{

attributes: {

"dataSource.category": "security",

"dataSource.name": "SecureLink",

"dataSource.vendor": "Imprivata",

"metadata.product.name": "SecureLink",

"metadata.product.vendor\_name": "Imprivata",

"metadata.version": "1.0.0"

},

patterns: {

tzPattern: "(\\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: [

{

format: "$timestamp=tzPattern$ $device\_ip=ipPattern$ $metadata.product.name$ - - - $log\_type$ ",

}, {

id: "audit\_msg\_format",

format: ".\*AUDIT $Text$",

}, {

id: "key\_value\_pair\_format",

format: ".\*$\_=identifier$: $\_$(,|$$)",

repeat: true

}, {

id: "key\_value\_pair\_format2",

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

repeat: true

},

],

"mappings": {

"version": 1,

"mappings": [

{

"transformations": [

{

"copy": {

"from": "timestamp",

"to": "event.time"

}

}

]

}

]

}

}