

2023年12月1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 (第2報)

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださり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。

※太字箇所は追記もしくは変更箇所となっております。

1. 概要

Cortex Data Lake チームは、**2024年1月31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。しかしながら当面の間は既存フィールド名もサポートが継続され、新規フィールド名と既存フィールド名の両方で転送が行われます。

そのためお客様にてご利用されるフィールド名を選択できますので、既存の構成を引き続きご利用される場合には即時でのご対応が不要となります。

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。

既存フィールド名が廃止される際には Palo Alto Networks 社より事前に共有がございますため、本トピックにてお知らせ致します。

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(**SplunkHEC /MicrosoftSentinel/Exabeam** への転送)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						
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						
IPtag	Rule Matched	Rule	RuleMatched	Rule	RuleMatched	Rule
Authentication	Rule Matched	Rule	RuleMatched	Rule	RuleMatched	Rule
IPtag						
IPtag	Rule Matched UUID	Rule UUID	RuleMatchedUUID	RuleUUID	RuleMatchedUUID	RuleUUID
Authentication	Rule Matched UUID	Rule UUID	RuleMatchedUUID	RuleUUID	RuleMatchedUUID	RuleUUID
Tunnel						
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、Google Chronicle への影響

CEF 形式を使用した Syslog ログ転送プロファイルと **Google Chronicle** への **HTTPS** ログ転送プロファイルでのトラフィックログを含む各種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