Qualys Endpoint Detection and Response v1.x

API Release Notes

Version 1.0

August 26, 2020

Qualys Endpoint Detection and Response (EDR) API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

Fetch events within a date range

Get event count for a date range

Fetch event details

Introduction

EDR is an evolved superset of the IOC app. EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets

The IOC endpoints documented in this Release Notes will work with the new EDR 1.0 release.

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.

Fetch events within a date range

APIs affected	/ioc/events
New or Updated APIs	Updated

Get EDR events in the user account filtered by date range.

Sample

Request:

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

Response:


```
[
  {
    "dateTime": "2020-08-17T04:15:06.000+0000",
    "actor": {
      "processId": 1612,
      "processName": "svchost.exe",
      "type": "PROCESS",
      "userName": "NT AUTHORITY\\LOCAL SERVICE",
      "imageFullPath": "C:\\Windows\\System32\\svchost.exe",
      "userId": "LOCAL SERVICE",
      "createDate": "1970-01-01T00:00:00.000+0000"
    },
    "score": "0",
    "eventProcessedTime": "2020-08-22T08:17:53.202+0000",
    "file": {
      "fullPath": "C:\\Windows\\System32",
      "path": "C:\\Windows\\System32",
      "extension": "dll",
      "fileName": "energyprov.dll",
      "createdDate": "2019-03-19T04:43:45.586+0000",
      "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364f60x3x81x24217x433x10x",
      "certificates": [
        {
          "certificateSigned": true,
          "certificateIssuer": "DigiCert High Assurance Code Signing CA-1",
          "certificateValid": true,
          "certificateIssuedTo": "Xxxxx Operations XxxX & Co. KG",
          "certificateSignedDate": "2019-12-16T00:00:00.000+0000"
```

```
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA 2010",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2019-05-02T21:25:42.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Windows Production PCA 2011",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Windows",
          "certificateSignedDate": "2019-03-27T19:21:43.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2008-10-22T21:24:55.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA 2011",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2020-03-04T18:39:48.000+0000"
        }
      ],
      "md5": "684475093x4x806350x80xxxx3x11332"
    },
    "action": "CREATED",
    "indicator2": [
      {
        "score": 0,
        "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x",
        "familyName": " ",
        "verdict": "KNOWN",
        "category": " ",
        "rowId": "-3836563445362934026"
      }
    ],
    "id": "RTF_x82xx34x-5xxx-4110-9878-x91x5x476f47_-
3836563445362934026",
    "type": "FILE",
    "asset": {
      "fullOSName": "Microsoft Windows 10 Enterprise 10.0.18363 Build
```

```
18363",
      "hostName": "132017-T490.corp.qualys.com",
      "agentId": "x82xx34x-5xxx-4110-9878-x91x5x476f47",
      "netBiosName": "132017-T490",
      "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
      "platform": "WINDOWS"
    }
  }
]
```

Get event count for a date range

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

Get number of events logged within a date range.

Sample

Request:

```
curl -G --data-urlencode "state=true" --data-urlencode "filter=type:file"
"https://gateway.qg2.apps.qualys.com/ioc/events/count" -H
"Authorization:Bearer <token>"
```

Response:

```
{
    "count": 55279
}
```

Fetch event details

APIs affected	ioc/events/{agentId}/{eventId}
New or Updated APIs	Updated

Fetch details for an event.

Sample

Request:

```
curl -G --data-urlencode "state=true"
"https://gateway.qg2.apps.qualys.com/ioc/events/fe1118a2-222a-
1111-abcd-28edac4ff111/F_fe1118a2-222a-1111-abcd-
28edac4ff111_111150815650803056" -H "Authorization:Bearer <token>"
```

Response:


```
{
  "score": 0,
  "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
  "verdict": [
    "KNOWN"
  ],
  "category": [
    ""
  ],
  "familyName": [
    ""
  ],
  "eventId": "RTF_x82xx34x-5xxx-4110-9878-x91x5x476x47_-
3836563445362934026",
  "dateTime": "2020-08-17T04:15:06.000+0000",
  "type": "FILE",
  "action": "CREATED",
  "asset": {
    "agentId": "x82xx34x-5xxx-4110-9878-x91x5x476x47",
    "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
    "netBiosName": "132017-T490",
    "platform": "WINDOWS",
    "fullOSName": "Microsoft Windows 10 Enterprise 10.0.18363 Build
18363",
    "hostName": "132017-X490.corp.qualys.com"
  },
  "file": {
    "path": "C:\\Windows\\System32",
    "fullPath": "C:\\Windows\\System32//energyprov.dll",
```

```
    "md5": "684475093x4x806350x80xxxx3x11332",
    "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x",
    "extension": "dll",
    "size": 178688,
    "accessDate": "2020-02-13T07:07:44.325+0000",
    "writeDate": "2019-03-19T04:43:45.586+0000",
    "deviceLetter": "C",
    "company": "Microsoft Corporation",
    "copyright": "© Microsoft Corporation. All rights reserved.",
    "version": "10.0.18362.1",
    "product": "Microsoft® Windows® Operating System",
    "securityAttributes": "O:S-1-5-80-956008885-3418522649-1831038044-
1853292631-2271478464G:S-1-5-80-956008885-3418522649-1831038044-
1853292631-2271478464D:PAI(A;;FA;;;S-1-5-80-956008885-3418522649-
1831038044-1853292631-
2271478464)(A;;0x1200a9;;;BA)(A;;0x1200a9;;;SY)(A;;0x1200a9;;;BU)(A;;0x12
00a9;;;AC)(A;;0x1200a9;;;S-1-15-2-2)S:AI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)",
    "fileName": "energyprov.dll",
    "createdDate": "2019-03-19T04:43:45.586+0000",
    "certificates": [
      {
        "certificateHash": "3484479880440166040",
        "certificateIssuer": "DigiCert High Assurance Code Signing CA-1",
        "certificateIssuedTo": "Avira Operations GmbH & Co. KG",
        "certificateValid": true,
        "certificateSigned": true,
        "certificateSignedDate": "2019-12-16T00:00:00.000+0000",
        "subject": "Avira Operations GmbH & Co. KG",
        "expiryDate": "2021-11-16T12:00:00.000+0000"
      },
      {
        "certificateHash": "3504057697670195553",
        "certificateIssuer": "Microsoft Code Signing PCA 2010",
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2019-05-02T21:25:42.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2020-05-02T21:25:42.000+0000"
      },
      {
        "certificateHash": "3538015942716645516",
        "certificateIssuer": "Microsoft Windows Production PCA 2011",
        "certificateIssuedTo": "Microsoft Windows",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2019-03-27T19:21:43.000+0000",
        "subject": "Microsoft Windows",
```

```
        "expiryDate": "2020-03-27T19:21:43.000+0000"
      },
      {
        "certificateHash": "3549218827299643443",
        "certificateIssuer": "Microsoft Code Signing PCA",
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2008-10-22T21:24:55.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2010-01-22T21:34:55.000+0000"
      },
      {
        "certificateHash": "3563733393992181563",
        "certificateIssuer": "Microsoft Code Signing PCA 2011",
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": true,
        "certificateSigned": true,
        "certificateSignedDate": "2020-03-04T18:39:48.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2021-03-03T18:39:48.000+0000"
      }
    ]
  },
  "indicator2": [
    {
      "score": "0",
      "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x",
      "familyName": " ",
      "verdict": "KNOWN",
      "category": " ",
      "rowId": "-3836563445362934026"
    }
  ],
  "actor": {
    "state": "RUNNING",
    "eventId": "RTP_x82xx34x-5xxx-4110-9878-x91x5x476x47_-
7916036775084163258_1612",
    "arguments": "-k LocalServiceNetworkRestricted -p -s TimeBrokerSvc",
    "elevated": "false",
    "userName": "NT AUTHORITY\\LOCAL SERVICE",
    "processId": 1612,
    "parentProcessId": 0,
    "processName": "svchost.exe",
    "imageFullPath": "C:\\Windows\\System32\\svchost.exe"
  }
}
```