Kenna Armis Integration Mapping

locator_field_in_address in_pAddress in_pAddress in_pAddress in_pAddress in_pVe	Armis Field Type	Asset Mapping Source	Comments / Example Values	Annia Paria Francia
iocator_field.external_id id in pAddress in pAddress in pAddress in pAddress in pAddress in pAddress in pV6 in				Armis Device Example
locator_field.ip_address ip.Address ip.Address ip.G ip.G		"id": 2172.		
locator_field.ip_address ipv6 locator_field.mac_address macAddress locator_field.file; locator_field.hostname, locator_field.ec2, locator_field.setplocator_field.setplocator_field.ec2, locator_field.gdn, locator_field. NA priority priority priority priority priority priority priority priority tags tags s operatingSystem os_version operatingSystemVersion tags manufacturer tags manufacturer tags name tags category tags tags tags t		"ipAddress": "10.77.27.183"		
locator_field.mac_address		"ipv6": "fe80::647b:ba0f:9628:6014",		
locator, field file, locator, field hostname, locator, field ec.2, cottor, field retibus, locator, field durit locator, field fider, locator, field image_id, locator, field container_id, locator, field image_id, locator, field image_id, locator, field container_id, locator, field image_id, locator, field retibus_id, locator_id, locator, field retibus_id, loc		"ipv6": "fe80::647b:ba0f:9628:6014", "macAddress": "50:76:AF:D3:3F:AB"		
licator, field.image_id, locator_field.container_id, NA application NA priority priority priority priority priority tags tags speratingSystem operatingSystemVersion operatingSystemVersion aname tags t	 	macAddress :: "50:76:AF:D3:3F:AB"		
locator, field. application NA priority tags tags tags sos operatings/ystem os_version tags manufacturer tags model tags name tags tags tags tags tags lit os os operatings/ystem/version tags tags tags tags lit os os operatings/ystem/version tags tags tags lit operatings/ystem/version tags tags lit operatings/ystem/version tags tags lit operatings/ystem/version tags tags lit operatings/ystem/version tags lit o				
priority priority tags tags III os operatingSystem operatingSystem operatingSystem operatingSystem operatingSystem operatingSystemVersion tags manufacturer model tags model tags name tags category tags tags tags III tags tags tags III tags tags type c Itags tags tags III tags tags III tags tags tags tags III tags tags tags tags III tags tags tags III tags tags tags tags tags tags tags tags			Values are not found in armis response.	
priority priority tags tags III os operatingSystem operatingSystem operatingSystem operatingSystem operatingSystem operatingSystemVersion tags manufacturer model tags model tags name tags category tags tags tags III tags tags tags III tags tags type c Itags tags tags III tags tags III tags tags tags tags III tags tags tags tags III tags tags tags III tags tags tags tags tags tags tags tags				
tags tags li os operatingSystem os_version operatingSystemVersion tags manufacturer tags model tags name tags category tags tags li sags tags li sags tags li sasset_type NA sensor.name sensor.type firstSeen d datasources.*.firstSeen d datasources.*.firstSeen d datasources.*.name s			Risk Level: The risk level assigned to the device: Low (1-3), Medium (4-7), or High (8-10).	{ "accessSwitch": null,
tags tags li os operatingSystem os_version operatingSystemVersion lags manufacturer lags model lags name lags category tags tags li sags lags li sags lags li saset_type NA sensor.name sensor.type firstSeen d last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s			Kenna Description of priority field:	"category": "Computers", "customProperties": { "location": "California, US",
os operatingSystem os_version operatingSystemVersion tags manufacturer tags model tags category tags category tags tags tags <t< td=""><td></td><td>"riskLevel": 5,</td><td>[010] Defaults to 10, which is recommended unless you have a documented risk appetite for assets. This field is used to adjust the asset score.</td><td>"accountType": "Corporate"</td></t<>		"riskLevel": 5,	[010] Defaults to 10, which is recommended unless you have a documented risk appetite for assets. This field is used to adjust the asset score.	"accountType": "Corporate"
os operatingSystem os_version operatingSystemVersion tags manufacturer tags model tags category tags category tags tags tags <t< td=""><td></td><td>"tags": ["SCCM", "ServiceNow".</td><td></td><td>"dataSources": [{</td></t<>		"tags": ["SCCM", "ServiceNow".		"dataSources": [{
os_version operatingSystemVersion tags manufacturer tags model tags name tags category tags type c c tags type c c c tags tags li sesset_type NA c sensor.name sensor.hype firstSeen d tast_seen_time lastSeen d datasources.*.firstSeen d d datasources.*.lastSeen d datasources.*.name s	list	"Corporate"		"firstSeen": "2021-12-30T07:36:57.837141+00:00", "lastSeen": "2022-04-18T14:39:01.867450+00:00", "name": "Active Directory",
os_version operatingSystemVersion tags manufacturer tags model tags name tags category tags type c c category c c c datasources. first Seen datasources. first Seen datasources. first Seen datasources. first Seen datasources. fir		"operatingSystem": "Windows",		"types": [
tegs manufacturer tags model tags name tags category tags tags tags tags tags lags tags lags tags lags lags lags		"operatingSystemVersion": "10",		"types": ["Asset & System Management",
tags model tags name tags category tags type c c saset_type NA sensor.name sensor.type firstSeen d last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"manufacturer": "Lenovo"		"Identity Provider"
tags name tags category tags type c c tags lype c c sensor.name sensor.name last_seen_time d datasources.*.firstSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"model": "ThinkPad X1 Yoga 3rd Gen",		_} ,
tags tags tags tags lit asset_type c sensor.name sensor.name firstSeen d d tast_seen_time tastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"name": "000000731194pc.corporate.acme.com",		{
tags tags lists tags l		"name": "000000731194pc.corporate.acme.com", "category": "Computers",	Exmaple values:	"firstSeen": "2021-01-03T07:20:24.560885+00:00", "lostSeen": "2022-04-49T20:44:45-977450+00:00",
tags tags lists tags l	1 1			"lastSeen": "2022-04-18T20:44:45.877450+00:00", "name": "CrowdStrike",
tags tags li asset_type NA sensor.name sensor.type firstSeen d datasources.*.firstSeen d datasources.*.firstSeen d datasources.*.astSeen d		"category:Computers"	"Computers", "Manufacturing Equipment", "Multimedia", "Medical", "Imaging", "Handhelds"	"types": [
tags tags li asset_type NA sensor.name sensor.type firstSeen d datasources.*.firstSeen d datasources.*.firstSeen d datasources.*.astSeen d		Device type will be mapped with tags as "deviceType:{armis- device-type}" like below:	Example values:	"Agent Based", "Endpoint Protection"
tags tags li asset_type NA sensor.name sensor.type firstSeen d datasources.*.firstSeen d datasources.*.firstSeen d datasources.*.astSeen d	can be null	"deviceType:Laptops" "deviceType:Engineering WorkStations"	"Laptops", "Engineering Workstations", "Virtual Assistants", "X-Rays", "PLCs", "CTs", "SCADA Servers", "Infusion Pumps", "IP Cameras", "Servers", "Virtual Machines", "Personal Computers", "Desktops", "Product Scanners"), }.
Sensor.name		Custom Properties will be mapped with tags in following structure:	r visorali computero i Desirupo i i roduci didililero	"firstSeen": "2022-04-11T16:59:58.360310+00:00", "id": 2172,
Sensor.name		"custome_properties_ <key>:<value>"</value></key>		"ipAddress": "10.77.27.183", "Ipv6": "680::647b:ba0f:9628:6014", "lastSeen": "2022-04-19T18:25:15.859450+00:00",
Sensor.name		Example,		"macAddress": "50:76:AF:D3:3F:AB", "manufacturer": "Lenovo"
Sensor.name		"customProperties": { "location": "California, US", "accountType": "Corporate"		"model": "ThinkPad X1 Yoga 3rd Gen", "name": '000000731194pc.corporate.acme.com", "operatingSystem": "Windows",
Sensor.name		will be mapped to tags as		"operatingSystemVersion": "10", "purdueLevel": 4.0, "riskLevel": 5.
Sensor.name	1 1	 "custom_properties_location:California, US", "custom_properties_account_type:Corporate",		"sensor": { "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise",
sensor.name sensor.type firstSeen d last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s	list			"type": "Access Switch"
sensor.type firstSeen d last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s				}, "site": {
sensor.type firstSeen d last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"sensor": { "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise", "type": "Access Switch"		"location": "Palo Alto", "name": "Palo Alto Enterprise" }.
		}, "sensor": { "name": "PALO_ALTO-IDF04-SW01:Gig1/0/44 Enterprise",		/, "ags": ["SCCM",
last_seen_time lastSeen d datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"type": "Access Switch" },		"ServiceNow", "Corporate"
datasources.*.firstSeen d datasources.*.lastSeen d datasources.*.name s		"firstSeen": "2022-03-29T08:00:16.047168+00:00",		, "type": "Laptops",
datasources.*.lastSeen d datasources.*.name s	datetime	"lastSeen": "2022-04-19T18:25:15.859450+00:00"		"userids": [
datasources.*.lastSeen d datasources.*.name s		"dataSources": [{		7],
datasources.*.name s	datetime	trirstSeen": "2021-12-04T05:50:02.246980+00:00" },		[*] visibility': "Full" }.
datasources.*.name s		"dataSources": [
	datetime	{ "lastSeen": "2022-03-23T12:52:06.277289+00:00", },		
		"dataSources": [{ "name": "Active Directory",		
	string	}		
datasources.*.types li	1 1	"dataSources": ["name": "Active Directory", "types": ["Asset & System Management","Identity Provider"]),		
	1	"		
		Vulnerability Mapping		
	Armis Field Type			Armis Vulnerability Example
		cveUid: "CVE-2019-2949",	Uniquely identifies data coming from a scanner.	
scanner_type* Default value: Armis s	string	Armis	Identifies the scanner the data came from. Paired with scanner_identifier (see above).	

Kenna Armis Integration Mapping

INA	integer	confidenceLevel: "High",	High - 8 Medium - 5 Low - 3 Unavailable - No mapping	{
	integer		The risk score [0100] for an informational vulnerability.	"deviceld": 1000,
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.	"firstDetected": "2021-12-19T01:46:31.327009+00:00", "lastDetected": "2022-02-03T01:01:26.671300+00:00",
lastDetected	string	lastDetected: "2022-03-20T11:07:22.269289+00:00",	ISO8601 timestamp indicating when the vulnerability was last observed.	"matchCriteriaString": "OS:(Cisco IOS XE 16.6.4) ", "status": "Open"
NA	string		ISO8601 timestamp indicating when the vulnerability was last fixed.	
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".	
NA	integer		Port that the vulnerability is referring to.	
cveUid	string	{scanner_type} {cveld}	The name of the vulnerability definition. The name of the vulnerability definition. Matches the name field in vuln_def section.	
		deviceld: 1,		
		matchCriteriaString: "App:(Java 11.0.4) ",		
Armis Field	Armis Field Ty	pe Source	Comments / Example Values	Armis Vulnerability Example
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", "ovelulid": "CVE-2021-1403", "deviceld": 1000, "firstDetected": "2021-12-19T01-46:31.327009+00:00", "lastDetected": "2022-0-203701:01-26:671300+00:00", "matchCriteriaString": "OS:(Cisco IOS XE 16.6.4)", "status": "Open" }
cveUid	string	cveUid: "CVE-2019-2949",	saved per vuln_def.	
NA	string		per vuln_def.	
NA	string		per vuln_def.	
NA	string	{scanner_type} {cveld}	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
NA 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. Stens or links for remediation.	CredUid: "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."
	lastDetected NA status NA cveUid Armis Field Default value: Armis cveUid NA NA NA	lastDetected string NA string Status string NA integer CveUid string Armis Field Armis Field Ty Default value: Armis string NA string NA string NA string NA string NA string NA string	lastDetected string lastDetected: "2022-03-20T11:07:22.269289+00:00", NA string	lastDetected string lastDetected: "2022-03-20T11.07-22.269289+00.00". ISO8601 timestamp indicating when the vulnerability was last observed. NA string lastDetected: "2022-03-20T11.07-22.269289+00.00". ISO8601 timestamp indicating when the vulnerability was last observed. ISO8601 timestamp indicating when the vulnerability was last observed. Iso8601 timestamp indicating when the vulnerability was last observed. Iso8601 timestamp indicating when the vulnerability was last observed. Iso86001 timestamp indicating when the vulnerability was last observed. Iso86001 timestamp indicating when the vulnerability was last observed. Iso86001 timestamp indicating when the vulnerability was last observed. Iso86001 timestamp indicating when the vulnerability was last observed. Iso86001 timestamp indicating when the vulnerability was last observed. If we will not a string is a status. Iso8601 timestamp indicating when the vulnerability was last observed. If either a description is a status will be closed and the field changes from 'open' to 'closed'. If either a description or hand to the vulnerability was last observed. If either a description or hand the vulnerability was last observed. If either a description or hand to status will be closed and the field changes from 'open vulnerability. Was last of the vulnerability was last observed. If either a description or hand the vulnerability is created as a generic informationar vulnerability. The substituted value is sufficient to avoid this.