**Attributes in Alert dataset**

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Barnyard2 Table Name |
| timestamp | time of when the event was logged | event |
| signature | Signature ID /alert ID | event |
| sig\_name | Signature Name /Alert Name | signature |
| sig\_class\_name | Classification name / Alert Class Name | sig\_class |
| sid | Sensor ID | iphdr |
| cid | Event ID | iphdr |
| ip\_src | Source IP address (32-bit unsigned int) | iphdr |
| ip\_dst | Destination IP address (32-bit unsigned int) | iphdr |
| ip\_ver | IP version | iphdr |
| ip\_hlen | IP Header length | iphdr |
| ip\_tos | IP type-of-service | iphdr |
| ip\_len | IP datagram length | iphdr |
| ip\_id | IP ID | iphdr |
| ip\_flags | IP flags | iphdr |
| ip\_off | IP fragment offset | iphdr |
| ip\_ttl | IP time-to-live | iphdr |
| ip\_proto | IP protocol | iphdr |
| ip\_csum | IP checksum | iphdr |
| sport | TCP & UDP soure port | tcphdr + uphdr |
| dport | TCP & UDP destination port | tcphdr + uphdr |
| seq | TCP sequence number | tcphdr |
| ack | TCP ACK number | tcphdr |
| offload | TCP offset | tcphdr |
| res | TCP reserved | tcphdr |
| csum | TCP checksum | tcphdr |
| win | TCP window | tcphdr |
| urp | TCP urgent pointer | tcphdr |
| udp\_len | UDP length | udphdr |
| icmp\_type | ICMP type | icmp |
| icmp\_code | ICMP code | icmp |
| protocol\_type | Type of Protocol | tcp/udp/icmp |