swagger

Nucleus API 1.0.0

[Base URL: /nucleus/api]

Nucleus API Specification.
Please contact support to request any additional functionality.

Contact the developer

Find out more about Nucleus

Schemes
HTTPS

Authorize

projects Everything about your Projects

GET /projects Gets list of all projects

Returns a list of all projects with the current status

Parameters Try it out

No parameters

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "tracking_method": "string", "project_name": "string", "project_description": "string", "project_id": 0, "project_groups": [ "string" ], "project_org": "string" } ]`
401	*API Key was not valid*
422	*Invalid value*

GET `/projects/{project_id}` Gets information on a specific project

Returns details on a specific project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "tracking_method": "string", "project_name": "string", "project_description": "string", "project_id": 0, "project_groups": [ "string" ], "project_org": "string" }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project assessments Information about your assessments

GET `/projects/{project_id}/assessments` Gets list of assessments

Returns a list of all assessments for a project. For data inside of an assessment use the assessment's project_id for any other API calls

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "project_id": 0,
    "assessment_data": [
      {
        "assessment_contacts": [
          {
            "contact_email": "string",
            "contact_name": "string",
            "contact_role": "string",
            "contact_phone": "string",
            "contact_title": "string"
          }
        ],
        "assessment_end": "string",
        "assessment_report_limitations": "string",
        "assessment_report_overview": "string",
        "assessment_provider_name": "string",
        "vulns": [
          {
            "uM": 0,
            "uL": 0,
            "tL": 0,
            "tM": 0,
            "uI": 0,
            "uH": 0,
            "tH": 0,
            "tI": 0,
            "uE": 0,
            "tE": 0,
            "tC": 0,
            "uC": 0
          }
        ],
        "assessment_type": "string",
        "assessment_provider": "string",
        "assessment_activity": [
          {
            "action": "string",
            "date": "string",
            "user": "string"
          }
        ],
        "assessment_report_intro": "string",
        "assessment_environment": "string",
        "assessment_scope": "string",
        "assessment_status": "string",
        "assessment_start": "string"
      }
    ],
    "parent_project_id": 0,
    "assessment_name": "string"
  }
]
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*

Code	Description
422	*Invalid value*

project assets Information about your assets

PUT **/projects/{project_id}/assets/{asset_id}** Update assets values.

WARNING This may affect future scan imports correctly mapping to this asset.

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
asset_id * required **integer** ***(path)***	Asset Id
body * required ***(body)***	Updated asset object **Example Value** Model


```
{
  "asset_data_sensitivity_score": 2,
  "operating_system_name": "string",
  "image_manifest": "string",
  "active": true,
  "asset_location": "string",
  "support_team": "string",
  "asset_match_name": "string",
  "image_registry": "string",
  "image_platform_os_version": "string",
  "asset_notes": "string",
  "ip_address": "string",
  "domain_name": "string",
  "image_tags": [
    "string"
  ],
  "image_platform_arch_features": [
    "string"
  ],
  "asset_name_link": 0,
  "image_config_digest": "string",
  "branch": "string",
  "mac_address": "string",
  "operating_system_features": "string",
  "operating_system_version": "string",
  "image_platform_os_features": [
    "string"
  ],
  "asset_name": "string",
  "asset_users": [
    "string"
  ],
  "ip_address_secondary": [
    "string"
  ],
  "asset_criticality": "string",
  "repo_url": "string",
  "image_secondary_registries": [
    "string"
  ],
  "image_distro": "string",
  "image_config": "string",
  "asset_type": "Application",
  "owner_team": "string",
  "image_repo": "string",
  "asset_info": {
    "infoKey": "infoValue"
  },
```

Name	Description


```
  "image_platform_arch": "string",
  "decommed": false,
  "asset_complianced_score": 0,
  "image_platform_os": "string",
  "asset_public": true,
  "asset_name_secondary": [
    "string"
  ],
  "asset_groups": [
    "string"
  ],
  "image_manifest_digest": "string",
  "image_platform_arch_variant": "string"
}
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "asset_id": 0, "unknown_fields": [ "string" ], "success": true }`
400	*Invalid asset parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid asset parameters supplied*

GET /projects/{project_id}/assets/{asset_id} Gets information on a specific asset

Returns a list of all assets in a project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
asset_id * required `integer` *(path)*	Asset Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model


```
{
  "asset_data_sensitivity_score": 0,
  "operating_system_name": "string",
  "asset_inactive_date": "string",
  "image_manifest": "string",
  "active": true,
  "asset_location": "string",
  "support_team": {
    "team_id": 0,
    "team_name": "string"
  },
  "image_registry": "string",
  "image_platform_os_version": "string",
  "asset_notes": "string",
  "asset_id": 0,
  "ip_address": "string",
  "domain_name": "string",
  "asset_criticality": "string",
  "image_tags": [
    "string"
  ],
  "image_platform_arch_features": [
    "string"
  ],
  "image_config_digest": "string",
  "branch": "string",
  "mac_address": "string",
  "operating_system_version": "string",
  "image_platform_os_features": [
    "string"
  ],
  "asset_name": "string",
  "asset_users": [
    "string"
  ],
  "ip_address_secondary": [
    "string"
  ],
  "repo_url": "string",
  "parent_host_id": "string",
  "image_secondary_registries": [
    "string"
  ],
  "image_distro": "string",
  "image_config": "string",
  "asset_type": "string",
  "owner_team": {
    "team_id": 0,
    "team_name": "string"
  },
  "image_repo": "string",
  "asset_info": {
    "infoKey": "infoValue"
  },
  "image_platform_arch": "string",
  "url": "string",
  "decommed": true,
  "asset_complianced_score": 0,
  "image_platform_os": "string",
  "asset_name_secondary": [
```

Code	Description

	<pre>"string"
	],
	"asset_groups": [
	"string"
	],
	"image_manifest_digest": "string",
	"image_platform_arch_variant": "string"
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

POST `/projects/{project_id}/assets` Creates a new asset with supplied parameters

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

body * required
(body)
	Updated asset object
	Example Value Model
	<pre>{
	"asset_data_sensitivity_score": 2,
	"operating_system_name": "string",
	"image_manifest": "string",
	"active": true,
	"asset_location": "string",
	"support_team": "string",
	"asset_match_name": "string",
	"image_registry": "string",
	"image_platform_os_version": "string",
	"asset_notes": "string",
	"ip_address": "string",
	"domain_name": "string",
	"image_tags": [
	"string"
	],
	"image_platform_arch_features": [
	"string"
	],
	"asset_name_link": 0,
	"image_config_digest": "string",
	"branch": "string",
	"mac_address": "string",
	"operating_system_features": "string",
	"operating_system_version": "string",
	"image_platform_os_features": [
	"string"
	],
	"asset_name": "string",
	"asset_users": [
	"string"
	],
	"ip_address_secondary": [
	"string"
	],
	"asset_criticality": "string",
	"repo_url": "string",
	"image_secondary_registries": [
	"string"
	],
	"image_distro": "string",
	"image_config": "string",
	"asset_type": "Application",
	"owner_team": "string",</pre>

Name	Description


```
  "image_repo": "string",
  "asset_info": {
    "infoKey": "infoValue"
  },
  "image_platform_arch": "string",
  "decommed": false,
  "asset_complianced_score": 0,
  "image_platform_os": "string",
  "asset_public": true,
  "asset_name_secondary": [
    "string"
  ],
  "asset_groups": [
    "string"
  ],
  "image_manifest_digest": "string",
  "image_platform_arch_variant": "string"
}
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "asset_id": 0, "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
405	*Invalid input*

GET /projects/{project_id}/assets Gets information on assets

Returns a list of all assets in a project

Parameters

Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Name	Description
start **integer** ***(query)***	
limit **integer** ***(query)***	If not included 100 is used. Maximum is 5000
ip_address **string** ***(query)***	Specific IP Address
asset_name **string** ***(query)***	Specific Asset Name
asset_name_ip **string** ***(query)***	Asset or IP Search
asset_groups **string** ***(query)***	Asset Groups Search - Comma Separated
asset_type **string** ***(query)***	Filter by asset type
inactive_assets **boolean** ***(query)***	Set to 'true' to request inactive assets
unscanned_assets **boolean** ***(query)***	Set to 'true' to request only unscanned assets, 'false' to request only scanned assets
assets_with_findings **boolean** ***(query)***	Set to 'true' to request only assets with findings, 'false' to request only assets without findings

Responses **Response content type** application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	[
	{
	"finding_count_fail": 0,
	"operating_system_name": "string",
	"asset_inactive_date": "string",
	"image_manifest": [
	"string"
	],
	"finding_count_low": 0,
	"ip_address": "string",
	"image_platform_arch": "string",
	"finding_count_medium": 0,
	"support_team": {
	"team_id": 0,
	"team_name": "string"
	},
	"image_registry": "string",
	"asset_criticality_score": "string",

Code	Description


```
    "asset_id": 0,
    "scan_date_timestamp": 0,
    "image_platform_os_version": "string",
    "asset_name": "string",
    "asset_criticality": "string",
    "image_tags": [
      "string"
    ],
    "image_platform_arch_features": [
      "string"
    ],
    "image_config_digest": "string",
    "branch": "string",
    "mac_address": "string",
    "operating_system_features": [
      "string"
    ],
    "finding_count_critical": 0,
    "operating_system_version": "string",
    "scan_date": "string",
    "finding_count_informational": 0,
    "finding_count_high": 0,
    "image_platform_os_features": [
      "string"
    ],
    "asset_data_sensitivity_score": "string",
    "ip_address_secondary": [
      "string"
    ],
    "repo_url": "string",
    "active": true,
    "image_distro": "string",
    "image_config": "string",
    "asset_type": "string",
    "image_secondary_registries": [
      "string"
    ],
    "owner_team": {
      "team_id": 0,
      "team_name": "string"
    },
    "image_repo": "string",
    "asset_info": {
      "infoKey": "infoValue"
    },
    "finding_vulnerability_score": 0,
    "asset_base_risk_score": "string",
    "asset_complianced_score": "string",
    "image_platform_os": "string",
    "asset_public": "string",
    "business_owners": [
      "string"
    ],
    "finding_count_pass": 0,
    "asset_name_secondary": [
      "string"
    ],
    "asset_groups": [
      "string"
    ],
    "image_manifest_digest": "string",
    "image_platform_arch_variant": "string"
  }
]
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

POST `/projects/{project_id}/assets/groups` Creates a new asset group with supplied parameters

Adds a new asset group for the project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Add asset group **Example Value** Model `{ "asset_group": "string" }` **Parameter content type** application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to edit project assets*
405	*Invalid input*
422	*Invalid value or Duplicate tag*

GET /projects/{project_id}/assets/groups Gets defined asset_groups and tag_ids

Returns a list of the asset groups and tag ids currently created

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "tag_id": 0, "asset_group": "string" } ]`
401	*API Key was not valid*
403	*API Key does not have permissions to view project assets*
422	*Invalid value*

DELETE **/projects/{project_id}/assets/groups** Deletes a specific asset group

Deletes a specific asset group and any sub groups. WARNING: This is permanent change

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
asset_group * required `string` *(query)*	Asset Group Name

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "success": true`

Code	Description
	} *API Key was not valid*
401	
403	*API Key does not have permissions to edit project assets*
405	*Invalid input*
422	*Invalid group name*

GET **/projects/{project_id}/assets/{asset_id}/findings** Gets findings information on a specific asset

Returns a list of the current findings for the asset

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
asset_id * required **integer** ***(path)***	Asset Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model [{ "finding_discovered": "string", "finding_severity": "string", "finding_name": "string", "finding_status": "string", "finding_count": 0, "scan_date": "string", "finding_exploitable": 0, "finding_severities": ["Critical"], "scan_type": "string", "issue_open_count": 0, "issue_closed_count": 0, "finding_number": "string", "asset_count": 0, "asset_fixed_count": 0, "finding_iava": "string", "asset_mitigated_count": 0,

Code	Description


```
      "finding_cve": "string",
      "mandiant_zero_day": "string",
      "mandiant_attacking_ease": "string",
      "mandiant_threat_actors": [
        "string"
      ],
      "mandiant_exploited_by_malware": "string",
      "mandiant_mitigations": [
        "string"
      ],
      "mandiant_vulnerable_products": "string",
      "mandiant_analysis": "string",
      "mandiant_associated_malware": [
        "string"
      ],
      "mandiant_exploit_rating": "string",
      "mandiant_exploitation_consequence": "string",
      "cisa_vulnerability_name": "string",
      "mandiant_fix_urls": [
        "string"
      ],
      "mandiant_exploit_vectors": [
        "string"
      ],
      "epss_score": 0,
      "mandiant_exploit_in_the_wild": "string",
      "mandiant_risk_rating": "string",
      "due_date": "string"
    }
  ]
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET /projects/{project_id}/assets/groups/metrics Gets metrics for specified asset group(s)

Returns a collection of metrics for the specified asset group(s).

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
asset_groups * required `string` *(query)*	JSON array containing a list of asset groups to include. You can request up to a maximum of 50 asset groups in a single call.
metrics `string` *(query)*	JSON array containing a list of metrics to include. If not specified, a default set of metrics will be returned. For a complete list of supported metrics, see Metrics API Reference.

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>[
	  {
	  "resolved_past_sla_pct_7d": 0,
	  "mttr_critical_7d": 0,
	  "mttr_7d": 0,
	  "past_due_pct_high": 0,
	  "compliance_pass_count": 0,
	  "vuln_count": 0,
	  "mandiant_exploit_in_the_wild_count_critical": 0,
	  "mandiant_zero_day_count_critical": 0,
	  "mandiant_exploit_in_the_wild_count": 0,
	  "vuln_count_critical": 0,
	  "resolved_past_sla_pct_critical_7d": 0,
	  "churn_pct_high_7d": 0,
	  "churn_pct_critical_7d": 0,
	  "avg_age_high": 0,
	  "churn_pct_7d": 0,
	  "resolved_past_sla_pct_high_7d": 0,
	  "compliance_fail_pct": 0,
	  "avg_age_critical": 0,
	  "mandiant_zero_day_count_high": 0,
	  "vuln_count_high": 0,
	  "mandiant_zero_day_count": 0,
	  "risk_score": 0,
	  "mttr_high_7d": 0,
	  "mandiant_exploit_in_the_wild_count_high": 0,
	  "asset_external_pct": 0,
	  "past_due_pct_critical": 0,
	  "compliance_pass_pct": 0,
	  "asset_count": 0
	  }
	]</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to view project assets*
422	*Invalid value(s)*

project automation

Information about your automation rules

POST `/projects/{project_id}/automation/assetprocessing` Creates a new asset processing automation rule

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

body * required
(body)
	Rule Information
	
	Example Value Model
	<pre>{
	  "asset_compliance_scope_type": "specific",
	  "asset_attribute_rule_support_dynamic": "string",
	  "asset_attribute_rule_support_team": "string",</pre>

Name	Description


```
    "asset_data_sensitivity": "Critical",
    "asset_criticality_type": "specific",
    "asset_group_dynamic": "string",
    "asset_data_sensitivity_dynamic": "string",
    "rule_name": "string",
    "asset_attribute_owner_type": "specific",
    "asset_criticality": "Critical",
    "rule_disabled": 0,
    "asset_criticality_dynamic": "string",
    "asset_compliance_scope": "Yes",
    "asset_group_type": "specific",
    "asset_attribute_owner_dynamic": "string",
    "asset_group": "string",
    "asset_attribute_rule_owner_team_type": "specific",
    "asset_compliance_scope_dynamic": "string",
    "rule_match_type": "All",
    "asset_attribute_owner": "string",
    "asset_attribute_rule_owner_team": "string",
    "asset_attribute_rule_support_team_type": "specific",
    "asset_public": "Yes",
    "asset_data_sensitivity_type": "specific",
    "rule_id": 0,
    "rule_criteria": [
      {
        "rule_match_condition": "asset_name",
        "rule_match_value": "name",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "ip_address",
        "rule_match_value": "192.168.1.1",
        "rule_match_qualifier": "is not"
      },
      {
        "rule_match_condition": "operating_system_name",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "scan_type",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "connection_id",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      }
    ],
    "apply_rule": true
  }
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "rule_id": 0, "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*

Code	Description
422	*Invalid value*

GET **/projects/{project_id}/automation/assetprocessing** Gets defined asset processing automation rules

Returns a list of the asset processing rules currently created

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "asset_compliance_scope_type": "specific",
    "asset_attribute_rule_support_dynamic": "string",
    "asset_attribute_rule_support_team": "string",
    "asset_data_sensitivity": "Critical",
    "asset_criticality_type": "specific",
    "asset_group_dynamic": "string",
    "asset_data_sensitivity_dynamic": "string",
    "rule_name": "string",
    "asset_attribute_owner_type": "specific",
    "asset_criticality": "Critical",
    "rule_disabled": 0,
    "asset_criticality_dynamic": "string",
    "asset_compliance_scope": "Yes",
    "asset_group_type": "specific",
    "asset_attribute_owner_dynamic": "string",
    "asset_group": "string",
    "asset_attribute_rule_owner_team_type": "specific",
    "asset_compliance_scope_dynamic": "string",
    "rule_match_type": "All",
    "asset_attribute_owner": "string",
    "asset_attribute_rule_owner_team": "string",
    "asset_attribute_rule_support_team_type": "specific",
    "asset_public": "Yes",
    "asset_data_sensitivity_type": "specific",
    "rule_id": 0,
    "rule_criteria": [
      {
        "rule_match_condition": "asset_name",
        "rule_match_value": "name",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "ip_address",
        "rule_match_value": "192.168.1.1",
        "rule_match_qualifier": "is not"
      },
      {
        "rule_match_condition": "operating_system_name",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      },
      {
```

Code	Description


```
          "rule_match_condition": "scan_type",
          "rule_match_value": "string",
          "rule_match_qualifier": "is"
        },
        {
          "rule_match_condition": "connection_id",
          "rule_match_value": "string",
          "rule_match_qualifier": "is"
        }
      ]
    }
]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

PUT `/projects/{project_id}/automation/ticketing/{rule_id}` Updates an ticketing automation rule

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
rule_id * required `string` *(path)*	Rule Id
body * required *(body)*	Rule Information **Example Value** Model


```
{
  "asset_match_type": "All",
  "connector_project": "string",
  "asset_criteria": [
    {
      "rule_match_condition": "asset_name",
      "rule_match_value": "host",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "ip_address",
      "rule_match_value": "192.168.1.1",
      "rule_match_qualifier": "is not"
    },
    {
      "rule_match_condition": "asset_type",
      "rule_match_value": [
        "Application",
        "Container",
        "Container Image",
        "Host",
        "Database"
      ],
      "rule_match_qualifier": "is one of"
    },
    {
      "rule_match_condition": "asset_tags",
      "rule_match_value": [
        "Group1",
        "Group2"
      ],
      "rule_match_qualifier": "is in all of"
    }
  ],
```

Name	Description


```
  "vuln_criteria": [
    {
      "rule_match_condition": "finding_name",
      "rule_match_value": "CVE-0000-00000",
      "rule_match_qualifier": "contains"
    },
    {
      "rule_match_condition": "finding_exploitable",
      "rule_match_value": 1,
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "finding_severity",
      "rule_match_value": [
        "Critical",
        "High",
        "Medium",
        "Low",
        "Informatonal"
      ],
      "rule_match_qualifier": "is one of"
    }
  ],
  "connection_id": "string",
  "rule_name": "string",
  "connector_type": "string",
  "issue_priority": "string",
  "issue_type": "string",
  "rule_disabled": 0,
  "rule_id": "string"
}
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "rule_id": "string", "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET /projects/{project_id}/automation/ticketing/{rule_id} Gets defined ticketing automation rule

Returns an object of the ticketing rule currently created

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
rule_id * required `string` *(path)*	Rule Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model


```
{
  "asset_match_type": "All",
  "connector_project": "string",
  "asset_criteria": [
    {
      "rule_match_condition": "asset_name",
      "rule_match_value": "host",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "ip_address",
      "rule_match_value": "192.168.1.1",
      "rule_match_qualifier": "is not"
    },
    {
      "rule_match_condition": "asset_type",
      "rule_match_value": [
        "Application",
        "Container",
        "Container Image",
        "Host",
        "Database"
      ],
      "rule_match_qualifier": "is one of"
    },
    {
      "rule_match_condition": "asset_tags",
      "rule_match_value": [
        "Group1",
        "Group2"
      ],
      "rule_match_qualifier": "is in all of"
    }
  ],
  "vuln_criteria": [
    {
      "rule_match_condition": "finding_name",
      "rule_match_value": "CVE-0000-00000",
      "rule_match_qualifier": "contains"
    },
    {
      "rule_match_condition": "finding_exploitable",
      "rule_match_value": 1,
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "finding_severity",
      "rule_match_value": [
        "Critical",
        "High",
        "Medium",
        "Low",
        "Informatonal"
      ],
      "rule_match_qualifier": "is one of"
    }
  ],
  "connection_id": "string",
  "rule_name": "string",
  "connector_type": "string",
```

Code	Description

	<pre>"issue_priority": "string",
	"issue_type": "string",
	"rule_disabled": 0,
	"rule_id": "string"
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

POST `/projects/{project_id}/automation/findingprocessing/{rule_id}/runnow` Schedules a single finding processing automation rule to run immediately

Schedules a single finding processing automation rule to run immediately

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
rule_id * required `integer` *(path)*	Rule Id

Responses Response content type application/json

Code	Description
200	*successful operation, msg will tell you if already scheduled*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

POST `/projects/{project_id}/automation/ticketing` Creates a new ticketing automation rule

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Rule Information

Example Value Model


```
{
  "asset_match_type": "All",
  "connector_project": "string",
  "asset_criteria": [
    {
      "rule_match_condition": "asset_name",
      "rule_match_value": "host",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "ip_address",
      "rule_match_value": "192.168.1.1",
      "rule_match_qualifier": "is not"
    },
    {
      "rule_match_condition": "asset_type",
      "rule_match_value": [
        "Application",
        "Container",
        "Container Image",
        "Host",
        "Database"
      ],
      "rule_match_qualifier": "is one of"
    },
    {
      "rule_match_condition": "asset_tags",
      "rule_match_value": [
        "Group1",
        "Group2"
      ],
      "rule_match_qualifier": "is in all of"
    }
  ],
  "vuln_criteria": [
    {
      "rule_match_condition": "finding_name",
      "rule_match_value": "CVE-0000-00000",
      "rule_match_qualifier": "contains"
    },
    {
      "rule_match_condition": "finding_exploitable",
      "rule_match_value": 1,
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "finding_severity",
      "rule_match_value": [
        "Critical",
        "High",
        "Medium",
        "Low",
        "Informatonal"
      ],
      "rule_match_qualifier": "is one of"
    }
  ],
  "connection_id": "string",
  "rule_name": "string",
  "connector_type": "string",
  "issue_priority": "string",
  "issue_type": "string",
  "rule_disabled": 0,
  "rule_id": "string"
}
```


Parameter content type

application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "rule_id": "string", "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/automation/ticketing** Gets defined ticketing automation rules

Returns a list of the ticketing rules currently created

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
start `integer` *(query)*	Start of page
limit `integer` *(query)*	Number of items per page, 50 max

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "asset_match_type": "All", "connector_project": "string", "asset_criteria": [ {`

Code	Description


```
          "rule_match_condition": "asset_name",
          "rule_match_value": "host",
          "rule_match_qualifier": "is"
        },
        {
          "rule_match_condition": "ip_address",
          "rule_match_value": "192.168.1.1",
          "rule_match_qualifier": "is not"
        },
        {
          "rule_match_condition": "asset_type",
          "rule_match_value": [
            "Application",
            "Container",
            "Container Image",
            "Host",
            "Database"
          ],
          "rule_match_qualifier": "is one of"
        },
        {
          "rule_match_condition": "asset_tags",
          "rule_match_value": [
            "Group1",
            "Group2"
          ],
          "rule_match_qualifier": "is in all of"
        }
      ],
      "vuln_criteria": [
        {
          "rule_match_condition": "finding_name",
          "rule_match_value": "CVE-0000-00000",
          "rule_match_qualifier": "contains"
        },
        {
          "rule_match_condition": "finding_exploitable",
          "rule_match_value": 1,
          "rule_match_qualifier": "is"
        },
        {
          "rule_match_condition": "finding_severity",
          "rule_match_value": [
            "Critical",
            "High",
            "Medium",
            "Low",
            "Informatonal"
          ],
          "rule_match_qualifier": "is one of"
        }
      ],
      "connection_id": "string",
      "rule_name": "string",
      "connector_type": "string",
      "issue_priority": "string",
      "issue_type": "string",
      "rule_disabled": 0,
      "rule_id": "string"
    }
]
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

PUT /projects/{project_id}/automation/assetprocessing/{rule_id} Updates an asset processing automation rule

Parameters Try it out

Name	Description
project_id * required	Project Id

Name	Description
integer *(path)*	
rule_id * required integer *(path)*	Rule Id
body * required *(body)*	Rule Information **Example Value** Model


```
{
  "asset_compliance_scope_type": "specific",
  "asset_attribute_rule_support_dynamic": "string",
  "asset_attribute_rule_support_team": "string",
  "asset_data_sensitivity": "Critical",
  "asset_criticality_type": "specific",
  "asset_group_dynamic": "string",
  "asset_data_sensitivity_dynamic": "string",
  "rule_name": "string",
  "asset_attribute_owner_type": "specific",
  "asset_criticality": "Critical",
  "rule_disabled": 0,
  "asset_criticality_dynamic": "string",
  "asset_compliance_scope": "Yes",
  "asset_group_type": "specific",
  "asset_attribute_owner_dynamic": "string",
  "asset_group": "string",
  "asset_attribute_rule_owner_team_type": "specific",
  "asset_compliance_scope_dynamic": "string",
  "rule_match_type": "All",
  "asset_attribute_owner": "string",
  "asset_attribute_rule_owner_team": "string",
  "asset_attribute_rule_support_team_type": "specific",
  "asset_public": "Yes",
  "asset_data_sensitivity_type": "specific",
  "rule_id": 0,
  "rule_criteria": [
    {
      "rule_match_condition": "asset_name",
      "rule_match_value": "name",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "ip_address",
      "rule_match_value": "192.168.1.1",
      "rule_match_qualifier": "is not"
    },
    {
      "rule_match_condition": "operating_system_name",
      "rule_match_value": "string",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "scan_type",
      "rule_match_value": "string",
      "rule_match_qualifier": "is"
    },
    {
      "rule_match_condition": "connection_id",
      "rule_match_value": "string",
      "rule_match_qualifier": "is"
    }
  ],
  "apply_rule": true
}
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation*

Code	Description

	Example Value Model
	<pre>{
	  "rule_id": 0,
	  "success": true
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/automation/assetprocessing/{rule_id}** Gets defined asset processing automation rule

Returns an object of the asset processing rule currently created

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
rule_id * required integer *(path)*	Rule Id

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>{
	  "asset_compliance_scope_type": "specific",
	  "asset_attribute_rule_support_dynamic": "string",
	  "asset_attribute_rule_support_team": "string",
	  "asset_data_sensitivity": "Critical",
	  "asset_criticality_type": "specific",
	  "asset_group_dynamic": "string",
	  "asset_data_sensitivity_dynamic": "string",
	  "rule_name": "string",
	  "asset_attribute_owner_type": "specific",
	  "asset_criticality": "Critical",
	  "rule_disabled": 0,
	  "asset_criticality_dynamic": "string",
	  "asset_compliance_scope": "Yes",
	  "asset_group_type": "specific",
	  "asset_attribute_owner_dynamic": "string",
	  "asset_group": "string",
	  "asset_attribute_rule_owner_team_type": "specific",
	  "asset_compliance_scope_dynamic": "string",
	  "rule_match_type": "All",</pre>

Code	Description


```
    "asset_attribute_owner": "string",
    "asset_attribute_rule_owner_team": "string",
    "asset_attribute_rule_support_team_type": "specific",
    "asset_public": "Yes",
    "asset_data_sensitivity_type": "specific",
    "rule_id": 0,
    "rule_criteria": [
      {
        "rule_match_condition": "asset_name",
        "rule_match_value": "name",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "ip_address",
        "rule_match_value": "192.168.1.1",
        "rule_match_qualifier": "is not"
      },
      {
        "rule_match_condition": "operating_system_name",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "scan_type",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      },
      {
        "rule_match_condition": "connection_id",
        "rule_match_value": "string",
        "rule_match_qualifier": "is"
      }
    ]
  }
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

project connectors Information about your connectors

PUT `/projects/{project_id}/connectors/{connection_type}/{connection_id}/settings` Update modifiable settings of the Amazon AWS connector.

Update the list of Amazon AWS connector roles that can be updated.
Warning: This will overwrite any existing roles defined in the Amazon AWS connector. When setting roles, include all roles that need to be in the connector settings.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
connection_type * required `string` *(path)*	Type of the connector. Use GET connectors API endpoint to retrieve this value for the connector you like to modify. e.g. AMAZONAWS
connection_id * required `string`	Connection ID of the connector. Use GET connectors to retrieve this value for the AWS connector you like to modify. To get the existing roles in the Amazon AWS connector use the GET operation on the Connector Settings API endpoint.

Name	Description
(path)	
body * required *(body)*	New list of roles. Include all roles that need to be in the connector settings. A role missing from here will be removed from the Amazon AWS connector settings. **Example Value** Model `{ "connector_fields": { "roles": [ { "crossaccountrole": "string", "label": "string" } ] } }` **Parameter content type** application/json

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "message": "Roles updated successfully.", "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value* **Example Value** Model `{ "msg": "Connection ID: 5 not found in Project: 1", "code": 422, "success": false }`

GET `/projects/{project_id}/connectors/{connection_type}/{connection_id}/settings` Gets user roles defined in the Amazon AWS connector

Returns a list of Amazon AWS connector roles that can be updated.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
connection_type * required `string` *(path)*	Type of the connector. Use GET connectors API endpoint to retrieve this value for the connector you like to modify. e.g. AMAZONAWS
connection_id * required `string` *(path)*	Connection ID of the connector. Use GET connectors API endpoint to retrieve this value for the AWS connector you like to modify.

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "roles": [ { "crossaccountrole": "string", "label": "string" } ] }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET /projects/{project_id}/connectors Gets defined connectors in project

Returns a list of the connectors currently created

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses

Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[{ "connector_type": "string", "connector_name": "string", "connection_id": "string", "connector_fields": { "assuming_account_id": "string", "allowed_issue_priority": ["Highest", "High", "Medium", "Low", "Lowest"], "roles": [{ "crossaccountrole": "string", "label": "string" }], "assuming_external_id": "string", "allowed_issue_type": ["issuetype1", "issuetype2", "issuetype3"], "allowed_issue_project": ["project1", "PRJ2", "TST"] }, "connector_description": "string" }]`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project data Information about your project

GET `/projects/{project_id}/riskscore` Gets risk score for that project

Returns the risk score

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "score": 0 }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Error – project score is 0 and project may not exist*
422	*Invalid value*

GET /projects/{project_id}/software Gets software for that project

Returns details of software that has been enumerated

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation*

Code	Description

Example Value Model


```
{
  "software_name": "string",
  "assets": [
    {
      "host_id": 0,
      "os_name": "string",
      "host_type": "string",
      "host_name": "string"
    }
  ],
  "asset_count": 0
}
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project findings Information about your findings

GET **/projects/{project_id}/findings/compliance** Gets information on current compliance findings

Returns information on the current compliance findings in a project

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
start **integer** ***(query)***	Start of page
limit **integer** ***(query)***	Number of items per page, 100 max

Responses Response content type application/json

Code	Description
200	*successful operation*

Example Value Model

Code	Description


```
[
  {
    "finding_discovered": "string",
    "finding_severity": "string",
    "finding_name": "string",
    "finding_status": "string",
    "finding_count": 0,
    "scan_date": "string",
    "finding_exploitable": 0,
    "finding_severities": [
      "Critical"
    ],
    "scan_type": "string",
    "issue_open_count": 0,
    "issue_closed_count": 0,
    "finding_number": "string",
    "asset_count": 0,
    "compliance_frameworks": [
      {
        "framework_name": "string"
      }
    ],
    "finding_result": "string"
  }
]
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

GET /projects/{project_id}/findings/details/{finding_number}/{finding_id}

Gets details on a specific asset's finding

Returns details on a specific finding

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
finding_number * required `string` *(path)*	
finding_id * required `integer` *(path)*	

Responses Response content type application/json

Code	Description
200	*successful operation*

Code	Description

Example Value Model


```
{
  "finding_discovered": "string",
  "finding_id": 0,
  "finding_cve": "string",
  "mandiant_zero_day": "string",
  "finding_exploitable": "string",
  "finding_severity": "string",
  "finding_package_fix_versions": [
    null
  ],
  "finding_package_version": "string",
  "mandiant_vulnerable_products": "string",
  "finding_iava": "string",
  "mandiant_analysis": "string",
  "asset_id": "string",
  "finding_justification_key": "string",
  "scan_id": 0,
  "finding_port": "string",
  "mandiant_fix_urls": [
    null
  ],
  "justification_external_issues": "string",
  "cisa_vulnerability_name": "string",
  "justification_assigned_teams": "string",
  "finding_result": "string",
  "finding_path": "string",
  "justification_has_file": "string",
  "mandiant_attacking_ease": "string",
  "epss_score": 0,
  "finding_severity_adjusted": "string",
  "mandiant_risk_rating": "string",
  "finding_name": "string",
  "mandiant_threat_actors": [
    null
  ],
  "due_date": "string",
  "scan_date": "string",
  "finding_recommendation": "string",
  "mandiant_exploit_vectors": [
    null
  ],
  "justification_status_name": "string",
  "mandiant_exploited_by_malware": "string",
  "finding_references": "string",
  "scan_type": "string",
  "asset_name": "string",
  "mandiant_mitigations": [
    null
  ],
  "justification_status_mitigating": "string",
  "mandiant_exploit_in_the_wild": "string",
  "justification_text": "string",
  "finding_description": "string",
  "ip_address": "string",
  "justification_datetime": "string",
  "justification_assigned_users": "string",
  "mandiant_associated_malware": [
    null
  ],
  "mandiant_exploit_rating": "string",
  "mandiant_exploitation_consequence": "string",
  "finding_package": "string",
  "finding_output": "string",
  "finding_number": "string"
}
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

POST **/projects/{project_id}/findings/toprisk** BETA - Gets information on current findings

This endpoint is currently in BETA and is subject to change. Feel free to take a look, but the results and filters are subject to change. Returns a list of current open findings for project ordered by risk. Limited to 100 at a time

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
start `integer` *(query)*	Start of page
limit `integer` *(query)*	Number of items per page, 100 max

filter
(body)
	Filter for assets and findings
	Example Value Model
	{
	"asset_filters": [
	0
	],
	"finding_filters": [
	{
	"operator": "=",
	"property": "finding_cve",
	"value": "string"
	}
	]
	}
	Parameter content type
	application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model [{ "finding_discovered": "string", "finding_id": 0, "finding_cve": "string", "mandiant_zero_day": "string", "finding_exploitable": "string", "finding_severity": "string", "finding_package_fix_versions": [null], "finding_package_version": "string", "mandiant_vulnerable_products": "string", "finding_iava": "string", "mandiant_analysis": "string", "asset_id": "string", "finding_justification_key": "string", "scan_id": 0, "finding_port": "string", "mandiant_fix_urls": ["string"], "justification_external_issues": "string",

Code	Description


```
      "cisa_vulnerability_name": "string",
      "justification_assigned_teams": "string",
      "finding_result": "string",
      "finding_path": "string",
      "justification_has_file": "string",
      "mandiant_attacking_ease": "string",
      "epss_score": 0,
      "finding_severity_adjusted": "string",
      "mandiant_risk_rating": "string",
      "finding_name": "string",
      "mandiant_threat_actors": [
        "string"
      ],
      "due_date": "string",
      "scan_date": "string",
      "finding_recommendation": "string",
      "finding_score": 0,
      "mandiant_exploit_vectors": [
        "string"
      ],
      "justification_status_name": "string",
      "mandiant_exploited_by_malware": "string",
      "finding_references": "string",
      "scan_type": "string",
      "asset_name": "string",
      "mandiant_mitigations": [
        "string"
      ],
      "justification_status_mitigating": "string",
      "mandiant_exploit_in_the_wild": "string",
      "justification_text": "string",
      "finding_description": "string",
      "ip_address": "string",
      "justification_datetime": "string",
      "justification_assigned_users": "string",
      "mandiant_associated_malware": [
        "string"
      ],
      "mandiant_exploit_rating": "string",
      "mandiant_exploitation_consequence": "string",
      "finding_package": "string",
      "finding_output": "string",
      "finding_number": "string"
    }
  ]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

POST `/projects/{project_id}/findings/summary` Gets information on current findings grouped by finding_number

Returns a list of all current findings in a project grouped by finding_number

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
start `integer` *(query)*	Start of page
limit	Number of items per page, 100 max

Name	Description
integer *(query)*	
filter *(body)*	Filter off of any field as a string compare. Some properties will accept filtering by array of values. Use exactMatch for exact match.

Example Value Model

```
[
  {
    "property": "string",
    "value": "string",
    "exactMatch": false
  },
  {
    "property": "string",
    "value": [
      "string"
    ],
    "exactMatch": false
  }
]
```

Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation*

Example Value Model

```
[
  {
    "finding_discovered": "string",
    "finding_severity": "string",
    "finding_name": "string",
    "finding_status": "string",
    "finding_count": 0,
    "scan_date": "string",
    "finding_exploitable": 0,
    "finding_severities": [
      "Critical"
    ],
    "scan_type": "string",
    "issue_open_count": 0,
    "issue_closed_count": 0,
    "finding_number": "string",
    "asset_count": 0,
    "asset_fixed_count": 0,
    "finding_iava": "string",
    "asset_mitigated_count": 0,
    "finding_cve": "string",
    "mandiant_zero_day": "string",
    "mandiant_attacking_ease": "string",
    "mandiant_threat_actors": [
      "string"
    ],
    "mandiant_exploited_by_malware": "string",
    "mandiant_mitigations": [
      "string"
    ],
    "mandiant_vulnerable_products": "string",
    "mandiant_analysis": "string",
    "mandiant_associated_malware": [
      "string"
    ],
    "mandiant_exploit_rating": "string",
    "mandiant_exploitation_consequence": "string",
    "cisa_vulnerability_name": "string",
    "mandiant_fix_urls": [
      "string"
    ],
    "mandiant_exploit_vectors": [
      "string"
    ],
```

Code	Description


```
    "epss_score": 0,
    "mandiant_exploit_in_the_wild": "string",
    "mandiant_risk_rating": "string",
    "finding_statuses": [
      "string"
    ],
    "finding_pinned": true,
    "finding_severity_score": 0
  }
]
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

GET /projects/{project_id}/findings/details/{finding_number} Gets details on a finding and hosts affected

Returns details on a finding and hosts affected

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
finding_number * required `string` *(path)*	
scan_type * required `string` *(query)*	Scan type of the finding.
start `integer` *(query)*	Start of page.
limit `integer` *(query)*	Number of items per page. Maximum is 10000

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model

Code	Description


```
{
  "finding_discovered": "string",
  "finding_discovered_short": "string",
  "finding_description_adjusted": "string",
  "finding_severity": "string",
  "finding_last_seen_short": "string",
  "mandiant_vulnerable_products": "string",
  "mandiant_analysis": "string",
  "finding_status_fixed": 0,
  "mandiant_fix_urls": [
    null
  ],
  "mandiant_zero_day": "string",
  "finding_exploitable": 0,
  "mandiant_attacking_ease": "string",
  "epss_score": 0,
  "mandiant_exploit_in_the_wild": "string",
  "mandiant_risk_rating": "string",
  "finding_name": "string",
  "finding_recommendation": "string",
  "cisa_vulnerability_name": "string",
  "mandiant_exploit_vectors": [
    null
  ],
  "mandiant_threat_actors": [
    null
  ],
  "finding_status_total": 0,
  "mandiant_exploited_by_malware": "string",
  "scan_type": "string",
  "mandiant_mitigations": [
    null
  ],
  "display_type": "string",
  "finding_recommendation_adjusted": "string",
  "finding_description": "string",
  "assets": [
    {
      "line_number": "string",
      "finding_discovered": "string",
      "finding_id": 0,
      "finding_justification_assigned_teams": "string",
      "finding_cve": "string",
      "operating_system_name": "string",
      "due_date": "string",
      "finding_justification_external_issues_count": 0,
      "finding_severity": "string",
      "finding_result": "string",
      "operating_system_version": "string",
      "host_ip": "string",
      "finding_package_version": "string",
      "finding_number": "string",
      "scan_date": "string",
      "asset_id": 0,
      "asset_name": "string",
      "finding_justification_assigned_users": "string",
      "asset_info": "string",
      "finding_port": "string",
      "url": "string",
      "finding_package": "string",
      "finding_name": "string",
      "finding_package_fix_versions": [
        null
      ],
      "finding_justification_file_count": 0
    }
  ],
  "mandiant_associated_malware": [
    null
  ],
  "mandiant_exploit_rating": "string",
  "mandiant_exploitation_consequence": "string",
  "finding_severity_adjusted": "string",
  "finding_severities": [
    "Critical"
  ],
  "finding_last_seen": "string",
  "finding_status_mitigated": 0
}
```


401

API Key was not valid

403

API Key does not have permissions to project

Code	Description
422	*Invalid value*

PUT **/projects/{project_id}/findings** Update finding status, severity, assigned team , assigned user, due date and/or comment.

Updates a finding's status, severity, assigned team, assigned user, due date or comment

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
finding_number * required `string` *(query)*	Finding Number
scan_type * required `string` *(query)*	Scan Type
asset_id `integer` *(query)*	Optional asset_id to apply status, due date and comment update to. Ignored for severity updates unless instance severity feature enabled.
finding_justification_key `string` *(query)*	Required when asset_id is passed when updating specific asset's values.
body * required *(body)*	Finding fields to update **Example Value** Model `{ "comment": "string", "due_date": "string", "team_id": 0, "user_id": 0, "finding_status": "string", "change_text": "string", "finding_severity": "Critical" }` **Parameter content type** application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "asset_id": 0,`

Code	Description

	<pre>{
	  "success": true
	}</pre>

400	*Invalid asset parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid asset parameters supplied*

POST /projects/{project_id}/findings Add a single custom finding to an asset.

Add a single custom finding to an asset.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

body * required
(body)
	Finding Information
	Example Value Model
	<pre>{
	  "finding_http_request": "string",
	  "finding_additional_information": "string",
	  "finding_discovered": "string",
	  "custom_finding_name": "string",
	  "custom_finding_type": "Code",
	  "finding_url": "string",
	  "finding_likelihood": "string",
	  "custom_finding_source": "string",
	  "finding_mitigated_date": "string",
	  "finding_http_response": "string",
	  "custom_finding_description": "string",
	  "custom_finding_cve": "string",
	  "host_id": 0,
	  "finding_reproduction_steps": "string",
	  "custom_finding_references": "string",
	  "finding_code_snippet": "string",
	  "finding_service": "string",
	  "finding_status": "string",
	  "finding_port": "string",
	  "custom_finding_severity": "Critical",
	  "custom_finding_likelihood": "string",
	  "finding_impact": "string",
	  "custom_finding_impact": "string",
	  "finding_line_number": "string",
	  "custom_finding_number": "string",
	  "custom_finding_exploitable": 0,
	  "finding_path": "string",
	  "custom_finding_cvss": "string",
	  "custom_finding_recommendation": "string",
	  "finding_output": "string"
	}</pre>
	Parameter content type

Name	Description
	application/json

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Missing Host ID, Missing Project ID, Finding name required, One of the following finding type is required: Code, Device, Web Application or General*

GET ~~/projects/{project_id}/findings~~

GET **/projects/{project_id}/findings/mitigationstatuses** Gets mitigation statuses

Returns list of mitigation statuses that can be used to update a finding

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "justification_status_name": "string", "justification_status_mitigating": "string" } ]`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

PUT `/projects/{project_id}/findings/bulk` Update findings in bulk

Updates a finding"s status, severity, assigned team, assigned user, due date or comment. Due dates will overwrite any existing due dates.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Array of finding updates **Example Value** Model `[ { "asset_id": 0, "finding_justification_key": "string", "user_id": 0, "finding_status": "string", "due_date": "string", "finding_severity": "Critical", "comment": "string", "scan_type": "string", "change_text": "string", "team_id": 0, "finding_number": "string" } ]` **Parameter content type** application/json

Responses Response content type application/json

Code	Description
202	*job created* **Example Value** Model `{ "msg": "string", "job_id": 0 }`
400	*Invalid parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid asset parameters supplied*

POST **/projects/{project_id}/findings/bulk** Add custom findings to assets in bulk

Add custom findings to assets in bulk

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Array of findings to add **Example Value** Model `[{ "finding_http_request": "string", "finding_additional_information": "string", "finding_discovered": "string", "custom_finding_name": "string", "custom_finding_type": "Code", "finding_url": "string", "finding_likelihood": "string", "custom_finding_source": "string", "finding_mitigated_date": "string", "finding_http_response": "string", "custom_finding_description": "string", "custom_finding_cve": "string", "host_id": 0, "finding_reproduction_steps": "string", "custom_finding_references": "string", "finding_code_snippet": "string", "finding_service": "string", "finding_status": "string", "finding_port": "string",`

Name	Description


```
    "custom_finding_severity": "Critical",
    "custom_finding_likelihood": "string",
    "finding_impact": "string",
    "custom_finding_impact": "string",
    "finding_line_number": "string",
    "custom_finding_number": "string",
    "custom_finding_exploitable": 0,
    "finding_path": "string",
    "custom_finding_cvss": "string",
    "custom_finding_recommendation": "string",
    "finding_output": "string"
  }
]
```


Parameter content type

application/json

Responses Response content type application/json

Code	Description
202	*job created* **Example Value** Model `{ "msg": "string", "job_id": 0 }`
400	*Invalid parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Missing Host ID, Missing Project ID, Finding name required, One of the following finding type is required: Code, Device, Web Application or General*

POST /projects/{project_id}/findings/search Gets information on current findings

Returns a list of findings for the project. Limited to 1000 at a time.

Parameters Try it out

Name	Description
project_id * required	Project Id

Name	Description
integer *(path)*	
start **integer** *(query)*	Start of page
limit **integer** *(query)*	Number of items per page, 1000 max
filter *(body)*	Filter off of any field as a string compare. Use exactMatch for exact match.

Example Value Model


```
{
  "scan_date": {
    "operator": ">=",
    "datetime": "string"
  },
  "finding_cve": "string",
  "mandiant": {
    "mandiant_zero_day": "Yes",
    "mandiant_attacking_ease": [
      "string"
    ],
    "mandiant_threat_actors": [
      "string"
    ],
    "mandiant_exploited_by_malware": "Yes",
    "mandiant_mitigations": [
      "string"
    ],
    "mandiant_vulnerable_products": [
      "string"
    ],
    "mandiant_analysis": [
      "string"
    ],
    "mandiant_associated_malware": [
      "string"
    ],
    "mandiant_exploit_rating": [
      "string"
    ],
    "mandiant_fix_urls": [
      {
        "url": "string",
        "name": "string"
      }
    ],
    "cisa_vulnerability_name": [
      "string"
    ],
    "mandiant_exploitation_consequence": [
      "string"
    ],
    "mandiant_exploit_vectors": [
      "string"
    ],
    "epss_score": {
      "operator": ">=",
      "score": 0
    },
    "mandiant_exploit_in_the_wild": "Yes",
    "mandiant_risk_rating": [
      "string"
    ]
  },
  "justification_status_name": [
    "string"
  ],
  "finding_severity": "string",
  "is_active": true,
  "scan_type": "string",
  "asset_name": "string",
  "user": "string",
  "ip_address": "string",
  "asset_id": 0,
  "mitigated_date": {
    "operator": ">=",
    "datetime": "string"
  },
  "finding_port": "string",
  "justification_status": [
    "string"
  ],
  "finding_exploitable": "string",
  "asset_groups": [
```

Name	Description


```
      "string"
    ],
    "asset_public": "string",
    "team": "string",
    "finding_name": "string"
  }
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation*

Example Value Model


```
[
  {
    "finding_discovered": "string",
    "finding_id": 0,
    "finding_cve": "string",
    "mandiant_zero_day": "string",
    "finding_exploitable": "string",
    "finding_severity": "string",
    "finding_package_fix_versions": [
      null
    ],
    "finding_package_version": "string",
    "mandiant_vulnerable_products": "string",
    "finding_iava": "string",
    "mandiant_analysis": "string",
    "asset_id": "string",
    "finding_justification_key": "string",
    "scan_id": 0,
    "finding_port": "string",
    "mandiant_fix_urls": [
      null
    ],
    "justification_external_issues": "string",
    "cisa_vulnerability_name": "string",
    "justification_assigned_teams": "string",
    "finding_result": "string",
    "finding_path": "string",
    "justification_has_file": "string",
    "mandiant_attacking_ease": "string",
    "epss_score": 0,
    "finding_severity_adjusted": "string",
    "mandiant_risk_rating": "string",
    "finding_name": "string",
    "mandiant_threat_actors": [
      null
    ],
    "due_date": "string",
    "scan_date": "string",
    "finding_recommendation": "string",
    "mandiant_exploit_vectors": [
      null
    ],
    "justification_status_name": "string",
    "mandiant_exploited_by_malware": "string",
    "finding_references": "string",
    "scan_type": "string",
    "asset_name": "string",
    "mandiant_mitigations": [
      null
    ],
    "justification_status_mitigating": "string",
    "mandiant_exploit_in_the_wild": "string",
    "justification_text": "string",
    "finding_description": "string",
    "ip_address": "string",
    "justification_datetime": "string",
    "justification_assigned_users": "string",
    "mandiant_associated_malware": [
      null
    ],
    "mandiant_exploit_rating": "string",
```

Code	Description

```
    "mandiant_exploitation_consequence": "string",
    "finding_package": "string",
    "finding_output": "string",
    "finding_number": "string"
  }
]
```

401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

GET /projects/{project_id}/findings/mitigated Gets information on mitigated vulnerabilities

Returns information on the mitigated vulnerabilities in a project

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
limit **integer** ***(query)***	Number of results to return. If not included 1 is used. Maximum is 100
start **integer** ***(query)***	Value to offset next set of results from.
start_date **string** ***(query)***	Start date to include (yyyy-mm-dd hh:ii:ss format, UTC). Default is 3 months. Maxiumum is 1 year ago

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model

```
[
  {
    "manual_mitigated": true,
    "finding_discovered": "string",
    "finding_name": "string",
    "total_manual": 0,
    "finding_remediation_days": "string",
    "finding_severity": "string",
    "finding_exploitable": "string",
    "finding_severities": [
```

Code	Description


```
        "Critical"
      ],
      "finding_remediated_date": "string",
      "scan_type": "string",
      "total_mitigated": 0,
      "total_open": 0,
      "finding_number": "string"
    }
  ]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

GET /projects/{project_id}/findings/frameworks Gets list of existing compliance frameworks

Returns a list of all applicable frameworks in a project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description

200

successful operation

Example Value Model


```
[
  {
    "framework_name": "string"
  }
]
```


401

API Key was not valid

403

API Key does not have permissions to project

Code	Description
422	*Invalid value*

GET **/projects/{project_id}/findings/metrics** Gets information on current vulnerability metrics

Returns information on the current vulnerability metrics in a project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>{
	"projectmetricsdiscovered90": 0,
	"projectmetricsknow30": 0,
	"metric_date": "string",
	"success": true,
	"projectmetricsremediated30": 0,
	"projectmetricsremdays180": 0,
	"projectmetricsdiscovered30": 0,
	"projectmetricsdiscovered180": 0,
	"projectmetricsremdays90": 0,
	"projectmetricsknow180": 0,
	"projectmetricsshowknow": true,
	"projectmetricsremediated180": 0,
	"projectmetricsremediated90": 0,
	"projectmetricsremdays30": 0,
	"projectmetricsknow90": 0
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/findings/trend** Gets information on current vulnerability trends

Returns information on the current vulnerability trends in a project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
start_date `string` *(query)*	Date to start the trend from. If not provided and offset not set below then 3 months ago is used. Date must be within last year. Format is "YYYY-MM-DD".
end_date `string` *(query)*	Date to end the trend. If not provided and offset not set then uses current date. Date must be within last year. Format is "YYYY-MM-DD".
offset_type `string` *(query)*	Used in conjunction with offset_value to determine a date. Date must be within last year. If both offset and start_date is passed, start_date is used
offset_value `integer` *(query)*	How many offset_types to offset.
asset_groups `string` *(query)*	JSON array with asset groups to include. Can also limit asset type using “asset_type_filter:Host” or "asset_type_filter:Application".
trend_pieces `string` *(query)*	JSON array with trend pieces to include. Options include vulnDiscoveredBar, vulnDiscoveredBarTotal, vulnRemediatedBar, vulnRemediatedBarTotal, vulnRemediatetimeBar, vulnRemediatetimeBarTotal, vulnTrendLine, vulnTrendLineTotal

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
{
  "vulnRemediatedBar": [
    {
      "High": 0,
      "Medium": 0,
      "vuln_date": "string",
      "vuln_date_full": "string",
      "Critical": 0,
      "Low": 0
    }
  ],
  "vulnRemediatetimeLine": [
    {
      "count": 0,
      "sevs": {
        "High": {
          "count": 0,
          "total": 0
        },
        "Critical": {
          "count": 0,
          "total": 0
        },
        "Medium": {
          "count": 0,
          "total": 0
        },
        "Low": {
          "count": 0,
```

Code	Description


```
            "total": 0
          }
        },
        "remediate_time": 0,
        "vuln_date_full": "string",
        "total": 0,
        "vuln_date": "string"
      }
    ],
    "vulnRemediatetimeBar": [
      {
        "count": 0,
        "total": 0,
        "severity": "Critical",
        "value": 0
      }
    ],
    "vulnDiscoveredBar": [
      {
        "High": 0,
        "Medium": 0,
        "vuln_date": "string",
        "vuln_date_full": "string",
        "Critical": 0,
        "Informational": 0,
        "Low": 0
      }
    ]
  }
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

GET /projects/{project_id}/findings/overview Gets overview information on current findings

Returns a simple overview of number of open findings for project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
{
  "finding_count_medium": 0,
  "finding_vulnerability_score": 0,
```

Code	Description


```
  "finding_count_low": 0,
  "finding_count_high": 0,
  "finding_count_crithigh": 0,
  "finding_count_cve": 0,
  "finding_count_iava": 0,
  "finding_count_exploitable": 0,
  "finding_count_critical": 0
}
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

project issues Information about your external issues

GET **/projects/{project_id}/issues** Gets list of current issues in a project

Returns a list of issues for a project

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
start **integer** ***(query)***	
limit **integer** ***(query)***	If not included 1 is used. Maximum is 100

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "issue_key": "string",
    "issue_assignee": "string",
    "finding_count": 0,
    "finding_severity": "string",
    "issue_comment": [
      {
```

Code	Description


```
            "comment": "string",
            "date": "string",
            "user": "string"
          }
        ],
        "scan_type": "string",
        "issue_comment_last": "string",
        "issue_updated": "string",
        "issue_status": "string",
        "issue_type": "string",
        "finding_name": "string",
        "issue_url": "string"
      }
    ]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

GET /projects/{project_id}/issues/{scan_type}/{finding_number} Gets details on an issues

Returns information on a specific issue

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
start `integer` *(query)*	
limit `integer` *(query)*	If not included 1 is used. Maximum is 100
scan_type * required `string` *(path)*	Scan type of the finding to get the issue
finding_number * required `string` *(path)*	Finding number of the finding to get the issue

Responses Response content type application/json

Code	Description
200	*successful operation*

Code	Description

Example Value Model


```
[
  {
    "issue_key": "string",
    "issue_assignee": "string",
    "finding_count": 0,
    "finding_severity": "string",
    "issue_comment": [
      {
        "comment": "string",
        "date": "string",
        "user": "string"
      }
    ],
    "scan_type": "string",
    "issue_comment_last": "string",
    "issue_updated": "string",
    "issue_status": "string",
    "issue_type": "string",
    "finding_name": "string",
    "issue_url": "string"
  }
]
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project jobs Information about your jobs

GET **/projects/{project_id}/jobs/{job_id}** Gets information on a specific job

Returns details on a specific job

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
job_id * required **integer** ***(path)***	Job Id

Responses Response content type application/json

Code	Description
200	*successful operation*

Code	Description

Example Value Model


```
[
  {
    "status": "string",
    "worker_type": "string",
    "job_id": 0,
    "status_message": "string",
    "results": [
      {}
    ],
    "archive": "string"
  }
]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

GET /projects/{project_id}/jobs Gets information on jobs

Returns a list of all jobs in a project

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
start **integer** ***(query)***	
limit **integer** ***(query)***	If not included 1 is used. Maximum is 100
include_archive **boolean** ***(query)***	Include archived jobs in the response
status **string** ***(query)***	Only get jobs with a certain status
worker_type **string** ***(query)***	Only get jobs with a certain worker_type

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>[
	  [
	  {
	  "status": "string",
	  "worker_type": "string",
	  "job_id": 0,
	  "status_message": "string",
	  "results": [
	  {}
	  ],
	  "archive": "string"
	  }
	  ]
	]</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project reports Information about your reports

GET /projects/{project_id}/reports/{report_id}/download Downloads a report

Returns a report file

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
report_id * required integer *(path)*	Report Id

Responses Response content type file

Code	Description
200	*successful operation*

Code	Description
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET `/projects/{project_id}/reports/{report_id}` Gets report info

Returns information on a specific report file

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
report_id * required `integer` *(path)*	Report Id

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>{
	"created_user_lastname": "string",
	"report_description": "string",
	"report_status": "string",
	"report_name": "string",
	"created_user_firstname": "string",
	"created_date": "string",
	"report_file_name": "string",
	"report_id": 0
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

Code	Description

POST ~~/projects/{project_id}/reports~~ request a new report to be created

GET **/projects/{project_id}/reports** Gets list of current reports in a project

Returns a list of reports for a project

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
start integer *(query)*	
limit integer *(query)*	If not included 1 is used. Maximum is 100

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	
	[
	{
	"created_user_lastname": "string",
	"report_description": "string",
	"report_status": "string",
	"report_name": "string",
	"created_user_firstname": "string",
	"created_date": "string",
	"report_file_name": "string",
	"report_id": 0
	}
	]

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project scans Information about your scans

POST `/projects/{project_id}/scans/{scan_id}/findings/summary` Gets information on current findings

Returns a list of all current findings in a scan

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
scan_id * required `integer` *(path)*	Scan Id
filter *(body)*	Filter off of any field as a string compare. Some properties will accept filtering by array of values. Use exactMatch for exact match. **Example Value** Model `[ { "property": "string", "value": "string", "exactMatch": false }, { "property": "string", "value": [ "string" ], "exactMatch": false } ]` **Parameter content type** application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `[{ "finding_discovered": "string", "finding_severity": "string", "finding_name": "string", "finding_status": "string", "finding_count": 0, "scan_date": "string", "finding_exploitable": 0, "finding_severities": ["Critical"], "scan_type": "string", "issue_open_count": 0, "issue_closed_count": 0, "finding_number": "string", "asset_count": 0, "asset_fixed_count": 0, "finding_iava": "string", "asset_mitigated_count": 0,`

Code	Description

	<pre>"finding_cve": "string"
	}
	]</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/scans/{scan_id}/findings/details/{finding_number}** Gets details on a finding and hosts affected for a scan

Returns details on a finding and hosts affected for a specfic scan

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
scan_id * required `integer` *(path)*	Scan Id
finding_number * required `string` *(path)*	

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model

<pre>{
"finding_discovered": "string",
"finding_discovered_short": "string",
"finding_description_adjusted": "string",
"finding_severity": "string",
"finding_last_seen_short": "string",
"mandiant_vulnerable_products": "string",
"mandiant_analysis": "string",
"finding_status_fixed": 0,
"mandiant_fix_urls": [
null
],
"mandiant_zero_day": "string",
"finding_exploitable": 0,
"mandiant_attacking_ease": "string",
"epss_score": 0,
"mandiant_exploit_in_the_wild": "string",</pre>

Code	Description


```
  "mandiant_risk_rating": "string",
  "finding_name": "string",
  "finding_recommendation": "string",
  "cisa_vulnerability_name": "string",
  "mandiant_exploit_vectors": [
    null
  ],
  "mandiant_threat_actors": [
    null
  ],
  "finding_status_total": 0,
  "mandiant_exploited_by_malware": "string",
  "scan_type": "string",
  "mandiant_mitigations": [
    null
  ],
  "display_type": "string",
  "finding_recommendation_adjusted": "string",
  "finding_description": "string",
  "assets": [
    {
      "line_number": "string",
      "finding_discovered": "string",
      "finding_id": 0,
      "finding_justification_assigned_teams": "string",
      "finding_cve": "string",
      "operating_system_name": "string",
      "due_date": "string",
      "finding_justification_external_issues_count": 0,
      "finding_severity": "string",
      "finding_result": "string",
      "operating_system_version": "string",
      "host_ip": "string",
      "finding_package_version": "string",
      "finding_number": "string",
      "scan_date": "string",
      "asset_id": 0,
      "asset_name": "string",
      "finding_justification_assigned_users": "string",
      "asset_info": "string",
      "finding_port": "string",
      "url": "string",
      "finding_package": "string",
      "finding_name": "string",
      "finding_package_fix_versions": [
        null
      ],
      "finding_justification_file_count": 0
    }
  ],
  "mandiant_associated_malware": [
    null
  ],
  "mandiant_exploit_rating": "string",
  "mandiant_exploitation_consequence": "string",
  "finding_severity_adjusted": "string",
  "finding_severities": [
    "Critical"
  ],
  "finding_last_seen": "string",
  "finding_status_mitigated": 0
}
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/scans/{scan_id}/findings/details/{finding_number}/{finding_id}** Gets details on a specific asset's finding for a scan

Returns details on a specific asset's finding for a scan

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
scan_id * required `integer` *(path)*	Scan Id
finding_number * required `string` *(path)*	
finding_id * required `integer` *(path)*	

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
{
  "finding_discovered": "string",
  "finding_id": 0,
  "finding_cve": "string",
  "mandiant_zero_day": "string",
  "finding_exploitable": "string",
  "finding_severity": "string",
  "finding_package_fix_versions": [
    null
  ],
  "finding_package_version": "string",
  "mandiant_vulnerable_products": "string",
  "finding_iava": "string",
  "mandiant_analysis": "string",
  "asset_id": "string",
  "finding_justification_key": "string",
  "scan_id": 0,
  "finding_port": "string",
  "mandiant_fix_urls": [
    null
  ],
  "justification_external_issues": "string",
  "cisa_vulnerability_name": "string",
  "justification_assigned_teams": "string",
  "finding_result": "string",
  "finding_path": "string",
  "justification_has_file": "string",
  "mandiant_attacking_ease": "string",
  "epss_score": 0,
  "finding_severity_adjusted": "string",
  "mandiant_risk_rating": "string",
  "finding_name": "string",
  "mandiant_threat_actors": [
    null
  ],
  "due_date": "string",
  "scan_date": "string",
  "finding_recommendation": "string",
  "mandiant_exploit_vectors": [
    null
  ],
  "justification_status_name": "string",
  "mandiant_exploited_by_malware": "string",
  "finding_references": "string",
```

Code	Description


```
  "scan_type": "string",
  "asset_name": "string",
  "mandiant_mitigations": [
    null
  ],
  "justification_status_mitigating": "string",
  "mandiant_exploit_in_the_wild": "string",
  "justification_text": "string",
  "finding_description": "string",
  "ip_address": "string",
  "justification_datetime": "string",
  "justification_assigned_users": "string",
  "mandiant_associated_malware": [
    null
  ],
  "mandiant_exploit_rating": "string",
  "mandiant_exploitation_consequence": "string",
  "finding_package": "string",
  "finding_output": "string",
  "finding_number": "string"
}
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET /projects/{project_id}/scans/{scan_id} Gets information a specific scan

Returns information on a specific scan for project

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
scan_id * required `integer` *(path)*	Scan Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "scan_file_name": "string",
    "scan_id": 0,
    "finding_count_medium": 0,
```

Code	Description


```
    "finding_count_informational": 0,
    "finding_count_high": 0,
    "scan_date": "string",
    "scan_description": "string",
    "finding_count_low": 0,
    "scan_type": "string",
    "finding_count_fail": 0,
    "finding_count_warning": 0,
    "finding_count_pass": 0,
    "asset_count": 0,
    "scan_mitigated": 0,
    "finding_count_critical": 0
  }
]
```


401

API Key was not valid

403

API Key does not have permissions to project

422

Invalid value

POST `/projects/{project_id}/scans` uploads a scan

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
scan_description `string` *(formData)*	Description for scan
file * required `file` *(formData)*	file to upload
file_in_body `boolean` *(query)*	File is in body and not in the form data
body_json_encoded `boolean` *(query)*	Only applicable if file_in_body is enabled, flag to JSON decode the body text before processing
scan_type `string` *(query)*	Only applicable with certain types. Not needed unless specfied by Support

Responses Response content type application/json

Code	Description
200	*successful operation*

Code	Description

	Example Value Model
	<pre>{
	  "msg": "string",
	  "job_id": 0
	}</pre>

401	*API Key was not valid*
403	*API Key does not have permissions to project*

GET `/projects/{project_id}/scans` Gets list of current scans in a project

Returns a list of scans for a project

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
start **integer** ***(query)***	
limit **integer** ***(query)***	If not included 1 is used. Maximum is 100

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>[
	  [
	  {
	  "scan_file_name": "string",
	  "scan_id": 0,
	  "finding_count_medium": 0,
	  "finding_count_informational": 0,
	  "finding_count_high": 0,
	  "scan_date": "string",
	  "scan_description": "string",
	  "finding_count_low": 0,
	  "scan_type": "string",
	  "finding_count_fail": 0,
	  "finding_count_warning": 0,
	  "finding_count_pass": 0,
	  "asset_count": 0,
	  "scan_mitigated": 0,
	  "finding_count_critical": 0</pre>

Code	Description
	}]]
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/scans/{scan_id}/download** Returns actual scan results

Returns scan file

Parameters Try it out

Name	Description
project_id * required **integer** ***(path)***	Project Id
scan_id * required **integer** ***(path)***	Scan Id

Responses Response content type: file

Code	Description
200	*successful operation*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

project teams Information about your teams

GET **/projects/{project_id}/teams/ssomaps** Gets a list of SSO mappings from all teams in the project

Returns a list of all SSO objects that will map a user to a team

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "team_id": 0, "project_id": 0, "sso_description": "string", "sso_object": "string", "sso_team_map_id": 0 } ]`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

POST /projects/{project_id}/teams Create a team

Creates a team for a project. Optionally adding users to the team. team_name required.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Updated asset object **Example Value** Model `{ "team_name": "string", "asset_groups": [`

Name	Description


```
    0
  ],
  "users": [
    {
      "user_id": 0
    }
  ]
}
```


Parameter content type

application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "project_id": 0,
    "team_id": 0,
    "asset_groups": [
      0
    ],
    "team_name": "string",
    "users": [
      {
        "lname": "string",
        "username": "string",
        "user_id": 0,
        "fname": "string"
      }
    ]
  }
]
```


401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET **/projects/{project_id}/teams** Gets list of teams

Returns a list of all teams for a project.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "project_id": 0, "team_id": 0, "asset_groups": [ 0 ], "team_name": "string" } ]`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

POST /projects/{project_id}/teams/{team_id}/ssomaps Create a SSO mapping to add users to this team

Creates a SSO to team match Users will be added to this team if they log in with a matching SSO object

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
team_id * required `integer` *(path)*	Team Id
body * required *(body)*	new SSO to team mapping **Example Value** Model `{ "sso_object": "string",`

Name	Description


```
  "sso_description": "string"
}
```


Parameter content type

application/json

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model


```
[
  {
    "team_id": 0,
    "project_id": 0,
    "sso_description": "string",
    "sso_object": "string",
    "sso_team_map_id": 0
  }
]
```


400	*Invalid asset parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

GET /projects/{project_id}/teams/{team_id}/ssomaps Gets a list of SSO mappings in the team

Returns a list of all sso objects that will map a user to this team

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
team_id * required integer *(path)*	Team Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "team_id": 0, "project_id": 0, "sso_description": "string", "sso_object": "string", "sso_team_map_id": 0 } ]`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

PUT `/projects/{project_id}/teams/bulk` Update team name or team users in bulk

Update bulk team names and optionally team users. Warning: This will overwrite any existing users in the team. When setting users, include all users that should be in the team. To only update the name, do not include the users key. team_name field is required in body.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
body * required *(body)*	Array of New team definitions **Example Value** Model `[ { "team_id": 0, "asset_groups": [ 0 ], "users": [ { "user_id": 0 } ] } ]` **Parameter content type** application/json

Responses

Response content type: application/json

Code	Description
202	*Job created* **Example Value** Model `{ "msg": "string", "job_id": 0 }`
400	*Invalid team parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid team parameters supplied*

PUT /projects/{project_id}/teams/{team_id} Update team name or team users

Update team name and optionally team users. Warning: This will overwrite any existing users in the team. When setting users, include all users that should be in the team. To only update the name, do not include the users key. team_name field is required in body.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
team_id * required `integer` *(path)*	Team Id
body * required *(body)*	New team definition **Example Value** Model `{ "team_name": "string", "asset_groups": [ 0 ], "users": [ { "user_id": 0 } ] }`

Name	Description

Parameter content type

application/json

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	<pre>{
	  "project_id": 0,
	  "team_id": 0,
	  "asset_groups": [
	  0
	  ],
	  "team_name": "string",
	  "users": [
	  {
	  "lname": "string",
	  "username": "string",
	  "user_id": 0,
	  "fname": "string"
	  }
	  ]
	}</pre>

400	*Invalid team parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid team parameters supplied*

GET /projects/{project_id}/teams/{team_id} Gets information on a specific team including members

Returns info about a specific team

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id

Name	Description
team_id * required `integer` *(path)*	Team Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "project_id": 0, "team_id": 0, "asset_groups": [ 0 ], "team_name": "string", "users": [ { "lname": "string", "username": "string", "user_id": 0, "fname": "string" } ] }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

DELETE /projects/{project_id}/teams/{team_id} Deletes a specific team

Deletes a specific team. WARNING: This is permanent change

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
team_id * required `integer` *(path)*	Team Id

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "success": true }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

PUT /projects/{project_id}/teams/{team_id}/ssomaps/{sso_team_map_id} Update a SSO Mapping

Update the matching SSO Object or description

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
team_id * required integer *(path)*	Team Id
sso_team_map_id * required integer *(path)*	SSO Team Map Id
body * required *(body)*	New SSO Mapping definition **Example Value** Model `{ "sso_object": "string", "sso_description": "string" }` **Parameter content type** application/json

Responses Response content type: application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "team_id": 0, "project_id": 0, "sso_description": "string", "sso_object": "string", "sso_team_map_id": 0 } ]`
400	*Invalid asset parameters supplied*
401	*API Key was not valid*
403	*API Key does not have permissions to project*
404	*Asset not found*
422	*Invalid asset parameters supplied*

GET `/projects/{project_id}/teams/{team_id}/ssomaps/{sso_team_map_id}` Gets information on a specific SSO mapping in the team

Returns info about a specific SSO mapping

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id
team_id * required `integer` *(path)*	Team Id
sso_team_map_id * required `integer` *(path)*	SSO Team Map Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "team_id": 0, "project_id": 0, "sso_description": "string", "sso_object": "string", "sso_team_map_id": 0 }`
401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

DELETE /projects/{project_id}/teams/{team_id}/ssomaps/{sso_team_map_id} Deletes a specific SSO Mapping

Deletes a specific SSO Mapping. WARNING: This is permanent change

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
team_id * required integer *(path)*	Team Id
sso_team_map_id * required integer *(path)*	SSO Team Map Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "success": true`

Code	Description
	} *API Key was not valid*
401	
403	*API Key does not have permissions to project*
422	*Invalid value*

project users Information about your users

GET `/projects/{project_id}/users` Gets list of users

Returns a list of all users for a project. For data inside of a user use the user's project_id for any other API calls

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	
	[
	{
	"lname": "string",
	"username": "string",
	"user_id": 0,
	"fname": "string"
	}
	]

401	*API Key was not valid*
403	*API Key does not have permissions to project*

Code	Description
422	*Invalid value*

GET **/projects/{project_id}/users/{user_id}** Gets information on a specific user

Returns info about a specific user

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
user_id * required integer *(path)*	User Id

Responses Response content type application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	{
	"lname": "string",
	"username": "string",
	"user_id": 0,
	"fname": "string"
	}

401	*API Key was not valid*
403	*API Key does not have permissions to project*
422	*Invalid value*

logs Audit logs from your org

GET **/logs** Gets audit logs from your orgs

Returns an array of logs since a specified date

Parameters Try it out

Name	Description
start `integer` *(query)*	Offset start
limit `integer` *(query)*	Return limit
after `string` *(query)*	Start date to include (yyyy-mm-dd hh:ii:ss format, UTC). Must include after or since parameter
since `integer` *(query)*	Minutes of logs to include. Max = 1 year. Must include after or since parameter

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `[ { "details": "string", "datetime": "string" } ]`
401	*API Key was not valid*
422	*Invalid value*

users User management for your org

DELETE `/users` Deletes a user from your org

Removes a user and permissions from an org

Parameters Try it out

Name	Description
user_id * required integer *(path)*	User Id

Responses Response content type: application/json

Code	Description

200	*successful operation*
	
	Example Value Model
	{
	"message": "string",
	"success": true
	}

401	*API Key was not valid*
403	*API Key does not have permissions to perform action*
422	*Invalid value*

beta

POST **/projects/{project_id}/findings/toprisk** BETA - Gets information on current findings

This endpoint is currently in BETA and is subject to change. Feel free to take a look, but the results and filters are subject to change. Returns a list of current open findings for project ordered by risk. Limited to 100 at a time

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
start integer *(query)*	Start of page
limit integer *(query)*	Number of items per page, 100 max
filter *(body)*	Filter for assets and findings **Example Value** Model

Name	Description


```
{
  "asset_filters": [
    0
  ],
  "finding_filters": [
    {
      "operator": "=",
      "property": "finding_cve",
      "value": "string"
    }
  ]
}
```


Parameter content type

application/json

Responses

Response content type application/json

Code	Description
200	*successful operation*

Example Value Model


```
[
  {
    "finding_discovered": "string",
    "finding_id": 0,
    "finding_cve": "string",
    "mandiant_zero_day": "string",
    "finding_exploitable": "string",
    "finding_severity": "string",
    "finding_package_fix_versions": [
      null
    ],
    "finding_package_version": "string",
    "mandiant_vulnerable_products": "string",
    "finding_iava": "string",
    "mandiant_analysis": "string",
    "asset_id": "string",
    "finding_justification_key": "string",
    "scan_id": 0,
    "finding_port": "string",
    "mandiant_fix_urls": [
      "string"
    ],
    "justification_external_issues": "string",
    "cisa_vulnerability_name": "string",
    "justification_assigned_teams": "string",
    "finding_result": "string",
    "finding_path": "string",
    "justification_has_file": "string",
    "mandiant_attacking_ease": "string",
    "epss_score": 0,
    "finding_severity_adjusted": "string",
    "mandiant_risk_rating": "string",
    "finding_name": "string",
    "mandiant_threat_actors": [
      "string"
    ],
    "due_date": "string",
    "scan_date": "string",
    "finding_recommendation": "string",
    "finding_score": 0,
    "mandiant_exploit_vectors": [
      "string"
    ],
    "justification_status_name": "string",
    "mandiant_exploited_by_malware": "string",
    "finding_references": "string",
    "scan_type": "string",
    "asset_name": "string",
    "mandiant_mitigations": [
      "string"
    ],
    "justification_status_mitigating": "string",
    "mandiant_exploit_in_the_wild": "string",
    "justification_text": "string",
```

Code	Description


```
    "finding_description": "string",
    "ip_address": "string",
    "justification_datetime": "string",
    "justification_assigned_users": "string",
    "mandiant_associated_malware": [
      "string"
    ],
    "mandiant_exploit_rating": "string",
    "mandiant_exploitation_consequence": "string",
    "finding_package": "string",
    "finding_output": "string",
    "finding_number": "string"
  }
]
```


401 *API Key was not valid*

403 *API Key does not have permissions to project*

422 *Invalid value*

data exports

POST **/projects/{project_id}/dataexport/{file_id}** Downloads a data export file for the specified project

Downloads a data export file, specified by file_id, from a project.

Parameters Try it out

Name	Description
project_id * required integer *(path)*	Project Id
file_id * required integer *(path)*	File Id

Responses Response content type application/zip

Code	Description
200	*successful operation* **Example Value** Model `"string"`
401	*API Key was not valid*

Code	Description
403	*Permission denied*
405	*Invalid HTTP method*
422	*Invalid value*

GET **/projects/{project_id}/dataexport** Gets a list of data export files available to download for the specified project

Returns a list of data export files available to download for the specified project_id. This is used to get file_id(s) for use in the POST /projects/{project_id}/dataexport/{file_id} endpoint to download a specific data export file.

Parameters Try it out

Name	Description
project_id * required `integer` *(path)*	Project Id

Responses Response content type application/json

Code	Description
200	*successful operation* **Example Value** Model `{ "data_type": "string", "file_path": "string", "file_upload_date": "string", "mime_type": "string", "file_id": 0 }`
401	*API Key was not valid*
403	*Permission denied*
405	*Invalid HTTP method*

Code	Description
422	*Invalid value*

Models

TeamsData {

```
description:  Data returned at the teams level

project_id    integer($int64)
team_id       integer($int64)
asset_groups
                 [integer($int64)
              tag_id

              ]
team_name     string
}
```

Log {

```
details       string
              Event details

datetime*     string
              Event date in Y-m-d H:i:s format (UTC timezone)

}
```

Connector {

```
connector_type*       string
connector_name*       string
connection_id*        string
connector_fields
                         {
                         assuming_account_id   string
                         allowed_issue_priority
                                                  [string]
                                               example: List [ "Highest", "High", "Medium", "Low", "Lowest" ]
                         roles
                                                  [    {
                                                  crossaccountrole string
                                                  label            string
                                                }]
                         assuming_external_id  string
                         allowed_issue_type
                                                  [string]
                                               example: List [ "issuetype1", "issuetype2", "issuetype3" ]
                         allowed_issue_project
                                                  [string]
                                               example: List [ "project1", "PRJ2", "TST" ]
                      }
connector_description*string
}
```

FindingTrendRemediatetimeLineRecord {

```
count          integer
sevs
```

FindingTrendRemediatetimeLineRecordSev {

```
                  High
                                 {
                                 count        integer
                                 total        integer
                              }
                  Critical
                                 {
                                 count        integer
                                 total        integer
                              }
                  Medium
                                 {
                                 count        integer
                                 total        integer
                              }
                  Low
                                 {
                                 count        integer
                                 total        integer
                              }
               }
remediate_time integer
```

```
    vuln_date_full string
    total          integer
    vuln_date      string
}
```

FindingSummaryFilter `[...]`

Asset `{`

```
    description:                Asset data

    asset_data_sensitivity_score integer
                                Asset sensitivity 2(Low), 5(Moderate), 7(High) or 10(Critical)

    operating_system_name       string
    asset_inactive_date         string
    image_manifest              string
    active                      boolean
                                Is the asset active?

    asset_location              string
    support_team
```

AssetTeamData `{`

```
                                    description:  Team data returned at asset level

                                    team_id       integer($int64)
                                    team_name     string
                                }
    image_registry              string
    image_platform_os_version   string
                                The version of the operating system which the image is built to run on.

    asset_notes                 string
    asset_id*                   integer($int64)
    ip_address                  string
    domain_name                 string
    asset_criticality           string
    image_tags
                                    [string]
    image_platform_arch_features
                                    [string]
                                description: An array of strings, each specifying a feature of the architecture.
    image_config_digest         string
    branch                      string
    mac_address                 string
    operating_system_version    string
    image_platform_os_features
                                    [string]
                                description: An array of strings, each specifying a mandatory OS feature.
    asset_name                  string
    asset_users
                                    [string]
    ip_address_secondary
                                    [string]
    repo_url                    string
    parent_host_id              string
                                If the asset is a container or web application, this identifies the host it is deployed on

    image_secondary_registries
                                    [string]
    image_distro                string
    image_config                string
    asset_type                  string
    owner_team
```

AssetTeamData `{`

```
                                    description:  Team data returned at asset level

                                    team_id       integer($int64)
                                    team_name     string
                                }
    image_repo                  string
    asset_info
                                    {
                                    description:  Array object of asset matching info that contains detailed keys for this asset
                                                  in “Key:value” format

                                }
    image_platform_arch         string
    url                         string
    decommed                    boolean
                                Is the asset decommissioned?

    asset_complianced_score     integer
                                In compliance scope 5=no 10=yes

    image_platform_os           string
    asset_name_secondary
                                    [string]
    asset_groups
                                    [string]
    image_manifest_digest       string
    image_platform_arch_variant string
                                The variant of the CPU architecture of this image.'
}
```

DataExportResponse {

data_type	string	The type of Nucleus contents stored in the file
file_path	string	The path to the file
file_upload_date	string	The date/time the file finished generating and saving
mime_type	string	The mime_type to use when requesting the file download
file_id	integer($int64)	The ID of the file

}

SoftwareResponse {

software_name	string	Name of software including version
assets	[SoftwareResponseAsset {	
host_id	integer($int32)	Asset's Id in Nucleus
os_name	string	Asset's OS Name
host_type	string	Type of Asset
host_name	string	Name of asset
}]		
asset_count	integer($int32)	

}

FindingTrendRemediatedBar [FindingTrendRemediatedBarRecord {...}]

FindingUnique {

finding_discovered*	string	First time this finding was found in this project
finding_severity*	string	
finding_name*	string	
finding_status*	string	
finding_count*	integer($int64)	Number of times this finding shows up across all hosts
scan_date*	string	
finding_exploitable*	integer	0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable
finding_severities	[string	Enum: Array [5]] *description: With instance level severities feature enabled, this includes all unique instance level severities*
scan_type*	string	
issue_open_count	integer($int64)	Number of external issues that are open
issue_closed_count	integer($int64)	Number of external issues that are closed
finding_number*	string	Unique identifier for this finding. It remains consistent across assets and scans for this specific finding.
asset_count*	integer($int64)	

}

Operators string

Enum:

Array [4]

FindingMitigated {

manual_mitigated	boolean	true = mitigated via manual methods and not via scan
finding_discovered	string	

```
    finding_name            string
    total_manual            integer
                            Total instances that were manually mitigated (mitigating status set in Nucleus)

    finding_remediation_days string
    finding_severity        string
    finding_exploitable     string
    finding_severities
                               [string
                            Enum:

                               Array [ 5 ]
                            ]
                            description: With instance level severities feature enabled, this includes all unique instance level
                            severities
    finding_remediated_date string
    scan_type               string
    total_mitigated         integer
                            Total mitigated instances, including manual and scan mitigated

    total_open              integer
                            Total open instances, if any

    finding_number          string
}
```

Framework {

```
    framework_name* string
}
```

Date string

```
pattern: ^\d{4}-\d{2}-\d{2}$
Format must be YYYY-MM-DD
```

FindingsTopRiskList {

```
    finding_discovered*             string
    finding_id*                     integer($int64)
    finding_cve*                    string
    mandiant_zero_day               string
    finding_exploitable*            string
    finding_severity*               string
    finding_package_fix_versions*
                                       [

                                    Could not render this component, see the console.

                                    ]
    finding_package_version*        string
    mandiant_vulnerable_products    string
    finding_iava*                   string
    mandiant_analysis               string
    asset_id*                       string
    finding_justification_key*      string
    scan_id*                        integer($int64)
    finding_port*                   string
    mandiant_fix_urls
                                       [string]
    justification_external_issues*  string
    cisa_vulnerability_name         string
    justification_assigned_teams*   string
    finding_result*                 string
    finding_path*                   string
    justification_has_file*         string
    mandiant_attacking_ease         string
    epss_score                      number
                                    multipleOf: 0.01
    finding_severity_adjusted*      string
    mandiant_risk_rating            string
    finding_name*                   string
    mandiant_threat_actors
                                       [string]
    due_date*                       string
    scan_date*                      string
    finding_recommendation*         string
    finding_score*                  integer
                                    Risk score of this specific instance. Max = 1000

    mandiant_exploit_vectors
                                       [string]
    justification_status_name*      string
    mandiant_exploited_by_malware   string
    finding_references*             string
    scan_type*                      string
    asset_name*                     string
    mandiant_mitigations
                                       [string]
    justification_status_mitigating* string
    mandiant_exploit_in_the_wild    string
    justification_text*             string
    finding_description*            string
    ip_address*                     string
    justification_datetime*         string
```

```
    justification_assigned_users*    string
    mandiant_associated_malware
                                        [string]
    mandiant_exploit_rating          string
    mandiant_exploitation_consequence string
    finding_package*                 string
    finding_output*                  string
    finding_number*                  string
}
```

JobRequest {

```
    status          string
                    Only get jobs with a certain status

                    Enum:

                        Array [ 5 ]
    start*          integer($int64)
    worker_type     string
                    Only get jobs with a certain worker_type

    limit           integer($int64)
                    minimum: 1
                    maximum: 100
                    If not included 1 is used. Maximum is 100

    include_archive boolean
                    Include archived jobs in the response. Default is no

}
```

TeamData {

```
    description:  Data returned for a specific team, including members

    project_id    integer($int64)
    team_id       integer($int64)
    asset_groups
                     [integer($int64)
                  tag_id

                  ]
    team_name     string
    users
                     [UserData    {
                     description:  Data specific to a user aka user metadata

                     lname         string
                     username      string
                     user_id       integer($int64)
                     fname         string
                   }]
}
```

BulkResponse {

```
    msg           string
    job_id        integer($int32)
                  Job Id of bulk request. Use jobs api to get status

}
```

AssetResult {

```
    description:  Data returned for success dealing with an asset

    asset_id      integer
    success       boolean
}
```

FindingSummaryRecord {

```
    finding_discovered*              string
                                     First time this finding was found in this project

    finding_severity*                string
    finding_name*                    string
    finding_status*                  string
    finding_count*                   integer($int64)
                                     Number of times this finding shows up across all hosts

    scan_date*                       string
    finding_exploitable*             integer
                                     0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable

    finding_severities
                                        [string
                                     Enum:

                                        Array [ 5 ]
                                     ]
```

```
                                description: With instance level severities feature enabled, this includes all unique
                                instance level severities
    scan_type*                  string
    issue_open_count            integer($int64)
                                Number of external issues that are open

    issue_closed_count          integer($int64)
                                Number of external issues that are closed

    finding_number*             string
                                Unique identifier for this finding. It remains consistent across assets and scans for this
                                specific finding.

    asset_count*                integer($int64)
    asset_fixed_count           integer($int64)
                                Fixed assets will be marked as active if a new scan comes in with this finding on the same
                                asset.

    finding_iava                string
    asset_mitigated_count       integer($int64)
                                Number of asset findings that have been manually mitigated.

    finding_cve                 string
    mandiant_zero_day           string
    mandiant_attacking_ease     string
    mandiant_threat_actors
                                    [string]
    mandiant_exploited_by_malware string
    mandiant_mitigations
                                    [string]
    mandiant_vulnerable_products string
    mandiant_analysis           string
    mandiant_associated_malware
                                    [string]
    mandiant_exploit_rating     string
    mandiant_exploitation_consequence string
    cisa_vulnerability_name     string
    mandiant_fix_urls
                                    [string]
    mandiant_exploit_vectors
                                    [string]
    epss_score                  number
                                multipleOf: 0.01
    mandiant_exploit_in_the_wild string
    mandiant_risk_rating        string
    finding_statuses
                                    [string]
    finding_pinned              boolean
    finding_severity_score      integer
}
```

Teams [TeamsData {...}]

description: Team

Project {

```
    tracking_method     string
    project_name        string
    project_description string
    project_id*         integer($int64)
    project_groups
                            [string]
    project_org         string
}
```

Report {

```
    created_user_lastname  string
    report_description     string
    report_status          string
    report_name            string
    created_user_firstname string
    created_date           string
    report_file_name       string
    report_id*             integer($int64)
}
```

RiskScoreResponse {

```
    items
                    {
                }
    score           integer($int32)
                    Risk score of project

}
```

FrameworkMap {

description: A key/value map of frameworks and the applicable control

```
    framework_name* string
```

```
}
```

ThreatIntel {

```
   mandiant_zero_day                string
   mandiant_attacking_ease          string
   mandiant_threat_actors
                                       [string]
   mandiant_exploited_by_malware    string
   mandiant_mitigations
                                       [string]
   mandiant_vulnerable_products     string
   mandiant_analysis                string
   mandiant_associated_malware
                                       [string]
   mandiant_exploit_rating          string
   mandiant_exploitation_consequence string
   cisa_vulnerability_name          string
   mandiant_fix_urls
                                       [string]
   mandiant_exploit_vectors
                                       [string]
   epss_score                       number
                                    multipleOf: 0.01
   mandiant_exploit_in_the_wild     string
   mandiant_risk_rating             string
}
```

AssetTeamData {

```
   description:  Team data returned at asset level

   team_id       integer($int64)
   team_name     string
}
```

ScanList [**Scan** {

```
   scan_file_name*              string
   scan_id*                     integer($int64)
   finding_count_medium*        integer($int64)
   finding_count_informational* integer($int64)
   finding_count_high*          integer($int64)
   scan_date*                   string
   scan_description*            string
   finding_count_low*           integer($int64)
   scan_type*                   string
   finding_count_fail*          integer($int64)
   finding_count_warning*       integer($int64)
   finding_count_pass*          integer($int64)
   asset_count*                 integer($int64)
   scan_mitigated*              integer($int64)
   finding_count_critical*      integer($int64)
 }]
```

AssessmentData {

```
   description:                 Data specific to an assessment aka assessment metadata

   assessment_contacts
                                   [   {
                                   contact_email string
                                   contact_name  string
                                   contact_role  string
                                   contact_phone string
                                   contact_title string
                                  }]
   assessment_end               string
   assessment_report_limitations string
   assessment_report_overview   string
   assessment_provider_name     string
   vulns
                                   [   {
                                   uM            integer
                                   uL            integer
                                   tL            integer
                                   tM            integer
                                   uI            integer
                                   uH            integer
                                   tH            integer
                                   tI            integer
                                   uE            integer
                                   tE            integer
                                   tC            integer
                                   uC            integer
                                  }]
   assessment_type              string
   assessment_provider          string
   assessment_activity
                                   [   {
                                   action        string
                                   date          string
                                   user          string
                                  }]
```

```
    assessment_report_intro      string
    assessment_environment       string
    assessment_scope             string
    assessment_status            string
    assessment_start             string
}
```

Scan {

```
    scan_file_name*              string
    scan_id*                     integer($int64)
    finding_count_medium*        integer($int64)
    finding_count_informational* integer($int64)
    finding_count_high*          integer($int64)
    scan_date*                   string
    scan_description*            string
    finding_count_low*           integer($int64)
    scan_type*                   string
    finding_count_fail*          integer($int64)
    finding_count_warning*       integer($int64)
    finding_count_pass*          integer($int64)
    asset_count*                 integer($int64)
    scan_mitigated*              integer($int64)
    finding_count_critical*      integer($int64)
}
```

Datetime string

pattern: ^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}$
Format must be YYYY-MM-DD HH:II:SS

JobList [Job {

```
    status         string
    worker_type    string
    job_id*        integer($int64)
    status_message string
                   The historical run data for this job

    results
                      [JobResult   {
                    }]
    archive        string
 }]
```

ScanFindingsRecord {

```
    finding_discovered*  string
                         First time this finding was found in this project

    finding_severity*    string
    finding_name*        string
    finding_status*      string
    finding_count*       integer($int64)
                         Number of times this finding shows up across all hosts

    scan_date*           string
    finding_exploitable* integer
                         0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable

    finding_severities
                            [string
                         Enum:

                            Array [ 5 ]
                         ]
                         description: With instance level severities feature enabled, this includes all unique instance level
                         severities
    scan_type*           string
    issue_open_count     integer($int64)
                         Number of external issues that are open

    issue_closed_count   integer($int64)
                         Number of external issues that are closed

    finding_number*      string
                         Unique identifier for this finding. It remains consistent across assets and scans for this specific
                         finding.

    asset_count*         integer($int64)
    asset_fixed_count    integer($int64)
                         Fixed assets will be marked as active if a new scan comes in with this finding on the same asset.

    finding_iava         string
    asset_mitigated_count integer($int64)
                         Number of asset findings that have been manually mitigated.

    finding_cve          string
}
```

FindingUpdateForBulk {

asset_id	integer	Optional asset_id to apply status, due date and comment update to. Ignored for severity updates unless instance severity feature enabled.
finding_justification_key	string	Required when asset_id is passed when updating specific asset's value.
user_id	integer	Use /users to get ids of teams
finding_status	string	New status of finding Valid options are from the justification_status_name values returned from GET /projects/{project_id}/findings/mitigationstatuses
due_date	string	Optional due_date to set the due date on a finding number. If asset id and finding justification key are not provided, then all instances will be updated with this due date. If both asset id and finding justification key are provided, then only the due date on that instance will be updated. Format is "YYYY-MM-DD", or an empty string "" to remove the due date.
finding_severity	string	New severity of finding. If instance level severity feature is not enabled asset_id and finding_justification_key will be ignored and update will apply to unique finding Enum: Array [5]
comment	string	Optional comment to add in finding
scan_type	string	Scan Type
change_text	string	Optional comment to add to severity update. Only used for severity updates
team_id	integer	Use /teams to get ids of teams or set null to unassign the team
finding_number	string	Finding Number

}

ConnectorSettings {

roles	[{	
	crossaccountrole	string
	label	string
	}]	

}

Ticketing {

asset_match_type*	string	Enum: Array [2]
connector_project	string	
asset_criteria	[{	
	rule_match_condition*	string Enum: Array [30]
	rule_match_value*	string Enum: Array [3]
	rule_match_qualifier	string Enum: Array [7]
	}]	
	example: List [OrderedMap { "rule_match_condition": "asset_name", "rule_match_value": "host", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition": "ip_address", "rule_match_value": "192.168.1.1", "rule_match_qualifier": "is not" }, OrderedMap { "rule_match_condition": "asset_type", "rule_match_value": List ["Application", "Container", "Container Image", "Host", "Database"], "rule_match_qualifier": "is one of" }, OrderedMap { "rule_match_condition": "asset_tags", "rule_match_value": List ["Group1", "Group2"], "rule_match_qualifier": "is in all of" }]	
vuln_criteria	[{	
	rule_match_condition	string Enum: Array [3]
	rule_match_value	string Enum: Array [3]
	rule_match_qualifier	string Enum: Array [3]
	}]	

```
                    example: List [ OrderedMap { "rule_match_condition": "finding_name", "rule_match_value": "CVE-0000-00000",
                    "rule_match_qualifier": "contains" }, OrderedMap { "rule_match_condition": "finding_exploitable",
                    "rule_match_value": 1, "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition":
                    "finding_severity", "rule_match_value": List [ "Critical", "High", "Medium", "Low", "Informatonal" ],
                    "rule_match_qualifier": "is one of" } ]
    connection_id*  string
    rule_name*      string
    connector_type* string
    issue_priority  string
    issue_type      string
    rule_disabled   integer
                    Enum:

                        Array [ 2 ]
    rule_id*        string
}
```

FindingMitigationStatuses {

```
    justification_status_name      string
    justification_status_mitigating string
}
```

SoftwareResponseAsset {

```
    host_id       integer($int32)
                  Asset's Id in Nucleus

    os_name       string
                  Asset's OS Name

    host_type     string
                  Type of Asset

    host_name     string
                  Name of asset

}
```

SsoTeamMaps [SsoTeamMap {

```
    description:  SSO Team Map Definition

    team_id       integer($int64)
                  The team that will be added or removed from a user if they having a matching sso_object

    project_id    integer($int64)
    sso_description string
                  Optional desription

    sso_object    string
                  The SSO object that must match

    sso_team_map_id integer($int64)
                  Unique Identifier for this SSO Team Map

 }]
description: SSO Team Maps
```

FindingAdd {

```
    finding_http_request          string
                                  For custom_finding_type = Web Application

    finding_additional_information string
                                  Type of finding

    finding_discovered            string
                                  Date finding was discovered. Format: YYYY-MM-DD HH:II:SS

    custom_finding_name*          string
                                  Name of finding, shows in active vulns grid

    custom_finding_type*          string
                                  Type of finding

                                  Enum:

                                      Array [ 4 ]
    finding_url                   string
                                  For custom_finding_type = Web Application

    finding_likelihood            string
    custom_finding_source         string
    finding_mitigated_date        string
                                  Date finding was mitigated, only used when the finding_status is set. Format: YYYY-MM-DD
                                  HH:II:SS

    finding_http_response         string
                                  For custom_finding_type = Web Application

    custom_finding_description    string
    custom_finding_cve            string
```

```
    host_id*                    integer
                                host_id (Asset ID)

    finding_reproduction_steps  string
                                For custom_finding_type = Web Application

    custom_finding_references   string
                                The string should be in JSON format and references are key-value mapped.

    finding_code_snippet        string
                                For custom_finding_type = Code

    finding_service             string
    finding_status              string
                                Accepted Statuses - (Accepted Risk, Active, Duplicate, Exception Granted, Exception Requested,
                                False Positive, Fixed, In Progress, Mitigated, Potential, Waiting For 3rd Party, Waiting For
                                Verification)

    finding_port                string
    custom_finding_severity*    string
                                Severity of finding

                                Enum:

                                    Array [ 5 ]
    custom_finding_likelihood   string
    finding_impact              string
    custom_finding_impact       string
    finding_line_number         string
                                For custom_finding_type = Code

    custom_finding_number*      string
    custom_finding_exploitable  integer
                                1 = finding is exploitable

                                Enum:

                                    Array [ 2 ]
    finding_path                string
    custom_finding_cvss         string
    custom_finding_recommendation string
    finding_output              string
}
```

AssetGroupResponse {

```
    tag_id*       integer
    asset_group*  string
}
```

AssetFindingsRecord {

```
    finding_discovered*         string
                                First time this finding was found in this project

    finding_severity*           string
    finding_name*               string
    finding_status*             string
    finding_count*              integer($int64)
                                Number of times this finding shows up across all hosts

    scan_date*                  string
    finding_exploitable*        integer
                                0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable

    finding_severities
                                    [string
                                Enum:

                                    Array [ 5 ]
                                ]
                                description: With instance level severities feature enabled, this includes all unique
                                instance level severities
    scan_type*                  string
    issue_open_count            integer($int64)
                                Number of external issues that are open

    issue_closed_count          integer($int64)
                                Number of external issues that are closed

    finding_number*             string
                                Unique identifier for this finding. It remains consistent across assets and scans for this
                                specific finding.

    asset_count*                integer($int64)
    asset_fixed_count           integer($int64)
                                Fixed assets will be marked as active if a new scan comes in with this finding on the same
                                asset.

    finding_iava                string
    asset_mitigated_count       integer($int64)
                                Number of asset findings that have been manually mitigated.

    finding_cve                 string
    mandiant_zero_day           string
    mandiant_attacking_ease     string
    mandiant_threat_actors
                                    [string]
```

```
    mandiant_exploited_by_malware    string
    mandiant_mitigations
                                        [string]
    mandiant_vulnerable_products     string
    mandiant_analysis                string
    mandiant_associated_malware
                                        [string]
    mandiant_exploit_rating          string
    mandiant_exploitation_consequence string
    cisa_vulnerability_name          string
    mandiant_fix_urls
                                        [string]
    mandiant_exploit_vectors
                                        [string]
    epss_score                       number
                                     multipleOf: 0.01
    mandiant_exploit_in_the_wild     string
    mandiant_risk_rating             string
    due_date                         string
}
```

JobResult

```
{
}
```

Finding

```
{
    finding_discovered*              string
    finding_id*                      integer($int64)
    finding_cve*                     string
    mandiant_zero_day                string
    finding_exploitable*             string
    finding_severity*                string
    finding_package_fix_versions*
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    finding_package_version*         string
    mandiant_vulnerable_products     string
    finding_iava*                    string
    mandiant_analysis                string
    asset_id*                        string
    finding_justification_key*       string
    scan_id*                         integer($int64)
    finding_port*                    string
    mandiant_fix_urls
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    justification_external_issues*   string
    cisa_vulnerability_name          string
    justification_assigned_teams*    string
    finding_result*                  string
    finding_path*                    string
    justification_has_file*          string
    mandiant_attacking_ease          string
    epss_score                       number
                                     multipleOf: 0.01
    finding_severity_adjusted*       string
    mandiant_risk_rating             string
    finding_name*                    string
    mandiant_threat_actors
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    due_date*                        string
    scan_date*                       string
    finding_recommendation*          string
    mandiant_exploit_vectors
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    justification_status_name*       string
    mandiant_exploited_by_malware    string
    finding_references*              string
    scan_type*                       string
    asset_name*                      string
    mandiant_mitigations
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    justification_status_mitigating* string
    mandiant_exploit_in_the_wild     string
    justification_text*              string
    finding_description*             string
    ip_address*                      string
```

```
    justification_datetime*          string
    justification_assigned_users*    string
    mandiant_associated_malware
                                        [

                                      😱 Could not render this component, see the console.

                                     ]
    mandiant_exploit_rating          string
    mandiant_exploitation_consequence string
    finding_package*                 string
    finding_output*                  string
    finding_number*                  string
}
```

BulkTeamUpdate [**TeamUpdate** {

```
    description:  For updating a team

    team_id       integer
    asset_groups
                     [integer($int64)
                  tag_id

                  ]
                  description: Optional data specific to asset group permissions for the team
    users
                     [    {
                     user_id       integer($int64)
                   }]
 }]
description: For updating teams in bulk
```

AssetGroup {

```
    asset_group*  string
}
```

Issue {

```
    issue_key*          string
    issue_assignee*     string
    finding_count       integer
                        Number of findings with this external issue linked

    finding_severity*   string
    issue_comment*
                           [IssueComment    {
                           comment       string
                           date          string
                           user          string
                         }]
    scan_type*          string
    issue_comment_last* string
    issue_updated*      string
    issue_status*       string
    issue_type*         string
    finding_name*       string
    issue_url*          string
}
```

TeamUpdate {

```
    description:  For updating a team

    team_id       integer
    asset_groups
                     [integer($int64)
                  tag_id

                  ]
                  description: Optional data specific to asset group permissions for the team
    users
                     [    {
                     user_id       integer($int64)
                   }]
}
```

Users [**UserData** {

```
    description:  Data specific to a user aka user metadata

    lname         string
    username      string
    user_id       integer($int64)
    fname         string
 }]
description: Users
```

AssetProcessingModify {

asset_compliance_scope_type	string	Enum: Array [2]
asset_attribute_rule_support_dynamic	string	
asset_attribute_rule_support_team	string	
asset_data_sensitivity*	string	Enum: Array [5]
asset_criticality_type	string	Enum: Array [2]
asset_group_dynamic	string	
asset_data_sensitivity_dynamic	string	
rule_name*	string	
asset_attribute_owner_type	string	Enum: Array [2]
asset_criticality*	string	Enum: Array [5]
rule_disabled	integer	Enum: Array [2]
asset_criticality_dynamic	string	
asset_compliance_scope*	string	Enum: Array [3]
asset_group_type	string	Enum: Array [2]
asset_attribute_owner_dynamic	string	
asset_group*	string	
asset_attribute_rule_owner_team_type	string	Enum: Array [2]
asset_compliance_scope_dynamic	string	
rule_match_type	string	Enum: Array [2]
asset_attribute_owner	string	
asset_attribute_rule_owner_team	string	
asset_attribute_rule_support_team_type	string	Enum: Array [2]
asset_public*	string	Enum: Array [3]
asset_data_sensitivity_type	string	Enum: Array [2]
rule_id	integer	
rule_criteria*	[{	
rule_match_condition*	string	Enum: Array [30]
rule_match_value*	string	
rule_match_qualifier	string	Enum: Array [7]
	}]	
	example: List [OrderedMap { "rule_match_condition": "asset_name", "rule_match_value": "name", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition": "ip_address", "rule_match_value": "192.168.1.1", "rule_match_qualifier": "is not" }, OrderedMap { "rule_match_condition": "operating_system_name", "rule_match_value": "string", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition": "scan_type", "rule_match_value": "string", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition": "connection_id", "rule_match_value": "string", "rule_match_qualifier": "is" }]	
apply_rule	boolean	Setting to true will run the rule immediately after this call. Default = false

}

FindingTrendRemediatetimeLine [**FindingTrendRemediatetimeLineRecord** {

count	integer	
sevs	**FindingTrendRemediatetimeLineRecordSev** {	
High	{	
count	integer	
total	integer	

}

```
                    Critical
                                {
                                count         integer
                                total         integer
                              }
                    Medium
                                {
                                count         integer
                                total         integer
                              }
                    Low
                                {
                                count         integer
                                total         integer
                              }
                  }
   remediate_time integer
   vuln_date_full string
   total          integer
   vuln_date      string
 }]
```

Assessment {

```
   description:     Assessment

   project_id*      integer($int64)
   assessment_data
                    [AssessmentData   {
                    description:                Data specific to an assessment aka assessment metadata

                    assessment_contacts
                                                   [   {
                                                   contact_email string
                                                   contact_name  string
                                                   contact_role  string
                                                   contact_phone string
                                                   contact_title string
                                                 }]
                    assessment_end              string
                    assessment_report_limitations string
                    assessment_report_overview  string
                    assessment_provider_name    string
                    vulns
                                                   [   {
                                                   uM            integer
                                                   uL            integer
                                                   tL            integer
                                                   tM            integer
                                                   uI            integer
                                                   uH            integer
                                                   tH            integer
                                                   tI            integer
                                                   uE            integer
                                                   tE            integer
                                                   tC            integer
                                                   uC            integer
                                                 }]
                    assessment_type             string
                    assessment_provider         string
                    assessment_activity
                                                   [   {
                                                   action        string
                                                   date          string
                                                   user          string
                                                 }]
                    assessment_report_intro     string
                    assessment_environment      string
                    assessment_scope            string
                    assessment_status           string
                    assessment_start            string
                  }]
   parent_project_id integer($int64)
   assessment_name   string
}
```

ApiResponse {

```
   msg          string
   code         integer($int32)
   type         string
}
```

FindingsSearch {

```
   description:             All values except groups can be passed as a string or an array to limit to multiple values. You may
                            also use a wildcard * or % for these fields asset_name, ip_address, finding_cve, finding_name, and
                            team.

   scan_date
                               {
                               operator      Operators      string
                                             Enum:

                                                Array [ 4 ]
```

```
                    datetime      Datetime      string
                                  pattern: ^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}$
                                  Format must be YYYY-MM-DD HH:II:SS

                }
    finding_cve     string
    mandiant
                    {
                    mandiant_zero_day                string
                                                     Enum:

                                                        Array [ 2 ]
                    mandiant_attacking_ease
                                                        [string]
                                                     enum: List [ "Difficult", "Moderate", "Easy", "No Info" ]
                    mandiant_threat_actors
                                                        [string]
                    mandiant_exploited_by_malware    string
                                                     items: OrderedMap { "type": "string" }
                                                     Enum:

                                                        Array [ 2 ]
                    mandiant_mitigations
                                                        [string]
                                                     enum: List [ "Patch", "Unavailable", "Workaround" ]
                    mandiant_vulnerable_products
                                                        [string]
                    mandiant_analysis
                                                        [string]
                    mandiant_associated_malware
                                                        [string]
                    mandiant_exploit_rating
                                                        [string]
                                                     enum: List [ "Wide", "Confirmed", "Available", "Anticipated",
                                                     "No Known" ]
                    mandiant_fix_urls
                                                        [   {
                                                        url           string
                                                        name          string
                                                      }]
                    cisa_vulnerability_name
                                                        [string]
                    mandiant_exploitation_consequence
                                                        [string]
                                                     enum: List [ "Code Execution", "Command Execution", "Denial-
                                                     of-Service", "Denial-of-Service (DoS)", "Information
                                                     Disclosure", "Security Bypass" ]
                    mandiant_exploit_vectors
                                                        [string]
                    epss_score
                                                        {
                                                        operator      Operators      string
                                                                      Enum:

                                                                          Array [ 4 ]
                                                        score         number
                                                     }
                    mandiant_exploit_in_the_wild     string
                                                     Enum:

                                                        Array [ 2 ]
                    mandiant_risk_rating
                                                        [string]
                                                     enum: List [ "CRITICAL", "HIGH", "MEDIUM", "LOW" ]
                }
    justification_status_name
                        [string]
                    description: Identical to justification_status
    finding_severity    string
    is_active           boolean
                        If true, only the active findings from the latest scan will be returned.

    scan_type           string
    asset_name          string
    user                string
    ip_address          string
    asset_id            integer
    mitigated_date
                        {
                        operator      Operators      string
                                      Enum:

                                          Array [ 4 ]
                        datetime      Date           string
                                      pattern: ^\d{4}-\d{2}-\d{2}$
                                      Format must be YYYY-MM-DD

                    }
    finding_port        string
    justification_status
                        [string]
                    description: Can be a string or array of strings of justification statuses. "Mitigated via Scan" as
                    a justification_status can only be combined with other justification statuses of mitigated
                    findings.
    finding_exploitable string
    asset_groups
                        [string]
    asset_public        string
                        Use “1” to filter publically accessible assets only

    team                string
    finding_name        string
}
```

Job {

status	string
worker_type	string
job_id*	integer($int64)
status_message	string
	The historical run data for this job
results	[JobResult { }]
archive	string

}

AssetAdd {

description:	*Asset data that can be created*
asset_data_sensitivity_score	integer Asset sensitivity 2(Low), 5(Moderate), 7(High) or 10(Critical) Enum: Array [4]
operating_system_name	string
image_manifest	string
active	boolean set to false to deactivate a host.
asset_location	string
support_team	string
asset_match_name	string 'Value used to determine if asset matches scan. Must be included to update a non-custom asset_name'
image_registry	string
image_platform_os_version	string The version of the operating system which the image is built to run on.
asset_notes	string
ip_address*	string Optional if asset_name is set
domain_name	string
image_tags	[string]
image_platform_arch_features	[string] *description: An array of strings, each specifying a feature of the architecture.*
asset_name_link	integer Must be updated to show the asset_name. Display Name = 0(Asset Match Name)[Default], 1(Asset Name) Enum: Array [2]
image_config_digest	string
branch	string
mac_address	string
operating_system_features	string
operating_system_version	string
image_platform_os_features	[string] *description: An array of strings, each specifying a mandatory OS feature.*
asset_name*	string 'Optional if ip_address is set. In order to change asset_name you must set a value for asset_name and asset_match_name OR change the asset_name_link field to 1'
asset_users	[string]
ip_address_secondary	[string]
asset_criticality	string
repo_url	string
image_secondary_registries	[string]
image_distro	string
image_config	string
asset_type*	string Enum: Array [4]
owner_team	string
image_repo	string

asset_info	{
	description: 'Array object of asset info that contains detailed keys and attributes for this asset in key:value format. Setting key's value to null will remove that key. Numeric keys are not allowed'
	
	}

image_platform_arch	string
decommed	boolean *default: false* set to true to decommission a host. Note this is not valid when creating an asset
asset_complianced_score	integer In compliance scope 5=no 10=yes
image_platform_os	string

```
    asset_public                boolean
    asset_name_secondary
                                   [string]
    asset_groups
                                   [string]
    image_manifest_digest       string
    image_platform_arch_variant string
                                The variant of the CPU architecture of this image.

}
```

AssetGroupMetricsResponse {

```
    resolved_past_sla_pct_7d                    integer
    mttr_critical_7d                            integer
    mttr_7d                                     integer
    past_due_pct_high                           integer
    compliance_pass_count                       integer
    vuln_count                                  integer
    mandiant_exploit_in_the_wild_count_critical integer
    mandiant_zero_day_count_critical            integer
    mandiant_exploit_in_the_wild_count          integer
    vuln_count_critical                         integer
    resolved_past_sla_pct_critical_7d           integer
    churn_pct_high_7d                           integer
    churn_pct_critical_7d                       integer
    avg_age_high                                integer
    churn_pct_7d                                integer
    resolved_past_sla_pct_high_7d               integer
    compliance_fail_pct                         integer
    avg_age_critical                            integer
    mandiant_zero_day_count_high                integer
    vuln_count_high                             integer
    mandiant_zero_day_count                     integer
    risk_score*                                 integer
    mttr_high_7d                                integer
    mandiant_exploit_in_the_wild_count_high     integer
    asset_external_pct                          integer
    past_due_pct_critical                       integer
    compliance_pass_pct                         integer
    asset_count                                 integer
}
```

FindingTrendDiscoveredBar [**FindingTrendDiscoveredBarRecord** {

```
    High          integer
    Medium        integer
    vuln_date     string
    vuln_date_full string
    Critical      integer
    Informational integer
    Low           integer
 }]
```

FindingTrendDiscoveredBarRecord {

```
    High          integer
    Medium        integer
    vuln_date     string
    vuln_date_full string
    Critical      integer
    Informational integer
    Low           integer
}
```

FindingsList [**Finding** {

```
    finding_discovered*             string
    finding_id*                     integer($int64)
    finding_cve*                    string
    mandiant_zero_day               string
    finding_exploitable*            string
    finding_severity*               string
    finding_package_fix_versions*
                                       [
                                    Could not render this component, see the console.
                                    ]
    finding_package_version*        string
    mandiant_vulnerable_products    string
    finding_iava*                   string
    mandiant_analysis               string
    asset_id*                       string
    finding_justification_key*      string
    scan_id*                        integer($int64)
    finding_port*                   string
    mandiant_fix_urls
                                       [
                                    Could not render this component, see the console.
```

```
                                ]
    justification_external_issues*   string
    cisa_vulnerability_name          string
    justification_assigned_teams*    string
    finding_result*                  string
    finding_path*                    string
    justification_has_file*          string
    mandiant_attacking_ease          string
    epss_score                       number
                                     multipleOf: 0.01
    finding_severity_adjusted*       string
    mandiant_risk_rating             string
    finding_name*                    string
    mandiant_threat_actors
                                        [

                                      😱 Could not render this component, see the console.

                                     ]
    due_date*                        string
    scan_date*                       string
    finding_recommendation*          string
    mandiant_exploit_vectors
                                        [

                                      😱 Could not render this component, see the console.

                                     ]
    justification_status_name*       string
    mandiant_exploited_by_malware    string
    finding_references*              string
    scan_type*                       string
    asset_name*                      string
    mandiant_mitigations
                                        [

                                      😱 Could not render this component, see the console.

                                     ]
    justification_status_mitigating* string
    mandiant_exploit_in_the_wild     string
    justification_text*              string
    finding_description*             string
    ip_address*                      string
    justification_datetime*          string
    justification_assigned_users*    string
    mandiant_associated_malware
                                        [

                                      😱 Could not render this component, see the console.

                                     ]
    mandiant_exploit_rating          string
    mandiant_exploitation_consequence string
    finding_package*                 string
    finding_output*                  string
    finding_number*                  string
 }]
```

FindingsTopRiskFilter {

```
   asset_filters
                    [integer
                group_id

                   ]
   finding_filters
                    [    {
                      operator*     string
                                    Enum:

                                       Array [ 10 ]
                      property*     string
                                    Field to filter by

                                    Enum:

                                       Array [ 13 ]
                      value*        string
                                    String value to match operator or Array when operator is “IN” or “NOT IN”

                     }]
}
```

FindingMetrics {

```
   projectmetricsdiscovered90 integer
   projectmetricsknow30       integer
   metric_date                string
   success                    boolean
   projectmetricsremediated30 integer
   projectmetricsremdays180   integer
   projectmetricsdiscovered30 integer
   projectmetricsdiscovered180 integer
   projectmetricsremdays90    integer
   projectmetricsknow180      integer
```

```
    projectmetricsshowknow      boolean
    projectmetricsremediated180 integer
    projectmetricsremediated90  integer
    projectmetricsremdays30     integer
    projectmetricsknow90        integer
}
```

FindingList {

```
    finding_discovered*              string
    finding_discovered_short*        string
    finding_description_adjusted*    string
    finding_severity*                string
    finding_last_seen_short*         string
    mandiant_vulnerable_products     string
    mandiant_analysis                string
    finding_status_fixed*            integer
    mandiant_fix_urls
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    mandiant_zero_day                string
    finding_exploitable*             integer
                                     0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable
    mandiant_attacking_ease          string
    epss_score                       number
                                     multipleOf: 0.01
    mandiant_exploit_in_the_wild     string
    mandiant_risk_rating             string
    finding_name*                    string
    finding_recommendation*          string
    cisa_vulnerability_name          string
    mandiant_exploit_vectors
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    mandiant_threat_actors
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    finding_status_total*            integer
    mandiant_exploited_by_malware    string
    scan_type*                       string
    mandiant_mitigations
                                        [
                                      😱 Could not render this component, see the console.
                                     ]
    display_type*                    string
    finding_recommendation_adjusted* string
    finding_description*             string
    assets*
                                        [FindingAsset {
                                       line_number*                                 string
                                       finding_discovered*                          string
                                       finding_id*                                  integer($int64)
                                       finding_justification_assigned_teams*        string
                                       finding_cve*                                 string
                                       operating_system_name                        string
                                       due_date*                                    string
                                       finding_justification_external_issues_count* integer
                                       finding_severity*                            string
                                       finding_result*                              string
                                       operating_system_version                     string
                                       host_ip*                                     string
                                       finding_package_version*                     string
                                       finding_number*                              string
                                       scan_date*                                   string
                                       asset_id*                                    integer
                                       asset_name*                                  string
                                       finding_justification_assigned_users         string
                                       asset_info                                   string
                                       finding_port*                                string
                                       url*                                         string
                                       finding_package*                             string
                                       finding_name*                                string
                                       finding_package_fix_versions*
                                                                                       [
                                                                                     😱 Could not render this component, see the console.
                                                                                    ]
                                       finding_justification_file_count*            integer
                                     }]
```

```
    mandiant_associated_malware
                                    [
                                      😱 Could not render this component, see the console.
                                    ]
    mandiant_exploit_rating         string
    mandiant_exploitation_consequence string
    finding_severity_adjusted*      string
                                    This will only populate with the original severity if it was manually adjusted
    finding_severities
                                       [string
                                    Enum:
                                       Array [ 5 ]
                                    ]
                                    description: With instance level severities feature enabled, this includes all unique
                                    instance level severities
    finding_last_seen*              string
    finding_status_mitigated*       integer
}
```

FindingOverview {

```
    finding_count_medium        integer($int64)
    finding_vulnerability_score integer($int64)
    finding_count_low           integer($int64)
    finding_count_high          integer($int64)
    finding_count_crithigh      integer($int64)
    finding_count_cve           integer($int64)
    finding_count_iava          integer($int64)
    finding_count_exploitable   integer($int64)
    finding_count_critical      integer($int64)
}
```

AssetVuln {

```
    description:                Asset data including vulnerability information

    finding_count_fail          integer($int64)
    operating_system_name       string
    asset_inactive_date         string
    image_manifest
                                   [string]
    finding_count_low           integer($int64)
    ip_address                  string
    image_platform_arch         string
    finding_count_medium        integer($int64)
    support_team
                                AssetTeamData {
                                   description:  Team data returned at asset level

                                   team_id       integer($int64)
                                   team_name     string
                                }
    image_registry              string
    asset_criticality_score     string
                                Risk attribute that ranks the asset's criticality, out of 10

    asset_id*                   integer($int64)
    scan_date_timestamp         integer
    image_platform_os_version   string
                                The version of the operating system which the image is built to run on.

    asset_name                  string
    asset_criticality           string
                                Human readable version of the asset_criticality_score attribute

    image_tags
                                   [string]
    image_platform_arch_features
                                   [string]
                                description: An array of strings, each specifying a feature of the architecture.
    image_config_digest         string
    branch                      string
    mac_address                 string
    operating_system_features
                                   [string]
    finding_count_critical      integer($int64)
    operating_system_version    string
    scan_date                   string
    finding_count_informational integer($int64)
    finding_count_high          integer($int64)
    image_platform_os_features
                                   [string]
                                description: An array of strings, each specifying a mandatory OS feature.
    asset_data_sensitivity_score string
                                Risk attribute that ranks the asset's data sensitivity, out of 10

    ip_address_secondary
                                   [string]
    repo_url                    string
    active                      boolean
    image_distro                string
    image_config                string
    asset_type                  string
```

```
    image_secondary_registries
                                [string]
    owner_team                  AssetTeamData    {
                                   description:  Team data returned at asset level

                                   team_id       integer($int64)
                                   team_name     string
                                }
    image_repo                  string
    asset_info
                                   {
                                   description:  Array object of asset matching info that contains detailed keys for this asset

                                }
    finding_vulnerability_score integer($int64)
    asset_base_risk_score       string
                                The weighted score of this asset's base risk, taking into account the risk attributes and
                                project weights

    asset_complianced_score     string
                                Risk attribute that determines if the asset is included in compliance audits, out of 10

    image_platform_os           string
    asset_public                string
                                Risk attribute that determines if the asset is public facing or not. 1 = public, 0 = non-public

    business_owners
                                   [string]
    finding_count_pass          integer($int64)
    asset_name_secondary
                                   [string]
    asset_groups
                                   [string]
    image_manifest_digest       string
    image_platform_arch_variant string
                                The variant of the CPU architecture of this image.

}


SsoTeamMapCreate    {
   description:   SSO Team Map Definition for creation and updating

   sso_object     string
                  The SSO object that must match

   sso_description string
                  Optional desription

}


FindingComplianceRecord    {
   finding_discovered*  string
                        First time this finding was found in this project

   finding_severity*    string
   finding_name*        string
   finding_status*      string
   finding_count*       integer($int64)
                        Number of times this finding shows up across all hosts

   scan_date*           string
   finding_exploitable* integer
                        0 = not exploitable, 1 = exploitable, 2 = manually set to exploitable

   finding_severities
                           [string
                        Enum:

                           Array [ 5 ]
                        ]
                        description: With instance level severities feature enabled, this includes all unique instance level
                        severities
   scan_type*           string
   issue_open_count     integer($int64)
                        Number of external issues that are open

   issue_closed_count   integer($int64)
                        Number of external issues that are closed

   finding_number*      string
                        Unique identifier for this finding. It remains consistent across assets and scans for this specific
                        finding.

   asset_count*         integer($int64)
   compliance_frameworks
                           [FrameworkMap    {
                           description:   A key/value map of frameworks and the applicable control

                           framework_name* string
                         }]
                        description: Array of applicable frameworks to this finding. Only populated on compliance call.
   finding_result*      string
}
```

FindingAsset {

line_number*	string
finding_discovered*	string
finding_id*	integer($int64)
finding_justification_assigned_teams*	string
finding_cve*	string
operating_system_name	string
due_date*	string
finding_justification_external_issues_count*	integer
finding_severity*	string
finding_result*	string
operating_system_version	string
host_ip*	string
finding_package_version*	string
finding_number*	string
scan_date*	string
asset_id*	integer
asset_name*	string
finding_justification_assigned_users	string
asset_info	string
finding_port*	string
url*	string
finding_package*	string
finding_name*	string
finding_package_fix_versions*	[😱 *Could not render this component, see the console.*]
finding_justification_file_count*	integer

}

BulkFindingAdd [**FindingAdd** {

finding_http_request	string For custom_finding_type = Web Application
finding_additional_information	string Type of finding
finding_discovered	string Date finding was discovered. Format: YYYY-MM-DD HH:II:SS
custom_finding_name*	string Name of finding, shows in active vulns grid
custom_finding_type*	string Type of finding Enum: Array [4]
finding_url	string For custom_finding_type = Web Application
finding_likelihood	string
custom_finding_source	string
finding_mitigated_date	string Date finding was mitigated, only used when the finding_status is set. Format: YYYY-MM-DD HH:II:SS
finding_http_response	string For custom_finding_type = Web Application
custom_finding_description	string
custom_finding_cve	string
host_id*	integer host_id (Asset ID)
finding_reproduction_steps	string For custom_finding_type = Web Application
custom_finding_references	string The string should be in JSON format and references are key-value mapped.
finding_code_snippet	string For custom_finding_type = Code
finding_service	string
finding_status	string Accepted Statuses - (Accepted Risk, Active, Duplicate, Exception Granted, Exception Requested, False Positive, Fixed, In Progress, Mitigated, Potential, Waiting For 3rd Party, Waiting For Verification)
finding_port	string
custom_finding_severity*	string Severity of finding Enum: Array [5]
custom_finding_likelihood	string
finding_impact	string
custom_finding_impact	string
finding_line_number	string For custom_finding_type = Code

```
    custom_finding_number*        string
    custom_finding_exploitable    integer
                                  1 = finding is exploitable

                                  Enum:

                                     Array [ 2 ]
    finding_path                  string
    custom_finding_cvss           string
    custom_finding_recommendation string
    finding_output                string
  }]
description: For adding findings in bulk
```

UserData {

```
    description:  Data specific to a user aka user metadata

    lname         string
    username      string
    user_id       integer($int64)
    fname         string
}
```

ConnectorSettingsUpdate {

```
    connector_fields
                      {
                     roles
                                  [    {
                                  crossaccountrole string
                                  label            string
                                 }]
                  }
}
```

FindingTrendRemediatedBarRecord {

```
    High          integer
    Medium        integer
    vuln_date     string
    vuln_date_full string
    Critical      integer
    Low           integer
}
```

ScanUploadResponse {

```
    msg           string
    job_id        integer($int32)
                  Job Id of import. Use jobs api to get status

}
```

BulkFindingUpdate [FindingUpdateForBulk {

```
    asset_id                  integer
                              Optional asset_id to apply status, due date and comment update to. Ignored for severity updates
                              unless instance severity feature enabled.

    finding_justification_key string
                              Required when asset_id is passed when updating specific asset’s value.

    user_id                   integer
                              Use /users to get ids of teams

    finding_status            string
                              New status of finding
                              Valid options are from the justification_status_name values returned from GET
                              /projects/{project_id}/findings/mitigationstatuses

    due_date                  string
                              Optional due_date to set the due date on a finding number. If asset id and finding justification
                              key are not provided, then all instances will be updated with this due date. If both asset id and
                              finding justification key are provided, then only the due date on that instance will be updated.
                              Format is "YYYY-MM-DD", or an empty string “” to remove the due date.

    finding_severity          string
                              New severity of finding. If instance level severity feature is not enabled asset_id and
                              finding_justification_key will be ignored and update will apply to unique finding

                              Enum:

                                 Array [ 5 ]
    comment                   string
                              Optional comment to add in finding

    scan_type                 string
                              Scan Type
```

```
    change_text              string
                             Optional comment to add to severity update. Only used for severity updates

    team_id                  integer
                             Use /teams to get ids of teams or set null to unassign the team

    finding_number           string
                             Finding Number

 }]
description: For updating findings in bulk
```

FindingTrendRecord {
}

FindingTrendRemediatetimeLineRecordSev {

```
   High
                  {
                  count        integer
                  total        integer
               }
   Critical
                  {
                  count        integer
                  total        integer
               }
   Medium
                  {
                  count        integer
                  total        integer
               }
   Low
                  {
                  count        integer
                  total        integer
               }
}
```

FindingTrendRemediatetimeBarRecord {

```
   count        integer
   total        integer
   severity     string
                Enum:

                   Array [ 4 ]
   value        integer
}
```

TeamCreate {

```
   description:  For creating a team

   team_name    string
   asset_groups
                   [integer($int64)
                tag_id

                ]
                description: Optional data specific to asset group permissions for the team
   users
                   [   {
                   user_id      integer($int64)
                 }]
}
```

FindingTrend {

```
   vulnRemediatedBar
```

FindingTrendRemediatedBar [**FindingTrendRemediatedBarRecord** {

```
      High          integer
      Medium        integer
      vuln_date     string
      vuln_date_full string
      Critical      integer
      Low           integer
   }]
   vulnRemediatetimeLine
```

FindingTrendRemediatetimeLine [**FindingTrendRemediatetimeLineRecord** {

```
      count         integer
      sevs
```

FindingTrendRemediatetimeLineRecordSev {

```
         High
                        {
                        count        integer
                        total        integer
                     }
         Critical
                        {
                        count        integer
                        total        integer
                     }
```

```
                                    Medium
                                      {
                                      count         integer
                                      total         integer
                                    }
                                    Low
                                      {
                                      count         integer
                                      total         integer
                                    }
                                  }
                    remediate_time integer
                    vuln_date_full string
                    total          integer
                    vuln_date      string
                  }]
    vulnRemediatetimeBar FindingTrendRemediatetimeBar  [FindingTrendRemediatetimeBarRecord  {
                    count          integer
                    total          integer
                    severity       string
                                   Enum:
                                      Array [ 4 ]
                    value          integer
                  }]
    vulnDiscoveredBar FindingTrendDiscoveredBar  [FindingTrendDiscoveredBarRecord  {
                    High           integer
                    Medium         integer
                    vuln_date      string
                    vuln_date_full string
                    Critical       integer
                    Informational  integer
                    Low            integer
                  }]
}
```

SsoTeamMap {

description: *SSO Team Map Definition*

```
    team_id         integer($int64)
                    The team that will be added or removed from a user if they having a matching sso_object

    project_id      integer($int64)
    sso_description string
                    Optional desription

    sso_object      string
                    The SSO object that must match

    sso_team_map_id integer($int64)
                    Unique Identifier for this SSO Team Map

}
```

FindingUpdate {

```
    comment          string
                     Optional comment to add in finding

    due_date         string
                     Optional due_date to set the due date on a finding number. If asset id and finding justification key are not
                     provided, then all instances will be updated with this due date. If both asset id and finding justification
                     key are provided, then only the due date on that instance will be updated. Format is "YYYY-MM-DD".

    team_id          integer
                     Use /teams to get ids of teams or set null to unassign the team

    user_id          integer
                     Use /users to get ids of teams

    finding_status   string
                     New status of finding
                     Valid options are from the justification_status_name values returned from GET
                     /projects/{project_id}/findings/mitigationstatuses

    change_text      string
                     Optional comment to add to severity update. Only used for severity updates

    finding_severity string
                     New severity of finding. If instance severity feature enabled asset_id and finding_justification_key will be
                     ignored and update will apply to unique finding

                     Enum:
                        Array [ 5 ]
}
```

IssueComment {

```
    comment       string
    date          string
    user          string
```

```
}
```

FindingTrendRemediatetimeBar [FindingTrendRemediatetimeBarRecord {

```
   count         integer
   total         integer
   severity      string
                 Enum:
                    Array [ 4 ]
   value         integer
 }]
```

AssetProcessing {

```
   asset_compliance_scope_type           string
                                         Enum:
                                            Array [ 2 ]
   asset_attribute_rule_support_dynamic  string
   asset_attribute_rule_support_team     string
   asset_data_sensitivity*               string
                                         Enum:
                                            Array [ 5 ]
   asset_criticality_type                string
                                         Enum:
                                            Array [ 2 ]
   asset_group_dynamic                   string
   asset_data_sensitivity_dynamic        string
   rule_name*                            string
   asset_attribute_owner_type            string
                                         Enum:
                                            Array [ 2 ]
   asset_criticality*                    string
                                         Enum:
                                            Array [ 5 ]
   rule_disabled                         integer
                                         Enum:
                                            Array [ 2 ]
   asset_criticality_dynamic             string
   asset_compliance_scope*               string
                                         Enum:
                                            Array [ 3 ]
   asset_group_type                      string
                                         Enum:
                                            Array [ 2 ]
   asset_attribute_owner_dynamic         string
   asset_group*                          string
   asset_attribute_rule_owner_team_type  string
                                         Enum:
                                            Array [ 2 ]
   asset_compliance_scope_dynamic        string
   rule_match_type                       string
                                         Enum:
                                            Array [ 2 ]
   asset_attribute_owner                 string
   asset_attribute_rule_owner_team       string
   asset_attribute_rule_support_team_type string
                                         Enum:
                                            Array [ 2 ]
   asset_public*                         string
                                         Enum:
                                            Array [ 3 ]
   asset_data_sensitivity_type           string
                                         Enum:
                                            Array [ 2 ]
   rule_id                               integer
   rule_criteria*
                                            [    {
                                         rule_match_condition* string
                                                               Enum:
                                                                  Array [ 30 ]
                                         rule_match_value*     string
                                         rule_match_qualifier  string
                                                               Enum:
                                                                  Array [ 7 ]
                                          }]
                                         example: List [ OrderedMap { "rule_match_condition": "asset_name", "rule_match_value":
                                         "name", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition":
                                         "ip_address", "rule_match_value": "192.168.1.1", "rule_match_qualifier": "is not" },
                                         OrderedMap { "rule_match_condition": "operating_system_name", "rule_match_value":
                                         "string", "rule_match_qualifier": "is" }, OrderedMap { "rule_match_condition":
                                         "scan_type", "rule_match_value": "string", "rule_match_qualifier": "is" }, OrderedMap
                                         { "rule_match_condition": "connection_id", "rule_match_value": "string",
                                         "rule_match_qualifier": "is" } ]
```

```
}
```