{

"attributes": {},

"patterns": {

"timestamp": "\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}(?:[+-]\\d{2}:\\d{2})|\\w{3}\\s+\\d{1,2}\\s+\\d{2}:\\d{2}:\\d{2}"

},

"formats": [

{

"attributes": {

"class\_uid": "4002",

"category\_uid": "4",

"severity\_id": "0",

"class\_name": "Infrastructure Events",

"category\_name": "Cisco IOS",

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

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

"dataSource.category": "security",

"dataSource.name": "Cisco IOS",

"dataSource.vendor": "Cisco"

},

"format": "<$code$>1 $timestamp=timestamp$ $device$ $protocol$ - $event\_type$ - Access attempted by unauthorized NMS: $nms\_ip$"

},

{

"attributes": {

"class\_uid": "4002",

"category\_uid": "4",

"severity\_id": "0",

"class\_name": "Infrastructure Events",

"category\_name": "Cisco IOS",

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

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

"dataSource.category": "security",

"dataSource.name": "Cisco IOS",

"dataSource.vendor": "Cisco"

},

"format": "<$code$>1 $timestamp=timestamp$ $device$ $protocol$ - $event\_type$ - $message$"

},

{

"attributes": {

"class\_uid": "4002",

"category\_uid": "4",

"severity\_id": "0",

"class\_name": "Infrastructure Events",

"category\_name": "Cisco IOS",

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

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

"dataSource.category": "security",

"dataSource.name": "Cisco IOS",

"dataSource.vendor": "Cisco"

},

"format": "<$code$>1 $timestamp=timestamp$ $device$ $protocol$ - $event\_type$ - Native VLAN mismatch detected on interface $interface$."

},

{

"attributes": {

"class\_uid": "4002",

"category\_uid": "4",

"severity\_id": "0",

"class\_name": "Infrastructure Events",

"category\_name": "Cisco IOS",

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

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

"dataSource.category": "security",

"dataSource.name": "Cisco IOS",

"dataSource.vendor": "Cisco"

},

"format": "<$code$>$log\_id1$: $device$: $log\_id2$: $log\_time$: %$facility$\_$severity$-$event\_code$: route-table-monitor: Route changed: Type: $route\_type$, Network: $network$, Mask/Prefix: $mask$, Protocol: $protocol$, GW: $gateway$, Intf: $intf$"

},

{

"attributes": {

"class\_uid": "4002",

"category\_uid": "4",

"severity\_id": "0",

"class\_name": "Infrastructure Events",

"category\_name": "Cisco IOS",

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

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

"dataSource.category": "security",

"dataSource.name": "Cisco IOS",

"dataSource.vendor": "Cisco"

},

"format": "<$code$>$timestamp=timestamp$ $device$ $severity$: $source$: Port $port$ $message$"

}

]

}