EXHIBIT 23

Sky ATP Open API

Sky ATP Public API

Default response content-types: application/json
Schemes: http

Summary

Tag: SubmitSample

Operation	Description
POST /v1/skyatp/submit/sample	Submit sample for malware analysis.

Tag: HashLookup

Operation	Description
GET /v1/skyatp/lookup/hash/{hash_string}	Lookup sample malware score by hash.

Tag: blwlOne

Operation	Description
GET /v1/skyatp/{list_type}/param/{server_type}	
PATCH /v1/skyatp/{list_type}/param/{server_type}	
DELETE /v1/skyatp/{list_type}/param/{server_type}	

Tag: blwlN

Operation	Description
GET /v1/skyatp/{list_type}/file/{server_type}	
PATCH /v1/skyatp/{list_type}/file/{server_type}	
DELETE /v1/skyatp/{list_type}/file/{server_type}	

Tag: default

Operation	Description
GET /ping	Ping the API to determine if it is alive.

Security

Bearer

name: Authorization
in: header

Paths

GET /ping — Ping the API to determine if it is alive.

DESCRIPTION

Uses default content-types: application/json

200 OK
Ping succeeded.

GET /v1/skyatp/lookup/hash/{hash_string}
Tags: HashLookup

Lookup sample malware score by hash.

DESCRIPTION

Lookup sample malware score by hash (sha256). Optional full scanning report may be requested.

REQUEST PARAMETERS

Name	Description	Type	Data type	
hash_string	Sample hash. Only SHA256 is supported at this time.	path	*string* (64 to 64 chars)	**required**
full_report	Whether to return a full scanning report. This should be set to true if user wants to retrieve a detailed sample analysis report in JSON format.	query	*boolean*	
Authorization	Bearer token of the form, Bearer token, token is application token generated from Customer Portal.	header	*string*	**required** **global** #/parameters/auth_header
X-Forwarded-For	This is a header that provides tracking information for API usage.	header	*string*	**global** #/parameters/forward_header

RESPONSES

Uses default content-types: application/json

200 OK
Hash lookup succeeded. Returns a result JSON object.

Example for application/json


```
{
    "last_update": 0,
    "malware_info": {
        "ident": "MemScan:Trojan.Pws"
    },
    "report": null,
    "scan_complete": false,
    "score": -1,
    "sha256": "516f3396086598142db5e242bc2c8f69f4f5058a637cd2f9bf5dcb4619869536"
}
```


ScanResult

401 Unauthorized
Invalid API key

Error

Error

422 Unprocessable Entity
Missing or invalid parameters to HTTP call.

Error

429 Too Many Requests
Client has sent too many requests in a given amount of time. Submission quota exceeded.

500 Internal Server Error
Internal server error.

Error

503 Service Unavailable
Service is temporarily not available. The Retry-After response header will indicate how long the service is expected to be unavailable to the requesting client.

SECURITY

Schema	Scopes
Bearer	

POST /v1/skyatp/submit/sample

Submit sample for malware analysis.

Tags: SubmitSample

DESCRIPTION

Submit sample for malware analysis. To call this method, the user must provide a `file` parameter containing file content to be uploaded. The user also may provide additional information related to the sample such as client/remote IP, sample URL, client host name, name of the user who downloaded the sample, etc. If the submitted sample is determined to be malicious, Sky ATP may use this additional information to track the client within the internal network and notify the user that the host is infected.

REQUEST BODY

multipart/form-data

REQUEST PARAMETERS

Name	Description	Type	Data type	
file	Sample file to submit.	formData	*file*	**required**
full_report	Whether to return a full scanning report. This should be set to true if user wants to retrieve a detailed sample analysis report in JSON format.	query	*boolean*	
sample_url	URL where the sample was downloaded from.	formData	*string*	
remote_ip	IP address where the sample was downloaded from.	formData	*string*	
client_ip	IP address of the client that downloaded this sample.	formData	*string*	

Name	Description	Type	Data type	
client_hostname	Hostname of the client that downloaded this sample.	formData	*string*	
username	Username of the client that downloaded this sample.	formData	*string*	
Authorization	Bearer token of the form, Bearer token, token is application token generated from Customer Portal.	header	*string*	**required** **global** #/parameters/auth_header
X-Forwarded-For	This is a header that provides tracking information for API usage.	header	*string*	**global** #/parameters/forward_header

RESPONSES

application/json

200 OK

File submission succeeded. Returns a submission JSON object.

Example for application/json


```
{
    "last_update": 1464891625,
    "malware_info": {
        "ident": "MemScan:Trojan.Pws"
    },
    "scan_complete": true,
    "score": 10,
    "sha256": "516f3396086598142db5e242bc2c8f69f4f5058a637cd2f9bf5dcb4619869536"
}
```


ScanResult

401 Unauthorized

Invalid API key.

Error

413 Request Entity Too Large

Sample file size over max limit.

Error

422 Unprocessable Entity

Missing or invalid parameters to HTTP call.

Error

429 Too Many Requests

Client has sent too many requests in a given amount of time. Submission quota exceeded.

Error

500 Internal Server Error

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.