Access Control	HIPAA	Yes	Aug 12, 2016	Jun 10, 2022		
Data Security	FEDRAMP	Yes	Aug 12, 2016	Jun 10, 2022		
Auditability	ISO 27001 / 27002	Yes	Aug 12, 2016	Jun 10, 2022		
Email Authenticity	COBIT	No	Aug 12, 2016	Jun 10, 2022		

18263606083476

Grâce à ces attributs d'application, les administrateurs Cisco Umbrella peuvent créer un contexte

supplémentaire sur les applications récemment découvertes dans leur environnement, tout en réduisant considérablement le temps de décision et de blocage des applications à risque.

Utilisant jusqu'à trente-huit attributs d'application dans six catégories, les administrateurs Cisco Umbrella disposent d'un large éventail d'informations supplémentaires sur les applications, qui complètent la classification des risques existante. Ces points de vue englobent :

- Conformité : existence de certifications telles que PCI-DSS, GDPR, HIPPA et FEDRAMP pour le fournisseur et l'application.
- Vulnérabilités : vulnérabilités TLS/SSL connues liées à l'application comme POODLE et BEAST.
- Contrôle d'accès : mécanismes de contrôle d'accès pris en charge comme SSO et MFA.
- Sécurité des données : spécifications de données en transit telles que la prise en charge de la version TLS, des chiffrements faibles, etc.
- Auditabilité : vérification de la disponibilité.
- Authentification des e-mails : mesures de contrôle de l'authenticité des e-mails.

Comment déterminer si les informations d'attributs sont mises à jour ?

Chaque attribut d'application comporte des dates de création et de mise à jour pour aider les administrateurs à déterminer si les informations sont pertinentes pour leur prise de décision.

Comment puis-je accéder à cette fonctionnalité ?

Vous pouvez accéder aux attributs de l'application en naviguant vers Reporting > Core Reports > App Discovery > [Application] > Attributes.

Additional Information

[Guide Cisco Umbrella SIG](#)

[Guide Cisco Umbrella DNS](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.