```
{
 "_index": ".ds-logs-suricata.eve-default-2026.01.27-000001",
 "_id": "AZwGhgPtV5wNIam4Lyce",
 "_version": 1,
 "_ignored": [
  "suricata.eve.direction",
  "suricata.eve.flow.dest_ip",
  "suricata.eve.flow.dest_port",
  "suricata.eve.flow.src_ip",
  "suricata.eve.flow.src_port"
 ],
 "_source": {
  "@timestamp": "2026-01-28T21:33:32.041Z",
  "agent": {
   "ephemeral_id": "a7431c30-c7c9-40f5-b6e0-8b5e34c7887c",
   "id": "3bc54355-ff61-4717-b744-2882c2f7d82b",
   "name": "kali",
   "type": "filebeat",
   "version": "9.2.4"
  },
  "data_stream": {
   "dataset": "suricata.eve",
   "namespace": "default",
   "type": "logs"
  },
  "destination": {
   "address": "192.168.250.103",
   "bytes": 74,
   "ip": "192.168.250.103",
   "packets": 1,
```

```
    "port": 40710
  },
  "ecs": {
    "version": "8.17.0"
  },
  "elastic_agent": {
    "id": "3bc54355-ff61-4717-b744-2882c2f7d82b",
    "snapshot": false,
    "version": "9.2.4"
  },
  "event": {
    "agent_id_status": "verified",
    "category": [
      "network",
      "intrusion_detection"
    ],
    "created": "2026-01-28T21:33:32.727Z",
    "dataset": "suricata.eve",
    "ingested": "2026-01-28T21:33:38Z",
    "kind": "alert",
    "severity": 3,
    "start": "2026-01-28T21:33:31.908Z",
    "type": [
      "allowed"
    ]
  },
  "input": {
    "type": "log"
  },
  "log": {
```

```
  "file": {
    "path": "/var/log/suricata/eve.json"
  },
  "offset": 38102682
},
"message": "",
"network": {
  "bytes": 148,
  "community_id": "1:G3zUgXtao3lgnKvMVEd4F5Kr1aQ=",
  "packets": 2,
  "transport": "tcp"
},
"observer": {
  "hostname": "kali",
  "ip": [
    "192.168.250.103",
    "fe80::61a8:e17c:6790:b2fe",
    "172.17.0.1"
  ],
  "mac": [
    "02-42-C2-09-9D-14",
    "08-00-27-62-6F-38"
  ],
  "product": "Suricata",
  "type": "ids",
  "vendor": "OISF"
},
"related": {
  "ip": [
    "34.68.177.88",
```

```
    "192.168.250.103"
  ]
},
"rule": {
  "id": "1",
  "name": "trafico detectado"
},
"source": {
  "address": "34.68.177.88",
  "as": {
    "number": 396982,
    "organization": {
      "name": "Google LLC"
    }
  },
  "bytes": 74,
  "geo": {
    "city_name": "Council Bluffs",
    "continent_name": "North America",
    "country_iso_code": "US",
    "country_name": "United States",
    "location": {
      "lat": 41.259099994786084,
      "lon": -95.85170005448163
    },
    "region_iso_code": "US-IA",
    "region_name": "Iowa"
  },
  "ip": "34.68.177.88",
  "packets": 1,
```

```
    "port": 443
  },
  "suricata": {
    "eve": {
      "alert": {
        "category": "",
        "gid": 1,
        "rev": 0,
        "signature": "trafico detectado",
        "signature_id": 1
      },
      "direction": "to_client",
      "event_type": "alert",
      "flow": {
        "dest_ip": "34.68.177.88",
        "dest_port": 443,
        "src_ip": "192.168.250.103",
        "src_port": 40710
      },
      "flow_id": "1086289812340734",
      "in_iface": "eth0",
      "ip_v": 4,
      "pkt_src": "wire/pcap"
    }
  },
  "tags": [
    "forwarded",
    "suricata-eve"
  ]
},
```

```
"fields": {
  "rule.id": [
    "1"
  ],
  "elastic_agent.version": [
    "9.2.4"
  ],
  "event.category": [
    "network",
    "intrusion_detection"
  ],
  "suricata.eve.flow.dest_ip": [
    "34.68.177.88"
  ],
  "observer.vendor": [
    "OISF"
  ],
  "source.geo.region_name": [
    "Iowa"
  ],
  "suricata.eve.alert.signature": [
    "trafico detectado"
  ],
  "source.ip": [
    "34.68.177.88"
  ],
  "suricata.eve.flow.src_ip": [
    "192.168.250.103"
  ],
  "agent.name": [
```

```
  "kali"
],
"destination.address": [
  "192.168.250.103"
],
"suricata.eve.event_type": [
  "alert"
],
"network.community_id": [
  "1:G3zUgXtao3lgnKvMVEd4F5Kr1aQ="
],
"observer.mac": [
  "02-42-C2-09-9D-14",
  "08-00-27-62-6F-38"
],
"event.agent_id_status": [
  "verified"
],
"source.geo.region_iso_code": [
  "US-IA"
],
"suricata.eve.alert.gid": [
  1
],
"event.kind": [
  "alert"
],
"suricata.eve.flow_id": [
  "1086289812340734"
],
```

```
"source.geo.city_name": [
  "Council Bluffs"
],
"event.severity": [
  3
],
"source.packets": [
  1
],
"rule.name": [
  "trafico detectado"
],
"network.packets": [
  2
],
"input.type": [
  "log"
],
"log.offset": [
  38102682
],
"suricata.eve.in_iface": [
  "eth0"
],
"data_stream.type": [
  "logs"
],
"tags": [
  "forwarded",
  "suricata-eve"
```

```
],
"agent.id": [
  "3bc54355-ff61-4717-b744-2882c2f7d82b"
],
"source.port": [
  443
],
"ecs.version": [
  "8.17.0"
],
"observer.type": [
  "ids"
],
"event.created": [
  "2026-01-28T21:33:32.727Z"
],
"suricata.eve.direction": [
  "to_client"
],
"agent.version": [
  "9.2.4"
],
"destination.bytes": [
  74
],
"event.start": [
  "2026-01-28T21:33:31.908Z"
],
"observer.ip": [
  "192.168.250.103",
```

```
  "fe80::61a8:e17c:6790:b2fe",
  "172.17.0.1"
],
"source.as.number": [
  396982
],
"suricata.eve.flow.dest_port": [
  443
],
"destination.port": [
  40710
],
"source.geo.location": [
  {
    "coordinates": [
      -95.85170005448163,
      41.259099994786084
    ],
    "type": "Point"
  }
],
"source.address": [
  "34.68.177.88"
],
"destination.packets": [
  1
],
"suricata.eve.alert.category": [
  ""
],
```

```
"suricata.eve.alert.signature_id": [
  1
],
"agent.type": [
  "filebeat"
],
"event.module": [
  "suricata"
],
"related.ip": [
  "34.68.177.88",
  "192.168.250.103"
],
"source.geo.country_iso_code": [
  "US"
],
"network.bytes": [
  148
],
"observer.product": [
  "Suricata"
],
"elastic_agent.snapshot": [
  false
],
"source.bytes": [
  74
],
"suricata.eve.pkt_src": [
  "wire/pcap"
```

```
],
"source.as.organization.name.text": [
  "Google LLC"
],
"suricata.eve.flow.src_port": [
  40710
],
"elastic_agent.id": [
  "3bc54355-ff61-4717-b744-2882c2f7d82b"
],
"data_stream.namespace": [
  "default"
],
"source.as.organization.name": [
  "Google LLC"
],
"source.geo.continent_name": [
  "North America"
],
"suricata.eve.ip_v": [
  4
],
"message": [
  ""
],
"destination.ip": [
  "192.168.250.103"
],
"observer.hostname": [
  "kali"
```

```
],
"network.transport": [
  "tcp"
],
"event.ingested": [
  "2026-01-28T21:33:38.000Z"
],
"@timestamp": [
  "2026-01-28T21:33:32.041Z"
],
"data_stream.dataset": [
  "suricata.eve"
],
"event.type": [
  "allowed"
],
"log.file.path": [
  "/var/log/suricata/eve.json"
],
"agent.ephemeral_id": [
  "a7431c30-c7c9-40f5-b6e0-8b5e34c7887c"
],
"source.geo.country_name": [
  "United States"
],
"suricata.eve.alert.rev": [
  0
],
"event.dataset": [
  "suricata.eve"
```

```
  ]
 }
}
```