Contents

```
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
```