Incidents API

Overview

This topic covers the API for **Cloud Threat Response Incidents**.

See the Threat Protection APIs topic for general API information - you will need the information in that topic for details about authentication.

Incident APIs Filters

This section includes the details for various filters on the Incidents APIs.

Table 1: Supported value types for filters

Value Type	API Identifier (valueType field)	Value validation
Time Range	time_range_filter	• start: <YYYY-MM-DD hh:mm:ss>, end: <YYYY-MM-DD hh:mm:ss>
Incident ID	incident_id_filters	Valid incident ID (For example, "583" for INC-583)

Value Type	API Identifier (valueType field)	Value validation
Incident State	other_filters	• open_incidents • closed_incidents
Incident Priority	priority_filters	• high • medium • low
Source	source_filters	• abuse_mailbox • tap • smart_search • message_csv_upload
Very Attacked Person (VAP)	other_filters	vap
Disposition	disposition_filters	• bulk • clean • impostor • in_progress • internal • low_risk • malware • manual_review • not_set • phish • scam • simulated_phish • spam • suspicious • tap_false_positive • toad • vendor

Value Type	API Identifier (valueType field)	Value validation
CLEAR Verdict	verdict_filters	• verdict_failed • verdict_low_risk • verdict_manual_review • verdict_threat
CLEAR Confidence	confidence_filters	• confidence_high • confidence_medium • confidence_low

Table 2: Supported pagination controls

Value Type	API Identifier (valueType field)	Value validation
Page Start and End	startRow and endRow	First page • 0 - First record • 200 - Last record Second page • 201 - First record • 400 - Second record

Table 3: Supported sorting controls

Value Type	API Identifier (valueType field)	Value validation

Sort Order	sortParams - sort	sortParams: [{
		"sort": "desc"
		}
		
		sortParams: [{
		"sort": "asc"
		}

Value Type	API Identifier (valueType field)	Value validation

Sort on Creation Time	sortParams - colId	sortParams: [{
		"colId": "createdAt"
		}

Incidents APIs

Get Incident Count

Path	/api/v1/tric/incidents/count
HTTP Method	POST
Description	Get count of incidents, filtered on specific criteria

Request

Headers

Header Name	Header Value	Notes
Authorization	Bearer <AUTH TOKEN>	See the API Authentication section on Threat Protection APIs for details on how to generate an auth token

Request Body Example

```
{
  "filters": {
    "time_range_filter": {"start": "2024-10-26 16:18:07", "end": "2024-11-27 16:18:07"},
    "source_filters":  ["tap"]
  }
}
```

Response

Response Code	200
Response Headers	Content-Type: application/json
Response Body	<COUNT>

Error Response Refer to Error Responses section

Example request with curl

```
#!/bin/bash
CONTENT_TYPE='Content-Type: application/json'
URL='https://threatprotection-api.proofpoint.com/api/v1/tric/incidents/count
AUTH_TOKEN='<GENERATED AUTH TOKEN>'
curl -X POST -H "$CONTENT_TYPE" -H "Authorization: Bearer $AUTH_TOKEN" "$URL" -d '{
  "filters": {
     "time_range_filter": {"start": "2024-10-26 16:18:07", "end": "2024-11-27 16:18:07"},
     "source_filters":  ["tap"]
   }
}'
```

Example JSON Response

```
785
```

Get Summary for Incident ID (TAP)

Path /api/v1/tric/incidents/

HTTP Method POST

Description Get incident summary for a specific incident, filtered on incident ID

Request

Headers

Header Name	Header Value	Notes

Authorization	Bearer <AUTH TOKEN>	See the API Authentication section on Threat Protection APIs for details on how to generate an auth token

Request Body Example

```
{
   "filters": {
      "incident_id_filters": ["781"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
}
```

Response

Response Code 200

Error Response Refer to Error Responses section

Example request with curl

```
#!/bin/bash
CONTENT_TYPE='Content-Type: application/json'
URL='https://threatprotection-api.proofpoint.com/api/v1/tric/incidents'
AUTH_TOKEN='<GENERATED AUTH TOKEN>'
curl -X POST -H "$CONTENT_TYPE" -H "Authorization: Bearer $AUTH_TOKEN" "$URL" -d '{
  "filters": {
      "incident_id_filters": ["781"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
}'
```

Example Response

Standard HTTP response with status code 201


```
{
   "total": 1,
   "startRow": 0,
   "endRow": 1,
   "incidents": [
      {
         "id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
         "sid": 9114748,
         "createdAt": "2024-10-22T23:26:17.239+00:00",
         "updatedAt": "2024-10-22T23:26:24.844+00:00",
         "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
         "closedAt": "2024-10-22T23:26:24.844+00:00",
         "displayId": 781,
         "title": "Message Delivered to bob[@]tricorion[.]tk with link hxxps://theexcelclub[.]com/",
         "state": "closed",
         "assignedTeamName": "Analyst",
         "assignedTeamId": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
         "messageCount": 2,
         "vap": true,
         "vip": false,
         "abuseSourceIds": [],
         "sourceTypes": [
            "tap_alert"
         ],
         "sourcesData": [
            {
               "type": "TapAlert"
            }
         ],
         "commentCount": 1,
         "dispositions": [
            "malware"
         ],
         "clearVerdicts": [],
         "clearConfidences": []
      }
   ]
}
```


Get All Details for Incident ID (TAP)

Path	/api/v1/tric/incidents/<ID>/messages Note: The **ID** is obtained from the "id" field in the Incident Summary API request.

HTTP Method	POST
Description	Get incident and message details for a specific incident, filtered on incident ID

Request

Headers

Header Name	Header Value	Notes
Authorization	Bearer <AUTH TOKEN>	See the API Authentication section on Threat Protection APIs for details on how to generate an auth token

Request Body Example

```
{
   "filters": {
      "incident_id_filters": ["781"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
}
```

Response

Response Code 201

Error Response Refer to Error Responses section

Example request with curl

```
#!/bin/bash
CONTENT_TYPE='Content-Type: application/json'
URL='https://threatprotection-api.proofpoint.com/api/v1/tric/incidents/63b97d57-0af4-4835-8a3e-8d9fe3949786/messages'
AUTH_TOKEN='<GENERATED AUTH TOKEN>'
```

```
curl -X POST -H "$CONTENT_TYPE" -H "Authorization: Bearer $AUTH_TOKEN" "$URL" -d '{
  "filters": {
      "incident_id_filters": ["781"]
  },
  "endRow": 200,
  "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
  }],
  "startRow": 0
}'
```

Example Response

Standard HTTP response with status code 201


```
{
  "summary": {
      "id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
      "sid": 9114748,
      "createdAt": "2024-10-22T23:26:17.239+00:00",
      "updatedAt": "2024-10-22T23:26:24.844+00:00",
      "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
      "displayId": 781,
      "state": "closed",
      "title": "Message Delivered to bob[@]tricorion[.]tk with link hxxps://theexcelclub[.]com/",
      "closedAt": "2024-10-22T23:26:24.844+00:00",
      "assignedTeamId": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
      "assignedTeamName": "Analyst",
      "falsePositiveCount": 0,
      "messageCount": 2,
      "messageSourceData": {
          "hasTapAlert": true,
          "hasAbuseAlert": false,
          "hasSmartSearchImport": false,
          "hasMessageCsvUpload": false
      }
  },
  "comments": [
      {
          "id": "e248ce9d-a1ed-41a1-a277-f6d3efd38ee8",
          "author": "Security Admin User",
          "comment": "This incident has been remediated.",
          "deleted": false,
          "author_id": "a8405822-c771-474c-9154-7d023c710764",
          "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
          "comment_id": "5e1bba31-3ce9-4d10-99e6-3644b128abe0",
          "created_at": "2024-11-26T20:51:44.427",
          "updated_at": "2024-11-26T20:51:44.427",
          "incident_id": "e6134e09-6d02-444e-b1a6-7f9d7fe72cc7",
          "activity_type": "comment_addition",
          "activity_details": {}
      }
```

```
  ],
  "activities": [
    {
      "id": "b0bf87d9-99be-4d8d-8848-4fb9870549a3",
      "content": null,
      "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
      "cause_type": "history",
      "comment_id": null,
      "created_at": "2024-10-22T23:26:24.845",
      "updated_at": "2024-10-22T23:26:24.845",
      "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
      "occurred_at": "2024-10-22T23:26:24.845075",
      "activity_type": "state_change",
      "causing_api_key": null,
      "activity_details": {
        "new_state": "closed",
        "old_state": "open"
      },
      "causing_user_name": null,
      "causing_workflow_name": "Close Incident"
    },
    {
      "id": "0a54bd08-d9b7-4706-a11e-e23a3e54979d",
      "content": null,
      "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
      "cause_type": "system",
      "comment_id": null,
      "created_at": "2024-10-22T23:26:17.341",
      "updated_at": "2024-10-22T23:26:17.341",
      "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
      "occurred_at": "2024-10-22T23:26:17.341324",
      "activity_type": "message_addition",
      "causing_api_key": null,
      "activity_details": {
        "source_name": "Proofpoint Targeted Attack Protection (TAP)",
        "message_count": 1
      },
      "causing_user_name": null,
      "causing_workflow_name": null
    },
    {
      "id": "f0d12a0a-877a-4df3-8e5b-978f9b213cee",
      "content": null,
      "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
      "cause_type": "system",
      "comment_id": null,
      "created_at": "2024-10-22T23:26:17.24",
      "updated_at": "2024-10-22T23:26:17.28",
      "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
      "occurred_at": "2024-10-22T23:26:17.240509",
      "activity_type": "incident_creation",
      "causing_api_key": null,
      "activity_details": {
        "source_name": "Proofpoint Targeted Attack Protection (TAP)",
```

```
            "initial_title": "Message Delivered to bob[@]tricorion[.]tk with link hxxps://theexcelclub[.
]com/",
            "message_count": 1,
            "initial_team_id": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
            "initial_priority": null,
            "initial_team_name": "Analyst",
            "initial_assignee_id": null,
            "initial_description": null,
            "initial_assignee_name": null
         },
         "causing_user_name": null,
         "causing_workflow_name": null
      },
      {
         "id": "6a23d87f-14ec-4a3f-9906-519259f870e1",
         "content": null,
         "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
         "cause_type": "history",
         "comment_id": null,
         "created_at": "2024-10-22T23:26:18.632",
         "updated_at": "2024-10-22T23:26:21.789",
         "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
         "occurred_at": "2024-10-22T23:26:18.632",
         "activity_type": "quarantine",
         "causing_api_key": null,
         "activity_details": {
            "quarantine_attempts": [
               {
                  "id": "8b96132a-751f-4131-abd4-2d5b74118988",
                  "state": "complete",
                  "disposition": "message_moved"
               }
            ]
         },
         "causing_user_name": null,
         "causing_workflow_name": null
      },
      {
         "id": "6d66c443-caa4-42e1-9091-e3a72ba157f2",
         "content": null,
         "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
         "cause_type": "history",
         "comment_id": null,
         "created_at": "2024-10-22T23:28:19.819",
         "updated_at": "2024-10-22T23:28:27.621",
         "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
         "occurred_at": "2024-10-22T23:28:19.819",
         "activity_type": "quarantine",
         "causing_api_key": null,
         "activity_details": {
            "quarantine_attempts": [
               {
                  "id": "f8295f5f-301a-43ce-af2c-11812cdb6f6d",
                  "state": "complete",
```

```
                "disposition": "mailbox_not_found"
            }
        ]
    },
    "causing_user_name": null,
    "causing_workflow_name": "Quarantine TAP Threats"
},
{
    "id": "7c412cd2-1d7d-42e1-a502-a79c56cbeac6",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-10-22T23:28:19.94",
    "updated_at": "2024-10-22T23:28:20.117",
    "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
    "occurred_at": "2024-10-22T23:28:19.94",
    "activity_type": "quarantine",
    "causing_api_key": null,
    "activity_details": {
        "quarantine_attempts": [
            {
                "id": "ba4e2739-4195-4e3e-a82b-46148c542ee6",
                "state": "complete",
                "disposition": "skipped"
            }
        ]
    },
    "causing_user_name": null,
    "causing_workflow_name": "Quarantine TAP Threats"
},
{
    "id": "dd361702-4f2a-44cc-b19a-2778e9e2129f",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-10-22T23:26:18.637",
    "updated_at": "2024-10-22T23:26:18.789",
    "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
    "occurred_at": "2024-10-22T23:26:18.637",
    "activity_type": "quarantine",
    "causing_api_key": null,
    "activity_details": {
        "quarantine_attempts": [
            {
                "id": "c8bf366d-3647-41b7-a044-a72c6cfc4ddf",
                "state": "complete",
                "disposition": "skipped"
            }
        ]
    },
    "causing_user_name": null,
    "causing_workflow_name": "Quarantine TAP Threats"
```

```
        },
        {
            "id": "dec9d17a-80a3-42fe-96bd-a8d4203ccb0c",
            "content": null,
            "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "cause_type": "history",
            "comment_id": null,
            "created_at": "2024-10-22T23:26:18.616",
            "updated_at": "2024-10-22T23:26:39.061",
            "incident_id": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
            "occurred_at": "2024-10-22T23:26:18.616",
            "activity_type": "quarantine",
            "causing_api_key": null,
            "activity_details": {
                "quarantine_attempts": [
                    {
                        "id": "f8fe78da-4e5b-4e23-8825-7e10462a7569",
                        "state": "complete",
                        "disposition": "message_moved"
                    }
                ]
            },
            "causing_user_name": null,
            "causing_workflow_name": "Quarantine TAP Threats"
        }
    ],
    "total": 2,
    "startRow": 0,
    "endRow": 200,
    "messages": [
        {
            "id": "768c0276-01eb-4e35-b0c3-f97fa9af6b95",
            "sid": 122547986,
            "createdAt": "2024-10-22T23:26:15.976+00:00",
            "updatedAt": "2024-11-26T15:43:28.015+00:00",
            "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "emailId": "9129c5fd-ca52-47a1-b5c3-049ca7d31e4c",
            "messageId": "<DS7PR12MB62861B30D1A2B5714E5473F3AC4C2@DS7PR12MB6286.namprd12.
prod.outlook.com>",
            "ppsGuid": "vMojOP7kQU8PdYJlBip0xGnkbo4Krl_j",
            "disposition": "malware",
            "emailSubject": "TDS test mail-3 - PL",
            "emailRecipientId": "768c0276-01eb-4e35-b0c3-f97fa9af6b95",
            "trapReceivedTime": "2024-10-22T23:26:15.976+00:00",
            "receivedAt": "2024-10-22T23:22:27.760+00:00",
            "remediationStatus": "mailbox_not_found",
            "quarantineStrategy": "forward_and_delete",
            "emailRecipientType": "to",
            "incidentId": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
            "association": "sender_and_subject",
            "mimeContentPresent": false,
            "bodyPresent": false,
            "senderId": "6ba5a494-bedb-4aad-a2f3-a20b8e3887c0",
            "senderAddress": "bad_guy@nefariousdomain.com",
```

```
            "senderIp": "148.163.159.21",
            "recipientAddress": "bob@tricorion.tk",
            "lastKnownType": "unknown",
            "tapCleared": false,
            "vip": false,
            "vap": true,
            "reports": 0,
            "messageStatus": {
               "permitted_clicks": 0,
               "message_delivered": true
            },
            "sources": [
               {
                  "type": "TapAlert"
               }
            ],
            "abuseReporterRank": "not_a_reporter",
            "tapThreatTypes": [
               "delivered_url_threat"
            ]
         },
         {
            "id": "5ef516f0-6c8a-466f-aecc-35411f4223e8",
            "sid": 122547990,
            "createdAt": "2024-10-22T23:26:15.976+00:00",
            "updatedAt": "2024-11-26T15:43:28.015+00:00",
            "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "emailId": "a3f90283-5965-45b3-a0a2-2e4e5acbe1c7",
            "messageId": "<DS7PR12MB6286CF00FF02FE3CF29635B0AC4C2@DS7PR12MB6286.namprd12.
prod.outlook.com>",
            "ppsGuid": "H71Xlu0wtulRm5oH0ERjJvEeWke_fHl0",
            "disposition": "malware",
            "emailSubject": "TDS test mail-3 - PL",
            "emailRecipientId": "5ef516f0-6c8a-466f-aecc-35411f4223e8",
            "trapReceivedTime": "2024-10-22T23:26:15.976+00:00",
            "receivedAt": "2024-10-22T23:22:10.246+00:00",
            "remediationStatus": "quarantined",
            "quarantineStrategy": "forward_and_delete",
            "emailRecipientType": "to",
            "incidentId": "63b97d57-0af4-4835-8a3e-8d9fe3949786",
            "mimeContentPresent": false,
            "bodyPresent": false,
            "senderId": "6ba5a494-bedb-4aad-a2f3-a20b8e3887c0",
            "senderAddress": "bad_guy@nefariousdomain.com",
            "senderIp": "148.163.159.21",
            "recipientAddress": "bob@tricorion.com",
            "lastKnownType": "unknown",
            "tapCleared": false,
            "vip": false,
            "vap": true,
            "reports": 0,
            "messageStatus": {
               "permitted_clicks": 0,
               "message_delivered": true,
```

```
            "is_read": false
         },
         "sources": [
            {
               "type": "TapAlert"
            }
         ],
         "abuseReporterRank": "not_a_reporter",
         "tapThreatTypes": [
            "delivered_url_threat"
         ]
      }
   ]
}
```

Get Summary for Manual Review Incidents (Abuse Mailbox)

Path	/api/v1/tric/incidents/
HTTP Method	POST
Description	Get incident summary for abuse mailbox incidents with a CLEAR Verdict of Manual Review, over the last 24 hours
Request	**Headers** **Header Name**: Authorization **Header Value**: Bearer <AUTH TOKEN> **Notes**: See the API Authentication section on Threat Protection APIs for details on how to generate an auth token **Request Body Example** `{ "filters": { "time_range_filter": {"start": "2024-11-26`

```
16:18:07", "end": "2024-11-27 16:18:07"},
      "source_filters": ["abuse_mailbox"],
      "verdict_filters": ["verdict_manual_review"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
}
```

Response	**Response Code** 200
Error Response	Refer to Error Responses section

Example request with curl

```
#!/bin/bash
CONTENT_TYPE='Content-Type: application/json'
URL='https://threatprotection-api.proofpoint.com/api/v1/tric/incidents'
AUTH_TOKEN='<GENERATED AUTH TOKEN>'
curl -X POST -H "$CONTENT_TYPE" -H "Authorization: Bearer $AUTH_TOKEN" "$URL" -d '{
  "filters": {
      "time_range_filter": {"start": "2024-11-26 16:18:07", "end": "2024-11-27 16:18:07"},
      "source_filters": ["abuse_mailbox"],
      "verdict_filters": ["verdict_manual_review"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
}'
```

Example Response

Standard HTTP response with status code 201

```
{
   "total": 1,
   "startRow": 0,
   "endRow": 1,
   "incidents": [
      {
         "id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
         "sid": 10659922,
```

```
            "createdAt": "2024-11-27T16:06:08.809+00:00",
            "updatedAt": "2024-11-27T16:06:17.880+00:00",
            "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "displayId": 855,
            "priority": "high",
            "title": "vindrayan[@]tricorion[.]tk reported a message \"Tomorrow's meeting\"",
            "state": "open",
            "assignedTeamName": "Analyst",
            "assignedTeamId": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
            "messageCount": 1,
            "vap": false,
            "vip": false,
            "abuseSourceIds": [
               "7db836de-f748-44ba-8f3d-b7103b3555b8"
            ],
            "sourceTypes": [
               "abuse_mailbox"
            ],
            "sourcesData": [
               {
                  "name": "Abuse Mailbox for TRICORION.TK",
                  "type": "AbuseMailbox"
               }
            ],
            "commentCount": 0,
            "dispositions": [
               "manual_review"
            ],
            "clearVerdicts": [
               "manual_review"
            ],
            "clearConfidences": [
               "low"
            ]
         }
      ]
   }
```


Get All Details for Manual Review Incidents (Abuse Mailbox)

Path	/api/v1/tric/incidents/<ID>/messages Note: The **ID** is obtained from the "id" field in the Incident Summary API request.
HTTP Method	POST

Description

Get incident and messages details for abuse mailbox incidents with a CLEAR Verdict of Manual Review, over the last 24 hours

Request

Headers

Header Name	Header Value	Notes
Authorization	Bearer <AUTH TOKEN>	See the API Authentication section on Threat Protection APIs for details on how to generate an auth token

Request Body Example

```
"filters": {
      "time_range_filter": {"start": "2024-11-26
16:18:07", "end": "2024-11-27 16:18:07"},
      "source_filters": ["abuse_mailbox"],
      "verdict_filters": ["verdict_manual_review"]
   },
   "endRow": 200,
   "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
   }],
   "startRow": 0
```

Response

Response Code 201

Error Response

Refer to Error Responses section

Example request with curl

```
#!/bin/bash
CONTENT_TYPE='Content-Type: application/json'
URL='https://threatprotection-api.proofpoint.com/api/v1/tric/incidents/63b97d57-0af4-4835-8a3e-8d9fe3949786/
messages'
AUTH_TOKEN='<GENERATED AUTH TOKEN>'
curl -X POST -H "$CONTENT_TYPE" -H "Authorization: Bearer $AUTH_TOKEN" "$URL" -d '{
```

```
  "filters": {
      "time_range_filter": {"start": "2024-11-26 16:18:07", "end": "2024-11-27 16:18:07"},
      "source_filters": ["abuse_mailbox"],
      "verdict_filters": ["verdict_manual_review"]
    },
    "endRow": 200,
    "sortParams": [{
      "sort": "desc",
      "colId": "createdAt"
    }],
    "startRow": 0
}'
```

Example Response

Standard HTTP response with status code 201


```
{
    "summary": {
        "id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
        "sid": 10659922,
        "createdAt": "2024-11-27T16:06:08.809+00:00",
        "updatedAt": "2024-11-27T16:06:17.880+00:00",
        "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
        "displayId": 855,
        "priority": "high",
        "state": "open",
        "title": "vindrayan[@]tricorion[.]tk reported a message \"Tomorrow's meeting\"",
        "openedAt": "2024-11-27T16:06:08.809+00:00",
        "assignedTeamId": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
        "assignedTeamName": "Analyst",
        "falsePositiveCount": 0,
        "messageCount": 1,
        "messageSourceData": {
            "hasTapAlert": false,
            "hasAbuseAlert": true,
            "hasSmartSearchImport": false,
            "hasMessageCsvUpload": false
        }
    },
    "comments": [],
    "activities": [
        {
            "id": "5a454074-8ef3-45d8-aeeb-65bb128180d9",
            "content": null,
            "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "cause_type": "history",
            "comment_id": null,
            "created_at": "2024-11-27T16:06:09.586",
            "updated_at": "2024-11-27T16:06:09.586",
            "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
            "occurred_at": "2024-11-27T16:06:09.584944",
            "activity_type": "assignment_change",
```

```
    "causing_api_key": null,
    "activity_details": {
      "new_team_id": "c6284d46-199e-483e-9869-1da1eeceb7ff",
      "new_user_id": "c43758e8-0be9-4205-90e9-fd2fcb865933",
      "old_team_id": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
      "old_user_id": null,
      "new_team_name": "Admin",
      "new_user_name": "Jeff Burstein",
      "old_team_name": "Analyst",
      "old_user_name": null,
      "new_user_email_address": "jburstein@tricorion.tk",
      "old_user_email_address": null
    },
    "causing_user_name": null,
    "causing_workflow_name": "Assign Incident - Protect Demo"
  },
  {
    "id": "1f7c1e46-5f8b-4305-857a-2538b2600c74",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-11-27T16:06:17.859",
    "updated_at": "2024-11-27T16:06:17.859",
    "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
    "occurred_at": "2024-11-27T16:06:17.857083",
    "activity_type": "assignment_change",
    "causing_api_key": null,
    "activity_details": {
      "new_team_id": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
      "new_user_id": null,
      "old_team_id": "c6284d46-199e-483e-9869-1da1eeceb7ff",
      "old_user_id": "c43758e8-0be9-4205-90e9-fd2fcb865933",
      "new_team_name": "Analyst",
      "new_user_name": null,
      "old_team_name": "Admin",
      "old_user_name": "Jeff Burstein",
      "new_user_email_address": null,
      "old_user_email_address": "jburstein@tricorion.tk"
    },
    "causing_user_name": null,
    "causing_workflow_name": "Review Unclassified Messages"
  },
  {
    "id": "3fce6528-f719-4468-81e6-5c0a2bed95e4",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-11-27T16:06:18.814",
    "updated_at": "2024-11-27T16:06:18.814",
    "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
    "occurred_at": "2024-11-27T16:06:18.814622",
    "activity_type": null,
```

```
    "causing_api_key": null,
    "activity_details": {},
    "causing_user_name": null,
    "causing_workflow_name": "Notify on Incident Assignment"
},
{
    "id": "eae5bd6e-ff0e-492c-9793-604fed8db394",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-11-27T16:06:10.826",
    "updated_at": "2024-11-27T16:06:10.826",
    "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
    "occurred_at": "2024-11-27T16:06:10.826318",
    "activity_type": null,
    "causing_api_key": null,
    "activity_details": {},
    "causing_user_name": null,
    "causing_workflow_name": "Notify on Incident Assignment"
},
{
    "id": "e8adfed4-e80f-4dc1-a73b-7353aef2d98b",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "system",
    "comment_id": null,
    "created_at": "2024-11-27T16:06:08.998",
    "updated_at": "2024-11-27T16:06:09.033",
    "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
    "occurred_at": "2024-11-27T16:06:08.998959",
    "activity_type": "incident_creation",
    "causing_api_key": null,
    "activity_details": {
        "source_name": "Abuse Mailbox for TRICORION.TK",
        "initial_title": "vindrayan[@]tricorion[.]tk reported a message \"Tomorrow's meeting\"",
        "message_count": 1,
        "initial_team_id": "a3672f71-fad5-46e1-a7d5-4d6c2a2b4521",
        "initial_priority": null,
        "initial_team_name": "Analyst",
        "initial_assignee_id": null,
        "initial_description": null,
        "initial_assignee_name": null
    },
    "causing_user_name": null,
    "causing_workflow_name": null
},
{
    "id": "ccec3ac5-a508-456a-b634-976dac4ca0b6",
    "content": null,
    "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
    "cause_type": "history",
    "comment_id": null,
    "created_at": "2024-11-27T16:06:17.882",
```

```
            "updated_at": "2024-11-27T16:06:17.882",
            "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
            "occurred_at": "2024-11-27T16:06:17.881123",
            "activity_type": "priority_change",
            "causing_api_key": null,
            "activity_details": {
               "new_priority": "high",
               "old_priority": null
            },
            "causing_user_name": null,
            "causing_workflow_name": "Review Unclassified Messages"
         },
         {
            "id": "107d72a5-e0d3-4b4f-9265-10816b323563",
            "content": null,
            "tenant_id": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "cause_type": "history",
            "comment_id": null,
            "created_at": "2024-11-27T16:06:18.839",
            "updated_at": "2024-11-27T16:06:18.839",
            "incident_id": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
            "occurred_at": "2024-11-27T16:06:18.839872",
            "activity_type": null,
            "causing_api_key": null,
            "activity_details": {},
            "causing_user_name": null,
            "causing_workflow_name": "Notify on Incident Assignment for CLEAR Manual Reviews and Suspicious"
         }
      ],
      "total": 1,
      "startRow": 0,
      "endRow": 100,
      "messages": [
         {
            "id": "598ba766-5c38-4ca6-be25-565faae3a3b8",
            "sid": 133761090,
            "createdAt": "2024-11-27T16:06:06.966+00:00",
            "updatedAt": "2024-11-27T16:06:07.182+00:00",
            "tenantId": "35873022-0c7d-4118-bca8-ad1eebc682cb",
            "emailId": "5fce3056-abff-4da2-8694-a7793d665188",
            "messageId": "<SA1PR13MB60556A43EBD392CA7B453D7FAE282@SA1PR13MB6055.namprd13.
prod.outlook.com>",
            "ppsGuid": "BEbfSUJZGjBjaFWNuOKQJ_9eNciWLlOH",
            "disposition": "manual_review",
            "clearVerdict": "manual_review",
            "clearConfidence": "low",
            "emailSubject": "Tomorrow's meeting",
            "emailRecipientId": "598ba766-5c38-4ca6-be25-565faae3a3b8",
            "trapReceivedTime": "2024-11-27T16:06:06.966+00:00",
            "receivedAt": "2024-11-27T16:04:40.000+00:00",
            "remediationStatus": "not_attempted",
            "quarantineStrategy": "forward_and_delete",
            "emailRecipientType": "to",
            "incidentId": "7f118f6f-3cd5-4191-97a7-a361e370ca84",
```

```
            "emailMessageSize": 75300,
            "mimeContentPresent": true,
            "bodyPresent": true,
            "senderId": "94491fd7-e1bd-4c94-9396-3a9227a7938b",
            "senderAddress": "black_widow@pfptproofpoint.onmicrosoft.com",
            "recipientAddress": "vindrayan@tricorion.tk",
            "lastKnownType": "mailbox",
            "tapCleared": false,
            "vip": false,
            "vap": false,
            "reports": 1,
            "messageStatus": {
               "permitted_clicks": 0,
               "message_delivered": false,
               "is_read": true
            },
            "sources": [
               {
                  "name": "Abuse Mailbox for TRICORION.TK",
                  "type": "AbuseMailbox",
                  "id": "7db836de-f748-44ba-8f3d-b7103b3555b8"
               }
            ],
            "abuseReporterRank": "first_reporter",
            "tapThreatTypes": []
         }
      ]
}
```