２０２３年１１月２１日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザーサポート

Cortex Data Lake のスキーマ名変更についてのお知らせ

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださいまして誠にありがとうございます。この度、Palo Alto Networks 社より、Cortex Data Lake のスキーマ名変更についてアナウンスされましたので、以下の通りご連絡いたします。

1. 概要

   Cortex Data Lake チームは、2023 年 12 月 8 日にログタイプ間でフィールド名を調整する変更を行います。これらの変更は、ログビューア（Explore）でのフィールド名と転送方法に影響します。転送されたログを参照する場合にはクエリ等のフィールド名を新しい名称で参照する必要があります。これらの変更前に転送されたログへの参照には、古い名前を使用する必要があります。

2. 対象のお客様

   Cortex Data Lake をご利用しているお客様

3. お客様への影響

Explore フィールド名、ログ転送(HTTPS/電子メール)への影響

これらの変更は、Explore フィールド名、HTTPS ログ転送プロファイルおよび電子メールログ転送プロファイルに影響します。

表 1. 変更点

Log Type	Old Display Name	New Display Name	Old Email Profile Name	New Email Profile Name	Old HTTPS Profile Name	New HTTPS Profile Name
DNS Security	Cortex Data Lake Tenant ID	Cortex Data Lake Tenant ID	CortexData-LakeTenantId	CortexData-LakeTenantID	CortexData-LakeTenantId	CortexData-LakeTenantID
GlobalProtect	Tenant ID	Cortex Data Lake Tenant ID	TenantID	CortexData-LakeTenantID	TenantID	CortexData-LakeTenantID
HIP Match	Tenant ID	Cortex Data Lake Tenant ID	TenantID	CortexData-LakeTenantID	TenantID	CortexData-LakeTenantID
IPtag	CDL Tenant ID	Cortex Data Lake Tenant ID	TenantID	CortexData-LakeTenantID	TenantID	CortexData-LakeTenantID
Authentication	Count Of Repeats	Repeat Count	CountOfRepeats	RepeatCount	CountOfRepeats	RepeatCount
Decryption	Count Of Repeat	Repeat Count	CountOfRepeat	RepeatCount	CountOfRepeat	RepeatCount
IPtag	Count Of Repeats	Repeat Count	CountOfRepeats	RepeatCount	CountOfRepeats	RepeatCount
GlobalProtect	Count Of Repeats	Repeat Count	CountOfRepeats	RepeatCount	CountOfRepeats	RepeatCount
UserID	Count of Repeats	Repeat Count	CountofRepeats	RepeatCount	CountofRepeats	RepeatCount
HIP Match	Count Of Repeats	Repeat Count	CountOfRepeats	RepeatCount	CountOfRepeats	RepeatCount
IPtag	Rule Matched	Rule	RuleMatched	Rule	RuleMatched	Rule
Authentication	Rule Matched	Rule	RuleMatched	Rule	RuleMatched	Rule
IPtag	Rule Matched UUID	Rule UUID	RuleMatchedUUID	RuleUUID	RuleMatchedUUID	RuleUUID
Authentication	Rule Matched UUID	Rule UUID	RuleMatchedUUID	RuleUUID	RuleMatchedUUID	RuleUUID
Tunnel	Sanctioned State Of App	Sanctioned State Of App	SanctionedStateofApp	Sanctioned-StateOfApp	SanctionedStateofApp	Sanctioned-StateOfApp
URL	Sanctioned State Of App	Sanctioned State Of App	SanctionedStateofApp	Sanctioned-StateOfApp	SanctionedStateofApp	Sanctioned-StateOfApp

SCTP	Is Inspection Before Session	Is Inspection Before Session	IsInspectionBefore-Session	IsInspectionBefore-Session	IsInspectionBefore-Session	IsInspectionBefore-Session
DNS Security	Sub Type	Sub Type	SubType	Subtype	SubType	Subtype
GlobalProtect	Log Subtype	Sub Type	LogSubtype	Subtype	LogSubtype	Subtype
File	Sub Type	Sub Type	SubType	Subtype	SubType	Subtype
Decryption	Sub Type	Sub Type	SubType	Subtype	SubType	Subtype

Syslog CEF フォーマット名への影響

CEF形式を使用したSyslogログ転送プロファイルでのトラフィックログの転送方法に影響します。

表 2. Traffic CEF Field 変更点

Log Type	Old Name	New Name
source_user_info.name	suser	susername
dest_user_info.name	duser	dusername

以上