

Contents

Rule	2
@id	2
@owner	2
@kbid	2
@enable	2
@ver	2
@file_name	2
filter_list	2
filter	2
action	2
alert	2
prerequisite	2
consequence	2
regulation	2
sequence	2

Rule

@id
@owner
@kbid
@enable
@ver
@file_name
filter_list

filter

Contains several dictionaries with the following structure

@id
@name
@occurrence
@weight
@timeout

source

ip

@location
@reference_id
@reference_type

port

target

ip

@location
@reference_id
@reference_type

port

flag_list

flag

event_list

event

@sensor_type
@class_type
tag

Contains several dictionaries with the following structure

@meaning
#text

action

alert

@priority
@category
message
source

ip

@reference_id
@reference_type

target

ip

@reference_id
@reference_type

prerequisite

predicate

Contains several dictionaries with the following structure

@type

Param

Contains several dictionaries with the following structure

@reference_type

consequence

predicate

Contains several dictionaries with the following structure

@type

Param

Contains several dictionaries with the following structure

@reference_type

regulation

sequence

filter

Contains several dictionaries with the following structure

@id