Malware Detection API

User Guide

February 16, 2021

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

CONTENTS

Preface

Chapter 1 Welcome

Get Started 7
Get API Notifications 7
MD API Framework 8
Base URL to the Qualys API Server 8
XML Output and Schemas 9
Introduction to MD API Paradigm 10
Know your Portal Version 14

Chapter 2 MD API

Search malware detections 18
View details of a malware detection 21
Current malware detection count 23

Appendix A Error Messages

Appendix B JSON Support

Preface

Using the Qualys Malware Detection (MD) API, third parties can integrate the Qualys Malware Detection solution into their own applications using an extensible XML interface. This user guide is intended for application developers who will use the Qualys MD API.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

CHAPTER 1

Welcome

Welcome to Qualys Malware Detection API.

Get Started

MD API Framework - Learn the basics about making API requests. The base URL depends on the platform where your Qualys account is located.

XML Output and Schemas - XML output uses schemas defined on your platform.

Introduction to MD API Paradigm - We'll tell you about making requests with authentication, making requests with payloads, using Curl, JSON and truncation/pagination logic. API requests must authenticate using Qualys credentials.

Authentication - We'll tell you about the method used for authentication. API requests must authenticate using Qualys credentials.

Get API Notifications

We recommend you join our Community and subscribe to our API notifications so you'll get email notifications telling you about important upcoming API enhancements and changes.

From our Community

Join our Community

Subscribe to API Notifications (select Receive email notifications)

MD API Framework

The new Qualys Malware Detection (MD) API framework introduces numerous innovations and new functionality compared to the other Qualys API frameworks.

Request URL

The URL for making API requests respects the following structure:

https://<baseurl>/qps/rest/1.0/<operation>/<module>/<object>/<object_id>

where the components are described below.

<baseurl>	The Qualys API server URL that you should use for API requests depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: https://qualysapi.qualys.com
<operation>	The request operation, such as get a list, search, and download.
<module>	The API module. For the MD API, the module is: “md”.
<object>	The module specific object.
<object_id>	(Optional) The module specific object ID, if appropriate.

Base URL to the Qualys API Server

The Qualys API documentation and sample code within it use the API server URL for Qualys US Platform 1: qualysapi.qualys.com.

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

Account Location	**API Server URL**
US Platform 1	https://qualysapi.qualys.com
US Platform 2	https://qualysapi.qg2.apps.qualys.com
EU Platform	https://qualysapi.qualys.eu

XML Output and Schemas

Detection XSD

https://<baseurl>/qps/xsd/1.0/md/detection.xsd

Asset XSD

https://<baseurl>/qps/xsd/1.0/md/detection/asset.xsd

URL XSD

https://<baseurl>/qps/xsd/1.0/md/detection/url.xsd

<baseurl> is the Qualys API server platform URL where your account is located. See Base URL to the Qualys API Server

Introduction to MD API Paradigm

Authentication

The application must authenticate using Qualys account credentials (user name and password) as part of the HTTP request. The credentials are transmitted using the “Basic Authentication Scheme” over HTTPS.

For more information, see the “Basic Authentication Scheme” section of RFC #2617:

```
http://www.faqs.org/rfcs/rfc2617.html
```

The exact method of implementing authentication will vary according to which programming language is used.

The allowed methods, POST and/or GET, for each API request are documented with each API call in this user guide.

Example

Basic authentication - recommended option:

```
curl -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection/
```

where qualysapi.qualys.com is the base URL to the Qualys API server where your account is located.

Making Requests with an XML Payload

While it is still possible to create simple API requests using the GET method, you can create API requests using the POST method with an XML payload to make an advanced request.

The XML payloads can be compared to a scripting language that allows user to make multiple actions within one single API request, like adding a parameter to an object and updating another parameter.

The XML structure of the payload is described in the XSD files.

Using Curl

Curl is a multi-platform command-line tool used to transfer data using multiple protocols. This tool is supported on many systems, including Windows, Unix, Linux and Mac. In this document Curl is used in the examples to build MD API requests using the HTTP over SSL (https) protocol, which i s required by the Qualys MD API framework.

Want to learn more? Visit http://curl/haxx/se

The following Curl options are used according to different situations:

Option	Description
-u “LOGIN:PASSWORD”	This option is used for basic authentication.
-X “POST”	This option is used to provide a method other than the default method, GET.
-H “content-type”	This option is used to provide a custom HTTP request header parameter for content type, to specify the MIME type of the curl’s payload.
--data-binary	This option is used to specify the POST data. See the examples below.

The sample below shows a typical Curl request using options mentioned above and how they interact with each other. The option -X “POST” tells Curl to execute the request using the HTTP POST method. The option “--data-binary @-” tells Curl to read the POST data from its standard input (stdin). The string “< file.xml” is interpreted by the shell to redirect the content of the file to the stdin of the command. The option -H “content-type: text/xml” tells Curl the POST data in “file.xml” is XML in text format.

```
curl -H "content-type: text/xml" -X "POST" --data-binary @- "https://example.com" <
file.xml
```

This documentation uses Curl examples showing the POST data in the “file.xml” file. This is referred to as Request POST Data. This can also be referred to as the Payload.

JSON Support

The Qualys MD API support JSON requests and responses. Learn more

XML Output Pagination / Truncation Logic

The XML output of a search API request is paginated and the default page size is 100 object records. The page size can be customized to a value between 1 and 1,000. If the number of records is greater than the page size then the <ServiceResponse> element shows the response code SUCCESS with the element <hasMoreRecords>true</hasMoreRecords> as shown below.

Follow the process below to obtain the first two the XML pages for an API request. Please apply the same logic to get all the next (n+1) pages until all records are returned. This is indicated when <hasMoreRecords>false</hasMoreRecords>.

Request 1:

Search for malware detection alerts of type behavioral. The service request in the POST data file “file.xml” defines this search critera.

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection/" <
file.xml
```

Note: “file.xml” contains the request POST data.

Request POST Data for Request 1:

```
<ServiceRequest>
  <preferences>
    <limitResults>5</limitResults>
  </preferences>
  <filters>
    <Criteria field="type" operator="EQUALS">BEHAVIORAL</Criteria>
  </filters>
</ServiceRequest>
```

Response:

The number of records is greater than the default pagination value so the <ServiceResponse> element identifies the last ID of the object in the current page output.

```
<ServiceResponse ...>
   <responseCode>SUCCESS</responseCode>
   <COUNT>5</COUNT>
   <hasMoreRecords>true</hasMoreRecords>
   <lastId>123</lastId>
   <data>
      <!--here you will find 5 alert records-->
   </data>
</ServiceResponse>
```

Request 2:

To get the next page of results, you need to edit your service request in “file.xml” that will be passed to API request as a POST payload. According to the <lastId> element returned in the first page, you want the next page of results to start with the object ID 124 or greater.

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/ps/rest/1.0/search/md/detection/" <
file.xml
```

Request POST Data for Request 2:

You’ll notice the operator field value is set to 123, which is the value returned in <lastId> of the previous page output. The GREATER operator is a logical “greater than” (it does not mean greater than or equal to).

```
<ServiceRequest>
   <filters>
      <Criteria field="type"operator="EQUALS">BEHAVIORAL
</Criteria>
      <Criteria field="id" operator="GREATER">123</Criteria>
   </filters>
</ServiceRequest>
```

Setting the Custom Page Size

The service request needs to contain the <preferences> section with the <limitResults> parameter. For the <limitResults> parameter you can enter a value from 1 to 1,000.

```
<ServiceRequest>
  <filters>
    <Criteria> ... </Criteria>
  </filters>
  <preferences>
    <limitResults>200</limitResults>
  </preferences>
</ServiceRequest>
```

Know your Portal Version

Using the Version API you can find out the installed version of Portal and its sub-modules that are available in your subscription.

URL:	https://qualysapi.qualys.com/qps/rest/portal/version
Methods allowed:	GET

Examples

Example 1: XML

API Request:

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Accept: application/xml"
https://qualysapi.qualys.com/qps/rest/portal/version
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/versi
on.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <PortalApplication-VERSION>3.5.0.0-SNAPSHOT-1 DEVELOP #92 (2021-
01-19T01:51:21Z)</PortalApplication-VERSION>
            <ITAM-VERSION>1.3.1.0-18</ITAM-VERSION>
            <CS-VERSION>1.9.0.0-SNAPSHOT</CS-VERSION>
            <CA-VERSION>3.4.0.0</CA-VERSION>
            <QGS-VERSION>1.2.0.0-6</QGS-VERSION>
            <QUESTIONNAIRE-VERSION>2.26.0.0</QUESTIONNAIRE-VERSION>
            <SAC-VERSION>1.0.0-SNAPSHOT</SAC-VERSION>
            <WAF-VERSION>2.12.6.0</WAF-VERSION>
            <QUESTIONNAIRE__V2-VERSION>1.13.1.0-
SNAPSHOT</QUESTIONNAIRE__V2-VERSION>
            <WAS-VERSION>6.17.0.0-SNAPSHOT-32</WAS-VERSION>
            <FIM-VERSION>2.6.0.0-23</FIM-VERSION>
            <ICS-VERSION>0.9.1.0-12</ICS-VERSION>
            <VM-VERSION>1.0.3</VM-VERSION>
            <CERTVIEW-VERSION>2.8.0.0-20</CERTVIEW-VERSION>
            <CLOUDVIEW-VERSION>1.9.2.0-SNAPSHOT</CLOUDVIEW-VERSION>
            <CM-VERSION>1.31.0.0</CM-VERSION>
            <MDS-VERSION>2.16.1.0-SNAPSHOT-2</MDS-VERSION>
            <PM-VERSION>1.5.0.0-2</PM-VERSION>
            <PS-VERSION>1.3.0.0-16</PS-VERSION>
            <IOC-VERSION>1.2.0-15</IOC-VERSION>
            <THREAT__PROTECT-VERSION>1.5.0-SNAPSHOT</THREAT__PROTECT-
VERSION>
            <AV2-VERSION>0.1.0</AV2-VERSION>
            <UD-VERSION>1.0.0</UD-VERSION>
        </Portal-Version>
        <QWeb-Version>
            <WEB-VERSION>10.7.0.0-1</WEB-VERSION>
            <SCANNER-VERSION>12.1.68-1</SCANNER-VERSION>
            <VULNSIGS-VERSION>2.5.84-2</VULNSIGS-VERSION>
        </QWeb-Version>
</data>
</ServiceResponse>
```

Example 2: JSON

API Request:

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Accept: application/json"
https://qualysapi.qualys.com/qps/rest/portal/version
```

Response:

```
{
  "ServiceResponse": {
    "data": [
      {
        "Portal-Version": {
          "PortalApplication-VERSION": "3.5.0.0-SNAPSHOT-1 DEVELOP #92
(2021-01-19T01:51:21Z)",
          "WAS-VERSION": "6.17.0.0-SNAPSHOT-32",
          "VM-VERSION": "1.0.3",
          "CM-VERSION": "1.20.1",
          "MDS-VERSION": "2.16.1.0-SNAPSHOT-2",
          "CA-VERSION": "2.9.1.0",
          "QUESTIONNAIRE-VERSION": "2.14.0.4",
          "WAF-VERSION": "2.7.0.0"
        },
...
               }
      }
    ],
    "responseCode": "SUCCESS",
    "count": 1
  }
}
```

MD API

Use these API functions to download information from the Malware Detection module in your Qualys account.

Search malware detections

View details of a malware detection

Current malware detection count

Search malware detections

Returns a list of alerts in the user’s account.

URL:	https://<baseurl>/qps/rest/1.0/search/md/detection/
Methods allowed:	POST

Input

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

id (Integer)	type (Keyword)
qid (Integer)	showDeactivatedSite (Boolean)
url (Text)	severity (Keyword)

Allowed Operators

Integer	EQUALS, NOT EQUALS, GREATER, LESSER, IN
Text	CONTAINS, EQUALS, NOT EQUALS
Date	EQUALS, NOT EQUALS, GREATER, LESSER
Keyword	EQUALS, NOT EQUALS, IN
Boolean	(true/false) EQUALS, NOT EQUALS

Permissions

User must have the Malware Detection (MD) module enabled
User must have "API ACCESS" permission)
Output includes web sites within the user's scope

Example

Request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection" <
file.xml
```

Request POST Data:

```
<ServiceRequest>
      <preferences>
          <limitResults>100</limitResults>
      </preferences>
      <filters>
        <Criteria field="id" operator="EQUALS">37747097</Criteria>
       <Criteria field="url"
       operator="CONTAINS">http://www.mwtest.info/
       malware-demos-named/</Criteria>
       <Criteria field="type"
       operator="EQUALS">BEHAVIORAL</Criteria>
      </filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xs
d/1.0/md/detection.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <hasMoreRecords>false</hasMoreRecords>
    <data>
        <Detection>
            <id>37747097</id>
            <qid>206012</qid>
            <name>
               <![CDATA[A Malicious Process Launch Was Detected]]>
            </name>
            <type>BEHAVIORAL</type>
            <severity>HIGH</severity>
            <url>
                <![CDATA[http://www.mwtest.info/
                 malware-demos-named/MS06-014-RemotePayload/
                 MS06-014-DEMO.html]]>
            </url>
        </Detection>
    </data>
</ServiceResponse>
```

View details of a malware detection

Returns details for a malware detection. Want to find a detection ID to use as input? See Search malware detections.

URL: https://<baseurL>/qps/rest/1.0/get/md/detection/<id>

Methods allowed: GET

Input

The element “id” (Integer) is required, where “id” identifies the alert.

Permissions

User must have the Malware Detection (MD) module enabled

User must have "API ACCESS" permission)

Output includes web sites within the user's scope

Example

Request:

```
curl -u "USERNAME:PASSWORD" -X GET
https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/
37747097
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xs
d/1.0/md/detection.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Detection>
            <id>37747097</id>
            <qid>206012</qid>
            <name>
               <![CDATA[A Malicious Process Launch Was Detected]]>
            </name>
            <type>BEHAVIORAL</type>
            <description>
```

```
                <![CDATA[Upon visiting the Web page, a process
                 launch was detected by the malware detection
                 service. External process launches should never
                 occur in normal Web browsing activity. This is an
                 indication of malicious behavior. The process
                 launched is noted in the Results section.]]>
            </description>
            <severity>HIGH</severity>
            <url>
                <![CDATA[http://www.mwtest.info/malware-demos
               -named/MS06-014-RemotePayload/MS06-014-DEMO.html]]>
            </url>
            <result>
                <![CDATA[Process creation was attempted on
                application
                C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\hgivV.exe
                with parameters (Undefined)]]>
            </result>
            <asset>
                <id>2688083</id>
                <name>
                    <![CDATA[http://www.mwtest.info/
                    malware-demos-named/]]>
                </name>
                <deactivated>false</deactivated>
                 </asset>
           </Detection>
     </data>
</ServiceResponse>
```

Current malware detection count

Returns the total number of malware detections in the user's account. Input elements are optional and are used to filter the number of detections in the count.

URL:	https://<baseurl>/qps/rest/1.0/download/md/detection/
Methods allowed:	POST

Input

The element "format" (Text) is required, where "format" is the file format (csv or cef).

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

id (Integer)	type (Keyword)
qid (Integer)	showDeactivatedSite (Boolean)
url (Text)	severity (Keyword)

Allowed Operators

Integer	EQUALS, NOT EQUALS, GREATER, LESSER, IN
Text	CONTAINS, EQUALS, NOT EQUALS
Date	EQUALS, NOT EQUALS, GREATER, LESSER
Keyword	EQUALS, NOT EQUALS, IN
Boolean	(true/false) EQUALS, NOT EQUALS

Permissions

User must have the Malware Detection (MD) module enabled
User must have "API ACCESS" permission)
Output includes web sites within the user's scope.

Example

Request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
```

```
"https://qualysapi.qualys.com/qps/rest/1.0/count/md/detection" <
file.xml
```

Request POST Data:

```
<ServiceRequest>
      <filters>
       <Criteria field="id" operator="GREATER">37747097</Criteria>
      </filters>
</ServiceRequest>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/x
sd/1.0/md/detection.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>41</count>
</ServiceResponse>
```

APPENDIX A

Error Messages

This appendix describes the types of error messages returned from MD API requests.

Error Message	Resolution
Element	
url: Invalid URL format (<value>).	URL format must be as follows: http://<baseUrl>/rest/1.0/?parameters
Url: Element is required	Element “Url” is required.
uris.<field>: Invalid URL format (<value>).	For the uri.<field> sub element, specify a URL like http://domain.name/base/url/?parameters
uris.<field>: Length of the field must not be greater than 2048 characters. (<value>).	For the uri.<field> sub element, the maximum field length is 2048 characters.
Attribute.category: Element is required.	The element Attribute.category is required.
Attribute.category: Invalid value (<value>).	Element Attribute.category must be set to one of these values: Business Function, Business Location, Business Description.
Attribute.value: Element is required.	Provide a value for the attribute in the Attribute.value element: function, location or description.
The attribute length cannot be greater than 64 characters.	The value for this attribute cannot exceed 64 characters.
The attribute length cannot be greater than 2048 characters.	The value for this attribute cannot exceed 2048 characters.
<element>: Element must not be set.	This element does not apply to this request.
set: Element must contain at least one child.	The set element requires at least one sub element.

Error Message	Resolution
headers: Length of all headers cannot exceed 2048 characters.	The values of all headers cannot exceed 2048 characters.
At least one of the following elements must be set: set, add, remove.	For an "update" request you must set at least one of these elements: set, add or remove.
UrlEntry: Element is required.	The element UrlEntry must be provided.
UrlEntry: Invalid URL format (value).	Specify a URL like http://domain.name/base/url/?parameters
<parent>: Length of all [URLs, regular expressions] cannot exceed 2048 characters	The list of entries for a given type shall not exceed 2048 characters.
UrlEntry: Only regular expressions are accepted for this element.	You must provide regular expressions for the element postDataBlackList.
tags.<element>: Element must not be set.	The tags element does not apply for this request
tags.set: Element must contain at least one child.	At least one sub element must be provided for the element tag.set.
Tag.id: Element is required.	Provide a value for the element Tag.id
Tag.id: Invalid value (value).	Value must be an integer set at least to 1.
Tag: Tag specified by ID <id> does not exist or is not available.	Provide a value for the element id that corresponds to a valid tag.
Criteria	
Criteria: Field is required.	Specify the name of the criteria to search against.
Criteria: Invalid criteria (<field name>).	Please search against one of the following criteria: %s.
Criteria: Invalid operator for criteria '<field>' (<operator>).	Allowed operations for this criteria are: %s.
Criteria: Value is required for criteria '<field>'.	Specify a value for a field name for search criteria.
Criteria: Invalid value format for criteria '<field>': <value>.	Boolean (true, false). Date and Time in UTC format Enumeration (allowed options separated by comma). Other: Specify criteria value(s) as <type>.
Authorization	
You are not authorized to access the application through the API.	You must be granted the API Access permission in your roles and scopes.
No data shall be passed for this operation.	The POST request does not specify a data element.
User is not authorized to perform this operation on specified object(s).	You must be granted access to these objects in your user scope.

Error Message	Resolution
Operation %s does not support search filters.	Do not provide search filters for this operation.
Report Storage Limit	
Your [subscription | user] storage limit of <NB> Mb has been reached.	Delete existing reports and try again.

APPENDIX B

JSON Support

The Qualys Malware Detection API supports JSON requests and responses. Samples are shown below.

Headers used in samples	
Send JSON request	"Content-Type: application/json"
Get response in JSON	"Accept: application/json"

Example 1: Search Malware Detections

Request:

```
cat {json} | curl -s -k -X POST -H "Accept: application/json" -H
"Content-Type: application/json" -H "user:{USERNAME}" -H
"password:{PASSWORD}" -d @-
https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection
```

Request POST Data:

```
{
  "ServiceRequest": {
    "preferences": { "limitResults": "100" },
    "filters": {
      "Criteria": [
        {
          "-field": "id",
          "-operator": "EQUALS",
          "#text": "37747097"
        },
        {
          "-field": "url",
          "-operator": "CONTAINS",
          "#text": "http://www.mwtest.info/malware-demos-named/"
        },
        {
          "-field": "type",
          "-operator": "EQUALS",
          "#text": "BEHAVIORAL"
        }
      ]
    }
  }
}
```

Response:

```
{
  "ServiceResponse": {
    "-xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
    "-xsi:noNamespaceSchemaLocation":
"https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",
    "responseCode": "SUCCESS",
    "count": "1",
    "hasMoreRecords": "false",
    "data": {
      "Detection": {
        "id": "37747097",
        "qid": "206012",
        "name": "
                A Malicious Process Launch Was Detected
            ",
        "type": "BEHAVIORAL",
        "severity": "HIGH",
        "url": "
        http://www.mwtest.info/malware-demos-named/
        MS06-014-RemotePayload/MS06-014-DEMO.html
            "
      }
    }
  }
}
```

Example 2: GET details for malware detection

Request:

```
curl -X GET -s -k -H "Accept: application/json" -n -u
"{USERNAME}:{PASSWORD}" “
https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/37747097”
```

Response:

```
{
  "ServiceResponse": {
    "-xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
    "-xsi:noNamespaceSchemaLocation":
"https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",
    "responseCode": "SUCCESS",
    "count": "1",
    "data": {
      "Detection": {
        "id": "37747097",
        "qid": "206012",
        "name": "
                A Malicious Process Launch Was Detected
            ",
        "type": "BEHAVIORAL",
        "description": "
                Upon visiting the Web page, a process launch was
detected by the malware detection service. External process launches
should never occur in normal Web browsing activity. This is an
indication of malicious behavior. The process launched is noted in the
Results section.
            ",
        "severity": "HIGH",
        "url": "
                http://www.mwtest.info/malware-demos-named/MS06-014-
RemotePayload/MS06-014-DEMO.html
            ",
        "result": "
                Process creation was attempted on application
C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\hgivV.exe with parameters
(Undefined)
            ",
        "asset": {
          "id": "2688083",
          "name": "
                    http://www.mwtest.info/malware-demos-named/
                ",
          "deactivated": "false"
        }
      }
    }
  }
}
```

Example 3: Count of Detection

Request:

```
cat {json} | curl -s -k -X POST -H "Accept: application/json" -H
"Content-Type: application/json" -H "user:{USERNAME}" -H
"password:{PASSWORD}" -d @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection"
```

Request POST Data:

```
{
  "ServiceRequest": {
    "filters": {
      "Criteria": {
        "-field": "id",
        "-operator": "GREATER",
        "#text": "37747097"
      }
    }
  }
}
```

Response

```
{
  "ServiceResponse": {
    "-xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
    "-xsi:noNamespaceSchemaLocation":
"https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",
    "responseCode": "SUCCESS",
    "count": "41"
  }
}
```