Precinct 6.0 API Documentation

Updated: 8/30/2020 by Charles Herring

Contents

Authentication

The following calls handle user authentication

Login

Endpoint: v1/login

Type: POST

Headers: None

Post Fields: email (email address)

password (plain-text string)

Codes: 200 (Success)

403 (Authentication failure)

Response: JSON

data_role: INTEGER

error: STRING

function_role: INTEGER

success: BOOLEAN

token: UUID

***Note**: All API calls require the token returned to be in the header as* **API-Token**

Logout

Logs out the current session

Endpoint: v1/logout

Type: DELETE

Headers: None

Post Fields: token

Codes: 200 (Success)

Response: Empty

Register

Creates the first user account

Endpoint: v1/register

Type: POST

Headers: None

Post Fields: email (email address)

name (string

password Array

password (string)

passwordConfirm (string)

Codes: 200 (Success)

403 (Authentication failure)

Incidents

The following calls handle retrieving and updating WitFoo incidents.

Get List of Incidents

Endpoint: v1/api/incident_groups

Type: GET

Headers: API-Token (required)

Querystring: status_id (array)

evidence_after: (date in YYYY-MM-DD format)

facet_ig_mos (array of integers)

facet_ig_products (array of integers)

facet_suspicion_score (array)

min_suspicion_score: float

max_suspicion_score: float

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Response: JSON

facets (array)

date_range (array)

count (integer)

evidence_after: (date)

range: (string) ex: “Today”

mos (array)

count (integer)

mo_id (integer)

mo_name (string)

products (array)

count (ineger)

id (integer)

label (string)

statuses (array)

count (integer)

name (string)

status_id (integer)

suspicion_score (array)

count (integer)

id (string)

label (string)

max_suspicion_score (float)

min_suspicion_score (float)

igs (array)

assigned (integer) Maps to user id

first_observed_at (unix timestamp)

last_observed_at (unix timestamp)

id (uuid)

mo_id (integer) Maps to MO id

mo_name (string)

name (string)

node_types (array)

file (integer)

host (integer)

target (integer)

user (integer)

email (integer)

products (array)

capex (integer)

enabled (integer)

foreign_id (integer)

id (integer)

logo (string)

name (string)

oppex (integer)

rule_source (integer)

vendor_name (string)

status_id (integer)

status_name (string)

suspicion_score (float)

username (string)

total_count (integer)

Example Request:

facet_users[]: 0

status_id[]: 0

status_id[]: 1

status_id[]: 2

status_id[]: 3

status_id[]: 4

status_id[]: 5

evidence_after: 2020-08-23

facet_products[]: 1

facet_ig_mos[]: 1

facet_ig_mos[]: 2

facet_ig_mos[]: 3

facet_ig_mos[]: 4

facet_ig_mos[]: 5

facet_suspicion_score[]: {"min_suspicion_score":0,"max_suspicion_score":0.49}

facet_suspicion_score[]: {"min_suspicion_score":0.5,"max_suspicion_score":0.74}

facet_suspicion_score[]: {"min_suspicion_score":0.75,"max_suspicion_score":0.99}

Example Response

{"facets":{"date_range":[{"count":0,"evidence_after":"2020-08-29","range":"Today"},{"count":1,"evidence_after":"2020-08-23","range":"Last 7 Days"},{"count":1,"evidence_after":"2020-07-31","range":"Last 30 Days"},{"count":1,"range":"All"}],"products":{"5":{"label":"Carbon Black Protect\/Defend","id":"5","count":1},"85":{"label":"WitFoo IOC Feed","id":"85","count":1},"1":{"label":"Stealthwatch","id":"1","count":1}},"users":[{"count":1,"id":0,"label":"Unassigned"}],"mos":[{"count":1,"mo_id":1,"mo_name":"Data Theft"},{"count":0,"mo_id":2,"mo_name":"Phishing"},{"count":0,"mo_id":3,"mo_name":"Ransomware"},{"count":0,"mo_id":4,"mo_name":"Service Disruption"},{"count":0,"mo_id":5,"mo_name":"Policy Violation"}],"statuses":[{"count":1,"name":"Open","status_id":0},{"count":0,"name":"Convicted","status_id":1},{"count":0,"name":"Acquitted","status_id":2},{"count":0,"name":"Cold Case","status_id":3},{"count":0,"name":"Disrupted","status_id":5}],"suspicion_score":[{"count":0,"id":"0","label":"Low","max_suspicion_score":0.49,"min_suspicion_score":0},{"count":0,"id":"1","label":"Medium","max_suspicion_score":0.75,"min_suspicion_score":0.5},{"count":1,"id":"2","label":"High","max_suspicion_score":1.01,"min_suspicion_score":0.76}]},"igs":[{"id":"8c09c8d0-e54f-11ea-8aa4-29d736fd72d6","first_observed_at":1598192066,"last_observed_at":1598193916,"suspicion_score":0.95550537109375,"tools":{"5":{"id":5,"name":"Carbon Black Protect\/Defend","vendor_name":"Carbon Black","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":5,"logo":"carbon-black.png"},"85":{"id":85,"name":"WitFoo IOC Feed","vendor_name":"WitFoo","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":85,"logo":"witfoo.png"},"1":{"id":1,"name":"Stealthwatch","vendor_name":"Cisco","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":1,"logo":"cisco.png"}},"mo_id":1,"mo_name":"Data Theft","status_id":0,"status_name":"Open","name":"Uptight Aardvark","node_types":{"host":5,"target":4,"user":1,"file":2},"products":{"5":{"id":5,"name":"Carbon Black Protect\/Defend","vendor_name":"Carbon Black","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":5,"logo":"carbon-black.png"},"85":{"id":85,"name":"WitFoo IOC Feed","vendor_name":"WitFoo","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":85,"logo":"witfoo.png"},"1":{"id":1,"name":"Stealthwatch","vendor_name":"Cisco","versions":1,"capex":0,"oppex":0,"rule_source":1,"enabled":1,"foreign_id":1,"logo":"cisco.png"}},"assigned":0,"username":null}],"total_count":1,"log":[]}

Get a specific Incident

To retrieve a specific incident, use its UUID in the URL

Endpoint: v1/api/ incident_groups/{uuid}

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Update a specific Incident

An updated Incident can be sent in its entirety to the API. Only PUT a full Incident.

Endpoint: v1/api/ incident_groups/{uuid}

Type: PUT

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Post Data: JSON Object in valid Incident Format

Artifact Search Jobs

The following calls are used to query artifacts. A search job must be created. Results are retrieved by pulling the job results. Incremental results are returned.

Create Search Job

This will return the Job ID

Endpoint: v1/api/ search/jobs/create/{base64_criteria}

Type: GET

Headers: API-Token (required)

base64_criteria: Search criteria encoded into base64

Querystring: start_date: timestamp

end: timestamp

limit: integer

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : UUID representing the job ID

Fetch Job Results

This will return the results of a search job

Endpoint: v1/api/ search/jobs/get/{job_id}

Type: GET

Headers: API-Token (required)

job_id: UUID of Job ID from Create or List Jobs

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : records (array of artifacts)

List Jobs

This will return the list of all cached jobs

Endpoint: v1/api/ search/jobs/list

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of jobs

Settings & Users

The following endpoints interact with Users and Settings

Fetch Settings

Fetch all settings

Endpoint: v1/settings

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of settings

Update Settings

Fetch all settings

Endpoint: v1/settings

Type: PUT

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of settings

Post Data: JSON Object in valid Settings Format

Fetch Users

Fetch all settings

Endpoint: v1/api/users

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of users

Update Settings

Fetch all settings

Endpoint: v1/api/users

Type: PUT

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of settings

Post Data: JSON Object in valid Users Format

Reports

The following endpoints grab report data

Fetch All Report Data

Fetch all reports for all ranges

Endpoint: v1/api/reports

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Return : array of report data

Fetch Specific Report

Fetch specific report

Endpoint: v1/api/reports/{subreport}

subreport: Name of specific report

Type: GET

Headers: API-Token (required)

Codes: 200 (Success)

403 (Authentication failure)

401 (Results not found)

Querystrings: days_back (1,5,30,180 or 365)

Mo_id (0 = all or valid MO ID - currently 1,2,3,4,5)

Return : array of report data