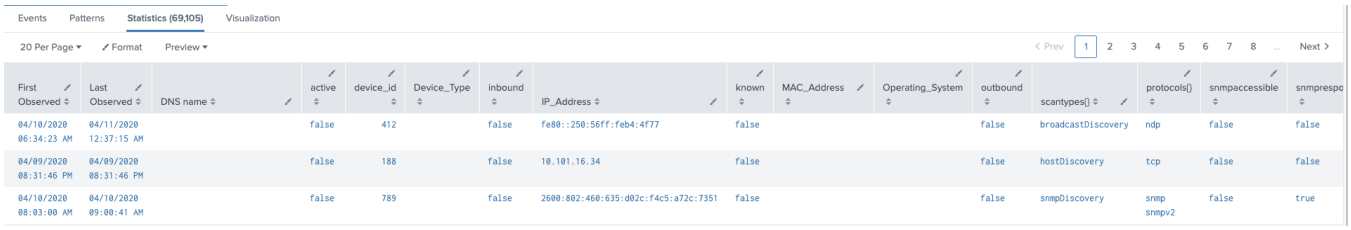
Search Results in Splunk

To view selected syslog data from Lumeta in Splunk:

1. On the Splunk Apps page, select **Lumeta App for Splunk**.
2. Select the Search tab (if you are not there already).
3. Enter your search criteria. Examples follow:
    a. source="tcp:9997"
    b. index=lumeta
    c. sourcetype="lumeta_log_parser"
    d. now combine all 3 into one search
    e. index=lumeta sourcetype="lumeta_log_parser" source="tcp:9997"
    f. index=lumeta sourcetype="lumetaapiparser" *|table "Account ID" "Instance ID" "Public IP Address" Provider numberofinterfaces Name Region securitygroupsids{}{} | where numberofinterfaces not null and Provider not null and Name not null and Region not null| rename securitygroupsids{}{} as securitygroupsids
    g. index=lumeta sourcetype=lumetaapiparser * |table "First Observed" "Last Observed" "DNS name" active device_id Device_Type inbound IP_Address known MAC_Address Operating_System outbound scantypes{} protocols{} snmpaccessible snmpresponder target vendor version zoneid zonename| search "First Observed"=* OR "DNS name"=* OR "Last Observed"=* OR active=* OR device_id=* OR Device_Type=* OR inbound=* OR IP_Address=* OR known=* OR MAC_Address=* OR Operating_System=* OR outbound=* OR scantypes{}=* OR protocols{}=* OR snmpaccessible=* OR snmpresponder=* OR target=* OR vendor=* OR version=* OR zoneid=* OR zonename=*
    h. index=lumeta sourcetype="lumetaapiparser" |table os count time| fields - time
    | where count not null and os not null
    i. index=lumeta sourcetype="lumetaapiparser" * source_name=* | table ip os devicetype dns mac ts
    j. index=lumeta sourcetype="lumetaapiparser" * |table integrationname enabled count ts|where integrationname not nul

Sample Search Results



Events Patterns Statistics (69,105) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

First Observed	Last Observed	DNS name	active	device_id	Device_Type	inbound	IP_Address	known	MAC_Address	Operating_System	outbound	scantypes{}	protocols{}	snmpaccessible	snmpresp
04/10/2020 06:34:23 AM	04/11/2020 12:37:15 AM		false	412		false	fe80::250:56ff:feb4:4f77	false			false	broadcastDiscovery	ndp	false	false
04/09/2020 08:31:46 PM	04/09/2020 08:31:46 PM		false	188		false	10.101.16.34	false			false	hostDiscovery	tcp	false	false
04/10/2020 08:03:00 AM	04/10/2020 09:00:41 AM		false	789		false	2600:802:460:635:d02c:f4c5:a72c:7351	false			false	snmpDiscovery	snmp snmpv2	false	true