DYNAMICSUMMARY

DYNAMICSUMMARY RESOURCE TYPE

API version: 2023-03-01-preview

SUMMARY MODEL

Field	Type	Description	Required?	Editable?
SummaryName	String	Name of the summary. Must be unique across a Sentinel workspace.	True	True
SourceInfo	Dictionary<string,string>	Source information including runtime attributes, query, and lookback, etc. Eaxmple: {"source": "Notebooks", "name": "Scheduled Credential Scan on Log Analytics", "version": "1.0"}		True
SearchKey	String	Name of a column in your summary that you expect to use as a join with other data or as a frequent object of searches. For example, ObservableType.		
Tactics	Enum: Reconnaissance, ResourceDevelopment, InitialAccess, Execution, Persistence, PrivilegeEscalation, DefenseEvasion, CredentialAccess, Discovery, LateralMovement, Collection, Exfiltration,	MITRE ATT&CK tactics.		True

	CommandAndControl, Impact			
Techniques	List<string>	MITRE ATT&CK techniques		True
RelationName	String	Name of the source that generates the summary or is linked to the summary. For example, Hunts, Notebooks, Playbooks, etc.		
SummaryDescription	String	Description of the summary		True
RelationId	String	Identifier of RelationName if RelationName is used. For example, a Hunting session ID.		
RawContent	String	Array of Summary Item Models in JSON. Example: "[{ \"EventTimeUtc\": \"2022-04-16T14:22:08Z\", \"ObservableType\": \"IP\", \"ObservableValue\": \"192.168.0.250\", \"RelationId\" : \"Hunting session 123\", \"SearchKey\" : \"ObservableaType\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]"		
Query	String	KQL query that is used to summarize data. Example: “SigninLogs | where ResultType == "50057" | extend Reason = case(ResultType == '50057', 'SigninLogs(Result Code- 50057) - User account is disabled. The account has been disabled by an administrator.', 'Unknown'), Account = UserPrincipalName | project Computer, Account, Reason, TimeGenerated”		
QueryStartDate	DateTime	Start date of the query		

QueryEndDate	DateTime	End date of the query		

SUMMARY ITEM MODEL

Field	Type	Description	Required	Editable
EventTimeUTC	DateTime	Datetime of the event when it occurred		
ObservableType	String	Type of the observable. For example, it can be an entity like IP **Address**, **Host**, **User account**, or non-entity observable such as a **Hunting query**.		
ObservableValue	String	Value of the observable.		
SearchKey	String	Real value from a column for quick search. For example, "123.25.25.23" as IP address.		
Tactics	Enum: Reconnaissance, ResourceDevelopment, InitialAccess, Execution, Persistence, PrivilegeEscalation, DefenseEvasion, CredentialAccess, Discovery, LateralMovement, Collection, Exfiltration, CommandAndControl, Impact,	MITRE ATT&CK		

	PreAttack, ImpairProcessControl, InhibitResponseFunction			
Techniques	List<string>	MITRE ATT&CK		
RelationName	String	Name of the source that generates the summary or is linked to the summary. For example, Hunts, Notebooks, Playbooks, etc.		
RelationId	String	Identifier of RelationName if RelationName is used. For example, a Hunting session ID.		
PackedContent	dynamic	For storing extra columns data by using KQL function pack_all()		

AUTHENTICATION AND AUTHORIZATION

AZURE_AUTH

Azure Active Directory OAuth2 Flow

Type: oauth2
Flow: implicit
Authorization URL: https://login.microsoftonline.com/common/oauth2/authorize

SCOPES

Name	Description
user_impersonation	impersonate your user account

The API supports the following operations.

- Create/Update a summary
- Get a summary

- List summaries
- Delete a summary

CREATE OR UPDATE

Create or update a Summary.

HTTP

PUT
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

URI PARAMETERS

Name	In	Required	Type	Description
resourceGroupName	Path	True	String	The name of the resource group. The name is not case sensitive.
subscriptionId	Path	True	String	The ID of the target subscription.
summaryId	Path	True	String	The ID of the summary
workspaceName	Path	True	String	The name of the workspace.
api-version	query	true	string	The API version to use for this operation.

REQUEST BODY

Field	Type	Description	Required

properties.summaryName	String	The Summary name	true
properties.sourceInfo	Dictionary<string,string>	Source information including runtime attributes, query, and lookback	
properties.searchKey	String	Name of a column in your summary that you expect to use as a join with other data or as a frequent object of searches. For example, ObservableType.	
properties.tactics	Enum: Reconnaissance, ResourceDevelopment, InitialAccess, Execution, Persistence, PrivilegeEscalation, DefenseEvasion, CredentialAccess, Discovery, LateralMovement, Collection, Exfiltration, CommandAndControl, Impact, PreAttack, ImpairProcessControl, InhibitResponseFunction	MITRE ATT&CK tactics	
properties.techniques	List<string>	MITRE ATT&CK techniques	
properties.relationName	String	Name of the source that generates the summary or is linked to the summary	
properties.summaryDescription	String	Description of summary	
properties.relationId	String	Identifier of RelationName if RelationName is used. For example, a Hunting session ID.	
properties.rawContent	String	Array of Summary Item Models in JSON. Example:	

		"[{ \"EventTimeUtc\": \"2022-04-16T14:22:08Z\", \"ObservableType\": \"IP\", \"ObservableValue\": \"SomeIp\", \"RelationId\" : \"Some Relation\", \"SearchKey\" : \"Some sear\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]"	
Query	String	KQL query for summary	
properties.queryStartDate	DateTime	Start date of the query	
properties.queryEndDate	DateTime	End date of the query	

RESPONSES

Status Code	Type	Description
200 OK	Summary	OK
201 Created	Summary	Created
Other status codes	CloudError	Error response describing why the operation failed.

EXAMPLE

Create or update a Summary and bulk creates summary items.

HTTP: PUT

https://management.azure.com/subscriptions/bd794837-4d29-4647-9105-6339bfdb4e6a/resourceGroups/mamahaj-rg/providers/Microsoft.OperationalInsights/workspaces/mm-watchlistestws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

```
{
    "etag": "\"d5038ac1-0000-0d00-0000-6387ea6d0000\"",
    "properties": {
      "summaryName":"My summary",
      "summaryDescription":"my new summary description",
      "SearchKey":"someKey",
      "Tactics":[],
      "Techniques":[],
      "RelationId":"relId",
      "RelationName":"relName",
      "rawContent":"[{ \"EventTimeUtc\": \"2022-04-16T14:22:08Z\", \"ObservableType\": \"IP\", \"ObservableValue\": \"SomeIp\", \"RelationId\" : \"Some Relation\", \"SearchKey\" : \"Some search\", \"PackedContent\" : {\"SomeKey\" : \"SomeValue\"} }]"
    }
}
```


RESPONSE


```
{
  "id": "/subscriptions/f117ae3d-d6b2-4031-8d76-e0ca15e838ab/resourceGroups/dynamicsummaries-prod-rg/providers/Microsoft.OperationalInsights/workspaces/dynamicsummaries-prod-weu/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-0097-0001-8178-a99aec5df9df",
  "name": "78f81fdc-0097-0001-8178-a99aec5df9df",
  "etag": "\"d5038ac1-0000-0d00-0000-6387ea6d0000\"",
  "type": "Microsoft.SecurityInsights/dynamicsummaries",
  "systemData": {
    "createdAt": "2022-11-16T23:31:59.3655436Z",
    "createdBy": "john@contoso.com",
    "createdByType": "User",
    "lastModifiedAt": "2022-11-30T23:42:35.5743509Z",
    "lastModifiedBy": "john@contoso.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "summaryId": "78f81fdc-0097-0001-8178-a99aec5df9df",
    "summaryName": "My summary",
    "searchKey": "someKey",
    "tactics": [],
    "techniques": [],
    "relationName": "relName",
    "summaryDescription": "my new summary description",
    "relationId": "relId",
    "tenantId": "f686d426-8d16-42db-81b7-ab578e110ccd",
    "summaryStatus": "Active",
    "provisioningState": "InProgress",
    "type": "dynamic-summary"
  }
}
```


DELETE

Delete a summary.

HTTP

DELETE

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

URI PARAMETERS

Name	In	Required	Type	Description
resourceGroupName	Path	True	String	The name of the resource group. The name is not case sensitive.
subscriptionId	Path	True	String	The ID of the target subscription.
summaryId	Path	True	String	The ID of the summary
workspaceName	Path	True	String	The name of the workspace.
api-version	query	true	string	The API version to use for this operation.

RESPONSES

Status Code	Type	Description
200 OK	Summary	OK
204 No Content	Summary	No Content

Other status codes	CloudError	Error response describing why the operation failed.

EXAMPLE

Delete a summary.

HTTP: DELETE

https://management.azure.com/subscriptions/bd794837-4d29-4647-9105-6339bfdb4e6a/resourceGroups/mamahaj-rg/providers/Microsoft.OperationalInsights/workspaces/mm-watchlistestws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

RESPONSE

Status code 200 or status code 204

GET

Get a summary by the summary ID.

HTTP

GET

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dynamicSummaries/**{summaryId}**?api-version=2023-03-01-preview

URI PARAMETERS

Name	In	Required	Type	Description
resourceGroupName	Path	True	String	The name of the resource group. The name is not case sensitive.

subscriptionId	Path	True	String	The ID of the target subscription.
summaryId	Path	True	String	The ID of the summary
workspaceName	Path	True	String	The name of the workspace.
api-version	query	true	string	The API version to use for this operation.

RESPONSES

Status Code	Type	Description
200 OK	Summary	OK
Other status codes	CloudError	Error response describing why the operation failed.

EXAMPLE

HTTP: GET

https://management.azure.com/subscriptions/bd794837-4d29-4647-9105-6339bfdb4e6a/resourceGroups/mamahaj-rg/providers/Microsoft.OperationalInsights/workspaces/mm-watchlistestws/providers/Microsoft.SecurityInsights/dynamicSummaries/78f81fdc-0097-0001-8178-a99aec5df9df?api-version=2023-03-01-preview

RESPONSE

```
{
  "id": "/subscriptions/f117ae3d-d6b2-4031-8d76-e0ca15e838ab/resourceGroups/dynamicsummaries-prod-
rg/providers/Microsoft.OperationalInsights/workspaces/dynamicsummaries-prod-
weu/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-0097-0001-8178-a99aec5df9df",
  "name": "78f81fdc-0097-0001-8178-a99aec5df9df",
  "etag": "\"d5038ac1-0000-0d00-0000-6387ea6d0000\"",
  "type": "Microsoft.SecurityInsights/dynamicsummaries",
  "systemData": {
    "createdAt": "2022-11-16T23:31:59.3655436Z",
    "createdBy": "john@contoso.com",
    "createdByType": "User",
    "lastModifiedAt": "2022-11-30T23:42:35.5743509Z",
    "lastModifiedBy": "john@contoso.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "summaryId": "78f81fdc-0097-0001-8178-a99aec5df9df",
    "summaryName": "My summary",
    "searchKey": "someKey",
    "tactics": [],
    "techniques": [],
    "relationName": "relName",
    "summaryDescription": "my new summary description",
    "relationId": "relId",
    "tenantId": "f686d426-8d16-42db-81b7-ab578e110ccd",
    "summaryStatus": "Active",
    "provisioningState": "InProgress",
    "type": "dynamic-summary"
  }
}
```


LIST

Get all summaries in workspace.

HTTP

GET

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dynamicSummaries?api-version=2023-03-01-preview

URI PARAMETERS

Name	In	Required	Type	Description
resourceGroupName	Path	True	String	The name of the resource group. The name is not case sensitive.
subscriptionId	Path	True	String	The ID of the target subscription.
workspaceName	Path	True	String	The name of the Sentinel workspace.
api-version	query	true	string	The API version to use for this operation.

RESPONSES

Status Code	Type	Description
200 OK	Summary	OK
Other status codes	CloudError	Error response describing why the operation failed.

EXAMPLE

HTTP: GET

https://management.azure.com/subscriptions/bd794837-4d29-4647-9105-6339bfdb4e6a/resourceGroups/mamahaj-rg/providers/Microsoft.OperationalInsights/workspaces/mm-watchlistestws/providers/Microsoft.SecurityInsights/dynamicSummaries?api-version=2023-03-01-preview

RESPONSE

```
{
  "value": [
    {
      "id": "/subscriptions/f117ae3d-d6b2-4031-8d76-e0ca15e838ab/resourceGroups/dynamicsummaries-prod-rg/providers/Microsoft.OperationalInsights/workspaces/dynamicsummaries-prod/providers/Microsoft.SecurityInsights/dynamicsummaries/78f81fdc-0097-0001-8178-a99aec5df9df",
      "name": "78f81fdc-0097-0001-8178-a99aec5df9df",
      "etag": "\"23013599-0000-0100-0000-638f683b0000\"",
      "type": "Microsoft.SecurityInsights/dynamicsummaries",
      "systemData": {
        "createdAt": "2022-12-06T16:05:15.0353841Z",
        "createdBy": "john@contoso.com",
        "createdByType": "User",
        "lastModifiedAt": "2022-12-06T16:05:15.0353841Z",
        "lastModifiedBy": "john@contoso.com",
        "lastModifiedByType": "User"
      },
      "properties": {
        "summaryId": "78f81fdc-0097-0001-8178-a99aec5df9df",
        "summaryName": "My summary",
        "searchKey": "someKey",
        "tactics": [],
        "techniques": [],
        "relationName": "relName",
        "summaryDescription": "my new summary description",
        "relationId": "relId",
        "tenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47",
        "summaryStatus": "Active",
        "provisioningState": "InProgress",
        "type": "dynamic-summary"
      }
    }
  ]
}
```