//Juniper networks. Reference https://www.juniper.net/documentation/us/en/software/nce/nce-srx-cluster-management-best/topics/task/chassis-cluster-srx-log-message-configuring.html

//TODO: OCSF field normalization

{

attributes: {

"dataSource.category": "security",

"dataSource.name": "Juniper Networks Firewall",

"dataSource.vendor": "Juniper Networks",

},

patterns: {

timestamp\_format: "\\w{3} \\d{1,2} \\d{2}:\\d{2}:\\d{2}",

ipPattern: "((\\d+\\.){3}\\d+|[a-zA-Z0-9:]+)", // Extract IPv4 or IPv6 addresses

},

formats: [

{

// All formats w/ pid number

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$\\[$pid=number$\\]:$system\_msg$"

}, {

// All formats w/out pid number

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$:$system\_msg$"

}, {

// UI\_CMDLINE\_READ\_LINE event

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$\\[$pid=number$\\]: UI\_CMDLINE\_READ\_LINE: User \\'$user$\\', command \\'$command$\\'",

halt: true

}, {

// UI\_LOGIN\_EVENT event

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$\\[$pid=number$\\]: UI\_LOGIN\_EVENT: User \\'$user$\\' login, class \\'$class$\\' \\S+, ssh-connection \\'$src\_ip=ipPattern$ $src\_port=number$ $dst\_ip=ipPattern$ $dst\_port=number$\\', client-mode \\'$client-mode$\\'",

halt: true

}, {

// UI\_LOGOUT\_EVENT event

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$\\[$pid=number$\\]: UI\_LOGOUT\_EVENT: User \\'$user$\\' logout",

halt: true

}, {

// UI\_CLI\_IDLE\_TIMEOUT event

format: "\\<\\d+\\>$timestamp=timestamp\_format$ UI\_CLI\_IDLE\_TIMEOUT: Idle timeout for user \\'$user$\\' exceeded",

halt: true

}, {

// UI\_AUTH\_EVENT event

format: "\\<\\d+\\>$timestamp=timestamp\_format$ $process\_name$\\[$pid=number$\\]: UI\_AUTH\_EVENT: Authenticated user \\'$user$\\' assigned to class \\'$class$\\'",

halt: true

}

]

}