Qualys Indication of Compromise v2.x

API Release Notes

Version 2.3.0

January 31, 2020

Qualys Indication of Compromise API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

Filtering events by processed time

Qualys API URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

Filtering events by processed time

APIs affected	/ioc/events /ioc/events/count
New or Updated APIs	Updated

You can use the event.eventProcessedTime filter to fetch all events processed at Qualys within a certain time duration.

Usually a time lag occurs between the time the events are generated on the asset and the time when they get processed at Qualys. You now have the option to filter events either based on the time they are generated on the asset (event.dateTime) or based on the time they are processed at Qualys (event.eventProcessedTime).

Note: Processed time is available only for newly generated events.

Sample - Fetch IOC events based on the processed time

Events are fetched for the event.eventProcessedTime duration provided in the API request.

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/ioc/events -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json

```
{
    "pageSize": 2,
    "pageNumber":0,
    "sort": "[{"event.eventProcessedTime":"asc"}]",
    "filter": "(event.eventProcessedTime:['2019-01-01T00:00:00Z'..'2020-
01-15T07:09:57Z'])"
}
```

Response:

```
[
  {
    "dateTime": "2019-12-23T08:12:32.000+0000",
    "process": {
      "fullPath": "C:\\Program
       Files\\Qualys\\QualysAgent\\QualysAgent.exe",
      "processFile": {
        "fullPath": "c:\\program
          files\\Qualys\\qualysagent\\QualysAgent.exe",
```

```
    "path": "c:\\program files\\Qualys\\qualysagent",
    "fileName": "QualysAgent.exe",
    "sha256":
 "ed201a76fec278336cdd409b0c95b67d9cb4c7d21ef75c87e8a88bec5aa49e07",
    "certificates": [
      {
        "certificateSigned": true,
       "certificateIssuer": "Symantec Class 3 SHA256 Code Signing CA
          - G2",
        "certificateValid": true,
        "certificateIssuedTo": "Qualys, Inc",
        "certificateSignedDate": "2017-03-22T00:00:00.000+0000",
        "certificateHash": "02f0abf61c26c5ba2e66960d5d807d9cb89398d4"
      }
    ],
    "moduleName": "QualysAgent",
    "md5": "10476bef9b8ba021ff0412605b7ed1e1"
  },
  "processEventId": "P_8ac0838b-ab98-3bb9-bead-b77bfbfe4e95_17-12-
      2019",
  "processName": "QualysAgent.exe",
  "elevated": true,
  "pid": 5580,
  "userName": "NT AUTHORITY\\SYSTEM"
},
"eventProcessedTime": "2019-12-30T06:27:21.135+0000",
"action": "ESTABLISHED",
"indicator2": [
  {
    "sha256":
 "ed201a76fec278336cdd409b0c95b67d9cb4c7d21ef75c87e8a88bec5aa49e07",
    "verdict": "UNKNOWN"
  }
],
"id": "N_703128b3-2d79-3d51-b332-309688de95d2_23-12-2019",
"type": "NETWORK",
"asset": {
  "fullOSName": "Microsoft Windows Server 2012 R2 Standard 6.3.9600
    Build 9600",
  "hostName": "WIN-890BLRMESC6",
  "agentId": "44a73a27-a4f3-419c-a710-6cf529bdf9e6",
  "interfaces": [
    {
      "ipAddress": "10.115.67.241"
    }
  ],
  "netBiosName": "WIN-890BLRMESC6",
  "customerId": "a25592dd-add3-421d-82d3-5fbe15f1f65b",
  "platform": "WINDOWS"
```

```
    },
    "network": {
      "protocol": "TCP",
      "remoteIP": "10.115.27.54",
      "localPort": "59298",
      "remotePort": "3128",
      "localIP": "10.115.67.241",
      "state": "ESTABLISHED"
    }
  }
]
```