



---

## A

app\_ids\_stats [5-4](#), [5-11](#), [5-13](#), [5-14](#), [5-16](#), [5-17](#), [5-18](#), [5-20](#), [5-22](#),  
[5-24](#), [5-25](#)  
app\_stats [5-6](#), [5-9](#), [5-10](#)  
application\_info [6-8](#)  
application\_ip\_map [6-6](#)  
application\_tag\_map [6-10](#), [6-11](#)  
audit\_log [3-1](#)

---

## C

compliance\_event [9-2](#)  
connection\_log [7-2](#), [7-19](#)  
connection\_summary [7-16](#)

---

## D

DHCP [2-2](#)  
discovered\_users [8-1](#)

---

## F

file\_event [10-1](#)  
fireamp\_event [3-2](#)

---

## H

health\_event [3-9](#)

---

## I

intrusion\_event [4-2](#)

intrusion\_event\_packet [4-7](#)

---

## N

network\_discovery\_event [6-12](#)  
network settings using DHCP [2-2](#)

---

## R

remediation\_status [9-6](#)  
rna\_host\_protocol [6-32](#)  
rna\_ip\_host\_attribute [6-16](#)  
rna\_ip\_host\_client\_app [6-17](#)  
rna\_ip\_host\_client\_app\_payload [6-20](#)  
rna\_ip\_host\_os [6-29](#)  
rna\_ip\_host\_os\_vulns [6-31](#)  
rna\_ip\_host\_sensor [6-34](#)  
rna\_ip\_host\_service [6-35](#)  
rna\_ip\_host\_service\_banner [6-37](#)  
rna\_ip\_host\_service\_info [6-39](#)  
rna\_ip\_host\_service\_payload [6-43](#)  
rna\_ip\_host\_service\_subtype [6-46](#)  
rna\_ip\_host\_service\_vulns [6-47](#)  
rna\_ip\_host\_third\_party\_vuln [6-49](#)  
rna\_ip\_host\_third\_party\_vuln\_bugtraq\_id [6-50](#)  
rna\_ip\_host\_third\_party\_vuln\_cve\_id [6-52](#)  
rna\_ip\_host\_third\_party\_vuln\_rna\_id [6-54](#)  
rna\_ip\_host\_user\_history [6-61](#)  
rna\_mac\_ip\_map [6-23](#), [6-26](#), [6-28](#), [8-5](#)  
rna\_vuln [6-56](#), [6-57](#)  
rule\_message [4-8](#)

---

## T

tag\_info [6-58](#)

---

## U

url\_categories [6-59](#)

url\_category\_stats [5-26](#)

url\_reputation\_stats [5-27](#)

url\_reputations [6-60](#)

user\_discovery\_event [8-3](#)

user\_ids\_stats [5-29](#)

user\_stats [5-30](#)

---

## W

white\_list\_event [9-7](#)

white\_list\_violation [9-9](#)