Storm Quick Reference - Example Filters	For a complete list of Storm filter operators and additional examples, see the Filtering section of the Storm Reference Guide.	
Type of Filter	**Example**	**Query / Question**
By form	`#rep.feye.fin7 -inet:ipv4`	Show me everything FireEye associates with FIN7 **except for the IPv4 addresses**
By primary property value	`#rep.moz.500 -inet:fqdn=google.com`	Show me the Moz Top 500 domains **except for google.com**
By secondary property	`inet:ipv4#rep.eset.sednit -:asn`	Show me the IPv4s ESET associates with Sednit **that do not have an AS number** (i.e., exclude IPv4s with an AS)
By secondary property value	`inet:ipv4#rep.eset.sednit +:asn=9009`	Show me the IPv4s ESET associates with Sednit **that are part of AS 9009**
By tag	`inet:fqdn#rep.eset.sednit +#cno.infra.ddns`	Show me the FQDNs ESET associates with Sednit **that are dynamic DNS (DDNS) domains**

Filters with Standard (Mathematical) Operators			
Type of Filter	**Comparison Operator**	**Example**	**Query / Question**
Greater than	>	`file:bytes#rep.eset.sednit +:size>60416`	Show me the files ESET associates with Sednit **that are larger than 60416 bytes**
Greater than or equal to	>=	`inet:whois:iprec:country=ua +:created>=2020`	Show me the network WHOIS records for Ukraine **registered during 2020 or later**
Less than	<	`ou:org:loc=fr +:founded<2017`	Show me organizations in France **founded prior to 2017**
Less than or equal to	<=	`inet:whois:rec:fqdn=elaxo.org +:asof<=2016/06/01`	Show me the domain WHOIS records for elaxo.org **observed on or before June 1, 2016**

Filters with Common Extended Operators			
Filter by regular expression	`~=`	`ou:org:loc^=us` **`+:name~=v.*x`**	Show me organizations in the U.S. **whose name contains a string that starts with 'v' followed by 0 or more characters followed by 'x'**
Filter by prefix	`^=`	`ou:org:loc^=us` **`+:name^=vertex`**	Show me organizations in the U.S. **whose name starts with 'vertex'**
Filter by element in array	`*[<operator>]`	`ou:org:loc^=us` **`+:names*[=vertex]`**	Show me organizations in the U.S. **whose names include an exact match for 'vertex'**
		`ou:org:loc^=us` **`+:names*[~=v.*x]`**	Show me organizations in the U.S. **whose names include a string that starts with 'v' followed by 0 or more characters followed by 'x'**
Filter by time / interval	`@=`	`inet:dns:a:fqdn=vertex.link` **`+.seen@=(2020/08/12, 2020/08/26)`**	Show me the DNS A records for vertex.link whose 'seen' window **overlaps with the period August 12, 2020 - August 26, 2020**
		`inet:dns:a:fqdn=vertex.link` **`+.seen@='2021/05/15 04:28'`**	Show me the DNS A records for vertex.link whose 'seen' window **includes May 15, 2021 at 04:28 (UTC)**

Specialized Filters			
Compound filter	`( )` with logical **and** / **or** / **not** *(evaluated in order from left to right)*	`inet:ipv4#rep.eset.sednit` **`+( :loc^=ro or :asn=9009 )`**	Show me the IPv4s ESET associates with Sednit **whose location is in Romania or whose AS is 9009**
		`inet:ipv4#rep.eset.sednit` **`+( :asn=9009 and not ( :loc^=ro or :loc^=cz ) )`**	Show me the IPv4s ESET associates with Sednit **in AS 9009 that are not in Romania or the Czech Republic**
Subquery filter	`{ }` with Storm	`inet:dns:a:fqdn=vertex.link` **`+{ -> inet:ipv4 +:type=unicast }`**	Show me the DNS A records for vertex.link **whose IPv4s are unicast** (i.e., exclude loopback, private, etc.)
		`file:bytes#rep.vt` **`+{ -> it:av:scan:result +:verdict=malicious }<=10`**	Show me the files reported by VirusTotal **that are have 10 or fewer 'malicious' detections**