Query Syntax Cheat Sheet

Syntax	
Rule: <category>.<filter> <operator> <value(s)>	asset.ip = "1.2.3.4"
OR: rule <logical operator> rule	asset.ip = "1.2.3.4" or asset.ip = "2.3.4.5"
Group OR/AND: (rule1 or rule2)	(asset.ip = "1.2.3.4" or asset.ip = "2.3.4.5")
AND: (rule1 and rule2)	(asset.ip = "1.2.3.4" and asset.ip = "2.3.4.5")
NOT: (rule1 and not rule 2)	(asset.ip = "1.2.3.4" and not asset.ip = "2.3.4.5")
Simple OR: <category>.<filter> = "item1, item2"	asset.ip = "1.2.3.4, 2.3.4.5"
Group NOT: rule1 and not (rule2 and rule3)	vuln.status in ["OPEN"] and not (asset.ip = "1.2.3.4" and asset.ip = "2.3.4.5")

Rule Operators	
Equals: <category>.<filter> = <value(s)>	asset.ip = "1.2.3.4"
IN: <category>.<filter> in ["item1", "item2"]	asset.os in ["windows", "mac"]
GT: <category>.<filter> > <value>	vuln.risk_score > 9
GTE: <category>.<filter> >= <value>	vuln.risk_score >= 9
LT: <category>.<filter> < <value>	vuln.risk_score < 9
LTE: <category>.<filter> <= <value>	vuln.risk_score <= 9

Details	
Author	NopSec
Version	1.0
Date	05/15/23

Categories	
Application	app
Artifact	artifact
Asset	asset
Cloud	aws
CMDB	cmdb
Scanner	scanner
Tags	tags
Threat	threat
Vulnerability	vuln

Date Support	
DATE: <filter> = MM/DD/YY	vuln.detected_date = 01/01/23
Older than: <filter> < MM/DD/YY	vuln.detected_date < 01/01/23
or: <filter> <= MM/DD/YY	vuln.detected_date <= 01/01/23
Newer than: <filter> > MM/DD/YY	vuln.detected_date > 01/01/24
or: <filter> >= MM/DD/YY	vuln.detected_date >= 01/01/23

Relative Date Support	
<filter> [>, >=, <, <=] <"[- , +] [#] [y, m, d, h]">	
Older than Today - 6 months	vuln.detected_date < "-6m"
Newer than Today - 3 days	vuln.detected_date > "-3d"
Upcoming, Today + 30 days	vuln.sla_due_date < "+30d"
Today	vuln.last_detected_date > "-0d"

Asset		
asset.criticality	1: Critical, 2: High, 3: Medium, 4: Low, 5: None	number
asset.fqdn	Fully qualified domain name	string
asset.hostname	Scanner Provided Hostname	string
asset.id	NopSec Asset ID	string
asset.instance_grade	NopSec's Risk Grade; A-D	string
asset.instance_score	NopSec's Risk Score; 0-100	number
asset.ip	IPv4 Address	string
asset.mitigating_controls	Does asset have EDR?	boolean
asset.name	Scanner Provided Name	string
asset.netbios	Scanner Provided Netbios	string
asset.os	Scanner Provided OS	string
asset.owner	Scanner Provided Owner	string
asset.type	Infra, Web App, Source Code, Artifact	string
asset.uuid	NopSec unique UUID	string

Vuln		
vuln.base_status	Vuln Status; OPEN or CLOSED	string
vuln.branch_id	Branch ID	string
vuln.component	Vuln Instance Component Location	string
vuln.cvss2_score	CVSS2 Score; 0-10	number
vuln.cvss3_score	CVSS3 Score; 0-10	number
vuln.cve	CVE ID	string
vuln.cwe	CWE ID	string
vuln.celebrity_name	Celebrity Name	string
vuln.detected_date	Date first scanner Detected Vuln	date
vuln.deep_link	Vuln Link to Scanner Reference	string
vuln.exception_type	False Positive or Risk Accepted	string
vuln.finding_type	Scanner Provided Metadata	string
id	NopSec Vuln ID	string
instance_grade	NopSec Vuln Instance Grade; A-D	string
instance_score	NopSec Vuln Instance Score; 0-100	number
location	Vuln Instance Location within Component	string
last_detected_date	Date scanner last detected vuln as Open	date
port	Vuln was found on this port	number
plugin_id	Scanner Provided Plugin ID	string
patch_available	Is Patch Available	boolean
vuln.reopened_date	Vuln was found open again on this date	date
vuln.remediated	Is vuln remediated?	boolean
vuln.remediation_date	Scanner confirmed vuln remedidated date	date
vuln.sla_due_date	SLA Due Date	date
vuln.service	Vuln was found on this service	string
vuln.score	NopSec Risk Score (no asset context); 0-10	number
vuln.serverity	NS Severity (no asset context); U, C, H, M, L	string

Application		
app.branch	Branch Name	string
app.default_branch	Branch is Default	boolean
app.https	App scanned on port 443	boolean
app.repo_host	Repository Host Provider	string
app.repo_owner	Repository Owner / User Name	string
app.repo_url	Repository URL	string
app.repo_type	Repository Type	string
app.repo_name	Repository Name	string

Artifact		
artifact.running	Image on Running Container	boolean
artifact.container	Container Name	string
artifact.version	Container Version	string
artifact.container_type	Container Name	string

Cloud		
aws.ami_id	Image AMI ID	string
aws.ec2_id	EC2 ID	string
aws.ec2_state	EC2 State	string
aws.ec2_type	EC2 Size Type	string
aws.ec2_name	EC2 Name	string
aws.region	Region: us-east1c	string
aws.subnet	Subnet ID	string
aws.vpc	VPC ID	string
aws.zone	Zone: us-east1	string

CMDB		
cmdb.source	CMDB Source	string
cmdb.id	CMDB Source ID	string
cmdb.ip	CMDB IP	string
cmdb.hostname	CMDB Hostname	string
cmdb.fqdn	CMDB FQDN	string
cmdb.domain_name	CMDB Domain Name	string
cmdb.system_name	CMDB System Name	string

Scanner		
scanner	Scanner Product ID	number
scanner.type	Infra, WebApp, Source, Artifact	string

Tags		
tags.key	Tag Category / Key	string
tags.value	Tag Value	string
tags.name	<Category> : <Value>	string

Threat		
threat.internet_facing	Scanner Provided	boolean
threat.cve_threat	Coming soon	boolean
threat.cve_ransomware	Coming soon	boolean
threat.remote_attack	Coming soon	boolean
threat.phishing_attack	Coming soon	boolean
app.lateral_movement	Coming soon	boolean

Vuln Contd.		
vuln.status	NopSec Specific Status	string
vuln.ticket	Vuln Instance Ticket Number	string
vuln.title	Vuln Title	string
vuln.type	Vuln Type	string