Sigma – Detection Expression

The detection expression is made up of two components – Search Identifiers & the Condition Expression. Search Identifiers are the fields and values the detection is targeting, while the Condition Expression ties those fields together and dictates how the detection tool will process each field in relation to the others.

```
18  detection:
19      rdp_outbound:
20          DestinationPort: 3389
21          Initiated: 'true'
22      filter:
23          Image|endswith:
24              - '\mstsc.exe'
25              - '\RTSApp.exe'
26              - '\RTS2App.exe'
27      condition: rdp_outbound and not filter
```

Search Identifiers

Condition Expression

FIELD: MAP VALUE

FIELD: MAP VALUE

FIELD | VALUE MODIFIER

LIST VALUE

LIST VALUE

LIST VALUE

This rule contains a map that looks for logs that have *3389* in the **DestinationPort** field AND *true* in the **Initiated** field.

The condition tells the detection engine to match both items in the **rdp_outbound** map, but to exclude any log whose **Image** field contains any of the values in the **filter** list.

In summary, generate an alert for outbound network connections with a destination port of 3389 (RDP) if the connection was not generated by a known legitimate process.

General Principles for the Detection Expression

Adapted from https://github.com/SigmaHQ/sigma/wiki/Specification

- YAML rules apply
- All values are case-insensitive strings with wildcards: '*' and '?'
- Wildcards can be escaped with \, e.g. *. If a wildcard after a backslash should be searched, the backslash has to be escaped: *
- Empty value: ''
- Null value is defined with 'null'

Feedback? Josh@DefensiveDepth.com

Sigma – Search Identifiers & Condition Expression

Search Identifiers

Search Identifiers can include multiple values in Lists (OR – dash bulleted) or Maps (AND – new lines). Value Modifiers can change search identifier behavior and are attached to the end of a field name after the pipe "|" character.

Data Type	Example	Operator
Lists	EventID: – 4605 – 8201	OR
Maps	Filter: EventID: 3325 EventID: 4523	AND

Value Modifier	What It Does	Example
contains	Adds a * to the beginning & end of the field value	CommandLine|contains
all	Changes the default list behavior from "or" to "and"	CommandLine|contains|all
startswith	Adds a * to the end of the field value	Image|startswith
endswith	Adds a * to the beginning of the field value	ParentImage|endswith
re:	Allows the use of Regex	Hostname|re: '^[A-Za-z0-9]{16}$'

Condition Expression

The Condition Expression uses Operators to tie the fields together and dictates how the detection tool will process each field in relation to the others.

Operator	Example
Logical and/or	selection1 or selection2
1/all of search-identifier	1 of selection
1/all of them	all of them
1/all of search-id-pattern	all of filter_*
Negation with 'not'	selection and not filter
Order of operation '()'	1 of selection and not (filter1 or filter2)

Feedback? Josh@DefensiveDepth.com
LearnSigmaRules.com