DLP

10.1

Protector Inspection API Integration Guide

Revision A

Published 07 March 2024

Contents

Chapter 1

Introduction

The purpose of the Forcepoint DLP Protector Inspection API Integration Guide is to help integrate the DLP Inspection API on the DLP protector. This API is a rich inspection API that permits sending various types of data on the main DLP channels (email, Web, CASB) and receiving information-rich responses. Such responses include information related to incident violations and recommended actions.

Related concepts

Inspection APIs on page 7
Enumerators on page 21
CASB Request Sample on page 25
Web Multipart Inspection on page 31

Chapter 2

Inspection APIs

Contents

This chapter provides detailed information about the specific Inspection APIs available in Forcepoint DLP.

Inspection Request

The general structure of the inspection request is made of 4 parts: "context", "contentDescriptors", "source" and "destinations". All parts are mandatory. Each part is described separately.

Related concepts

Context Object on page 8
Content Descriptor Object on page 11
Source object on page 12
Destination Object on page 14

Parameters for the Inspection Request

Parameter	Value	Required
Accept	application/json	Yes
Content-Type	multipart/form-data	Yes

Definition of the Inspection Request

Field	Required	Type	Description	comments
context	Yes	Inspection Context	A list of content attributes submitted with each inspection request.	

Field	Required	Type	Description	comments
contentDescriptors	Yes		Meta data of the files to inspect including reference to the file data in the request body.	Until 10.1 release and further notice, only 1 request is being supported.
source	*Yes except for CASB DAR		Object describing the source of the inspection request.	
destinations	Yes		Object describing the destinations of the inspection request.	

Example of the Inspection Request

```
{
    "context": {context Object},
    "contentDescriptors": [List of One Object],
    "source": {source Object},
    "destinations": [List of Destination Objects]
}
```

Context Object

The context object contains details about the inspection request arriving at DPS like the unique id of the request, what agent sent it, on which channel, what cloud operation it represents etc...

Example of the Context Object

```
{
    "context": {
        "global_message_id": "...",
        "client_name": "...",
        "data_channel": "...",
        "activity_type": "...",
        "occurred_message_timestamp_utc_ms": ...,
        "inspection_request_timeout_ms" : 123445,
        "is_device_managed": "...",
        "policy_groups" : ["policy_group1", "policy_group2", "policy_group3"],
        "customer_name" : "customer_name_1"
}
```

Definition of the Context Object

Field	Required	Type	Description	Values	comments
global_message_id	Yes	String	An arbitrary string created by the client, principally for linking log records across services.	Examples: HVD6mj:gPkf:282054 vwB7mj:l62d:7970 ZlM2mj:r7dg:891191	
client_name	Yes	Enumerator	The client that sent the inspection request.	[FORCEPOINT_WEB, FORCEPOINT_EMAIL, FONE_CASB, FONE_SWG, CUSTOM_APPLICATION, UNKNOWN]	For API protector, the client name should always be Custom Application.
data_channel	Yes	Enumerator	The channel through which the transaction came.	[EMAIL, HTTP, HTTPS, CASB_API, CASB_REAL_TIME, CASB_DISCOVERY, TESTING_CHANNEL]	For API protector, the data_channel field's value should always be one of the following: [HTTP, HTTPS, CASB_API, CASB_REAL_TIME, EMAIL]

Field	Required	Type	Description	Values	comments
activity_type	Yes	Enumerator	The operation performed by the source.	[NONE, UPLOAD, DOWNLOAD, SHARE, EXTERNAL_SHARE, REQUEST, SYNC, UNSHARE, DELETE, CREATE, MODIFY, VIEW, MOVE, LOCK, RENAME, RESTORE, PRINT, COPY, SEND, INTERNAL_SHARE, PUBLIC_SHARE, UNKNOWN]	For API protector these are the allowed operations (activity_type values) per each channel: **HTTP**: UPLOAD **HTTPS**: UPLOAD **CASB_API**: CREATE, MODIFY, DOWNLOAD, EXTERNAL_SHARE, INTERNAL_SHARE, PUBLIC_SHARE **CASB_REAL_TIME**: UPLOAD, DOWNLOAD **EMAIL**: SEND
occurred_message_timestamp_utc_ms	Yes	long	The event detection time stamp by the client in the format of utc in ms units		
inspection_request_timeout_ms	No	long	The timeout assigned for the inspection request	Between 20 and 300000 (returns HTTP error 400 if not in range).	If this is empty, the rest server will assign a timeout of 300 sec for offline channels and 10 sec for all the other channels. *1ms setting.
is_device_managed	No - if the client has this information than it should send it.	Boolean	True if the device performing the operation is managed	true, false	

Content Descriptor Object

The contentDescriptors part is a list of items that are sent for analysis in the inspection request. Currently the list includes only a single item. It is a list for future compatibility in order to be able to support a few items on a single inspection request.

Each content descriptor includes meta data on the data that it represents.

Example of the Content Descriptor Object

```
"contentDescriptors": [{
        "id": "0",
        "name": "...",
        "size_bytes": 34567,
        "item_type": "...",
        "email_subject" : "...",
        "file_path": "...",
        "file_id" : "...",
        "sharing_status": "...",
        "shared_with": ["...", "..."],
        "owner_name": "...",
        "owner_email": "...",
        "creation_time_utc_ms": 1505897456,
        "modification_time_utc_ms": 1505897456,
        "access_time_utc_ms": 1505897456
    }]
```

Definition of the Content Descriptor Object

Field	Required	Type	Description	Values	comments
id		Integer	file id is a sequential number of the file (to be inspected, not including the json) inside the multi part request: first file: 0 second file: 1 ... ... K'th file: k-1	As long as the contentDescriptors is an array of only 1 file (meaning the multipart request contains only 1 file to be inspected) it Should always be 0	
name	No, since the cloud web agent isn't always capable of retrieving it.	String	file name		

Field	Required	Type	Description	Values	comments
size_bytes	Yes	Long	size of the content in bytes	should be larger than 0, and equal to 0 **only** in case the agent cannot obtain the file size. In any case, the file sent must not be empty.	
item_type	Yes	Enumerator		[FILE, FOLDER]	Currently this should always be 'FILE'
email_subject	Only for CES (cloud email)	String			
file_path	No	String			
file_id	No	String	unique ID of the file in the customer system		
sharing_status	No	String		internal, external, none	
shared_with	No	array of strings	List of emails/ groups/Everyone		
owner_name	No	String	Owner's login name		
owner_email	No	String			
creation_time _utc_ms	No	Long	utc creation timestamp in mili seconds		
modification_time _utc_ms	No	Long	utc modification timestamp in mili seconds		
access_time _utc_ms	No	Long	utc access timestamp in mili seconds		

Source object

The source part includes information on the source of the data. It is mainly used to describe the user that the data originated from. At least 1 source attribute is mandatory.

Example of the Source Object

```
"source": {
     "user_principal_name": "...",
     "down_level_logon_name": "...",
     "sam_account_name": "...",
     "distinguished_name": "...",
     "user_email_address": "...",
     "host_ips": ["...", "..."],
     "host_name": "...",
     "user_agent": "...",
     "host_domain": "..."
 }
```

Definition of the Source Object

Field	Required	Type	Description	Values	comments
user_principal_name	At least 1 of the 5: user_principal_name/ down_level_logon_ name/ sam_account_name/ distinguished_name/ user_email_address should be present if the agent is capable of obtaining it.	string		"example @forcepoint.com"	
down_level_ logon_name		string		"nis1\example"	
sam_account _name		string		"example"	
distinguished _name		string		"CN=Smith\, John,OU=Users, OU=Raanana, DC=example, DC=com"	
user_email _address		string		"example @forcepoint.com"	
host_ips	yes	array of strings	the ip of the machine the operation originated from	["192.168.31.14"]	it can be more than 1 because it can be obtained before and after the NAT. If available, the machine's internal address will be the second address in the list.

Field	Required	Type	Description	Values	comments
host_name	no	string	the name of the machine the operation originated from	"asi_laptop"	
user_agent	no	string		"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.12 Safari/537.36"	
host_domain	no	string	the domain to which the computer belongs. The full compute name is a concatenation of : ***host_name.host_domain***	"example" NIS1	In Cloud Web, the machine name comes from Endpoint, which provides it in "NTLM" form, so this may be a single word rather than a DNS-style domain.

Destination Object

The destination part is a list of destinations that the data was sent to. For most channels, this is a list containing a single object. Only the email channel supports multiple destinations.

Example of the Destination Object

```
"destinations": [{
    "destination_type": "...",
    "http_request_url": "...",
    "http_request_url_hostname": "...",
    "http_request_method": "...",
    "cloud_application_name": "...",
    "cloud_service_name": "...",
    "cloud_application_id" : "...",
    "sub_cloud_application_id" : "...",
    "destination_address_ip" : "...",
    "url_categories": ["...", "..."],
    "hybrid_url_categories" : ["...", "..."],
    "email_address": "..."
}]
```

Definition of the Destination Object

Field	Required	Type	Description	Values	Comments
destination_type	yes	Enumerator		[WEB_APPLICATION, CLOUD_APPLICATION, EMAIL_ADDRESS]	
http_request_url	yes-only for Web	String		"https://www.facebook.com/responses?usersname=asi&status=never_been_on_facebook"	
http_request_url_hostname	No	String		"www.facebook.com"	
http_request_method	destination_address_ip No	Enumerator		[POST, PUT, ...]	This can be any method that carries data content; so, for example, not GET or OPTIONS, but may be PROPPATCH (WebDAV)
cloud_application_name	yes-only for CASB	String		"myBoxFinanceApp"	
cloud_service_name	yes-only for CASB	String		"Box"	
cloud_application_id	yes-only for CASB	String		"3576"	
sub_cloud_application_id	No	String	this field will indicate the exact cloud application under the Office365 suit		
destination_address_ip	No	String	ip address of the cloud app		

Field	Required	Type	Description	Values	Comments
url_categories	yes-only for Web. Either 'url_categories' or 'hybrid_url_categ ories' should be present not both of them.	an array of strings each representing a url category id		Example: ["72378", "72374"]	
hybrid_url_categ ories		an array of strings each representing a url category id		Example: ["71078", "72380"]	
email_address	yes-only for Email	String	the 'TO' email address	example @forcepoint.com	

Inspection Response

The inspection response will return to the agent as a single json.

Related concepts
CPE_Transaction_Info Object on page 17
Violation Object on page 17
Rule Object on page 18
Action Object on page 19

Definition of the Inspection Response

Field	Required	Type	Description	API V4.0 Limitations
global_message_id	Yes	String	The corresponding global message id.	
resolution	Yes	Enumerator	Resolution of the response.	
cpe_transaction_info	Yes	cpe_transaction_info Object	Info regarding the DLP transaction.	
violations	No	List of Violation Objects	List of violations, including policies and rules.	
actions	Yes	List of Action Object	List of actions.	

Field	Required	Type	Description	API V4.0 Limitations
max_number_of_matches	No	Integer	The maximum number of matches of any of the violated rules.	

Example of the Inspection Response

```
{
    "global_message_id": “String”,
    "resolution" : “Enumerator String”,
    "cpe_transaction_info": {cpe_transaction_info Object},
    "violations": [List of Violation Object],
    "actions": [List of Action Object],
    "max_number_of_matches": integer
}
```

Resolution Enumerator

Value	Description
MATCHED	
UNMATCHED	

CPE_Transaction_Info Object

The CPE_Transaction_Info Object includes an internal engine event ID that can be used for troubleshooting.

```
{
    "id": "String"
}
```

Definition of the Info Object

Field	Required	Type	Description	Values	API V4.0 Limitations
id	Yes	String	a UID numeric string of the DLP transaction		

Violation Object

Example of the Violation Object

```
{
   "policy_id": “String”,
   "policy_name": “String”,
   "violated_rules": [List of Rule objects],
}
```

Description of the Violation Object

Field	Required	Type	Description	Values	API V4.0 Limitations
policy_id	Yes	String	DLP Policy ID		
policy_name	Yes	String	DLP Policy name		
violated_rules	Yes	List	List of Rule Objects		

Rule Object

Example of the Rule Object

```
{
      "rule_id": "String",
      "rule_name": "String",
      "rule_severity": "Enumerator String",
      "rule_number_of_matches": integer
}
```

Description of the Rule Object

Field	Required	Type	Description	Values	API V4.0 Limitations
rule_id	Yes	String	The violated rule ID		
rule_name	Yes	String	The violated rule name		
rule_severity	Yes	Enumerator	Severity of the violated rule		
rule_number_of_matches	Yes	Integer	Number of rule matches found	>0	

Severity Enumerator

1) LOW
2) MEDIUM
3) HIGH
4) NA

Action Object

Example of the Action Object

```
{
      "action_type": “String from a closed set of strings”
}
```

Definition of the Action Object

Field	Required	Type	Description	Values	API V4.0 Limitations
action_type	Yes	String from a closed set of strings	Actual Action		

Set of Possible Values for Action Type

1) Unknown
2) Permit
3) Pe Request
4) Confirm allow
5) Confirm Block
6) Encrypt

7) Drop

8) Block

9) User Encrypt

10) Safe copy

11) Quarantine

12) Quarantine with note

13) Unshare external

14) Unshare all

Chapter 3

Enumerators

Contents

Following are all the json properties that are Enumerators by value:

Enumerators based on "client_name"

1) `FORCEPOINT_CASB`
2) `FORCEPOINT_WEB`
3) `FORCEPOINT__EMAIL`
4) `FONE_CASB`
5) `FONE_SWG`
6) `UNKNOWN`

Enumerators based on "data_channel"

1) `HTTP`
2) `HTTPS`
3) `CASB_API`
4) `CASB_REAL_TIME`

5) `CASB_DISCOVERY`

6) `TESTING_CHANNEL`

Enumerators based on "activity_type"

Following is the list of "activity_type" along with it's corresponding ENUM number.

1) `NONE (0)`

2) `UPLOAD (1)`

3) `DOWNLOAD (2)`

4) `SHARE (3)`

5) `EXTERNAL_SHARE (4)`

6) `REQUEST (5)`

7) `SYNC (6)`

8) `UNSHARE (7)`

9) `DELETE (8)`

10) `CREATE (9)`

11) `MODIFY (10)`

12) `VIEW (11)`

13) `MOVE (12)`

14) `LOCK (13)`

15) `RENAME (14)`

16) `RESTORE (15)`

17) `PRINT (16)`

18) `COPY (17)`

19) `SEND (18)`

20) `INTERNAL_SHARE (22)`

21) `PUBLIC_SHARE (23)`

22) `UNKNOWN (19)`

Enumerators based on "item_type"

1) `FILE`

2) `FOLDER`

Enumerators based on "destination_type"

1) `WEB_APPLICATION`

2) `CLOUD_APPLICATION`

Enumerators based on "http_request_method"

1) `POST`

2) `PUT`

3) `GET`

Enumerators based on "url_category_type"

1) `PRE_DEFINED`
2) `USER_DEFINED`

Chapter 4

CASB Request Sample

Contents

CASB Multipart Mime Inspection Request Sample:

```
POST /inspection/v4.0 HTTP/1.1
Host: localhost:8080
User-Agent: Forcepoint_CASB
Accept: */*
Authorization: Bearer <jwt token>
Content-Length: 1106
Content-Type: multipart/form-data; boundary=------------------------4881f7ecd6edc9e8

--------------------------4881f7ecd6edc9e8
Content-Disposition: form-data; name="metadata"; filename="casbInspectionRequest.json"
Content-Type: application/json

{
    "context": {
        "global_message_id": "1564953753559",
        "client_name": "FORCEPOINT_CASB",
        "data_channel": "CASB_REAL_TIME",
        "activity_type": "UPLOAD",
        "occurred_message_timestamp_utc_ms": 1585657815000,
        "isDeviceManaged": "false"
    },
    "contentDescriptors": [{
        "id": "0",
        "name": "tal1.txt",
        "item_type" : "FILE",
        "size_bytes": 388
    }],
    "source": {
        "user_email_address": "alan@veridinet.onmicrosoft.com",
        "host_ips": ["157.167.3.2"],
        "host_domain": "onmicrosoft.com"
    },
    "destinations": [{
        "destination_type": "CLOUD_APPLICATION",
        "http_request_url_hostname": "veridinet-my.sharepoint.com",
        "http_request_method": "POST",
        "cloud_application_name": "Office365 (1)",
        "cloud_service_name": "Office365",
        "cloud_application_id" : "3576",
        "destination_address_ip" : "13.107.136.9"
    }]
}
--------------------------4881f7ecd6edc9e8
Content-Disposition: form-data; name="0"; filename="tal1.txt"
Content-Type: text/plain

catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
catch22 catch22 catch23
```

CASB API Inspection Request json Sample:


```
{
    "context": {
        "global_message_id": "1564953753559",
        "client_name": "FORCEPOINT_CASB",
        "data_channel": "CASB_API",
        "activity_type": "UPLOAD",
        "occurred_message_timestamp_utc_ms": 1585657815000,
        "isDeviceManaged": "false"
    },
    "contentDescriptors": [{
        "id": "0",
        "name": "tal1.txt",
        "item_type" : "FILE",
        "size_bytes": 388,
        "file_path": "C:\myFolder\folder1",
        "sharing_status": "internal",
        "shared_with": ["email1@gmail.com", "email2@gmail.com"],
        "owner_name": "tbennaim",
        "owner_email": "tbennaim@forcepoint.com",
        "creation_time_utc_ms": 1505897456000,
        "modification_time_utc_ms": 1505897456000,
        "access_time_utc_ms": 1505897456000
    }],
    "source": {
        "user_email_address": "alan@veridinet.onmicrosoft.com",
        "host_ips": ["157.167.3.2"],
        "host_domain": "onmicrosoft.com"
    },
    "destinations": [{
        "destination_type": "CLOUD_APPLICATION",
        "http_request_url_hostname": "veridinet-my.sharepoint.com",
        "cloud_application_name": "Office365 (1)",
        "cloud_service_name": "Office365",
        "cloud_application_id" : "3576",
        "destination_address_ip" : "13.107.136.9"
    }]
}
```

CASB DAR Inspection Request json Sample:


```
{
    "context": {
        "global_message_id": "1564953753559",
        "client_name": "FORCEPOINT_CASB",
        "data_channel": "CASB_DISCOVERY",
        "activity_type": "NONE",
        "occurred_message_timestamp_utc_ms": 1585657815000,
        "isDeviceManaged": "false"
    },
    "contentDescriptors": [{
        "id": "0",
        "name": "tal1.txt",
        "item_type" : "FILE",
        "size_bytes": 388,
        "file_path": "C:\myFolder\folder1",
        "sharing_status": "internal",
        "shared_with": ["email1@gmail.com", "email2@gmail.com"],
        "owner_name": "tbennaim",
        "owner_email": "tbennaim@forcepoint.com",
        "creation_time_utc_ms": 1505897456000,
        "modification_time_utc_ms": 1505897456000,
        "access_time_utc_ms": 1505897456000
    }],
    "source": {
        "user_email_address": "alan@veridinet.onmicrosoft.com",
        "host_ips": ["157.167.3.2"],
        "host_domain": "onmicrosoft.com"
    },
    "destinations": [{
        "destination_type": "CLOUD_APPLICATION",
        "cloud_application_name": "Office365 (1)",
        "cloud_service_name": "Office365",
        "cloud_application_id" : "3576",
        "destination_address_ip" : "13.107.136.9"
    }]
}
```

CASB DAR large file Inspection Request json Sample:


```
{
    "context": {
        "global_message_id": "request_id",
        "client_name": "FORCEPOINT_CASB",
        "activity_type": "UPLOAD",
        "data_channel": "CASB_API",
        "occurred_message_timestamp_utc_ms": 1600087464660
    },
    "contentDescriptors": [
        {
            "oss_object_access_parameters": {
                "download_parameters" : {
                    "request_parameters" : {
                        "tenant_id": "abceee0000000000000000000000000",
                        "object_type": "configuration/policy/tal",
                        "object_name": "Picture.docx.object"
                    },
                    "header_parameters" : {
                        "global_tenant_id" : "abceee00000000000000000000000000"
                    }
                },
                "delete_parameters": {
                    "request_parameters" : {
                        "tenant_id" : "abceee00000000000000000000000000",
                        "object_type" : "configuration/policy/tal",
                        "object_name_prefix" : "Picture.docx.object"
                    },
                    "header_parameters" : {
                        "global_tenant_id" : "abceee00000000000000000000000000"
                    }
                }
            },
            "name": "matchTal.docx",
            "size_bytes": 13989638,
            "item_type": "FILE",
            "file_id": "{\"id\":\"1234\"}",
            "file_path": "/folder1/folder2/matchTal.docx",
            "sharing_status": "internal",
            "shared_with": [
                "email1@gmail.com",
                "email2@gmail.com"
            ],
            "owner_name": "Turing, Alan",
            "creation_time_utc_ms": 1532603842961,
            "modification_time_utc_ms": 1532603878922,
            "access_time_utc_ms": 1532603921874
        }
    ],
    "source":
    {
        "user_principal_name": "john.smith@forcepoint.com",
        "down_level_logon_name": "nis1/jsmith",
        "sam_account_name": "jsmith",
        "user_email_address": "jsmith@forcepoint.com",
        "distinguished_name" : "CN=Smith,John,OU=Users,OU=Raanana,DC=example,DC=com",
        "host_ips": ["192.168.31.14", "127.0.0.1"],
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
         like Gecko) Chrome/81.0.4044.122 Safari/537.36",
        "host_domain": "dlptest.com"
    },
```

CASB DAR large file Inspection Request json Sample: (continued...)

```
    "destinations": [
        {
            "destination_type": "CLOUD_APPLICATION",
            "cloud_application_name": "MyBox",
            "cloud_service_name": "Box",
            "cloud_application_id": "7"
        }
    ]
}
```

CASB Cloud Email Inspection Request json Sample:

```
{
    "context":
    {
        "global_message_id": "nRzHqj:xMf:729",
        "client_name": "FORCEPOINT_EMAIL",
        "data_channel": "EMAIL",
        "activity_type": "SEND",
        "occurred_message_timestamp_utc_ms": 1600087464660
    },
    "contentDescriptors":
    [{
        "id": "0",
        "name": "mail1.eml",
        "item_type" : "FILE",
        "size_bytes": 4096
    }],
    "source":
    {
        "user_principal_name": "john.smith@forcepoint.com",
        "host_ips": ["192.168.31.14"]
    },
    "destinations":
    [{
        "destination_type": "EMAIL_ADDRESS",
        "email_address": "eelkes@qaexch2010.wbsn"
    },
    {
        "destination_type": "EMAIL_ADDRESS",
        "email_address": "tbennaim@qaexch2010.wbsn"
    }]
}
```

Chapter 5

Web Multipart Inspection

Contents

Web Multipart Mime Inspection Request

The below sample is the whole HTTP inspection request that comprises of a multi part mime containing in its first part the Inspection Request json and in its second part a mime file called 'trans_0_5397024941029260958.dat'. This mime file was generated by the website https://dlptest.com/ when uploading a docx file called 'matchTal.docx'. Using a curl client, the Inspection Request json and the trans_0_5397024941029260958.dat mime file were sent to the the REST server for inspection by running the following command:

```
curl -v POST -H "Content-Type:multipart/form-data" -H "Authorization: Bearer jwttokenTalTal"
 -F "metadata=@C:/temp/WebInspectionRequest.json;type=application/json" -F "0=@C:/temp/
trans_0_5397024941029260958.dat;type=application/http" http://10.0.190.45:8080/inspection/v4.0
```

Complete HTTP Web Inspection Request Sample

```
POST /inspection/v4.0 HTTP/1.1
Host: 10.0.190.45:8080
User-Agent: curl/7.55.1
Accept: */*
Authorization: Bearer jwttokenTalTal
Content-Length: 13431
Expect: 100-continue
Content-Type:multipart/form-data; boundary=------------------------c5f7846b2b41227e

--------------------------c5f7846b2b41227e
Content-Disposition: form-data; name="metadata"; filename="WebInspectionRequest.json"
Content-Type: application/json

{
    "context":
    {
        "global_message_id": "11111",
        "client_name": "FORCEPOINT_WEB",
        "data_channel": "HTTPS",
        "activity_type": "UPLOAD",
        "occurred_message_timestamp_utc_ms": 1505897456000
    },
    "contentDescriptors":
    [{
        "id": "0",
        "name": "trans_0_5397024941029260958.dat",
        "item_type" : "FILE",
        "size_bytes": 16384
    }],
    "source":
    {
        "user_principal_name": "john.smith@forcepoint.com",
        "down_level_logon_name": "nis1\jsmith",
        "sam_account_name": "jsmith",
        "distinguished_name": "CN=Smith\, John,OU=Users,OU=Raanana,DC=example,DC=com",
        "user_email_address": "jsmith@forcepoint.com",
        "host_ips": ["192.168.31.14"],
        "host_name": "john_laptop",
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/81.0.4044.122 Safari/537.36",
        "host_domain": "dlptest.com"
    },
    "destinations":
    [{
        "destination_type": "WEB_APPLICATION",
        "http_request_url": "https://dlptest.com/",
        "http_request_url_hostname": "www.dlptest.com",
        "http_request_method": "POST",
        "url_categories": ["72378"]
    }]
}
--------------------------c5f7846b2b41227e
Content-Disposition: form-data; name="0"; filename="trans_0_5397024941029260958.dat"
Content-Type: application/http

Accept: application/json
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------7e4278b104be
Referer: http://dlptest.com/http-post/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
```

Complete HTTP Web Inspection Request Sample(continued….)

```
-----------------------------7e4278b104be
Content-Disposition: form-data; name="action"

frm_submit_dropzone
-----------------------------7e4278b104be
Content-Disposition: form-data; name="field_id"

8
-----------------------------7e4278b104be
Content-Disposition: form-data; name="form_id"

5
-----------------------------7e4278b104be
Content-Disposition: form-data; name="nonce"

6df5b2205b
-----------------------------7e4278b104be
Content-Disposition: form-data; name="file8"; filename="matchTal.docx"
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
```

Web Multipart Mime Inspection Response


```
{
    "global_message_id": "1564953753559",
    "resolution": "MATCHED",
    "cpe_transaction_info": {
        "id": "14073523857063450160"
    },
    "violations": [
        {
            "policy_id": "19967",
            "policy_name": "catch22",
            "violated_rules": [
                {
                    "rule_name": "catch22",
                    "rule_severity": "MEDIUM",
                    "rule_number_of_matches": 6,
                    "rule_id": "rule_19967"
                }
            ]
        },
        {
            "policy_id": "19972",
            "policy_name": "KOKO_policy",
            "violated_rules": [
                {
                    "rule_name": "KOKO_rule",
                    "rule_severity": "MEDIUM",
                    "rule_number_of_matches": 11,
                    "rule_id": "rule_19972"
                }
            ]
        }
    ],
    "actions": [
        {
            "action_type": "Block"
        }
    ],
    "max_number_of_matches": 11
}
```

Complete HTTP Web Inspection Response Sample

```
< HTTP/1.1 100
< HTTP/1.1 200
< Content-Type: application/json;charset=UTF-8
< Transfer-Encoding: chunked
< Date: Mon, 27 Apr 2020 12:45:24 GMT
<
{
    "global_message_id": "1564953753559",
    "resolution": "MATCHED",
    "cpe_transaction_info": {
        "id": "14073523857063450160"
    },
    "violations": [
        {
            "policy_id": "19967",
            "policy_name": "catch22",
            "violated_rules": [
                {
                    "rule_name": "catch22",
                    "rule_severity": "MEDIUM",
                    "rule_number_of_matches": 6,
                    "rule_id": "rule_19967"
                }
            ]
        },
        {
            "policy_id": "19972",
            "policy_name": "KOKO_policy",
            "violated_rules": [
                {
                    "rule_name": "KOKO_rule",
                    "rule_severity": "MEDIUM",
                    "rule_number_of_matches": 11,
                    "rule_id": "rule_19972"
                }
            ]
        }
    ],
    "actions": [
        {
            "action_type": "Block"
        }
    ],
    "max_number_of_matches": 11
}
* Connection #1 to host 10.0.190.45 left intact
```