{

// specify a time zone if the timestamps in your log are not in GMT

// timezone: "GMT-0800"

// NEW DATASOURCE FROM CRIBL

attributes: {

"dataSource.category": "security",

"dataSource.name": "Cisco ISE",

"dataSource.vendor": "Cisco",

"metadata.product.name": "Cisco ISE",

"metadata.product.vendor": "Cisco",

"sourcetype": "cisco:ise:syslog"

},

patterns: {

datetime: "\\w{3} \\d{1,2} \\d{2}:\\d{2}:\\d{2}",

datetime2: "\\d{4}-\\d{2}-\\d{2} \\d{2}:\\d{2}:\\d{2}.\\d{3} (\\+|-)\\d{2}:\\d{2}"

},

formats: [

{

format: "<181>$time=datetime$ $device.hostname$ $cat\_name$ $msg\_id$ $total\_seg$ $seg\_num$ $timestamp=datetime2$ $procid$ $msg\_code$ $msg$" // discardAttributes: ["message"], // uncomment to drop the raw message after parsing it (recommended)

}, {

format: "${parse=gron}$" // discardAttributes: ["message"], // uncomment to drop the raw message after parsing it (recommended)

repeat: true

}, {

format: ".\*$\_=identifier$=$\_$,",

repeat: true

}

]

"mappings": {

"version": 1,

"mappings": [

{

"transformations": [

{

cast: {

type: "datetime",

field: "timestamp",

format: "yyyy-MM-dd HH:mm:ss.nnn xxx"

}

}, {

"copy": {

from: "time",

to: "metadata.original\_time"

}

}, {

"copy": {

from: "DestinationIPAddress",

to: "dst\_endpoint.ip"

}

}, {

"copy": {

from: "DestinationPort",

to: "dst\_endpoint.port"

}

}, {

"copy": {

from: "User",

to: "actor.user.name"

}

},

]

}

]

}

}