Table of Contents

Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ñ Ð¾Ñ Ð¼Ð°Ñ Ð¾Ð² Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð³Ð¾Ð»Ð¾Ð².....1
Ð−ÐºÑ Ð¿Ð¾Ñ Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð³Ð¾Ð² Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ CEF.....1
Ð−ÐºÑ Ð¿Ð¾Ñ Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð³Ð¾Ð² Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ JSON.....44

Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ñ Ð¾Ñ Ð¼Ð°Ñ Ð¾Ð² Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð²

Ð–ÐºÑ Ð¿Ð¾Ñ Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð² Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ CEF

Documentation: ☑
Product: LogAn
Version: 7.x

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.	CEF:0
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	UserGate
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	NGFW
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð¿ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	events
	Origin	Ð Ð¾Ð´Ñ Ð»Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¿Ñ Ð¾Ð¸Ð·Ð¾Ñ Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	admin_cor
	Severity	Ð Ð°Ð¶Ñ Ñ Ñ Ñ Ð±Ñ .	Ð Ð¾Ð¶Ð¶Ð Ð·Ð½Ð°Ñ • 1 â • 4 â • 7 â • 10
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð¾: Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð´ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	16523444
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÑÑ Ñ ÐµÑ Ñ Ð¾Ð¹ Ñ Ñ Ñ Ñ Ð¾Ð¹ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
	act	Ð¢Ð¸Ð¿ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	login_succ
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	Admin
	src	IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	192.168.1
	cat	Ð Ð¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼	console_au

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
		Ð¿Ñ Ð¾Ð¸Ñ Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð´ÐµÑ Ð°Ð»ÐµÐ¹ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	Attributes
	cs1	Ð ÐµÑ Ð°Ð»Ð¸ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ JSON.	{"name":"

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð» Ð²ÐµÐ±-Ð´Ð¾Ñ Ñ Ñ Ð¿Ð°

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð´Ñ Ð°.
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Source	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.
	Name	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ ÐºÐ°Ñ ÐµÐ³Ð¾ URL.
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¼ Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð¸Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½ÑÐ¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ ÐµÐ¼ Ñ Ñ Ð¾Ñ Ð±Ñ.
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½ Ñ Ð¾Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾ Ñ Ð¾Ð¾Ñ Ð²Ðµ Ñ Ð¾Ð¾Ð¾Ñ Ð²Ð¸Ð¼ Ð¿Ñ Ð¸Ð½ Ñ Ð¸Ð¼Ð°Ð½Ð¸Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ñ Ð¸Ð¸Ð¼Ð¾Ð¸Ð¸Ñ.
	reason	Ð Ñ Ð¸Ñ Ð¸Ð½Ð°, Ð¿Ð¾ ÐºÐ¾Ð¾Ñ Ð¾Ñ Ð±Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¼, Ð½Ð°Ð¿Ñ Ð¸Ð¼Ñ Ð¿Ñ Ð¸Ñ Ð¸Ð½Ð° Ð±Ð»Ð¾ÐºÐ¸Ñ Ð¾Ñ Ð²Ð¾Ð°Ñ Ð°.
	proto	

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .
app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ Ð¸ ÐµÐ³Ð¾ Ð²ÐµÑ Ñ Ð
suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ
src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
requestMethod	Ð ÐµÑ Ð¾Ð´, Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð´Ð»Ñ Ð´Ð¾Ñ Ñ Ñ Ð¿Ð° Ðº URL-Ð°Ð´Ñ ÐµÑ Ñ (POST, GET Ð¸ Ñ .Ð¿.).
request	Ð Ñ Ð»Ñ Ñ Ð°Ðµ HTTP-Ð·Ð°Ð¿Ñ Ð¾Ñ Ð¿Ð¾Ð»Ðµ Ñ Ð¾Ð´ÐµÑ Ð¶Ð¸Ñ URL-Ð°Ð´Ñ ÐµÑ Ð·Ð°Ð¿Ñ Ð°Ñ Ð¸Ð²Ð°ÐµÐ¼Ð¾Ð³Ð¾ Ñ ÐµÑ Ñ Ñ Ñ Ð° Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ð Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ð¾Ð³Ð¾ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð»Ð°.
requestContext	URL Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð·Ð°Ð¿Ñ Ð¾Ñ Ð° (Ñ ÐµÑ ÐµÑ ÐµÑ HT
requestClientApplication	Useragent Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ Ñ ÐºÐ¾Ð Ð±Ñ Ð°Ñ Ð·ÐµÑ Ð°.
in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ
	Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.
cs1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.
cs1	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.
cs2Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
cs2	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
cs3Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
cs4	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
cs5Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
cs5	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
cs6Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ±Ñ Đ»Đ¸ Ñ Đ¾Đ´ĐµÑ Đ¶Đ¸Đ¼Đ¾Đµ Ñ Đ°Ñ Ñ Đ¸Ñ Ñ Đ¾Đ²Đ°Đ½Đ¾.
cs6	Đ Đ°Ñ Ñ Đ¸Ñ Ñ Đ¾Đ²Đ°Đ½Đ¾ Đ¸Đ»Đ¸ Đ½ĐµÑ .
flexString1Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ½Đ° Ñ Đ¸Đ¿ ĐºĐ¾Đ½Ñ ĐµĐ½Ñ Đ°.
flexString1	Đ¢Đ¸Đ¿ ĐºĐ¾Đ½Ñ ĐµĐ½Ñ Đ°.
flexString2Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ½Đ° ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ Đ·Đ°Đ¿Ñ Đ°Ñ Đ¸Đ²Đ°ĐµĐ¼Đ¾Đ³Đ¾ URL-Đ°Đ´Ñ ĐµÑ Đ°.
flexString2	Đ Đ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ URL.
cn1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Đ¾Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ° Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¿Đ°ĐºĐµÑ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
		Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
	cn1	Ð Ð¾Ð»Ð¸ Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¿Ð°ÐºÐµÑ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
	cn2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ ÐºÐ¾Ð»Ñ Ñ Ð²Ð° Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¿Ð°ÐºÐµÑ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	cn2	Ð Ð¾Ð»Ð¸ Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¿Ð°ÐºÐµÑ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	cn3Label	Ð Ð¾Ð»Ðµ Ñ ÐºÐ°Ð·Ñ Ð²Ð°ÐµÑ Ð¸Ñ Ñ Ð¾Ð´Ð½Ñ Ð¹ Ð¾Ñ Ð²ÐµÑ Ñ ÐµÑ Ð²Ð°.
	cn3	Ð Ð¾Ð´ Ð¾Ñ Ð²ÐµÑ Ð° HTTP.

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ð²ÐµÐ±-Ð´Ð¾Ñ Ñ Ñ Ð¿Ð° **CEF Compact**:

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Source	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.
	Name	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸ URL.
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¸ Ð¸Ð»Ð¸ Ð¿ÐµÑ ÐµÐ´Ð°Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ñ Ð¸Ñ

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.
act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ð¸Ð½Ð¸Ñ Ð¸Ð½Ð¸Ñ Ð¸Ð¸Ð¸

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ
	in	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ²Ñ Đ¾Đ´Ñ Ñ Đ¸Ñ Đ±Đ°Đ¹Ñ Đ¾Đ² Đ´Đ°Đ½Đ½Ñ Đµ Đ¿ĐµÑ ĐµĐ´Đ°Ñ Ñ Ñ Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.
	out	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¸Ñ Ñ Đ¾Ñ Đ±Đ°Đ¹Ñ Đ¾Đ² Đ´Đ°Đ½Đ½Ñ Đµ Đ¿ĐµÑ ĐµĐ´Đ°Ñ Ñ Ñ Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.
	cs1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đ¸ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.
	cs1	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.
	cs2Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
	cs2	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
	cs3Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
	cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
	flexString1Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ½Đ° ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ Đ·Đ°Đ¿Ñ Đ°Ñ Đ¸Đ²Đ°ĐµĐ¼Đ¾Đ³Đ¾ URL-Đ°Đ´Ñ ĐµÑ Đ°.
	flexString1	Đ Đ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ URL.
	cn1Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ¸Ñ Đ¾Ñ Đ´Đ½Ñ Đ¹ Đ¾Ñ Đ²ĐµÑ Ñ ĐµÑ Đ²ĐµÑ Đ°.
	cn1	Đ Đ¾Đ´ Đ¾Ñ Đ²ĐµÑ Đ° HTTP.

Đ Ñ Đ¸Đ¼ĐµÑ Đ°Đ½Đ¸ĐµĐ Đ±Ñ ĐµĐµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ¾ Đ´Đ»Ñ ĐºĐ¾Đ¼Đ¿Đ°ĐºÑ Đ½Đ¾Đ³Đ¾ Ñ Đ¾Ñ Đ¼Đ°Ñ Đ° â Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đ¸ Đ½ĐµĐºĐ¾Đ¾Ñ Đ¾Ñ Ñ Đ¸Đ¾Đ»ĐµĐ¹ Đ¾Đ±Ñ ĐµĐ·Đ°Ñ Ñ Ñ Đ¿Đ¾ Đ´Đ»Đ¸Đ½Đµ Đ´Đ¾ 80 Ñ Đ¸Đ¼Đ²Đ¾Đ»Đ¾Đ². Đ Đ°Đ¿Ñ Đ¸Đ¼ĐµÑ , Ñ Đ¿Đ¸Ñ Đ¾ĐºÐ°Ñ ĐµÐ³Đ¾Ñ Đ¸Ñ url-ĐºĐ°Ñ ĐµÐ³Đ¾Ñ Đ¸Đ¹, url, Đ¸Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ½Đ¾Ñ Đ·Đ¾Đ²Đ°Ñ ĐµÐ»Ñ , Đ¸Đ¼Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Đ¸Đ¼Ñ Đ·Đ¾Đ½Ñ , Đ¸ Ñ .Đ´.

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° DNS

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Đ¸ URL.
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ: Đ¼Đ¸Đ»Đ»Đ¸Ñ ĐµĐºÑ Đ½Đ´Ñ Ñ 1 Ñ Đ½Đ²Đ°Ñ Ñ 1970 Đ³Đ¾Đ´Đ°.
	deviceExternalId	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Đ¸Đ±Ñ Ñ Đ¸Đµ.
	act	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.
	reason	Đ Ñ Đ¸Ñ Đ¸Đ½Đ°, Đ¿Đ¾ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Đ±Ñ Đ»Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ, Đ½Đ°Đ¿Ñ Đ¸Đ¼ĐµÑ , url ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ , Đ½Đ° ĐºĐ¾Ñ Đ¾Ñ Ñ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ»Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ¾.
	proto	Đ Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµĐ¼Ñ Đ¹ Đ¿Ñ Đ¾ĐºĐ¾Đ» 4-Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ
	dhost	Đ Đ¼Ñ Ñ Đ¾Ñ Ñ Đ° Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đ°Đ´Ñ ĐµÑ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ¾Đ¿Ñ ĐµĐ´Đ¸Đ»Ñ ĐµÑ Ñ Ñ Đ¿Đ¾Đ¼Đ¾Ñ Ñ Ñ DNS Ñ ĐµÑ Đ²ĐµÑ Đ°.
	app	Đ Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ» Đ¿Ñ Đ¸ĐºĐ°Đ»Đ°Đ´Đ½Đ¾Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ .
	suser	Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .
	src	IPv4 Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.
	spt	Đ Đ¾Ñ Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
	smac	MAC-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.
	dst	IPv4 Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.
	dpt	Đ Đ¾Ñ Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
	cs1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ð½ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
	cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð Ñ ÐºÐ°Ð·Ð°Ð½Ð¸ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
	cs3	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
	cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs4	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs5Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð Ñ ÐºÐ°Ð·Ð°Ð½Ð¸ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs5	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs6Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð Ñ ÐºÐ°Ð·Ð°Ð½Ð¸ Ð¿ÐµÑ ÐµÐ´Ð°Ð²Ð°ÐµÐ¼Ñ Ñ Ð´Ð°Ð½Ð½Ñ Ñ
	cs6	Ð ÐµÑ ÐµÐ´Ð°Ð²Ð°ÐµÐ¼Ñ Ðµ Ð´Ð°Ð½Ð½Ñ Ð
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	**flexString1Label**	Ð Ð¾Ð»Ðµ Ñ ÐºÐ°Ð·Ñ Ð²Ð°ÐµÐ¼Ð¾Ð³Ð¾ Ð¸Ð¼Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ URL-Ð°Ð´Ñ ÐµÑ Ð°.
	flexString1	Ð Ð°Ñ ÐµÐ³Ð¾Ñ Ð¸Ñ URL.

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° DNS **CEF Compact**:

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Source	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.
	Name	Ð¢Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ ÐºÐ°Ñ ÐµÐ¼Ð¾Ñ Ð¸Ð¸ URL.

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð¸ Ð¸Ð¸Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾Ñ Ñ Ð¸Ðµ.
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸Ð¸Ð¸.
	reason	Ð Ñ Ð¸Ñ Ð¸Ð½Ð°, Ð¿Ð¾ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ð±Ð¾ Ð¾Ñ Ð¾Ð¸Ñ Ð¾Ð¾Ð¾Ñ Ð¾Ñ Ð¾Ð¸Ñ Ñ Ð¾Ð¸Ð¼, Ð½Ð°Ð¿Ð¸Ñ Ð¸Ð¼ÐµÐ½Ð¸Ñ , url ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ñ , Ð½Ð° ÐºÐ¾Ñ Ð¾Ñ Ñ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð»Ð¾ Ð¿Ñ Ð°Ð²Ð¸Ð».
	proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ
	dhost	Ð Ð¼Ñ Ñ Ð¾Ñ Ñ Ð° Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ð°Ð°Ñ Ð°Ñ ÐµÐ¼Ñ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¾ Ð¾Ð¿Ñ ÐµÐ´ÐµÐ»Ñ ÐµÐ¼Ñ Ñ Ñ Ñ Ð¿Ð¾Ð¼Ð¼Ñ Ñ Ñ DNS Ñ ÐµÑ Ð²ÐµÑ Ð°.
	app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð°Ñ Ð´Ð½Ð¾Ð¾Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	smac	MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ñ ÐºÐ°Ð·Ð°Ñ Ð¸Ñ Ñ Ð°Ð±Ð¾Ñ Ð²Ð°Ñ ÐµÐ¼Ð¾ Ð¿Ñ Ð°Ð²Ð¸Ð»
	cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð», Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ð¼Ñ Ð²Ñ Ð·Ð²Ð¾Ð»Ñ Ñ Ð¾Ð±Ñ.
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð¸Ð½Ð¸Ð°Ñ Ð¸Ð·Ð¾Ð²Ð°Ñ Ñ Ñ Ð¾Ñ Ð¸Ð¸.
	cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð½Ð°Ñ Ñ Ñ Ð¾Ñ Ð¸Ð¸.
	cs3Label	

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ
		Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
	cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .
	cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Ñ Ñ Đ´Đ°Đ½Đ½Ñ Ñ
	cs4	Đ ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Ñ Đµ Đ´Đ°Đ½Đ½Ñ Đ
	flexString1Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ½Đ° ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ Đ·Đ°Đ¿Ñ Đ°Ñ Đ¸Đ²Đ°ĐµĐ¼Đ¾Đ³Đ¾ URL-Đ°Đ´Ñ ĐµÑ Đ°.
	flexString1	Đ Đ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ URL.

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ
Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ **CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº**	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ
	Source	Đ¢Đ¸Đ¿ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.
	Rule Type	Đ¢Đ¸Đ¿ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đ
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ: Đ¼Đ¸Đ»Đ»Đ¸Ñ ĐµĐºÑ Đ½Đ´Ñ Ñ Ñ Đ½Đ²Đ°Ñ Ñ 1970 Đ³Đ¾Đ´Đ°.
	deviceExternalId	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.
proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .
app	Ð Ð¼Ñ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ³Ð¾ Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ
suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .
src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ
smac	MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
dmac	MAC-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾ Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
sourceTranslatedAddress	Ð Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº Ð¿Ð¾Ñ Ð»Ðµ

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ð°Ð²Ð»Ð° NAT).
sourceTranslatedPort	Ð Ð¾Ñ Ñ Ð¸Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð¿Ð¾Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ð°Ð²Ð»Ð° NAT).
destinationTranslatedAddress	Ð Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ Ð¿Ð¾Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ð°Ð²Ð»Ð° NAT).
destinationTranslatedPort	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ Ð¿Ð¾Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ð°Ð²Ð»Ð° NAT).
cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð° ÐµÑ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ð°Ð±Ð¾Ð½ÐµÐ½Ñ Ñ Ñ Ð°Ð²Ð½Ñ Ð¿Ð°Ð²Ð»Ð°.
cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð°Ð²Ð»Ð°, Ñ Ñ Ð°Ð±Ð¾Ð½ÐµÐ½Ñ Ð²Ð½ÐµÑ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð¾Ð²Ð° Ñ Ð¾Ð±Ð± Ð¸
cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð° ÐµÑ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸ Ð·Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¸ÐºÐ°
cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ð°Ð²Ð»Ð°.
cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð° ÐµÑ Ñ Ð´Ð»Ñ Ñ Ð°Ð²Ð½Ñ Ð¿Ð°Ð²Ð»Ð°.
cs3	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð²Ð½Ñ Ð¿Ð°Ð²Ð»Ð°.
cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð° ÐµÑ Ñ Ð´Ð»Ñ Ð·Ð½Ð°Ñ Ð¸ Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ .
cs4	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð½Ð°Ñ Ñ Ð¾ÐµÐ½Ñ .

	Ð °Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	cs5Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ ÑºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs5	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cn1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÑºÐ°Ð·Ð°Ð½Ð¸Ñ ÐºÐ¾Ð»Ð¸ÑÐµÑ Ñ Ð²Ð° Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¿Ð°ÐºÐµÑ Ð¾Ð² Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
	cn1	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¿Ð°ÐºÐµÑ Ð¾Ð² Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
	cn2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÑºÐ°Ð·Ð°Ð½Ð¸Ñ ÐºÐ¾Ð»Ð¸ÑÐµÑ Ñ Ð²Ð° Ð¿Ð°ÐºÐµÑ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
	cn2	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿Ð°ÐºÐµÑ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð» Ñ Ñ Ð°Ñ Ð¸ÐºÐ° **CEF Compact**:

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ð¾Ð´Ñ ÑºÑ Ð°.
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ð¾Ð´Ñ ÑºÑ Ð°.
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ð¾Ð´Ñ ÑºÑ Ð
	Source	Ð¢Ð¸Ð¿ Ñ Ð½Ð°Ð»Ð°.
	Rule Type	Ð¢Ð¸Ð¿ Ð°Ð²Ð»Ð¾, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð½Ð¾Ð³Ð¾

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ		ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.
	proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .
	app	Ð Ð¼Ñ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ³Ð¾ Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ
	smac	MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
dmac	MAC-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð´Ð°Ð½Ð½Ñ ÐµÐ¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ð¸ â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.
out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ; Ð´Ð°Ð½Ð½Ñ ÐµÐ¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.
sourceTranslatedAddress	Ð Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº Ð¿Ð¾ÑÐ»Ðµ Ð¿Ñ Ð¾Ð»Ðµ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð» NAT).
sourceTranslatedPort	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð¿Ð¾ÑÐ»Ðµ Ð¿Ñ Ð¾Ð»Ðµ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð» NAT).
destinationTranslatedAddress	Ð Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¿Ð¾ÑÐ»Ðµ Ð¿Ñ Ð¾Ð»Ðµ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð» NAT).
destinationTranslatedPort	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¿Ð¾ÑÐ»Ðµ Ð¿Ñ Ð¾Ð»Ðµ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð» NAT).
cs1Label	Ð Ð¾Ð»Ðµ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð».
cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð», Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
		Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ
	cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .
	cs3	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° ÐiÐ Ð

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.	CEF:0
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	UserGate
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	NGFW
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	idps
	Signature	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ¹ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ Ñ ÐiÐ Ð .	BlackSun T
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	**Threat Level**	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ (Ñ Ñ Ñ Ð Ñ Ñ Ð¾Ð Ñ Ð¼Ð½Ð 2); Unknow ÐºÐ°Ñ Ðµ Ð¾Ð¿Ñ Ð
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	16523444
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ	accept

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
	Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	
proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP Ð¸Ð»Ð
app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	HTTP
suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.1
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.226.1
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.	231
out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	40
msg	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ Ñ Ð¸ ÐµÑ Ð½Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ.	[2] BlackS
cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Rule

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
	cs1	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	IDPS Rule
	cs2Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	Source Zo
	cs2	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	Trusted
	cs3Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	Source Co
	cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	RU (Đ¾Ñ Đ´Đ²Ñ Ñ ĐºĐ¾Đ´ Ñ
	cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs4	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Untrusted
	cs5Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs5	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	RU (Đ¾Ñ Đ´Đ²Ñ Ñ ĐºĐ¾Đ´ Ñ

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đi Đ **CEF Compact**:

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	**Device Vendor**	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ¢Đ¸Đ¿ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	idps
	Signature	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ¹ Ñ Đ¸Đ³Đ½Đ°Ñ Ñ Ñ Ñ ĐiĐ Đ .	BlackSun
	Threat Level		

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
		Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ (Ñ Ñ Ñ Ð Ñ Ñ Ð¾Ð Ñ Ð¼Ð½Ð 2); Unknov ÐºÐ°Ñ Ðµ Ð¾Ð¿Ñ Ð
CEF **[Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]**	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	16523444
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	accept
	proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP Ð¸Ð»Ð
	app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	HTTP
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.1
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.226.1
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ	231

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
		Đ±Đ°Đ¹Ñ Đ¾Đ²; Đ´Đ°Đ½Đ½Ñ Đµ Đ¿ĐµÑ ĐµĐ´Đ°Ñ Ñ Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	
	out	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¸Ñ Ñ Đ¾Ñ Đ´Ñ Ñ Đ¸Ñ Đ±Đ°Đ¹Ñ Đ¾Đ²; Đ´Đ°Đ½Đ½Ñ Đµ Đ¿ĐµÑ ĐµĐ´Đ°Ñ Ñ Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.	40
	msg	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Ñ Đ¸Đ³Đ½Đ°Ñ Ñ Ñ Ñ Đ¸ ĐµÑ Đ½Đ°Đ·Đ²Đ°Đ½Đ¸Đµ.	[2] BlackS
	cs1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	Rule
	cs1	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	IDPS Rule

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ

Đ¤Đ¾Ñ Đ¾Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ ĐiĐ£ Đ¢Đ

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	scada
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
	PDU Severity	Đ Ñ Đ¸Ñ Đ¸Ñ Đ½Đ¾Ñ Ñ Ñ Đ ĐiĐ£ Đ¢Đ .	Đ Đ¾Đ¶Đ • 1 â • 2 â • 3 â • 4 â • 5 â
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ:	16523444

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
	Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	
deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	accept
app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	Modbus
src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.1
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð¶Ð 0 Ð´Ð¾ 65
dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.226.1
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð¶Ð 0 Ð´Ð¾ 65
cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Rule
cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	Scada Rul
cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Source Zo
cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Trusted
cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Source Co
cs3	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	RU (Ð¾Ñ Ð´Ð²Ñ Ñ

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
	cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs4	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Untrusted
	cs5Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs5	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	RU (Đ¾Ñ Đ´Đ²Ñ Ñ
	cs6Label	Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ½Đ° Đ¸Đ½Ñ Đ¾Ñ Đ¼Đ°Ñ Đ¸Ñ Đ¾Đ± Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đµ.	PDU Detai
	cs6	Đ Đ½Ñ Đ¾Ñ Đ¼Đ°Ñ Đ¸Ñ Đ¾Đ± Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đµ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ JSON.	{"protocol "mb_value "mb_mess

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ¸Đ½Ñ Đ¿ĐµĐºÑ Đ¸Ñ Đ¾Đ²Đ°Đ½Đ¸Ñ SSH

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ
Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ **CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº**	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	ssh
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶Đ Đ¿Ñ Đ¸Đ½ Đ·Đ½Đ°Ñ (Ñ Ñ Ñ Đ Ñ Ñ Đ¾Đ Ñ Đ¼Đ½Đ 2); Unknow ĐºĐ°Ñ Đµ Đ¾Đ¿Ñ Đ
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ: Đ¼Đ¸Đ»Đ»Đ¸Ñ ĐµĐºÑ Đ½Đ´Ñ Ñ 1 Ñ Đ½Đ²Đ°Ñ Ñ 1970 Đ³Đ¾Đ´Đ°.	16523444
	deviceExternalId	Đ Đ¼Ñ , ĐºĐ¾Đ¾Ñ Đ¾Ñ Đ¾Đµ	utmcore@

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
	Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	
act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	accept
app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	SSH Ð¸Ð»Ð
suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.1
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
smac	MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	FA:16:3E:6
dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.226.1
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Rule
cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	SSH inspe
cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Source Zo
cs2	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Trusted
cs3Label		Source Co

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
		Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	
	cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	RU (Đ¾Ñ Đ´Đ²Ñ Ñ ĐºĐ¾Đ´ Ñ
	cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ¸ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs4	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Untrusted
	cs5Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Destinatio
	cs5	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	RU (Đ¾Ñ Đ´Đ²Ñ Ñ ĐºĐ¾Đ´ Ñ
	cs6Label	Đ£ĐºĐ°Đ·Đ°Đ½Đ¸Đµ Đ½Đ° ĐºĐ¾Đ¼Đ°Đ½Đ´Ñ , Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Ñ Ñ Đ¿Đ¾ SSH.	Command
	cs6	Đ Đ¾Đ¼Đ°Đ½Đ´Đ°, Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Đ°Ñ Đ¿Đ¾ SSH, Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ JSON.	whoami

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ¸Đ½Ñ Đ¿ĐµĐºÑ Đ¸Ñ Đ¾Đ²Đ°Đ½Đ¸Ñ SSH **CEF Compact**:

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	7
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	ssh
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶Đ Đ¿Ñ Đ¸Đ½Đ·Đ½Ñ (Ñ Ñ Ñ Đ Ñ Ñ Đ¾Đ

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
			Ñ Ð¼Ð½Ð 2); Unknov ÐºÐ°Ñ Ðµ Ð¾Ð¿Ñ Ð
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	16523444
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ñ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ð² Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸Ð¸Ð¸Ñ Ð¿Ð¾Ð»Ñ Ñ Ð¾Ð¾Ð¼Ð¿Ð¾Ð¼.	accept
	app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	SSH Ð¸Ð»Ñ
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.1
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	smac	MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	FA:16:3E:6
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.226.1
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ Ñ Ñ Ð´Ð»Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð¿Ð°Ð²Ð¸Ð»Ð°.	Rule
	cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ	SSH inspe

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
		ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	
	cs2Label	Đ Đ¾Đ»Đµ Đ¸Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	SrcZone
	cs2	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	Trusted
	cs3Label	Đ Đ¾Đ»Đµ Đ¸Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¸Đ½Đ´Đ¸ĐºĐ°Ñ Đ¸Đ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	DstZone
	cs3	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Untrusted
	cs4Label	Đ£ĐºĐ°Đ·Đ°Đ½Đ¸Đµ Đ½Đ° ĐºĐ¾Đ¼Đ°Đ½Đ´Ñ , Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Ñ Ñ Đ¿Đ¾ SSH.	Command
	cs4	Đ Đ¾Đ¼Đ°Đ½Đ´Đ°, Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Đ°Ñ Đ¿Đ¾ SSH, Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ JSON.	whoami

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ·Đ°Ñ Đ¸Ñ Ñ Đ¿Đ¾Ñ Ñ Đ¾Đ²Đ¾Đ³Đ¾ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾ĐºÐ	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ¢Đ¸Đ¿ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	mailsecuri
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶Đ Đ¿Ñ Đ¸Đ½ Đ·Đ½Đ°Ñ (Ñ Ñ Ñ Đ Ñ Ñ Đ¾Đ Ñ Đ¼Đ½Đ 2); Unknow ĐºĐ°Ñ Đµ Đ¾Đ¿Ñ Đ
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ:	16523444

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
	Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	
deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð²Ñ Ð¿Ð¾Ð»Ð½ÐµÐ½Ð½Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	mark
app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	SMTP
suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
src	IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	10.10.10.1
spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
dst	IPv4-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	10.10.10.1
dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.	10
out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	10
cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ	Rule

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
	Ð½Ð°Ð·Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð».	
cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð» Ð·Ð°Ñ Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Mail secur
cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	Source Zo
cs2	Ð Ð¾Ð½Ðº Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Untrusted
cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	Source Co
cs3	Ðiñ Ñ Ð°Ð½Ð° Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	RU (Ð¾Ñ Ð´Ð²Ñ Ñ ÐºÐ¾Ð´ Ñ
cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¾Ð½Ð½Ð°Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ð¸Ð½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Destinatio
cs4	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ð¸Ð½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrusted
cs5Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ð¸Ð½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Destinatio
cs5	Ðiñ Ñ Ð°Ð½Ð° Ð½Ð°Ð·Ð½Ð°Ñ Ð¸Ð½Ð¸Ñ .	RU (Ð¾Ñ Ð´Ð²Ñ Ñ ÐºÐ¾Ð´ Ñ
cs6Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ð°Ð´Ñ ÐµÑ Ð° Ð¸Ð»Ð¸ Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	To
cs6	Email Ð¿Ð¾Ñ Ñ Ð°Ñ ÐµÐ»Ñ .	receiver@
flexString1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ð°	From

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
		Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Ñ ĐµĐ»Ñ .	
	flexString1	Email Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Ñ ĐµĐ»Ñ .	sender@e
	cn1Label	Đ Đ¾Đµ Đ¸Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ ĐºĐ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ° Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¿Đ°ĐºĐµÑ Đ¾Đ² Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	Packets se
	cn1	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¿Đ°ĐºĐµÑ Đ¾Đ² Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	3
	cn2Label	Đ Đ¾Đµ Đ¸Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ ĐºĐ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ° Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¿Đ°ĐºĐµÑ Đ¾Đ² Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đµ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.	Packets re
	cn2	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ¿Đ°ĐºĐµÑ Đ¾Đ² Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đµ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.	1

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ·Đ°Ñ Đ¸Ñ Ñ Đ¿Đ¾Ñ Ñ Đ¾Đ²Đ¾Đ³Đ¾ Ñ Ñ Đ°Ñ Đ¸ĐºĐ° **CEF Compact**:

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ·
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºĐ°.	7
	Source	Đ¢Đ¸Đ¿ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	mailsecuri
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
	Threat Level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶Đ Đ¿Ñ Đ¸Đ½ Đ·Đ½Đ°Ñ (Ñ Ñ Ñ Đ Ñ Ñ Đ¾Đ

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
			Ñ Ð¼Ð½Ð 2); Unknov ÐºÐ°Ñ Ðµ Ð¾Ð¿Ñ Ð
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	16523444
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð²Ñ Ð¿Ð¾Ð»Ð½ÐµÐ½Ð½Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	mark
	app	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	SMTP
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_exam Ð¿Ð¾Ð»Ñ Ð½ÐµÐ¸Ð
	src	IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	10.10.10.1
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	dst	IPv4-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	10.10.10.1
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶Ð Ð¿Ñ Ð¸Ð½ Ð·Ð½Ð°Ñ 65535.
	in	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ.	10
	out	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð¸Ñ Ñ Ð¾Ð´Ñ Ñ Ð¸Ñ Ð±Ð°Ð¹Ñ Ð¾Ð²; Ð´Ð°Ð½Ð½Ñ Ðµ	10

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð·
		Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ñ Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð°Ð·Ð²Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Rule
	cs1	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð° Ð·Ð°Ñ Ð¸Ñ Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Mail secur
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	SrcZone
	cs2	Ð Ð¾Ð½Ð° Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Untrusted
	cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	DstZone
	cs4	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrusted
	cs5Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ð°Ð´Ñ ÐµÑ Ð° Ð¾Ñ Ð¿Ñ Ð°Ð²Ð¸Ñ ÐµÐ»Ñ .	From
	cs5	Email Ð¾Ñ Ð¿Ñ Ð°Ð²Ð¸Ñ ÐµÐ»Ñ .	sender@e
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	**cs6Label**	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¿Ð¾Ñ Ñ Ð¾Ð²Ð¾Ð³Ð¾ Ð°Ð´Ñ ÐµÑ Ð° Ð¿Ð¾Ð»Ñ Ñ Ð°Ñ ÐµÐ»Ñ .	To
	cs6	Email Ð¿Ð¾Ð»Ñ Ñ Ð°Ñ ÐµÐ»Ñ .	receiver@

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹ ÐºÐ¾Ð½ÐµÑ Ð½Ñ Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð
	CEF:Version	Ð ÐµÑ Ñ Ð¸Ñ CEF.	CEF:
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**Device Vendor**		User

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð
		Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	NGF
	Device Version	Ð ÐµÑ Ñ Ð¸ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð¿ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	endp
	Name	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	log
	Severity	Ð Ð°Ð¶Ð½Ð¾Ñ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	Ð Ð Ð·Ð
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	165
	deviceExternalId	Ð Ð´ÐµÐ½Ñ Ð¸Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°, Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ð²Ñ ÐµÐ³Ð¾ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	35fb
	msg	Ð Ð¾Ð´Ñ Ð¾Ð±Ð½Ð°Ñ Ð¸Ð½Ñ Ð¾Ñ Ð¼ Ð¾Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¸.	ÐiÐ Defe Ð¸Ð SEC
	suser	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	Adm
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ð¸ÐºÐ°Ñ Ð¼ ÐºÐ¾Ð¼Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs1	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð¼Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð° Ð¸Ð»Ð¸ Ñ ÐµÐ½Ñ Ð¾Ñ Ð°.	35fb
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ÐºÐ¾Ð¼ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð° Ð¸Ð»Ð¸ Ñ ÐµÐ½Ñ Ð¾Ñ Ð°.	endp
	cs2	Ð Ð¼Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð° Ð¸Ð»Ð¸ Ñ ÐµÐ½Ñ Ð¾Ñ Ð°.	DES
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ñ Ð¸	logL

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð
		Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	
	cs3	Ð¢Ð¸Ð¿ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	Ð Ñ Ð Ñ ÐiÐ Ð¾Ñ
	cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	logC
	cs4	Ð Ð°Ñ ÐµÐ³Ð¾Ñ Ð¸Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	Spec
	cs5Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ñ Ð¸Ð¿Ð° Ð¶Ñ Ñ Ð½Ð°Ð».	logF
	cs5	Ð¢Ð¸Ð¿ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°, Ñ Ð¾Ð´ÐµÑ Ð¶Ð°Ñ ÐµÐ³Ð¾ Ð²Ð°Ð¶Ð½Ñ Ñ Ð¸Ð½Ñ Ð¾Ñ Ð¼Ð°Ñ Ð¾ Ð¿Ñ Ð¾Ð³Ñ Ð°Ñ Ð¼Ñ Ñ Ð¸ Ð°Ð¿Ð¿Ð°Ñ Ð°Ñ Ð½Ñ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ñ .	Secu Ð±Ð App Ð¶Ñ Ð¿Ñ (Ñ Ð Ð¶Ñ
	cs6Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹.	sour
	cs6	Ð Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹.	Micr
	cn1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ ÐºÐ¾Ð´Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	logE
	cn1	Ð Ð¾Ð´ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	115
	cn2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	logE
	cn2	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	100
	cn3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð½Ð°Ñ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ñ Ð¸Ð¿Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð»Ð¾Ð³Ð°.	logE
	cn3	Ð¢Ð¸Ð¿ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð»Ð¾Ð³Ð°.	1 (e (auc
	flexString1Label		inse

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð
		Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸Ð¸ Ñ Ñ Ð¾Ð¿Ð¸ Ð²Ð°Ñ Ñ Ð°Ð²ÐºÐ¸.	
	flexString1	Ðiñ Ñ Ð¾ÐºÐ° Ð²Ñ Ñ Ð°Ð²ÐºÐ¸ - Ð´Ð°Ð½Ð½Ñ Ðµ Ð±Ð»Ð¾ÐºÐ° EventData Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Windows.	Wind Defe

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð» Ð¿Ñ Ð°Ð²Ð¸Ð» ÐºÐ¾Ð½Ð²ÐµÑ Ñ Ð¾Ð¹Ñ Ñ Ð²

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.	CEF
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	User
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	NGF
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð ¶Ñ Ñ Ð½Ð°Ð»Ð°.	endp
	Name	Ð¢Ð¸Ð Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	log
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð URL.	Ð Ð Ð·Ð¾ (Ñ Ñ Ñ Ñ Ð Unk Ð½Ð
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð¸ÑÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	165
	deviceExternalId	Ð Ð´ÐµÐ½Ñ Ð¸Ð¸Ð°Ñ Ð¾Ð¾Ð°Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°, Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ð²Ð°Ñ ÐµÐ³Ð¾ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	35fb
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ð¸ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ñ Ð¸Ð¸Ð°Ñ Ð¸Ð¸Ð¼.	acce
	proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾Ð» 4-Ð³Ð¾Ð¼ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP
	shost	Ð Ð¼Ñ Ñ Ð¾Ñ Ñ Ð°.	www
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.1
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð Ð·Ð¾

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð Ð·Ð
	filePath	Ð Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ðµ, Ðº ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼Ñ Ð±Ñ Ð»Ð¾ Ð¿Ñ Ð¸Ð²ÐµÐ´Ñ Ð¾ Ð²Ð¾ Ð¼Ñ ÐµÐ¶Ñ ÐµÐ²Ð¾Ð¾Ð¾Ð¾ Ñ ÐºÑ Ð°Ð½.	C:\\P (x86
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð° ÐºÐ¾Ð½ÐºÑÐµÑ Ð½Ñ Ð¾Ð¹ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs1	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð½ÐºÑÐµÑ Ð½Ð¾Ð¹ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð° Ð¸Ð»Ð¸ Ñ ÐµÐ½Ð¸Ñ Ð°.	35fb
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ð¸Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐºÑÐµÑ Ð½Ð¾Ð¹ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs2	Ð Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐºÑÐµÑ Ð½Ð¾Ð¹ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	DES
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ñ Ð°Ð²Ð¸Ð», Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ ÐºÐ¾Ð¼Ñ Ð¾Ð¼Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¾ Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¾.	Rule
	cs3	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Test
	flexString1Label	Ð Ð¾Ð»Ðµ Ñ ÐºÐ°Ð·Ð²Ð°Ð½Ð¸Ñ Ð½Ð° Ñ Ð¸ ÐºÐ¾Ð¼Ð¾Ð½ÐµÐ½Ñ Ð°.	Med
	flexString1	Ð¢Ð¸Ð¿ ÐºÐ¾Ð½ÐµÐ½Ñ Ð°.	text
	flexString2Label	Ð Ð¾Ð»Ðµ Ñ ÐºÐ°Ð·Ð²Ð°Ð½Ð¸Ñ Ð½Ð° ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð° Ð·Ð¾Ð½Ñ Ð°Ð²Ð¸Ð»Ð¾Ð¼ URL-Ð°Ð´Ñ ÐµÑ Ð°.	Cate
	flexString2	Ð Ð°Ñ ÐµÐ³Ð¾Ñ Ð¸Ñ URL.	Com

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ð¿Ñ Ð°Ð²Ð¸Ð» ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð½Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð² **CEF Format**:

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ñ CEF.	CEF

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	**Device Vendor**	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	User
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	NGF
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð¿ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	endp
	Name	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	log
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸ URL.	Ð Ð Ð·Ð³ (Ñ Ñ Ñ Ñ Ñ Ð Unk Ð½Ð
	rt	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	165
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**deviceExternalId**	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°, Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ð²Ñ ÐµÐ³Ð¾ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	35fb
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	acce
	proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP
	shost	Ð Ð¼Ñ Ñ Ð¾Ñ Ñ Ð°.	www
	src	IPv4 Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.1
	spt	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð Ð·Ð³
	dst	IPv4 Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	194.
	dpt	Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð Ð·Ð³
	filePath	Ð Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ðµ, Ðº ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼Ñ Ð±Ñ Ð»Ð¾ Ð¿Ñ Ð¸Ð¼ÐµÐ½ÐµÐ½Ð¾ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð¾ Ð¼ÐµÐ¶Ñ ÐµÑ ÐµÐ²Ð¾Ð³Ð¾ Ñ ÐºÑ Ð°Ð½Ð°.	C:\\P (x86
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ	endp

	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
		Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	
	cs1	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð° Ð¸Ð»Ð¸ Ñ ÐµÐ½Ñ Ð¾Ñ Ð°.	35fb
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ð¸Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs2	Ð Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	DES
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¿Ð¾ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ñ Ð·Ð°Ð¿Ð¸ Ñ Ð² Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾.	Rule
Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	**cs3**	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Test

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð» Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ð¹ ÐºÐ¾Ð½ÐµÑ Ð½Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
	CEF:Version	Ð ÐµÑ Ñ Ð¸Ñ CEF.	CEF
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**Device Vendor**	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.	User
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð´Ñ ÐºÑ Ð°.	NGF
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð´Ñ ÐºÑ Ð°.	7
	Source	Ð¢Ð¸Ð¿ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	endp
	Name	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	log
	Threat Level	Ð Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ Ð¿Ð¾ Ñ Ð¾Ñ Ñ Ð¼Ð¾Ð»Ñ Ð°Ð½Ð¸Ñ .	0
	rt	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¸: Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	165
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**deviceExternalId**	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°, Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ð½Ð¾ ÐµÐ³Ð¾ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¸.	35fb
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ (Ð·Ð°Ð¿Ñ Ñ ÐºÐ° Ð¸Ð»Ð¸ Ð¾Ñ Ð°Ð½Ð¾Ð²ÐºÐ°	start

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
		Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ).	
	suser	Ð Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	DES
	filePath	Ð Ð°Ñ Ð¿Ð¾Ð»Ð¾Ð¶ÐµÐ½Ð¸Ðµ Ñ Ð°Ð¹Ð»Ð°.	C:\\\
	spid	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ñ ÐµÑ Ñ Ð°.	386
	fileHash	Ð¥Ñ Ñ Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	B49
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ñ‚ÐµÐ»Ñ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs1	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	35fb
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ñ‚ÐµÐ»Ñ Ð½Ð° Ð¸Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	endp
	cs2	Ð Ð¼Ñ NetBIOS ÐºÐ¾Ð½ÐµÑ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.	DES
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¸ Ð¾ÐºÐ¾Ð½Ñ Ð¾Ð¹Ñ Ñ Ñ Ñ Ð¾ÐºÐ¾Ð¿.	cmd
	cs3	Ð Ð°Ð¿Ñ Ð¾ÐºÐ¾Ð½Ñ Ð¾Ð¹Ñ Ñ Ñ Ñ Ð¾ÐºÐ¾Ð¿.	C:\\\ task
	cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ð¸Ð½Ð´Ð¸ÐºÐ°Ñ Ð¾Ñ ÐµÑ Ñ Ð¸.	sess
	cs4	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐµÑ Ñ Ð¸.	165

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð» Ð°Ð¿Ð¿Ð°Ñ Ð°Ñ Ñ Ñ Ñ ÐºÐ¾Ð½ÐµÑ Ð½Ñ Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	CEF:Version	Ð ÐµÑ Ñ Ð¸Ñ CEF.
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**Device Vendor**	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ ÐºÑ Ð°.
	Source	Ð¢Ð¸Ð¿ Ð¶Ñ Ð½Ð°Ð»Ð°.

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
	Name	Ð¢Ð¸Ð Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.
	Threat Level	Ð Ð½Ð°Ñ ÐµÐ½Ð¸Ðµ Ð¿Ð¾ Ñ Ð¼Ð¾Ð»Ñ Ð°
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ñ Ð¾Ð±Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð: Ð¼Ð¸Ð»Ð»Ð¸Ñ ÐµÐºÑ Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.
	deviceExternalId	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ñ Ñ Ð Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ð²Ð°Ñ ÐµÐ³Ð¾ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¼.
	act	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ (Ð¿Ð¾Ð´ÐºÐ»Ñ Ñ ÐµÐ½Ð¸Ð¸ Ð¸Ð·Ð²Ð»ÐµÑ ÐµÐ½Ð¸Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ
	sourceServiceName	Ð Ñ Ð°Ð¹Ð²ÐµÑ Windows, Ð¾Ð±ÐµÑ Ð¿ÐµÑ Ð²Ð·Ð°Ð¸Ð¼Ð¾Ð´ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ ÐºÐ¾Ð¾Ð¼Ð¿Ð¾Ð¾Ð±Ð¾Ñ Ñ Ð´Ð¾Ð²Ð°Ð½Ð¸Ñ/Ñ Ñ Ñ
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ñ Ð¸ÐºÐ°ÐºÐ¾ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ
	cs1	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð½Ð° Ð¸Ñ NetBIOS ÐºÐ¾Ð¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ
	cs2	Ð Ð¼Ñ NetBIOS ÐºÐ¾Ð¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð½Ð¾Ð³Ð¾ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ñ Ð¸ÐºÐ°ÐºÐ¾ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð¿Ð¾Ð´Ð´ÐµÑ Ð¶Ð¸Ð²Ð°ÐµÐ¼Ð¾Ð³Ð¾/Ð¸Ð·Ð²Ð»ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°.
	cs3	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ñ Ñ Ð
	cs4Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¸Ñ Ð¸ Ð¸Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ñ
	cs4	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°

Ð¤Ð¾Ñ Ð¼Ð°Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Syslog

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
CEF Ð·Ð°Ð³Ð¾Ð»Ð¾Ð²Ð¾Ðº	**CEF:Version**	Ð ÐµÑ Ñ Ð¸Ñ CEF.	C
	Device Vendor	Ð Ñ Ð¾Ð¸Ð·Ð²Ð¾Ð´Ð¸Ñ ÐµÐ»Ñ Ð¿Ñ Ð¾Ð´Ñ Ð¾Ñ Ð°.	U
	Device Product	Ð¢Ð¸Ð¿ Ð¿Ñ Ð¾Ð´Ñ Ð¾Ñ Ð°.	N
	Device Version	Ð ÐµÑ Ñ Ð¸Ñ Ð¿Ñ Ð¾Ð´Ñ Ð¾Ñ Ð°.	7
	Source	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð°.	s
	Name	Ð¢Ð¸Ð Ñ Ñ Ð¾Ð¼Ð¸Ð½Ð¸Ð°Ñ Ð°.	lo
	Threat Level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ .	Ð

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
CEF [Ñ Ð°Ñ Ñ Ð¸Ñ ÐµÐ½Ð¸Ðµ]	**rt**	Ð Ñ ÐµÐ¼Ñ , ÐºÐ¾Ð³Ð´Ð° Ð±Ñ Ð»Ð¾ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ: Ð¼Ð¸Ð»Ð»Ð¸ÑÐµÐºÑ Ð½Ð´Ñ Ñ 1 Ñ Ð½Ð²Ð°Ñ Ñ 1970 Ð³Ð¾Ð´Ð°.	1
	deviceExternalId	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð¸ Ð¸ÑÑ Ð¸ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸ÑÑ Ñ Ð¸ÑÑ Ñ ÐµÐ¼ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	u
	msg	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	[d (
	cn1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ñ Ð¸Ð¿Ð° Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¾Ðº Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹ syslog. Ð Ð¾Ð´Ñ Ð¾Ð±Ð½ÐµÐµ Ð¾Ð· Ð·Ð½Ð°Ñ Ð½Ð¸Ñ Ñ syslog facility Ñ Ð¼Ð¾Ñ Ñ Ð¸Ñ Ðµ Ð² RFC 5424.	F
	cn1	Ð¢Ð¸Ð¿ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹ syslog. Ð Ð°Ð¿Ñ Ð¸Ð¼Ñ , user-level messages.	1
	cs1Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ð¼ÐµÐ½Ð¸ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð°, Ð½Ð° ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ð¿Ð¾Ð»Ðµ Ð¿Ð¾Ð»Ñ Ð¾Ð¶Ð½Ð¾ Ñ Ð¾Ð·Ð´Ð°Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	H
	cs1	Ð Ð¼Ñ ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ñ Ñ ÐµÑ Ð°, Ð½Ð° ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ð¿Ð¾Ð»Ðµ Ð¿Ð¾Ð»Ñ Ð¾Ð¶Ð½Ð¾ Ñ Ð¾Ð·Ð´Ð°Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	n
	cs2Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ð¼ÐµÐ½Ð¸ , Ð²Ñ Ð·Ð²Ð°Ð²Ð¾Ð¼ÐµÐ½Ð¸ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	T
	cs2	Ð Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ðµ, Ð²Ñ Ð·Ð²Ð°Ð²ÑÐµÐµ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	o
	cs3Label	Ð Ð¾Ð»Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÑ Ñ Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ñ Ð¸Ð¼ÐµÐ½Ð¸ Ñ Ð¸ÑÑ Ñ ÐµÐ¼Ñ Ð¿Ð¾Ð»Ñ Ð¾Ð¶Ð½Ð¾ Ñ Ð¾Ð·Ð´Ð°Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	P
	cs3	PID Ð¿Ñ Ð¾Ñ ÐµÑ Ñ Ð° Ð²Ñ Ð·Ð²Ð°Ð²ÑÐµÐµ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	3

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
	cs4Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	R
	cs4	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	E

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° RADIUS

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµÐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGa
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	radius
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ] Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ: Đ¼Đ¸Đ»Đ»Đ¸Ñ ĐµĐºÑ Đ½Đ´Ñ Ñ 1 Ñ Đ½Đ²Đ°Ñ Ñ 1970 Đ³Đ¾Đ´Đ°.	17010
	deviceExternalId	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´Đ¸Đ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcon
	act	ĐiÑ Đ°Ñ Ñ Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ (acct_status_type).	start, s accoun
	suser	Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Unkno Đ¿Đ¾Đ Đ½ĐµĐ
	src_ip	IP-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°, Đ¾Ñ ĐºÑ Đ´Đ° Đ¿Ñ Đ¸Đ»Đ¾ Ñ Đ¾Đ¾Đ±Ñ ĐµĐ½Đ¸Đµ.	192.16
	dst	IP-Đ°Đ´Ñ ĐµÑ NAS, Đ°Đ²Ñ Đ¾Ñ Đ¸Đ·Đ¾Đ²Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	172.16
	dvc	IP-Đ°Đ´Ñ ĐµÑ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ (framed ip address).	192.16
	cs1Label	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ	user gr

	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ
		Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	
	cs1	ĐiÑ Ñ Đ¾ĐºĐ° Đ³Ñ Ñ Đ¿Đ¿ Đ² ĐºĐ¾Ñ Đ¾Ñ Ñ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	test_gr

Đ¤Đ¾Ñ Đ¼Đ°Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° UserID

Đ¢Đ¸Đ¿ Đ¿Đ¾Đ»Ñ	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
CEF Đ·Đ°Đ³Đ¾Đ»Đ¾Đ²Đ¾Đº	**CEF:Version**	Đ ĐµÑ Ñ Đ¸Ñ CEF.	CEF:0
	Device Vendor	Đ Ñ Đ¾Đ¸Đ·Đ²Đ¾Đ´Đ¸Ñ ĐµĐ»Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	UserGate
	Device Product	Đ¢Đ¸Đ¿ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	NGFW
	Device Version	Đ ĐµÑ Ñ Đ¸Ñ Đ¿Ñ Đ¾Đ´Ñ ĐºÑ Đ°.	7
	Source	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	userid
	Name	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	log
CEF [Ñ Đ°Ñ Ñ Đ¸Ñ ĐµĐ½Đ¸Đµ]	**rt**	Đ Ñ ĐµĐ¼Ñ , ĐºĐ¾Đ³Đ´Đ° Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ: Đ¼Đ¸Đ»Đ»Đ¸Ñ ĐµĐºÑ Đ½Đ´Ñ Ñ 1 Ñ Đ½Đ²Đ°Ñ Ñ 1970 Đ³Đ¾Đ´Đ°.	17010850
	deviceExternalId	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@
	act	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	login
	reason	Đ Ñ Đ¸Ñ Đ¸Đ½Đ°, Đ¿Đ¾ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Đ±Ñ Đ»Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	{"user_gro "user_sid"
	suser	Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	user1 (Unk
	src	IPv4 Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	10.10.0.11
	cs1Label	Đ Đ¾Đ»Đµ Đ¸Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	Rule
	cs1	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°,	dev.local

Ð¢Ð¸Ð¿ Ð¿Ð¾Ð»Ñ	Ð Ð°Ð·Ð²Ð°Ñ½Ñ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ñ½Ñ	
		Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ñ½Ñ Ðº Ð¾Ñ Ð¾Ñ Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ñ Ð¸Ñ.	

Ð–ÐºÑ Ð¿Ð¾Ñ Ñ Ð¶Ñ Ñ Ð½Ð°Ð»Ð¾Ð² Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ñ Ñ JSON

Documentation: ☑
Product: LogAn
Version: 7.x

Ð Ð¿Ð¸Ñ Ð°Ð½Ñ Ð¶Ñ Ð»Ð° Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¹

Ð Ð°Ð·Ð²Ð°Ñ½Ñ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ñ	
timestamp	Ð Ñ ÐµÐ¼Ñ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¸Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ñ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð¼Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ð¼.	utmcore@ersthetatica
ip_address	IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	192.168.174.134
attributes	Ð ÐµÑ Ð°Ð»Ð¸ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ñ ÐµÐ JSON.	{"rule":{"logrotate":12,"attributes":{"timez log export ftp"}
event_type	Ð¢Ð¸Ð¿ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	logexport_rule_updated
event_severity	Ð Ð°Ð¶Ð½Ð¾Ñ Ñ Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ .	info (Ð¸Ð½Ñ Ð¾Ñ Ð¼Ð°Ñ Ð¸Ð¾Ð½Ð½Ñ (ÐºÑ Ð¸Ñ Ð¸Ñ Ð¼Ñ Ðµ).
event_origin	Ð Ð¾Ð´Ñ Ð»Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¿Ñ Ð¾Ð¸Ð·Ð¾Ð¾Ñ Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ.	core
event_component	Ð Ð¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¿Ñ Ð¾Ð¸Ð·Ð¾Ð¾Ñ Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ.	console_auth
user	Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	{"guid":"37333739-3733-3734-3635-36640

Ð Ð¿Ð¸Ñ Ð°Ð½Ñ Ð¶Ñ Ð»Ð° Ð²ÐµÐ±-Ð´Ð¾Ñ Ñ Ñ Ð¿Ð°

Ð Ð°Ð·Ð²Ð°Ñ½Ñ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ñ	Ð Ñ Ð
timestamp	Ð Ñ ÐµÐ¼Ñ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¸Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ñ:	2022-05-

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð
	yyyy-mm-ddThh:mm:ssZ.	
session	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ð¾Ñ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð¸.	a7a3cd49 (ÐµÑ Ð»Ñ 0000000
node	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ñ Ð¾Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑÐ¸Ñ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@
reasons	Ð Ñ Ð¸Ñ Ð¸Ð½Ð°, Ð¿Ð¾ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ð±Ñ Ð¾Ð·Ð¾Ð´Ð°Ñ Ð¾Ñ Ð¾Ð¼, Ð½Ð°Ð¿Ñ Ð¸Ð¼Ñ , Ð¿Ñ Ð¸Ñ Ð¸Ð½Ð° Ð±Ð»Ð¾ÐºÐ¸Ñ Ð¾Ð²ÐºÐ¸ Ñ Ð°Ð¹Ñ Ð°.	"url_cats" Networkir
proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾Ð¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP
host	Ð Ð¼Ñ Ñ Ð¾Ñ Ñ Ð°.	www.goo
action	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ñ Ð¸ÐºÐ¾Ð»Ñ Ð¸ÐºÐ°Ð¾Ð¼Ð¼.	block
bytes_sent	Ð Ð¾Ð»Ñ ÐµÑ Ñ Ð²Ð¾ Ð±Ð°Ð¹Ñ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð¾Ñ Ð²Ð»ÐµÐ½Ð¸Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ.	52
bytes_recv	Ð Ð¾Ð»Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿Ð°ÐºÐµÑ Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð¾Ð²Ð»ÐµÐ½Ð¸Ñ Ð¸Ñ Ð¸Ñ Ð¾Ñ Ð¾Ð¼ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	100
packets_sent	Ð Ð¾Ð»Ñ ÐµÑ Ñ Ð²Ð¾ Ð¿Ð°ÐºÐµÑ Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð¾Ð²Ð»ÐµÐ½Ð¸Ñ Ð¸Ñ Ð¸Ñ Ð¾Ñ Ð¾Ð¼ â Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ.	2
packets_recv	Ð Ð¾Ð»Ñ ÐµÑ Ñ Ð²Ð¾ Ð±Ð°Ð¹Ñ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð¾Ð²Ð»ÐµÐ½Ð¸Ñ Ð¸Ñ Ð¸Ñ Ð¾Ñ Ð¾Ð¼ â Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	5
request_method	Ð ÐµÑ Ð¾Ð´, Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð´Ð»Ñ Ñ Ð´Ñ Ñ Ñ Ð¿Ð° Ðº URL-Ð°Ð´Ñ ÐµÑ (POST, GET Ð¸ Ñ .Ð¿.).	GET
url	Ð Ð¾Ð»Ðµ Ð¾Ð´ÐµÑ Ð¶Ð¸Ñ URL-Ð°Ð´Ñ ÐµÑ Ð·Ð°Ð¿Ñ Ð¾Ñ Ð¸Ð²Ð°ÐµÐ¾Ð¼Ð¾Ð¾ Ñ ÐµÑ Ñ Ñ Ñ Ð° Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸Ðµ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ð½Ð¾.	http://ww
media_type	Ð¢Ð¸Ð¿ ÐºÐ¾Ð½ÑÐµÐ½Ñ Ð°.	applicatio
status_code	Ð Ð¾Ð´ Ð¾Ñ Ð²ÐµÑ Ð° HTTP.	302

Р Р°Р·Р²Р°Р½Р¸Ро Р¿Р¾Р»Ñ			Р Р¿Р¸Ñ Р°Р½Р¸Ро	Р Ñ Р
http_referer			URL Р¸Ñ Ñ Р¾Ñ Р½Р¸РºР° Р·Р°Р¿Ñ Р¾Ñ Р° (Ñ РѕÑ РѕÑ РѕÑ HTTP).	https://ww
decrypted			Р Р¾Р»Ро Ñ РєР°Р·Ñ Р²Р°РѕÑ Р±Ñ Р»Р¾ Р»Р¸ Ñ Р¾Р´РѕÑ Р¶Р¸Р¼Р¾Ро Ñ Р°Ñ Ñ Р¸Ñ Ñ Р¾Р²Р°Р½Р¾.	true, false
useragent			Useragent Р¿Р¾Р»Ñ Р·Р¾Р²Р°Ñ РѕР»Ñ Ñ РєР¾Р³Р¾ Р±Ñ Р°Ñ Р·РѕÑ Р°.	Mozilla/5. rv:96.0) G
application		**id**	Р Р´РѕР½Ñ Р¸Ñ Р¸РєР°Ñ Р¾Ñ Р¿Ñ Р¸Р»Р¾Р¶РѕР½Р¸Ñ .	20
		name	Р Р°Р·Р²Р°Р½Р¸Ро Р¿Ñ Р¸Р»Р¾Р¶РѕР½Р¸Ñ .	Youtube
		threat_level	Р£Ñ Р¾Р²РѕР½Ñ Ñ Р³Ñ Р¾Р·Ñ Р¿Ñ Р¸Р»Р¾Р¶РѕР½Р¸Ñ .	0
		app_protocol	Р Ñ Р¾Ñ Р¾РєР¾Р» Р¿Ñ Р¸РєР»Р°Р´Р½Р¾Р³Р¾ Ñ Ñ Р¾Р²Р½Ñ Р¸ РѕР³Р¾ Р²РѕÑ Р¸Ñ .	HTTP\/1.1
url_categories	**id**		Р Р´РѕР½Ñ Р¸Ñ Р¸РєР°Ñ Р¾Ñ РєР°Ñ РѕР³Р¾Ñ Р¸Р¸, Рє РєР¾Ñ Р¾Ñ Р¾Р¹ Р¾Ñ Р½Р¾Ñ Р¸Ñ Ñ Ñ URL.	39
	threat_level		Р£Ñ Р¾Р²РѕР½Ñ Ñ Р³Ñ Р¾Р·Ñ РєР°Ñ РѕР³Р¾Ñ Р¸Р¸ URL.	Р Р¾Р¶ Р·Р½Р°Ñ • 1 Р • 2 • 3 • 4 • 5 Р²
	name		Р Р°Р·Р²Р°Р½Р¸Ро РєР°Ñ РѕР³Р¾Ñ Р¸Р¸, Рє РєР¾Ñ Р¾Р¹ Р¾Ñ Р½Р¾Ñ Р¸Ñ Ñ Ñ URL.	Social Ne
source	**zone**	**guid**	Р£Р½Р¸РєР°Р»Ñ Р½Ñ Р¹ Р¸Р´РѕР½Ñ Р¸Ñ Р¸РєР°Ñ Р¾Ñ Р·Р¾Р½Ñ Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР°.	d003891
		name	Р Р°Р·Р²Р°Р½Р¸Ро Р·Р¾Р½Ñ Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР°.	Trusted
	country		Рiѕ Ñ Р°Р½Р° Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР° Ñ Ñ Р°Ñ Р¸РєР°.	RU (Р¾Ñ Р´Р²Ñ Ñ Ñ Ñ Р
	ip		IPv4-Р°Р´Ñ РѕÑ Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР°.	10.10.10.
	port		Р Р¾Ñ Ñ Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР°.	Р Р¾Р¶ Р·Р½Р°Ñ 65535.
	mac		MAC-Р°Р´Ñ РѕÑ Р¸Ñ Ñ Р¾Ñ Р½Р¸РєР°	01:23:45:
destination	**zone**	**guid**	Р£Р½Р¸РєР°Р»Ñ Р½Ñ Р¹ Р¸Р´РѕР½Ñ Р¸Ñ Р¸РєР°Ñ Р¾Ñ Р·Р¾Р½Ñ Р½Р°Р·Р½Р°Ñ Р¸Ñ Ñ Р°Ñ Р¸РєР°.	3c0b1253
		name	Р Р°Р·Р²Р°Р½Р¸Ро Р·Р¾Р½Ñ Р½Р°Р·Р½Р°Ñ Р¸Ñ Ñ Р°Ñ Р¸РєР°.	Untrusted
	country		Рiѕ Ñ Р°Р½Р° Р½Р°Р·Р½Р°Ñ Р¸Р½Р¸Ñ .	

			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ
				RU (Đ¾Ñ Đ´Đ²Ñ Ñ Ñ Ñ Đ
Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	**ip**		IPv4-Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	192.168.
	port		Đ Đ¾Ñ Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶Đ·Đ½Đ°Ñ 65535.
rule	**mac**		MAC-Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	01:23:45
	guid		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ½Đ¸Đµ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	f93da24d
	name		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	Default a
	type		Đ¢Đ¸Đ¿ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	
	guid		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	a7a3cd49
	name		Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ	user_nam
user	**groups**	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	919878b
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Default G

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° DNS

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-0
session	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ ĐµÑ Ñ Đ¸Đ¸.	00000
node	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcon
reasons	Đ Ñ Đ¸Ñ Đ¸Đ½Đ°, Đ¿Đ¾ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Đ±Ñ Đ»Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ½Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ, Đ½Đ°Đ¿Ñ Đ¸Đ¼ĐµÑ , url ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ , Đ½Đ° ĐºĐ¾Ñ Đ¾Ñ Ñ Ñ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ»Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ¾.	{"url_c
proto	Đ Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµĐ¼Ñ Đ¹ Đ¿Ñ Đ¾Đ¾ĐºĐ¾Đ» 4-Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ .	UDP
host	Đ Đ¼Ñ Ñ Đ¾Ñ Ñ Đ°.	google
data	Đ Đ¾Đ»Đµ Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Ñ ĐºĐ°Đ·Đ°Đ½Đ¸Ñ Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Ñ Ñ	{"ques

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
			Ð´Ð°Ð½Ð½Ñ Ñ .	"answe
url_categories	**id**		Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¿ÐºÐ°Ñ Ð¾Ñ Ñ Ñ Ð°Ð±Ð¾Ð½ Ð°Ð²Ñ ÐµÐ¹ URL-ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸.	37
	threat_level		Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ñ Ñ Ð°Ð±Ð¾Ð½ Ð°Ð²Ñ ÐµÐ¹ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸.	Ð Ð¾Ð¿ • • • • •
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð±Ð¾Ð½ Ð°Ð²Ñ ÐµÐ¹ ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸.	Search
action			Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ð, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ð¿ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸Ð»Ð¸ Ð¸ÐºÐ°Ð¸.	block
application		**id**	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ð¾Ð»Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	5
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	
		threat_level	Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ð¿Ð¾Ð»Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	0
		app_protocol	Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	DNS
source	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð·Ð¾Ð½Ñ Ñ Ð¾Ñ Ð¸ÐºÐ°.	d0038
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ñ Ð¾Ñ Ð¸ÐºÐ°.	Truste
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ð½Ñ Ð¸ÐºÐ°.	RU (Ð¾
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.
	port		Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¿
	mac		MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	01:23:
destination	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	3c0b12
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrus
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ .	RU (Ð¾
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	104.19
	port		Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ	Ð Ð¾Ð¿ Ð¿Ð¾Ñ
	mac		MAC-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð½Ñ	01:23:
rule	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹	59e38

			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ			Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	Rule1
	Type		Ð¢Ð¸Ð¿ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ³Ð¾ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	
user	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ . Ð Ñ Ð»Ð¸ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ Ñ Ð¸Ð¿Ð° Unknown, Ñ Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ : 00000000-0000-0000-0000-000000000000.	a7a3cd
	name		Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user1
	groups	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð³Ñ Ñ Ð¿Ð¿Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ñ Ñ Ñ Ð¾Ñ Ñ Ð¾Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	919878
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð³Ñ Ñ Ð¿Ð¿Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ñ Ð¾Ñ Ñ Ð¾Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	Default

Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸Ð¼ÐµÑ Ð·Ð½
timestamp	Ð Ñ ÐµÐ¼Ñ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¸Ñ Ñ Ð¾Ð±Ñ Ñ Ð¸Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15
session	Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð¸.	a7a3cd49-8232-4f1a-962 (ÐµÑ Ð»Ð¸ System: 00000000-0000-0000-00
node	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	utmcore@ersthetatica
proto	Ð Ñ Ð¿Ð¾Ð»Ñ Ð·Ñ ÐµÐ¼Ñ Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» 4-Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	TCP Ð¸Ð»Ð¸ UDP
action	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ð¸Ñ Ð¸ÐºÐ°Ð¼Ð¸.	accept
bytes_sent	Ð Ð¾Ð»Ð¸Ñ ÐµÑ Ñ Ð²Ð¾ Ð±Ð°Ð¹Ñ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð²	100

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½
			Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	
bytes_recv			Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ±Đ°Đ¹Ñ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.	6
packets_recv			Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿Đ°ĐºĐµÑ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº.	1
packets_sent			Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿Đ°ĐºĐµÑ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	1
json_data			Đ Đ¾Đ¿Đ¾Đ»Đ½Đ¸Ñ ĐµĐ»Ñ Đ½Ñ Đµ Đ´Đ°Đ½Đ½Ñ Đµ.	null
application	**id**		Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	195
	threat_level		Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶ĐµÑ Đ¿Ñ Đ¸Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ : • 1 â Đ¾Ñ ĐµĐ½ Đ½Đ¸Đ·ĐºĐ¸Đ¹. • 2 â Đ½Đ¸Đ·ĐºĐ • 3 â Ñ Ñ ĐµĐ´Đ • 4 â Đ²Ñ Ñ Đ¾ • 5 â Đ¾Ñ ĐµĐ½ Đ²Ñ Ñ Đ¾ĐºĐ¸Đ¸Đ
	app_protocol		Đ Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ» Đ¿Ñ Đ¸ĐºĐ»Đ°Đ´Đ½Đ¾Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ .	HTTP
	name		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Youtube
source	**zone**	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	d0038912-0d8a-4583-a5
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	Trusted
	country		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	RU (Đ¾Ñ Đ¾Đ±Ñ Đ°Đ¶Đ´Đ²Ñ Ñ Đ±Ñ ĐºĐ²ĐµÑ Ñ Ñ Ñ Đ°Đ½Ñ)
	ip		IPv4-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	10.10.10.10

			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ð¼Ñ	Ð Ñ Ð¸Ð¼ÐµÑ Ð·Ð½Ð
	port		Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾Ð¶Ð¸Ð´Ð°ÐµÑ Ð¿Ð Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð 65535.
Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ñ Ð¿Ð¾Ð»Ñ **destination**	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	3c0b1253-f069-4060-90
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	RU (Ð¾Ñ Ð¾Ð±Ñ Ð°Ð´Ð²Ð¾Ð´Ñ Ñ Ð±Ñ ÐºÐ²Ðµ Ñ Ñ Ñ Ð°Ð½Ñ)
	ip		IPv4-Ð°Ð´Ñ Ðµ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	104.19.197.151
	port		Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ	Ð Ð¾Ð¶Ð¸Ð´Ð°ÐµÑ Ð¿Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð 65535.
nat	**source**	**ip**	Ð Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð¿Ð¾Ð»Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð° NAT).	192.168.117.85 (ÐµÑ Ð Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½,
		port	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð¿Ð¾Ð»Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð° NAT).	Ð Ð¾Ð¶Ð¸Ð´Ð°ÐµÑ Ð¿Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ (ÐµÑ Ð»Ð¸ NAT Ð½Ðµ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½,
	destination	**ip**	Ð Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð° NAT).	64.233.164.198 (ÐµÑ Ð Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½,
		port	Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ð¿Ð¾Ð»Ñ Ð»Ðµ Ð¿ÐµÑ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ (ÐµÑ Ð»Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð° NAT).	Ð Ð¾Ð¶Ð¸Ð´Ð°ÐµÑ Ð¿Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð°Ð·Ð½Ð°Ñ ÐµÐ (ÐµÑ Ð»Ð¸ NAT Ð½Ðµ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½,
rule	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¿Ñ Ð°Ð²Ð¸Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð½ÐµÐ¼ ÐºÐ¾Ð¼Ð¾Ð½ÐµÐ½Ñ Ð¾Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ð±ÑÐµÐºÑ Ð¾Ð².	59e38e06-533a-4771-96
	type		Ð¢Ð¸Ð¿ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	firewall
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð½ÐµÐ¼ ÐºÐ¾Ð¼Ð¾Ð½ÐµÐ½Ñ Ð¾Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ð±ÑÐµÐºÑ Ð¾Ð².	Allow trusted to untruste
user	**guid**			a7a3cd49-8232-4f1a-96

			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½
Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ . Đ Ñ Đ»Đ¸ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ Ñ Đ¸Đ° Unknown, Ñ Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ : 00000000-0000-0000-0000-000000000000.	
	name		Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Admin
	groups	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ³Ñ Ñ Đ¿Đ¸Ñ , Đ² ĐºĐ¾Đ¾Ñ Đ¾Ñ Ñ Ñ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	919878b2-e882-49ed-33
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ³Ñ Ñ Đ¿Đ¸Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Default Group

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° ĐiĐ Đ

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.158
session	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ ĐµÑ Ñ Đ¸Đ¸.	a7a3cd49-8232-4f1a-962a (ĐµÑ Đ»Đ¸ System: 00000000-0000-0000-000
node	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ersthetatica
proto	Đ Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµĐ¼Ñ Đ¹ Đ¿Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ» 4-Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ .	TCP Đ¸Đ»Đ¸ UDP
action	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	accept
bytes_sent	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ±Đ°Đ¹Ñ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	100
bytes_recv	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ±Đ°Đ¹Ñ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đ¼.	6
packets_sent		1

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸Ð¼ÐµÑ Ð·Ð½
			Ð Ð¾Ð»Ð¸Ñ Ñ Ð²Ð¾ Ð¿Ð°ÐºÐµÑ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº â Ð½Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ.	
packets_recv			Ð Ð¾Ð»Ð¸Ñ Ñ Ð²Ð¾ Ð¿Ð°ÐºÐµÑ Ð¾Ð², Ð¿ÐµÑ ÐµÐ´Ð°Ð½Ð½Ñ Ñ Ð² Ð½Ð°Ð¿Ñ Ð°Ð²Ð»ÐµÐ½Ð¸Ð¸ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ðº.	1
json_data			Ð Ð¾Ð¿Ð¾Ð»Ð½Ð¸Ñ ÐµÐ»Ñ Ð½Ñ Ðµ Ð´Ð°Ð½Ð½Ñ Ðµ.	null
application	**id**		Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ð¸Ñ Ð¸ Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	195
	threat_level		Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ð¿Ð¸Ñ Ð¸ Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶ÐµÑ Ð¿Ñ Ð¸Ð½Ð·Ð½Ð°Ðº : • 1 â Ð¾Ñ ÐµÐ½Ð½Ð¸Ð·ÐºÐ¸Ð¹. • 2 â Ð½Ð¸Ð·ÐºÐ¸ • 3 â Ñ Ñ ÐµÐ´Ð¹ • 4 â Ð²Ñ Ñ Ð¾Ð • 5 â Ð¾Ñ ÐµÐ½Ð½Ð² Ð²Ñ Ñ Ð¾ÐºÐ¸Ð¹
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð¸Ð»Ð¾Ð¶Ð¸Ñ .	Youtube
	app_protocol		Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¾ÐºÐ¾Ð»Ð° Ñ Ñ Ð¾Ð²Ð½Ñ .	HTTP
user	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ÑÐ¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ð¸Ñ Ð¸ Ð·Ð¾Ð²Ð°Ð½Ñ . Ð Ñ Ð»Ð¸Ð¿Ð¾Ñ Ð·Ð¾Ð²Ð°Ð½Ñ Ñ Ð¿Ð¿Ð° Unknown, Ñ Ð¾ Ð¸Ð´ÐµÐ½Ñ Ð¸ÑÐ¸ÐºÐ°Ñ Ð¾Ñ : 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a
	name		Ð Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	Admin
	groups	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ÑÐ¸ÐºÐ°Ñ Ð¾Ñ Ð³Ñ Ñ Ð¿Ð¿Ñ , Ð² ÐºÐ¾Ð¼Ð¾Ñ Ñ Ñ Ð¾Ð¼Ñ Ñ Ð¾Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ .	919878b2-e882-49ed-333
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð³Ñ Ñ Ð¿Ð¿Ñ , Ð² ÐºÐ¾Ð¼Ð¾Ñ Ð¾Ð¹ Ñ Ð¾Ð¼Ñ Ñ Ð¾Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ .	Default Group
rule	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ÑÐ¸ÐºÐ°Ñ Ð¾Ñ Ð¿Ð¸Ñ Ð¸ Ð°Ð²Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð½Ð¾Ðµ	59e38e06-533a-4771-966

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸Ð¼ÐµÑ Ð·Ð½Ð
			ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð³Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ ÐºÐ¾Ñ Ð¾Ð³Ð¾ Ð²Ñ Ð·Ð²Ð°Ð» Ñ Ð¾Ð±Ñ Ñ Ð¸Ðµ.	Allow trusted to untrusted
	type		Ð¢Ð¸Ð¿ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ³Ð¾ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°	idps
signatures	**id**		Ð Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ¹ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ .	999999
	threat_level		Ð£Ñ Ð¾Ð²ÐµÐ½Ñ Ñ Ð³Ñ Ð¾Ð·Ñ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ¹ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ .	Ð Ð¾Ð¶ÐµÑ Ð¿Ñ Ð¸Ð·Ð½Ð°Ñ ÐµÐ½Ñ : • 1 â Ð¾Ñ ÐµÐ½Ñ Ð½Ð¸Ð·ÐºÐ¸Ð¹. • 2 â Ð½Ð¸Ð·ÐºÐ¸ • 3 â Ñ Ñ ÐµÐ´Ð¸ • 4 â Ð²Ñ Ñ Ð¾Ð • 5 â Ð¾Ñ ÐµÐ½Ñ Ð²Ñ Ñ Ð¾ÐºÐ¸Ð¹
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ ÐµÐ¹ Ñ Ð¸Ð³Ð½Ð°Ñ Ñ Ñ .	BlackSun Test
source	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¾Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¾Ð° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	d0038912-0d8a-4583-a52
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¾Ð° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Trusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð½Ñ Ñ Ñ Ð¾Ñ Ð½Ð°.	RU (Ð¾Ñ Ð¾Ð±Ñ Ð°Ð¶Ð²Ð°Ñ Ñ Ð±Ñ ÐºÐ²ÐµÐ½Ñ Ñ Ñ Ð°Ñ Ð½Ñ)
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ð°Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.10
	port		Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ð°Ñ Ð¸ÐºÐ°.	Ð Ð¾Ð¶ÐµÑ Ð¿Ñ Ð¸Ð½Ð°Ñ ÐµÐ½Ñ Ð¾Ñ Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¾Ñ 65535.
	mac		MAC-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸Ð°Ñ Ð¸ÐºÐ°.	01:23:45:67:89:AB
	zone	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¾Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð°Ð°Ð½Ð½Ð¾Ð¹ Ð¿Ñ Ð¾Ñ Ð¸Ð»Ð¸ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	3c0b1253-f069-4060-903b
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrusted
destination	**country**		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ñ .	RU (Ð¾Ñ Ð¾Ð±Ñ Ð°Ð´Ð²Ð°Ñ Ñ Ñ Ð±Ñ ÐºÐ²ÐµÐ½Ñ Ñ Ñ Ð°Ñ Ð½Ñ)
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	104.19.197.151
	port		Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	Ð Ð¾Ð¶ÐµÑ Ð¿Ñ Ð¸Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¾Ñ

		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½
Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			65535.
	mac	MAC Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	01:23:45:67:89:AB

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶ÑÑ Đ½Đ°Đ»Đ° Đ ĐiĐ£ Đ¢Đ

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ Đµ
timestamp		Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Đ Ñ Đ¸Ñ Đ¸Ñ Đ½Đ¾Ñ Ñ Ñ Đ ĐiĐ£ Đ¢Đ .	1
pdu_func		Đ Đ¾Đ´ Ñ Ñ Đ½ĐºÑ Đ¸Đ¸ (Đ³Đ¾Đ²Đ¾Ñ Đ¸Ñ Đ²ĐµĐ´Đ¾Đ¼Đ¾Đ¼Ñ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Ñ , ĐºĐ°ĐºĐ¸Đµ Đ´Đ°Đ½Đ½Ñ Đµ Đ¸Đ»Đ¸ Đ²Ñ Đ¿Đ¾Đ»Đ½ĐµĐ½Đ¸Đµ ĐºĐ°ĐºĐ¾Đ³Đ¾ Đ´ĐµĐ¹Ñ Ñ Đ²Đ¸Ñ Ñ Ñ ĐµĐ±Ñ ĐµÑ Đ¾Ñ Đ½ĐµĐ³Đ¾ Đ²ĐµĐ´Ñ Ñ ĐµĐµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾).	12
pdu_address		Đ Đ´Ñ ĐµÑ Ñ ĐµĐ³Đ¸Ñ Ñ Ñ Đ°, Ñ ĐºĐ¾Ñ Đ¾Ñ Ñ Đ¼ Đ½ĐµĐ¾Đ±Ñ Đ¾Đ´Đ¸Đ¼Đ¾ Đ¿Ñ Đ¾Đ²ĐµÑ Ñ Đ¸ Đ¾Đ¿ĐµÑ Đ°Ñ Đ¸Ñ .	3154
node		Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ersthetatica
details	**pdu_varname**	Đ Đ¼Ñ Đ¿ĐµÑ ĐµĐ¼ĐµĐ½Đ½Đ¾Đ¹. Đ Đ°Ñ Đ°Đ¼ĐµÑ Ñ , Đ² Đ¾Ñ Đ½Đ¾Đ²Đ½Đ¾Đ¼, Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµÑ Ñ Ñ Đ´Đ»Ñ Đ¾Đ±Đ¼ĐµĐ½Đ° Đ´Đ°Đ½Đ½Ñ Đ¼Đ¸ Đ² Ñ ĐµĐ¶Đ¸Đ¼Đ¸ Ñ ĐµĐ°Đ»Ñ Đ½Đ¾Đ³Đ¾ Đ²Ñ ĐµĐ¼ĐµĐ½Đ¸. Đ Đ°Ñ Đ°Đ¼ĐµÑ Ñ Đ¾Ñ Đ½Đ¾Ñ Đ¸Ñ Ñ Ñ Đº Đ¿Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ»Ñ MMS.	VAR
	pdu_device	Đ Đ´Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°, Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµĐ¼Ñ Đ¹ Đ² Đ¿Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ»Đ°Ñ MMS Đ¸ OPCUA.	DEV
	mb_write_quantity	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đ¹ Đ´Đ»Ñ Đ·Đ°Đ¿Đ¸Ñ Đ¸ (ĐºĐ¾Đ¼Đ¼Đ°Đ½Đ´Đ° Read Write Register).	998
	mb_write_addr		776

		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ Đµ
		Đ Đ°Ñ Đ°Đ»Ñ Đ½Ñ Đ¹ Đ°Đ´Ñ ĐµÑ Ñ ĐµĐ³Đ¸Ñ Ñ Ñ Đ° Đ´Đ»Ñ Đ·Đ°Đ¿Đ¸Ñ Đ¸ (ĐºĐ¾Đ¼Đ°Đ½Đ´Đ° Read Write Register).	
	mb_value	Đ Đ°Đ¿Đ¸Ñ Ñ Đ²Đ°ĐµĐ¼Đ¾Đµ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ (Đ´Đ»Ñ ĐºĐ¾Đ¼Đ°Đ½Đ´ Write Single Coil, Write Single Register).	322
	mb_unit_id	Đ Đ´Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°.	186
	mb_read_quantity	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đ¹ Đ´Đ»Ñ Ñ Ñ ĐµĐ½Đ¸Ñ (ĐºĐ¾Đ¼Đ°Đ½Đ´Đ° Read Write Register).	658
	mb_read_addr	Đ Đ°Ñ Đ°Đ»Ñ Đ½Ñ Đ¹ Đ°Đ´Ñ ĐµÑ Ñ ĐµĐ³Đ¸Ñ Ñ Ñ Đ° Đ´Đ»Ñ Ñ Ñ ĐµĐ½Đ¸Ñ (ĐºĐ¾Đ¼Đ°Đ½Đ´Đ° Read Write Register).	122
	mb_quantity	Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đ¹ Đ´Đ»Ñ Ñ Ñ ĐµĐ½Đ¸Ñ .	875
	mb_payload	Đ Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ ĐµĐ³Đ¸Ñ Ñ Ñ Đ¾Đ² (Đ´Đ»Ñ ĐºĐ¾Đ¼Đ°Đ½Đ´ Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdc24f9883
	mb_or_mask	Đ Đ½Đ°Ñ ĐµĐ½Đ¸Đµ Đ¼Đ°Ñ ĐºĐ¸ OR ĐºĐ¾Đ¼Đ°Đ½Đ´Ñ Mask Write Register.	1024
Đ Đ°Đ·Đ²Đ¾Đ¼Đ¸Đµ Đ¿Đ¾Đ»Ñ	**mb_message**	Đ¡Đ¾Đ¾Đ±Ñ ĐµĐ½Đ¸Đµ Modbus.	exception
	mb_exception_code	Đ Đ¾Đ´ Đ¾Ñ Đ¸Đ±ĐºĐ¸. Đ¢Đ°Đ»ĐµĐ½ Đ°Đ»ĐµĐ½ Ñ Đ¸Đ¼Đ²Đ¾Đ» Đ´Đ»Ñ Ñ Đ¸Đ¼Đ²Đ¾Đ»Ñ ĐµĐ½Đ¸Ñ error_response.	255
	mb_and_mask	Đ Đ½Đ°Ñ ĐµĐ½Đ¸Đµ Đ¼Đ°Ñ ĐºĐ¸ AND ĐºĐ¾Đ¼Đ°Đ½Đ´Ñ Mask Write Register.	121
	mb_addr	Đ Đ´Ñ ĐµÑ Ñ ĐµĐ³Đ¸Ñ Ñ Ñ Đ°.	3154
	iec104_msgtype	Đ¢Đ¸Đ¿ Đ·Đ°Đ¿Ñ Đ¾Ñ Đ°.	request, response, error_respons
	iec104_ioa	Đ Đ´Ñ ĐµÑ Đ¾Đ±Ñ ĐµĐºÑ Đ° Đ¸Đ½Ñ Đ¾Đ¾Ñ Đ¼Đ°Ñ Đ¸, ĐºĐ¾Đ¾Ñ Đ¾Ñ Ñ Đ¹ Đ¿Đ¾Đ·Đ²Đ¾Đ»Ñ ĐµÑ Đ¾Đ´ĐµĐ½Ñ Đ¾Ñ Đ¾Ñ Đ¾Ñ Đ¾Đ²Đ°Ñ Ñ Đ¿Ñ Đ¾Ñ Đ¼Đ½Đ¾Đ¹ Ñ Ñ Đ¾Ñ Đ¾Đ½Đ¾Đ¹ Ñ Đ¾Đ¿ Ñ Đ¾Đ±Ñ Ñ Đ¾Ñ .	23
	iec104_cot	Đ Ñ Đ¾Ñ Đ¾Đ½Đ° Đ¿ĐµÑ ĐµĐ´Đ°Ñ Đ¾ Đ¿Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ»Ñ Đ½Đ¾Đ³Đ¾ Đ±Đ»Đ¾ĐºĐ° Đ´Đ°Đ½Đ½Ñ Ñ Đ¿Ñ Đ¾ĐºĐ»Đ°Đ´Đ½Đ¾Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ (Application Protocol Data Unit, APDU).	6

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸ÐµÑ Ð·Ð½Ð°Ñ Ð
	iec104_asdu		Ð Ð´Ñ ÐµÑ ASDU (COA â Common Object Address). Ð Ð°Ñ Ð°Ð¼ÐµÑ Ñ Ð¾Ñ Ð½Ð¾Ñ Ð¸Ñ Ñ Ñ Ðº Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð»Ñ IEC-104.	123
app_protocol			Ð Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð» Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	Modbus
action			Ð ÐµÐ¹Ñ Ñ Ð²Ð¸, Ð¿Ñ Ð¸Ð½Ñ Ñ Ð¾Ð¼ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸ Ð½Ð°Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ð¼Ð¸ Ð¿Ð¾Ð»Ñ Ð¸Ð¼Ð¸.	pass
source	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¾Ð¾Ñ Ð¾Ð¶Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð¸Ð½Ð¾Ð° Ñ Ñ Ð°Ñ Ð¸Ð¼Ñ	d0038912-0d8a-4583-a525-e639
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ñ Ñ Ð¾Ð¾Ñ Ð¾Ð¶Ð½Ñ Ñ Ñ Ð°Ñ Ð¸Ð¼Ñ	Trusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ñ Ñ Ñ Ð¾Ñ Ð¾Ð¾Ñ Ð°Ð½Ð¸Ñ.	RU (Ð¾Ñ Ð¾Ð±Ð°Ð°Ñ Ð°Ð¿Ð°Ñ Ð´Ð²Ñ Ñ Ð±Ð²ÐµÐ½Ð½Ñ ÐºÐ¾Ð´ Ñ Ñ Ñ Ð°Ð½Ñ)
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¾ÐºÐ° Ñ Ñ Ð°Ñ Ð¸Ñ.	10.10.10.10
	port		Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¾ÐºÐ°.	Ð Ð¾Ð¶Ð¸ÐµÑ Ð¿Ñ Ð¸Ð½Ð¸Ð¼Ð°Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¾Ñ 0 Ð 65535.
destination	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¾Ð¾Ñ Ð¾Ð¶Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸Ð¼Ñ	3c0b1253-f069-4060-903b-5fec4
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸Ð¼Ñ	Untrusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ .	RU (Ð¾Ñ Ð¾Ð±Ð°Ð°Ñ Ð°Ð¿Ð°Ñ Ð´Ð²Ñ Ñ Ð±Ð²ÐµÐ½Ð½Ñ ÐºÐ¾Ð´ Ñ Ñ Ñ Ð°Ð½Ñ)
	ip		IPv4-Ð°Ð´Ñ ÐµÑ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¸Ñ.	104.19.197.151
	port		Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ	Ð Ð¾Ð¶Ð¸ÐµÑ Ð¿Ñ Ð¸Ð½Ð¸Ð¼Ð°Ñ Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ Ð¾Ñ 0 Ð 65535.
rule	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸ Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð¾Ð¾Ñ Ð¾Ð¶Ð½Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð½Ñ ÐºÐ¾Ð¼Ð¿Ð¾Ð½Ñ Ð¾Ð¼Ñ Ñ Ð¾Ð·Ð´Ð°Ð»Ð¾ Ñ Ð¾Ð±Ñ Ñ Ð¾Ñ.	59e38e06-533a-4771-9664-031c

		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ Đµ
	name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	SCADA Sample Rule

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ¸Đ½Ñ Đ¿ĐµĐºÑ Đ¸Ñ Đ¾Đ²Đ°Đ½Đ¸Ñ SSH

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ
timestamp			Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:1
node			Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ersthet
command			Đ Đ¾Đ¼Đ°Đ½Đ´Đ°, Đ¿ĐµÑ ĐµĐ´Đ°Đ²Đ°ĐµĐ¼Đ°Ñ Đ¿Đ¾ SSH.	whoami
action Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	block
application		**id**	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	195
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	
		threat_level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶ĐµÑ Đ¿ Đ·Đ½Đ°Ñ ĐµĐ½ (Ñ Ñ Ñ Đ°Đ½Đ¾ Ñ Ñ Đ¾Đ²ĐµĐ½ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ Ñ Đ¼Đ½Đ¾Đ¶Đ
		app_protocol	Đ Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ» Đ¿Ñ Đ¸ĐºĐ»Đ°Đ´Đ½Đ¾Đ³Đ¾ Ñ Ñ Đ¾Đ²Đ½Ñ .	SSH Đ¸Đ» SFTP
source	**zone**	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	d0038912-0d8a-4
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	Trusted
	country		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	RU (Đ¾Ñ Đ¾Đ±Ñ Đ´Đ²Ñ Ñ Đ±Ñ Đ ĐºĐ¾Đ´ Ñ Ñ Ñ Đ
	ip		IPv4-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	10.10.10.10
	port		Đ Đ¾Ñ Ñ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	Đ Đ¾Đ¶ĐµÑ Đ¿ Đ·Đ½Đ°Ñ ĐµĐ½ 65535.

			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ
	mac		MAC-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	FA:16:3E:65:1C:B4
destination	**zone**	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	3c0b1253-f069-40
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ·Đ¾Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	Untrusted
	country		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Đ°Đ½Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	RU (Đ¾Ñ Đ¾Đ±Ñ Đ´Đ²Ñ Ñ Đ±Ñ Đ ĐºĐ¾Đ´ Ñ Ñ Ñ Đ
	ip		IPv4-Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°.	104.19.197.151
	port		Đ Đ¾Ñ Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶ĐµÑ Đ¿Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ 65535.
rule	**mac**		MAC-Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	01:23:45:67:89:AI
	guid		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	59e38e06-533a-4
	name		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	SSH Rule Example
	type		Đ¢Đ¸Đ¿ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	ssh
user	**guid**		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ . Đ Ñ Đ»Đ¸Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ Ñ Đ¸Đ¿Đ° Unknown, Ñ Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ : 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4
	name		Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Admin
	groups	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Ñ Ñ Ñ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	919878b2-e882-4
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Default Group

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ·Đ°Ñ Đ¸Ñ Ñ Đ¿Đ¾Ñ Ñ Đ¾Đ²Đ¾Đ³Đ¾ Ñ Ñ Đ°Ñ Đ¸ĐºĐ°

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ
node		Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾Đ¸Đ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ersthetatic
action		Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	mark
bytes_sent		Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ±Đ°Đ¹Ñ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	0
bytes_recv		Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ±Đ°Đ¹Ñ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	0
packets_sent		Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿Đ°ĐºĐµÑ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	0
packets_rcv		Đ Đ¾Đ»Đ¸Ñ ĐµÑ Ñ Đ²Đ¾ Đ¿Đ°ĐºĐµÑ Đ¾Đ², Đ¿ĐµÑ ĐµĐ´Đ°Đ½Đ½Ñ Ñ Đ² Đ½Đ°Đ¿Ñ Đ°Đ²Đ»ĐµĐ½Đ¸Đ¸ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸Đº â Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Đµ.	0
decrypted		Đ Đ¾Đ»Đµ Ñ ĐºĐ°Đ·Ñ Đ²Đ°ĐµÑ Đ±Ñ Đ»Đ¾ Đ»Đ¸ Ñ Đ¾Đ´ĐµÑ Đ¶Đ¸Đ¼Đ¾Đµ Ñ Đ°Ñ Ñ Đ¸Ñ Ñ Đ¾Đ²Đ°Đ½Đ¾.	true, false
from		Đ Đ¾Ñ Ñ Đ¾Đ²Ñ Đ¹ Đ°Đ´Ñ ĐµÑ Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Đ» .	sender@example.cor
to		Đ Đ¾Ñ Ñ Đ¾Đ²Ñ Đ¹ Đ°Đ´Ñ ĐµÑ Đ¿Đ¾Đ»Ñ Ñ Đ°Ñ ĐµĐ»Ñ .	receiver@example.co
application	**id**	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	9
	name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	
	threat_level	Đ£Ñ Đ¾Đ²ĐµĐ½Ñ Ñ Đ³Ñ Đ¾Đ·Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	Đ Đ¾Đ¶ĐµÑ Đ¿Ñ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ (Ñ Ñ Ñ Đ°Đ½Đ¾Đ² Ñ Ñ Đ¾Đ²ĐµĐ½Ñ

			Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸Ð¼ÐµÑ Ð
Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ				Ð¿Ñ Ð¸Ð»Ð¾Ð¶ÐµÐ½Ð¸Ñ Ð¼Ð¾Ð¶ÐµÑ
		app_protocol	Ði ÐµÑ ÐµÐ²Ð¾Ð¹ Ð¿Ñ Ð¾Ñ Ð¾ÐºÐ¾Ð»Ð¾ Ð¿Ñ Ð¸ÐºÐ»Ð°Ð´Ð½Ð¾Ð³Ð¾ Ñ Ñ Ð¾Ð²Ð½Ñ .	SMTP
source	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ð·Ð½Ð°Ñ Ð¸Ñ Ñ Ð¾Ñ Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°	d0038912-0d8a-4583
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð¸ÐºÐ°.	Trusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð¸Ñ Ñ Ð¾Ñ Ð¸ÐºÐ°.	RU (Ð¾Ñ Ð¾Ð±Ñ Ð´Ð²Ñ Ñ Ð±Ñ ÐºÐ²Ð¾Ð´ Ñ Ñ Ñ Ð°Ð
	ip		IPv4-Ð°Ð´Ñ Ðµ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ° Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.10
	port		Ð Ð¾Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	Ð Ð¾ÐµÐ¼Ñ Ð¿Ñ Ð·Ð½Ð°Ñ Ðµ 65535.
	mac		MAC-Ð°Ð´Ñ Ðµ Ð¸Ñ Ñ Ð¾Ñ Ð½Ð¸ÐºÐ°.	01:23:45:67:89:AB
destination	**zone**	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ð·Ð½Ð°Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	3c0b1253-f069-4060
		name	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð·Ð¾Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	Untrusted
	country		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ñ Ñ Ñ Ð°Ð½Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ .	RU (Ð¾Ñ Ð¾Ð±Ñ Ð´Ð²Ñ Ñ Ð±Ñ ÐºÐ²Ð¾Ð´ Ñ Ñ Ñ Ð°Ð
	ip		IPv4-Ð°Ð´Ñ Ðµ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ Ñ Ð°Ñ Ð¸ÐºÐ°.	10.10.10.10
	port		Ð Ð¾Ñ Ñ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ .	Ð Ð¾ÐµÐ¼Ñ Ð¿Ñ Ð·Ð½Ð°Ñ Ðµ 65535.
	port		MAC-Ð°Ð´Ñ Ðµ Ð½Ð°Ð·Ð½Ð°Ñ Ðµ Ð¸Ñ .	01:23:45:67:89:AB
rule	**guid**		Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ð±Ñ Ð°Ñ Ð²Ð»Ñ Ñ Ñ Ð°Ð±Ð°Ñ Ð²Ð»Ðµ Ð¸Ñ Ñ Ð¾Ð²Ð°Ð½Ð¸Ñ Ð¸Ñ Ñ Ð¾Ð²Ð°Ð½Ð¸Ñ Ð¸Ñ Ð¾Ð±Ñ.	59e38e06-533a-4771
	name		Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ñ Ð°Ð±Ð°Ñ Ñ Ð²Ð°Ð½Ð¸Ðµ Ð¸Ñ Ñ Ð¾Ð²Ð°Ð½Ð¸Ñ Ð²Ñ Ð·Ð²Ð°Ð½Ð¸Ñ Ð¸Ñ Ð¾Ð±Ñ.	Mail security rule
	type		Ð¢Ð¸Ð¿ Ñ Ñ Ð°Ð±Ð¾Ñ Ð°Ð²Ñ Ðµ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°.	Mail security rule

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ
user	**guid**		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	a7a3cd49-8232-4f1a
	name		Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	user_name
	groups	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	919878b2-e882-49ec
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	Default Group

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Ñ Đ¾Đ±Ñ Ñ Đ¸Đ¹ ĐºĐ¾Đ½ĐµÑ Đ½Ñ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
user_name	Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	DESKTOP-0731NFQ\\Username
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
status	Đ ĐµĐ·Ñ Đ»Ñ Ñ Đ°Ñ Đ²Ñ Đ¿Đ¾Đ»Đ½ĐµĐ½Đ¸Ñ WMI Đ¸Đ»Đ¸ SNMP Đ·Đ°Đ¿Ñ Đ¾Ñ Đ°.	OK, Error
source_name	Đ Ñ Ñ Đ¾Ñ Đ½Đ¸Đº Đ¸Ñ Ñ Đ½Đ°Đ»Đ° Ñ Đ¾Đ±Ñ Ñ Đ¸Đ¹.	Microsoft-Windows-Security-Auditing
endpoint_name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	DESKTOP-0731NFQ
endpoint_id	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	35fb5820-74db-4eac-b05b-d01bc284c4e8
node	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ Đ·Đ»Đ°, Đ½Đ° ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¼ Đ·Đ°Đ¿Ñ Ñ ĐµĐ½ Ñ ĐµĐ½Ñ Đ¾Ñ .	35fb5820-74db-4eac-b05b-d01bc284c4e8
log_level	Đ¢Đ¸Đ¿ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	Đ Ñ Đ´Đ¸Ñ Ñ Ñ Đ¿ĐµÑ Đ°, Đ Ñ ĐµĐ´Ñ Đ¿Ñ ĐµĐ¶Đ´ĐµĐ½Đ¸Đµ, ĐiĐ²ĐµĐ´ĐµĐ½Đ¸Ñ , Đ Ñ Đ´Đ¸Ñ Đ¾Ñ ĐºĐ°Đ·Đ°, Đ Ñ Đ¸Đ±ĐºĐ°
log_file	Đ¢Đ¸Đ¿ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°, Ñ Đ¾Đ´ĐµÑ Đ¶Đ°Ñ ĐµĐ³Đ¾ Đ²Đ°Đ¶Đ½Ñ Ñ	Security (Ñ Đ°Đ¹Đ» Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ±ĐµĐ·Đ¾Đ¿Đ°Ñ Đ½Đ¾Ñ Ñ Đ¸), Application (Ñ Đ°Đ¹Đ» Đ¶Ñ Ñ Đ½Đ°Đ»Đ°

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
	Đ¸Đ½Ñ Đ¾Ñ Đ¼Đ°Ñ Đ¸Ñ Đ¾ Đ¿Ñ Đ¾Đ³Ñ Đ°Đ¼Đ¼Đ½Ñ Ñ Đ¸ Đ°Đ¿Đ¿Đ°Ñ Đ°Ñ Đ½Ñ Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Ñ .	Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Đ¹), System (Ñ Đ°Đ¹Đ» Ñ Đ¸Ñ Ñ ĐµĐ¼Đ½Đ¾Đ³Đ¾ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°), Windows PowerShell
log_event_type	Đ¢Đ¸Đ¿ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ¾Đ»Đ¾Đ³Đ°.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
log_event_id	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	4672
log_event_code	Đ Đ¾Đ´ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ¶Ñ Ñ Đ½Đ°Đ»Đ°.	14056
log_category_string	Đ Đ°Ñ ĐµĐ³Đ¾Ñ Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	Special Logon
insertion_string	Đi Ñ Ñ Đ¾ĐºĐ° Đ²Ñ Ñ Đ°Đ²ĐºĐ¸ - Đ´Đ°Đ½Đ½Ñ Đµ Đ±Đ»Đ¾ĐºĐ° EventData Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON
error	Đ Ñ Đ¸Đ±ĐºĐ° WMI Đ¸Đ»Đ¸ SNMP, Đ²Đ¾Đ·Đ½Đ¸ĐºĐ°Ñ Đ°Ñ Đ² Ñ ĐµĐ·Ñ Đ»Ñ Ñ Đ°Ñ Đµ Đ²Ñ Đ¿Đ¾Đ»Đ½ĐµĐ½Đ¸Ñ Đ·Đ°Đ¿Ñ Đ¾Ñ Đ°.	0
data	Đ Đ¾Đ´Ñ Đ¾Đ±Đ½Đ°Ñ Đ¸Đ½Ñ Đ¾Ñ Đ¼Đ°Ñ Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đ¸.	Đ¢Đ¸Đ¿ Đ·Đ°Đ¿Ñ Ñ ĐºĐ° Ñ Đ»Ñ Đ¶Đ±Ñ "Đ£Ñ Ñ Đ°Đ½Đ¾Đ²Ñ Đ¸Đº Đ¼Đ¾Đ´Ñ Đ»ĐµĐ¹ Windows" Đ±Ñ Đ» Đ¸Đ·Đ¼ĐµĐ½ĐµĐ½Đ½ Ñ "Đ Đ²Ñ Đ¾Đ¼Đ°Đ¸Ñ Đ¸Ñ ĐµĐ¸" Đ½Đ° "Đ Ñ Ñ Ñ Đ½Ñ Ñ ".
counter_id	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ Ñ Ñ Ñ Đ¸ĐºĐ°, Đ´Đ¾Đ±Đ°Đ²Đ»ĐµĐ½Đ½Đ¾Đ³Đ¾ Đ² WMI Đ¸Đ»Đ¸ SNMP Ñ ĐµĐ½Đ¾Ñ .	35fb5820-74db-4eac-b05b-d01bc284c4e8
computer_name	Đ¸Đ¼Ñ ĐºĐ¾Đ¼Đ¿Ñ Ñ Ñ ĐµÑ Đ°.	DESKTOP-0731NFQ

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ¿Ñ Đ°Đ²Đ¸Đ» ĐºĐ¾Đ½ĐµÑ Đ½Ñ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Ñ Đ¼Đ°Ñ Đ¹ Ñ Đ¾Đ¼Đ°Đ¼Đ¼Đ°: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ ĐµÑ Ñ Đ¸Đ¸.	00000006-0000-0000-f04d-14bdad0f01bb
proto	Đ Ñ Đ¿Đ¾Đ»Ñ Đ·Ñ ĐµĐ¼Ñ Đ¹ Đ¿Ñ Đ¾Ñ Đ¾ĐºĐ¾Đ» 4-Đ³Đ¾Ñ Ñ Đ¾Đ²Đ½Ñ .	TCP
host	Đ Đ¼Ñ Ñ Đ¾Ñ Ñ Đ°.	www.google.com
action	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ,	drop, accept, nat

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
	Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼ Đ² Ñ Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Đ½Ñ Đ¼Đ¸ Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	
endpoint_name	Đ Đ¼Ñ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°.	DESKTOP-0731NFQ
endpoint_id	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°.	35fb5820-74db-4eac-b05b-d01bc284c4e8
media_type	Đ¢Đ¸Đ¿ ĐºĐ¾Đ½ĐµÑ ĐµĐ½Ñ Đ°.	application/json
app_name	Đ Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Đµ, Đº ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¼Ñ Đ±Ñ Đ»Đ¾ Đ¿Ñ Đ¸Đ¼ĐµĐ½ĐµĐ½Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ¾ Đ¼ĐµĐ¶Ñ ĐµÑ ĐµĐ²Đ¾Đ³Đ¾ Ñ ĐºÑ Đ°Đ½Đ°.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
source	**ip** IPv4-Đ°Đ´Ñ ĐµÑ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ°.	10.10.10.10
	port Đ Đ¾Ñ Ñ Đ¸Ñ Đ½Đ¸ĐºĐ°.	Đ Đ¾Đ¶ĐµÑ Đ¿Ñ Đ¸Đ½Đ¸Đ¼Đ°Ñ Ñ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Đ¾Ñ 0 Đ´Đ¾ 65535.
destination	**ip** IPv4-Đ°Đ´Ñ ĐµÑ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ .	104.19.197.151
	port Đ Đ¾Ñ Ñ Đ½Đ°Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ	Đ Đ¾Đ¶ĐµÑ Đ¿Ñ Đ¸Đ½Đ¸Đ¼Đ°Ñ Ñ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Đ¾Ñ 0 Đ´Đ¾ 65535.
rule	**guid** Đ£Đ½Đ¸ĐºÐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ ĐºĐ°Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Đ¾Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¼Ñ Ñ Đ¾Đ·Đ´Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¼Ñ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đ.	Default allow
	type Đ¢Đ¸Đ¿ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	
url_categories	**id** Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Đ¸, Đº ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Đ¾Ñ Đ½Đ¾Ñ Đ¸Ñ Ñ Ñ URL.	39
	threat_level Đ£ĐºĐ°Đ·ÑĐ²Đ°ĐµÑ Ñ Đ³Ñ Đ¾Đ·Ñ ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Đ¸ URL.	Đ Đ¾Đ¶ĐµÑ Đ¿Ñ Đ¸Đ½Đ¸Đ¼Đ°Ñ Ñ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ :

		Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			• 1 â Đ¾Ñ ĐµĐ½Ñ Đ½Đ¸Đ·ĐºĐ¸Đ¹. • 2 â Đ½Đ¸Đ·ĐºĐ¸Đ¹. • 3 â Ñ Ñ ĐµĐ´Đ½Đ¸Đ¹. • 4 â Đ²Ñ Ñ Đ¾ĐºĐ¸Đ¹. • 5 â Đ¾Ñ ĐµĐ½Ñ Đ²Ñ Ñ Đ¾ĐºĐ¸Đ¹.
		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ ĐºĐ°Ñ ĐµĐ³Đ¾Ñ Đ¸Đ¸, Đº Đ¾Đ¼Ñ Đ¾Ñ Đ¾Đ¹ Đ¾Ñ Đ½Đ¾Ñ Đ¸Ñ Ñ Ñ URL.	**name** Social Networking

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Đ¹ ĐºĐ¾Đ½ĐµÑ Đ½Ñ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸
	Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ , Đ¿Đ¾Đ´Ñ Ñ Ñ Ñ Đ½Đ¾Đ¹ Đ·Đ°Đ¿Đ¸Ñ Ñ Ñ Đ¾Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ¿Đ¾Đ»Đ½ĐµĐ½ Đ²Ñ Đ¾Đ´ Đ½Đ° ĐºĐ¾Đ¼Đ¿ĐµĐ½Ñ Đ½Đ¾Đ¼ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đµ.	**user_name** DESKTOP-0731NFQ\\User
	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Đ¾Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	**timestamp** 2022-05-12T08:11:46.15869Z
	Đ¸Đ°Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	**endpoint_name** DESKTOP-0731NFQ
	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ¸ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	**endpoint_id** 35fb5820-74db-4eac-b05b-d01bc284c4e8
	Đ Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Ñ ĐµĐ½Ñ Đ°.	**process_id** 3916
	Đ¾Ñ Ñ Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	**hash** B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4
	Đ Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Đµ, ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¸Ñ Đ¿Đ¾Đ»Đ½ÑĐµÑ Ñ Đ¾Đ·Đ°Đ¿Ñ Ñ ĐµĐ½Đ¸Ñ/Đ¾Ñ Ñ Đ°Đ½Đ¾Đ²Đ»ĐµĐ½Đ¾.	**app_name** C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge
	Đ¸ĐµĐ¹Ñ Ñ Đ²Đ¸Đ (Đ·Đ°Đ¿Ñ Ñ Đº Đ¸Đ»Đ¸ Đ¾Ñ Ñ Đ°Đ½Đ¾Đ²ĐºĐ° Đ¿Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ).	**action** start, stop
	Đ¾Ñ Ñ Đ¸Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	**version** 6.2.19041.746
	Đ¾Đ±Ñ ĐµĐºÑ Đ¿Đ¾Đ´Đ¿Đ¸Ñ Đ¸.	**subject** Microsoft Corporation
	Đ Đ¸Đ´Đ°Ñ ĐµĐ»Ñ Ñ ĐµÑ Ñ Đ¸Đ¸ Đ¾Đ° Đ¸Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Ñ .	**issuer** Microsoft Windows Production PCA 2011
	Đ¸Đ¿Đ¾Ñ ĐºĐ¾Đ¼Đ°Đ½Đ´Đ½Đ¾Đ¹ Ñ Ñ Đ¾ĐºĐ¸.	**cmd_line** C:\\Windows\\system32\\svchost.exe -k wsappx -p -s AppXSvc
	Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Ñ ĐµÑ Đ¸Đ¸.	**session_id** 1656038456

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Đ°Đ¿Đ¿Đ°Ñ Đ°Ñ Ñ Ñ Ñ ĐºĐ¾Đ½ĐµÑ Đ½Ñ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ
	Đ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Đ¸	**timestamp** 2022-05-12T08:11:46.15869Z

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ
	Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	
endpoint_name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	DESKTOP-0731NFQ
endpoint_id	Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ ĐºĐ¾Đ½ĐµÑ Đ½Đ¾Đ³Đ¾ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ° Đ¸Đ»Đ¸ Ñ ĐµĐ½Ñ Đ¾Ñ Đ°.	35fb5820-74db-4eac-b05b-d0
action	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đ¹ (Đ¾Đ´ĐºĐ»Ñ Ñ ĐµĐ½Đ¸Đ/Đ¸Đ·Đ²Đ»ĐµÑ ĐµĐ½Đ¸Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°).	add_device, remove_device
device_name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°, ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ±Ñ Đ»Đ¾ Đ¿Đ¾Đ´ĐºĐ»Ñ Ñ ĐµĐ½Đ¾/Đ¸Đ·Đ²Đ»ĐµÑ ĐµĐ½Đ¾.	Generic USB Hub
device_id	Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°.	USB\\VID_0E0F&PID_0002\\6&
service	Đ Ñ Đ°Đ¹Đ²ĐµÑ Windows, Đ¾Đ±ĐµÑ Đ¿ĐµÑ Đ¸Đ²Đ°Ñ Ñ Đ¸Đ¹ Đ¾Đ¸Đ¼Đ¾Đ´ĐµĐ¹Ñ Ñ Đ²Đ¸Đ Đ¾Đ¼Đ¿Ñ Ñ Ñ ĐµÑ Đ° Ñ Đ¾Đ±Đ¾Ñ Ñ Đ´Đ¾Đ²Đ°Đ½Đ¸Đ¼/Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¼.	USBHUB3

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đ¼ Đ¶Ñ Ñ Đ½Đ°Đ»Đ° Syslog

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Đ½Đ¸Đ¼Đ°Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ntoorereaeda
syslog_facility	Đ¢Đ¸Đ¿ Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ syslog. Đ Đ°Đ¿Ñ Đ¸Đ¼ĐµÑ , user-level messages.	1
syslog_severity	Đ Đ¾Đ´Ñ Đ¾Đ±Đ½ĐµĐµ Đ¾ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ Ñ syslog facility Ñ Đ¼Đ¾Ñ Ñ Đ¸Ñ Đµ Đ² RFC 5424.	4
computer_name	Đ£Ñ Đ¾Đ²ĐµĐ½Đ²Đ°Đ¶Đ½Đ¾Ñ Ñ Đ¸ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ syslog. Đ Đ°Đ¿Ñ Đ¸Đ¼ĐµÑ , warning.	4
		node1

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸
	Đ Đ¼Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ°, Đ½Đ° ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¼ Đ¿Ñ Đ¾Đ¸Đ·Đ¾Ñ Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	
app_name	Đ Ñ Đ¸Đ»Đ¾Đ¶ĐµĐ½Đ¸Đµ, Đ²Ñ Đ·Đ²Đ°Đ²Ñ ĐµĐ¼ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	org.gnome.Shell.desktop
process_id	PID Đ¿Ñ Đ¾Ñ ĐµÑ Ñ Đ°, Đ²Ñ Đ·Đ²Đ°Đ²Ñ ĐµĐ³Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	3036
data	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"d devtools://devtools/bundled/devtools-frontend/front_end/p (6)
rule		
	guid Đ£Đ½Đ¸ĐºÐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºÐ°Ñ Đ¾Ñ Đ¿Đ¾Đ²Đ¸Đ», Ñ Đ°Đ±Đ»Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	16535060-5a1a-4e92-8331-239406ec34da
	name Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ°Đ²Đ¸Đ», Ñ Ñ Đ°Đ±Đ»Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾ Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	Example â Allow user-level messages
	type Đ¢Đ¸Đ¿ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	

Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ Đ¶Ñ Ñ Đ½Đ°Đ» RADIUS

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ	Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	Đ Ñ Đ¸Đ¼ĐµÑ Đ·Đ½Đ°Ñ ĐµĐ½Đ¸Ñ
timestamp	Đ Ñ ĐµĐ¼Ñ Đ¿Đ¾Đ»Ñ Ñ ĐµĐ½Đ¸Ñ Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ Đ² Ñ Đ¾Ñ Đ¼Đ°Ñ Đµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Đ Đ¼Ñ , ĐºĐ¾Ñ Đ¾Ñ Đ¾Đµ Đ¾Đ´Đ½Đ¾Đ·Đ½Đ°Ñ Đ½Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸Ñ Đ¸Ñ Ñ ĐµÑ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾, Đ³ĐµĐ½ĐµÑ Đ¸Ñ Ñ Ñ Ñ ĐµĐµ Ñ Ñ Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	utmcore@ntoorereaeda
event_type	Đi Ñ Đ°Ñ Ñ Ñ Đ¾Đ¾Đ±Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
action	Đ ĐµĐ¹Ñ Ñ Đ²Đ¸Đµ, Đ¿Ñ Đ¸Đ½Ñ Ñ Đ¾Đµ Ñ Ñ Ñ Ñ Đ¾Đ¹Ñ Ñ Đ²Đ¾Đ¾Ñ Đ²ĐµÑ Ñ Ñ Đ²Đ¸Đ¸ Ñ Đ½Đ°Ñ Ñ Ñ Đ¾ĐµĐ½Ñ Đ¼Đ¸	login

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ		Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	Ð Ñ Ð¸Ð¼ÐµÑ Ð·Ð½Ð°Ñ ÐµÐ½Ð¸Ñ
		Ð¿Ð¾Ð»Ñ Ð¸ÐºÐ°Ð¼Ð¸.	
src_ip		IP-Ð°Ð´Ñ ÐµÑ Ð¸ÑÑ Ð¾Ð´ÑÐ°, Ð¾Ñ ÐºÑ Ð´Ð° Ð¿Ñ Ð¸Ñ Ð»Ð¾ Ñ Ð¾Ð¾Ð±Ñ ÐµÐ½Ð¸Ðµ.	192.168.57.4
nas_ip		IP-Ð°Ð´Ñ ÐµÑ NAS, Ð°Ð²Ñ Ð¾Ñ Ð¸Ð·Ð¾Ð²Ð°Ð²Ñ ÐµÐ³Ð¾ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	172.16.1.4
framed_ip		IP-Ð°Ð´Ñ ÐµÑ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	192.168.57.29
rule	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ Ð°Ð²Ð¸Ð»Ð°, Ñ Ð°Ð±Ð»Ð¾Ð½ ÐºÐ¾Ð¼Ð¿Ð¾Ð½ÐµÐ½Ñ Ð¾Ð².	16535060-5a1a-4e92-8331-239406ec34da
user	**guid**	Ð£Ð½Ð¸ÐºÐ°Ð»Ñ Ð½Ñ Ð¹ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ . Ð¡Ð»Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ Ñ Ð¿Ð° Unknown, Ñ Ð¾Ð¸ÑÐºÐ¸Ð²Ð°Ñ ÐµÑ Ð¸Ð´ÐµÐ½Ñ Ð¸Ñ Ð¸ÐºÐ°Ñ Ð¾Ñ : 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name	Ð¸Ð¼Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	user_name
	groups	Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ñ Ð³Ñ Ñ Ð¿Ð¿Ñ , Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¹ Ñ Ð¾Ñ Ñ Ð¾Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ .	test_group

Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ð¶Ñ Ñ Ð½Ð°Ð»Ð° UserID

Ð Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¿Ð¾Ð»Ñ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ	
timestamp	Ð Ñ ÐµÐ¼Ñ Ð¿Ð¾Ð»Ñ Ñ ÐµÐ½Ð¸Ñ Ñ Ð¾Ð±Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Ð Ð¼Ñ , ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ð¾Ð´Ð½Ð¾Ð·Ð½Ð°Ñ Ð½Ð¾Ð³Ð¾ Ð¿Ð¾Ð´Ñ Ð¸Ñ Ð¸Ñ Ñ ÐµÑ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾, Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ñ Ñ Ñ ÐµÐµ Ñ Ñ Ð¾Ñ Ñ Ð¸Ñ Ð±Ð¾Ñ Ñ Ð¸Ðµ.	utmcore@ntoorereaeda
reasons	Ð Ñ Ð¸Ñ Ð¸Ð½Ð°, Ð¿Ð¾Ñ Ð¾Ñ Ð¾Ð¹ Ð±Ð»Ð¾Ñ Ð¾Ð²Ð¾Ñ Ð¸Ñ Ð¾Ð²Ð°Ñ Ñ Ð¾Ð²Ð¸Ðµ.	{\"user_groups_sids\":[\"S-1-5-21-379 \"user_sid\":\"S-1-5-21-3795870133-5
action	Ð ÐµÐ¹Ñ Ñ Ð²Ð¸Ðµ, Ð¿Ñ Ð¸Ð²Ñ Ð·Ð°Ð½Ð½Ð¾Ðµ Ñ Ñ Ñ Ñ Ð¾Ð¹Ñ Ñ Ð²Ð¾Ð¼ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ð¾Ð¾Ð±Ñ Ðµ Ð½Ð¸Ñ Ñ Ñ Ð¾ÐµÐ½Ð½Ñ Ñ Ð¾	login

Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Đ¾Đ»Ñ			Đ Đ¿Đ¸Ñ Đ°Đ½Đ¸Đµ	
			Đ¿Đ¾Đ»Đ¸Ñ Đ¸ĐºĐ°Đ¼Đ¸.	
src_ip			IPv4 Đ¸Ñ Ñ Đ¾Ñ Đ½Đ¸ĐºĐ° Ñ Đ¾Đ±Ñ Ñ Đ¸Ñ .	10.10.0.11
rule	**guid**		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Ñ Đ¾Đ·Đ´Đ°Đ»Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	16535060-5a1a-4e92-8331-239406e
	name		Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°, Ñ Ñ Đ°Đ±Đ°Ñ Ñ Đ²Đ°Đ½Đ¸Đµ ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ³Đ¾ Đ²Ñ Đ·Đ²Đ°Đ»Đ¾Ñ Đ¾Đ±Ñ Ñ Đ¸Đµ.	dev.local
	type		Đ¢Đ¸Đ¿ Ñ Ñ Đ°Đ±Đ¾Ñ Đ°Đ²Ñ ĐµĐ³Đ¾ Đ¿Ñ Đ°Đ²Đ¸Đ»Đ°.	syslog
user	**guid**		Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ . Đ Ñ Đ»Đ¸ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ Ñ Đ¸Đ¿Đ° Unknown, Ñ Đ¾ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ : 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b000
	name		Đ Đ¼Ñ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	user1
	groups	**guid**	Đ£Đ½Đ¸ĐºĐ°Đ»Ñ Đ½Ñ Đ¹ Đ¸Đ´ĐµĐ½Ñ Đ¸Ñ Đ¸ĐºĐ°Ñ Đ¾Ñ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Ñ Ñ Ñ Đ¾Ñ Ñ Đ¾Đ¸ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	aa218609-8716-9252-df20-88c43a0d
		name	Đ Đ°Đ·Đ²Đ°Đ½Đ¸Đµ Đ³Ñ Ñ Đ¿Đ¿Ñ , Đ² ĐºĐ¾Ñ Đ¾Ñ Đ¾Đ¹ Ñ Đ¾Ñ Ñ Đ¾Đ¸ Đ¿Đ¾Đ»Ñ Đ·Đ¾Đ²Đ°Ñ ĐµĐ»Ñ .	CN=Domain Users,CN=Users,DC=dev