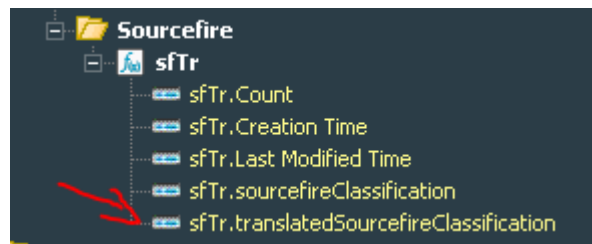


My variables – Based in GetActiveListValue



Event Inspector | Command:Send IP Zabbix | Global Variable:sfTr

Attributes | Parameters | Local Variables | Notes

Function: GetActiveListValue

Retrieve ActiveList value

Arguments

List: Traducao Classification

Field Mapping

For each key field, select a matching SecurityEvent field.

Name	Field	Key
sourcefireClassification	Device Event Category	<input checked="" type="checkbox"/>

Preview

Set a value for each key field.

Name	Value
Key Fields	
sourcefireClassification	

Event Inspector | Command:Send IP Zabbix | Global Variable:sfTr

Attributes | Parameters | Local Variables | Notes

Global Variable

- Name: sfTr
- Type: Event Global Variable
- Group: Variables

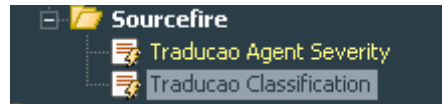
Common

- Resource ID: TnJncJkcBABCCpOe0LEur9A ==
- External ID:
- Alias (Display Name):
- Description:
- Version ID: AAAAAA1y6CMtBV0gG
- Deprecated:

Assign

- Owner:
- Notification Groups:

My ActiveList



Fields:

Event Inspector Command:Send IP Zabbix
Global Variable:sfTr Active List:Traducao Classific...

Attributes Notes

+ Add Entry

Active List

Name	Traducao Classification
Optimize Data	<input type="checkbox"/>
Capacity (x1000)	1
TTL Days	0
TTL Hours	0
TTL Minutes	0
Allow multi-mappings	<input type="checkbox"/>
Partially cached	<input type="checkbox"/>
Time partitioned	<input type="checkbox"/>
Case-Sensitivity	Case-Sensitive

Common

(Name)
(Description)

* **Data:** Event-based Fields-based Key Fields

Name	Type	Sub-type	Key-field
sourcefireClassification	String		<input checked="" type="checkbox"/>
translatedSourcefireClassification	String		<input type="checkbox"/>

The values of my ActiveList:

sourcefireClassification		translatedSourcefireClassification	Creation Time	Last Modified
attempted-admin	↓	Tentativa de Acesso Administrativo	11 jul 2014 16:15:51 BRT	10 set 2
attempted-dos		Tentativa de Negação de Serviço	11 jul 2014 16:15:51 BRT	10 set 2
attempted-recon		Tentativa de Reconhecimento	11 jul 2014 16:15:51 BRT	10 set 2
attempted-user		Tentativa de Comprometimento de Usuário	11 jul 2014 16:24:56 BRT	10 set 2
bad-unknown		Tráfego Potencialmente Malicioso	11 jul 2014 16:15:51 BRT	10 set 2
C2-HTTP		Tentativa de Comprometimento de Sistemas HTTP	11 jul 2014 16:33:12 BRT	10/26 14
denial-of-service		Negação de Serviço	11 jul 2014 16:29:08 BRT	10 set 2
misc-activity		Atividade Aleatória	11 jul 2014 16:15:51 BRT	10 set 2
misc-attack		Ataque Aleatório	11 jul 2014 16:15:51 BRT	10 set 2
network-scan		Varredura de Rede	11 jul 2014 16:35:41 BRT	10 set 2
non-standard-protocol		Protocolo Incomum	11 jul 2014 16:15:51 BRT	10 set 2
not-suspicious		Não suspeito	11 jul 2014 16:15:51 BRT	10 set 2
policy-violation		Violação de política	11 jul 2014 16:15:51 BRT	10 set 2
porn-filters		Filtro de Pornografia	11 jul 2014 16:29:20 BRT	10 set 2
PROTOCOL		Protocolo	11 jul 2014 16:15:51 BRT	10 set 2
protocol-command-decode		Comando de Decodificação de Protocolo	11 jul 2014 16:15:51 BRT	10 set 2
shellcode-detect		Código Malicioso Detectado	11 jul 2014 16:37:26 BRT	10 set 2
string-detect		Palavra Chave Identificada	10/29 16:35:11	10/29 16
successful-recon-limited		Reconhecimento Limitado com Sucesso	11 jul 2014 16:15:51 BRT	10 set 2
successful-user		Privilegio de Usuário Ganho	11 jul 2014 16:32:39 BRT	10 set 2
suspicious-filename-detect		Arquivo Com Nome Suspeito	11 jul 2014 16:30:46 BRT	10 set 2
suspicious-login		Login Suspeito	11 jul 2014 16:36:17 BRT	10 set 2
system-call-detect		Chamada de Sistema Detectada	11 jul 2014 16:35:59 BRT	10 set 2
tcp-connection		Conexão com Limite/Suspeita	2 jun 2016 10:09:08 BRT	10 set 2
trojan-activity		Atividade de Cavalo de Tróia	11 jul 2014 16:15:51 BRT	10 set 2
unknown		Tráfego Desconhecido	11 jul 2014 16:15:51 BRT	10 set 2
unusual-client-port-connection		Porta de Conexão de Cliente Incomum	11 jul 2014 16:31:24 BRT	10 set 2
web-application-attack		Ataque de Aplicação Web	11 jul 2014 16:15:51 BRT	10 set 2