Kenna Armis Integration Mapping

Asset Mapping					
Kenna KDI V2 Field	**Armis Field**	**Armis Field Type**	**Source**	**Comments / Example Values**	**Armis Device Example**
locator_field.external_id	id	int	**"id": 2172,**		
locator_field.ip_address	ipAddress		**"ipAddress": "10.77.27.183"**		
locator_field.ip_address	ipv6		**"ipv6": "fe80::647b:ba0f:9628:6014",**		
locator_field.mac_address	macAddress		**"macAddress": "50:76:AF:D3:3F:AB"**		
locator_field.file, locator_field.hostname, locator_field.ec2, locator_field.netbios, locator_field.url, locator_field.fqdn, locator_field.image_id, locator_field.container_id, locator_field.	NA			Values are not found in armis response.	
application	NA				
priority	priority		**"riskLevel": 5,**	**Risk Level:** The risk level assigned to the device: Low (1-3), Medium (4-7), or High (8-10). **Kenna Description of priority field:** [0..10] Defaults to 10, which is recommended unless you have a documented risk appetite for assets. This field is used to adjust the asset score.	
tags	tags	list	**"tags": ["SCCM", "ServiceNow", "Corporate"],**		
os	operatingSystem		**"operatingSystem": "Windows",**		
os_version	operatingSystemVersion		**"operatingSystemVersion": "10",**		
tags	manufacturer		**"manufacturer": "Lenovo"**		
tags	model		**"model": "ThinkPad X1 Yoga 3rd Gen",**		
tags	name		**"name": "000000731194pc.corporate.acme.com",**		
tags	category		**"category": "Computers",** **"category:Computers"**	**Exmaple values:** "Computers", "Manufacturing Equipment", "Multimedia", "Medical", "Imaging", "Handhelds"	
tags	type	can be null	**Device type will be mapped with tags as "deviceType:{armis-device-type}" like below:** **"deviceType:Laptops"** **"deviceType:Engineering WorkStations"** ...	**Example values:** "Laptops", "Engineering Workstations", "Virtual Assistants", "X-Rays", "PLCs", "CTs", "SCADA Servers", "Infusion Pumps", "IP Cameras", "Servers", "Virtual Machines", "Personal Computers", "Desktops", "Product Scanners"	
asset_type	NA				
	sensor.name		**"sensor": { "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise", "type": "Access Switch" },**		
	sensor.type		**"sensor": { "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise", "type": "Access Switch" },**		
	firstSeen	datetime	**"firstSeen": "2022-03-29T08:00:16.047168+00:00",**		
	lastSeen	datetime	**"lastSeen": "2022-04-19T18:25:15.859450+00:00"**		
	datasources.*.firstSeen	datetime	**"dataSources": [{ "firstSeen": "2021-12-04T05:50:02.246980+00:00" },**		
	datasources.*.lastSeen	datetime	**"dataSources": [{ "lastSeen": "2022-03-23T12:52:06.277289+00:00", },**		
	datasources.*.name	string	**"dataSources": [{ "name": "Active Directory", }**		
	datasources.*.types	list	**"dataSources": [{ "name": "Active Directory", "types": ["Asset & System Management","Identity Provider"] },**		
Vulnerability Mapping					
Kenna KDI V2 Field	**Armis Field**	**Armis Field Type**	**Source**	**Comments / Example Values**	**Armis Vulnerability Example**
scanner_identifier*	cveUid	string	cveUid: "CVE-2019-2949",	Uniquely identifies data coming from a scanner.	
scanner_type*	Default value: Armis	string	Armis	Identifies the scanner the data came from. Paired with scanner_identifier (see above).	
scanner_score*	confidenceLevel	integer	confidenceLevel: "High",	Score given by the scanner. [0..10] Used for scoring in some cases where the Kenna algorithm is not used. Normalized to a Kenna risk score by multiplying x 10. confidenceLevel to scanner_score can be mapped as below: **Confirmed - 10** **High - 8** **Medium - 5** **Low - 3** **Unavailable - No mapping**	
override_score	NA	integer		The risk score [0..100] for an informational vulnerability.	
created_at	firstDetected	string	firstDetected: "2022-03-20T11:07:22.269289+00:00",	ISO8601 timestamp indicating when the vulnerability was first found by the scanner. Defaults to current date if not provided.	
last_seen_at*	lastDetected	string	lastDetected: "2022-03-20T11:07:22.269289+00:00",	ISO8601 timestamp indicating when the vulnerability was last observed.	
last_fixed_on	NA	string		ISO8601 timestamp indicating when the vulnerability was last fixed.	
status*	status	string	status: "Open"	Vulnerability remediation status. Valid values are: "open", and "closed". If skip_autoclose is set to false, open vulnerabilities that already exist in Kenna will be closed and this field changes from "open" to "closed".	
port	NA	integer		Port that the vulnerability is referring to.	
vuln_def_name*	cveUid	string	{scanner_type} {cveId}	The name of the vulnerability definition. The name of the vulnerability definition. Matches the name field in vuln_def section.	


```
{
  "accessSwitch": null,
  "category": "Computers",
  "customProperties": {

  },
  "dataSources": [
    {
      "firstSeen": "2021-12-30T07:36:57.837141+00:00",
      "lastSeen": "2022-04-18T14:39:01.867450+00:00",
      "name": "Active Directory",
      "types": [
        "Asset & System Management",
        "Identity Provider"
      ]
    },
    {
      "firstSeen": "2021-01-03T07:20:24.560885+00:00",
      "lastSeen": "2022-04-18T20:44:45.877450+00:00",
      "name": "CrowdStrike",
      "types": [
        "Agent Based",
        "Endpoint Protection"
      ]
    }
  ],
  "firstSeen": "2022-04-11T16:59:58.360310+00:00",
  "id": 2172,
  "ipAddress": "10.77.27.183",
  "ipv6": "fe80::647b:ba0f:9628:6014",
  "lastSeen": "2022-04-19T18:25:15.859450+00:00",
  "macAddress": "50:76:AF:D3:3F:AB",
  "manufacturer": "Lenovo",
  "model": "ThinkPad X1 Yoga 3rd Gen",
  "name": "000000731194pc.corporate.acme.com",
  "operatingSystem": "Windows",
  "operatingSystemVersion": "10",
  "purdueLevel": 4.0,
  "riskLevel": 5,
  "sensor": {
    "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise",
    "type": "Access Switch"
  },
  "site": {
    "location": "Palo Alto",
    "name": "Palo Alto Enterprise"
  },
  "tags": [
    "SCCM",
    "ServiceNow",
    "Corporate"
  ],
  "type": "Laptops",
  "userIds": [
    7
  ],
  "visibility": "Full"
},
```



```
{
  "confidenceLevel": "High",
  "cveUid": "CVE-2021-1403",
  "deviceId": 1000,
  "firstDetected": "2021-12-19T01:46:31.327009+00:00",
  "lastDetected": "2022-02-03T01:01:26.671300+00:00",
  "matchCriteriaString": "OS:(Cisco IOS XE 16.6.4) ",
  "status": "Open"
}
```

Kenna Armis Integration Mapping

			deviceId: 1,		
			matchCriteriaString: "App:(Java 11.0.4) ",		
Vulnerability Def Mapping					
Kenna KDI V2 Field	**Armis Field**	**Armis Field Type**	**Source**	**Comments / Example Values**	**Armis Vulnerability Example**
scanner_type*	Default value: Armis	string	Armis	Identifies the scanner the data came from. Paired with scanner_identifier to form a unique key (see above).	{ "confidenceLevel": "High", "cveUid": "CVE-2021-1403", "deviceId": 1000, "firstDetected": "2021-12-19T01:46:31.327009+00:00", "lastDetected": "2022-02-03T01:01:26.671300+00:00", "matchCriteriaString": "OS:(Cisco IOS XE 16.6.4) ", "status": "Open" }
cve_identifiers	cveUid	string	cveUid: "CVE-2019-2949",	Comma delimited list with format CVE-000-0000. Only one set of identifiers will be saved per vuln_def.	
wasc_identifiers	NA	string		Comma delimited list with format WASC-00. Only one set of identifiers will be saved per vuln_def.	
cwe_identifiers	NA	string		Comma delimited list with format CWE-000. Only one set of identifiers will be saved per vuln_def.	
name	NA	string	{scanner_type} {cveId}	Title or short name of the vulnerability and is used with scanner_type as a key. This name matches the vul_def_name field in vuln/finding sections.	# search devices
description	NA	string		Full description of the vulnerability. Note: If the value of the field is blank, a blank description is displayed in Kenna. If the field is omitted entirely, a default value of "No description was provided" is substituted. If either a description or name is not provided, the vulnerability is created as a generic "Informational" vulnerability. The substituted value is sufficient to avoid this.	{ "cveUid": "CVE-2021-1403", "description": "A vulnerability in the web UI feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site WebSocket hijacking (CSWSH) attack and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient HTTP protections in the web UI on an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the web UI to follow a crafted link. A successful exploit could allow the attacker to corrupt memory on the affected device, forcing it to reload and causing a DoS condition." }
solution	NA	string		Steps or links for remediation.	