BAN-Attacks

Attacks
58,630
1,25,973 Total

Sum of Attack_or_not and count of Attack_or_not. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Numfailedlogins

Fail Logins
154
61 attacked

Sum of Numfailedlogins and sum of Numfailedlogins_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Wrongfrags

Wrong Frags
2,858
2,858 attacked

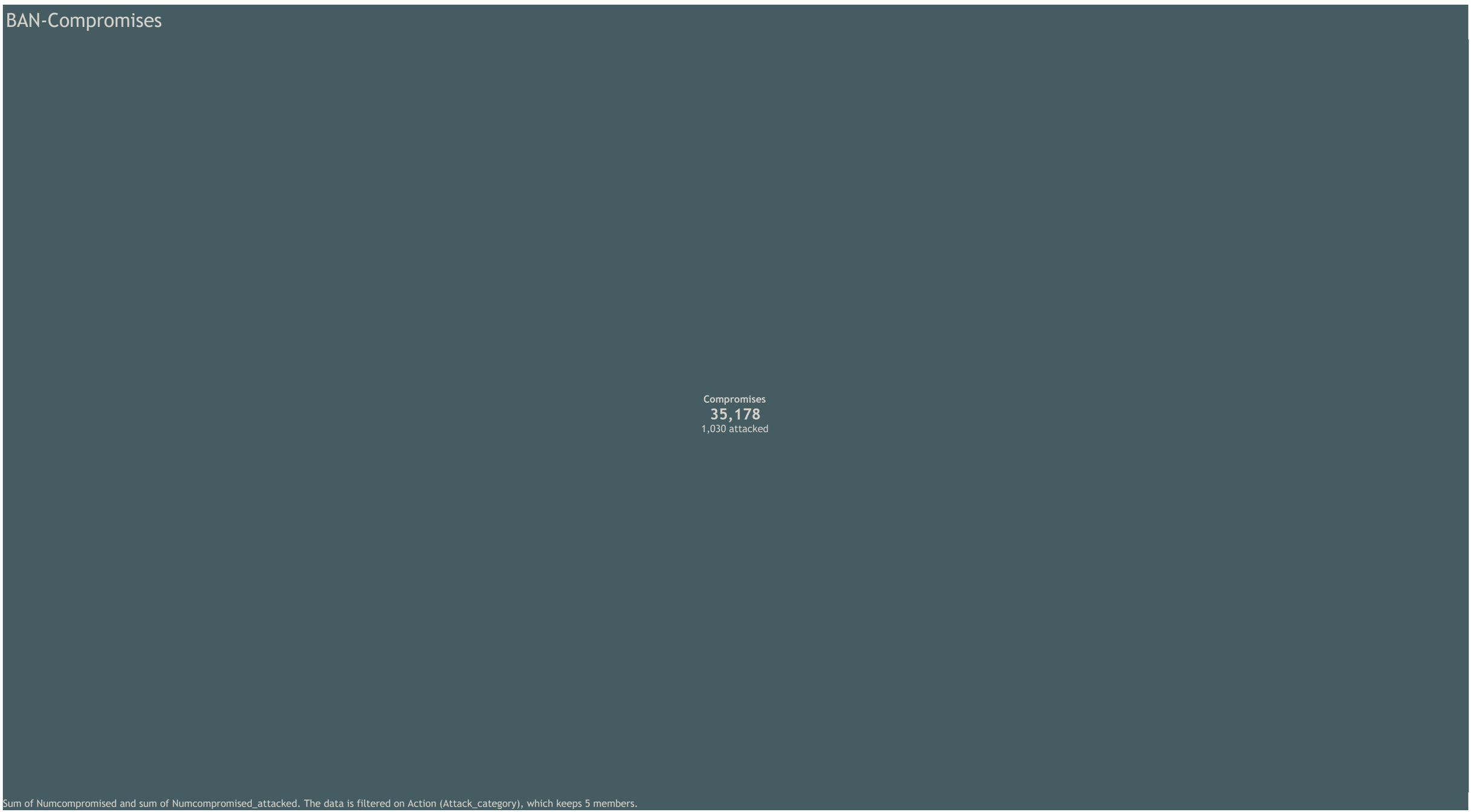
Sum of Wrongfragment and sum of Wrongfragment_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Urgentpkts

Urgent Pkts
14
4 attacked

Sum of Urgent and sum of Urgent_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Compromises



Sum of Numcompromised and sum of Numcompromised_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Numroot

Root Accesses
38,068
159 attacked

Sum of Numroot and sum of Numroot_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Numfilecreations

File Creations
1,596
96 attacked

Sum of Numfilecreations and sum of Numfilecreations_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-HotInds

Hot Inds
25,750
10,217 attacked

Sum of Hot and sum of Hot_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Shellprompts

Shell Prompts
52
11 attacked

Sum of Numshells and sum of Numshells_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Numaccessfiles

Access File Ops
516
11 attacked

Sum of Numaccessfiles and sum of Numaccessfiles_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Dstbytes

Dstbytes
2.49GB
2.20GB attacked

Sum of Dstbytes and sum of Dstbytes_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

BAN-Srcbytes

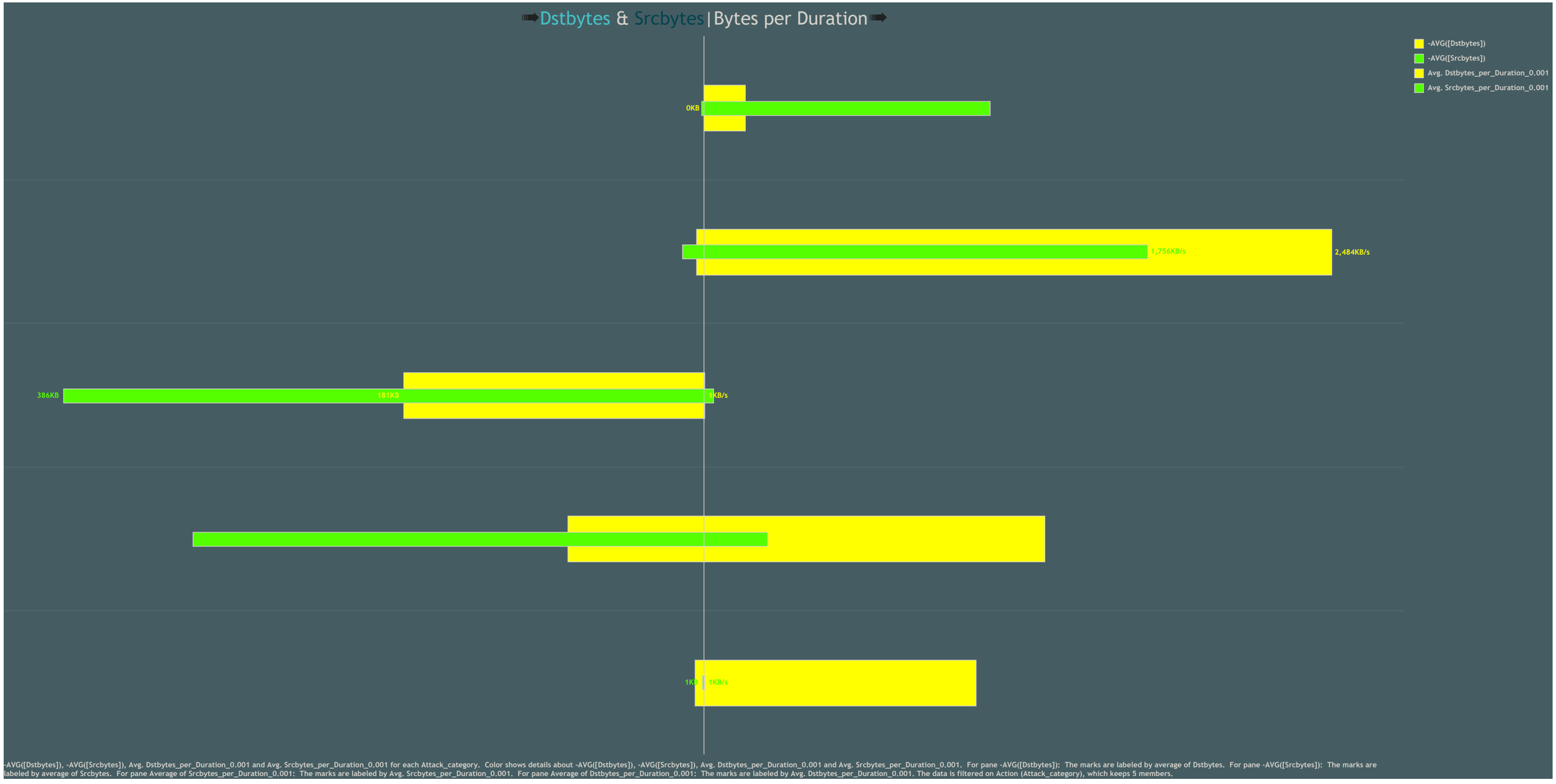
Srcbytes
5.74GB
4.86GB attacked

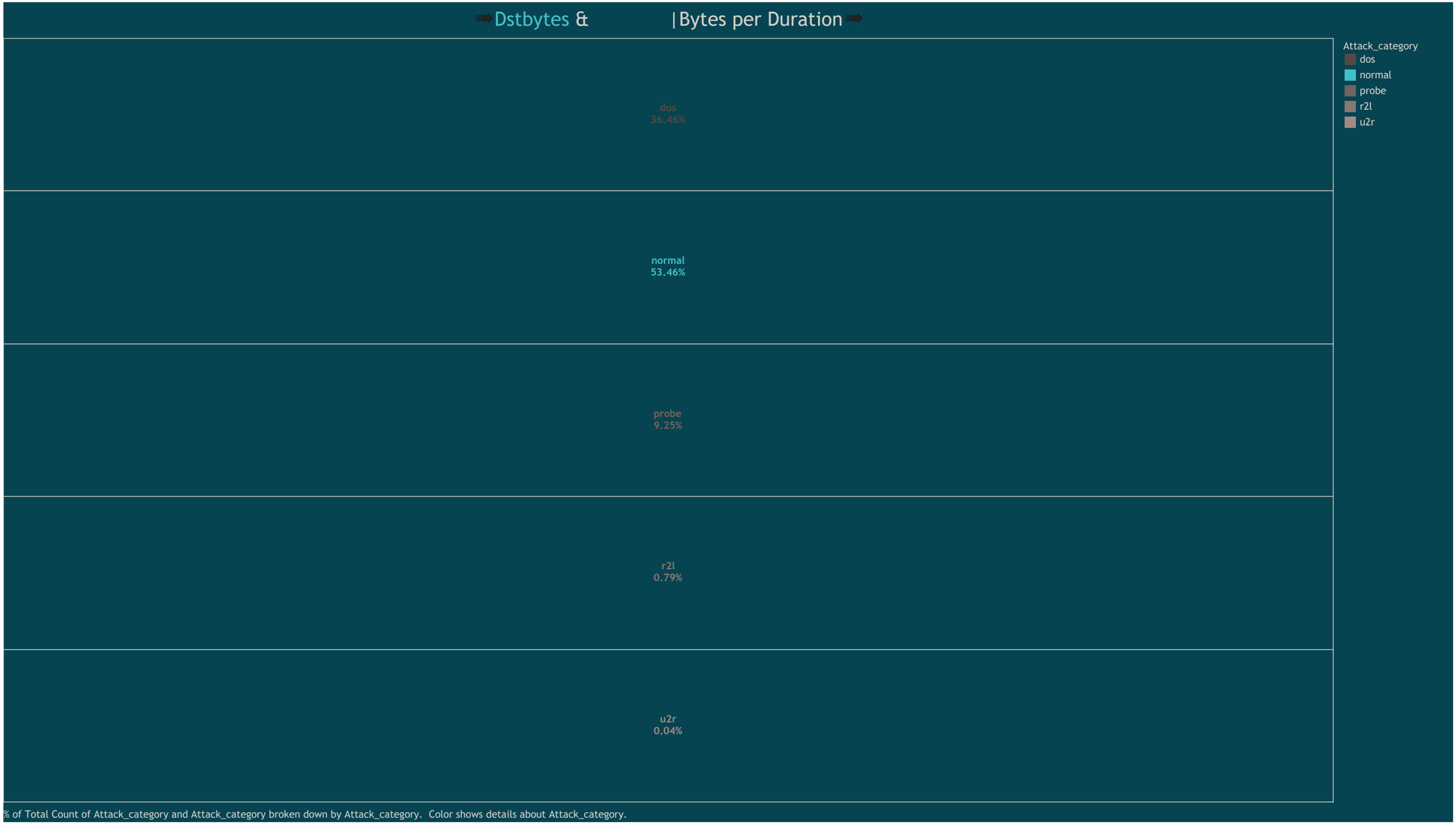
Sum of Srcbytes and sum of Srcbytes_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.

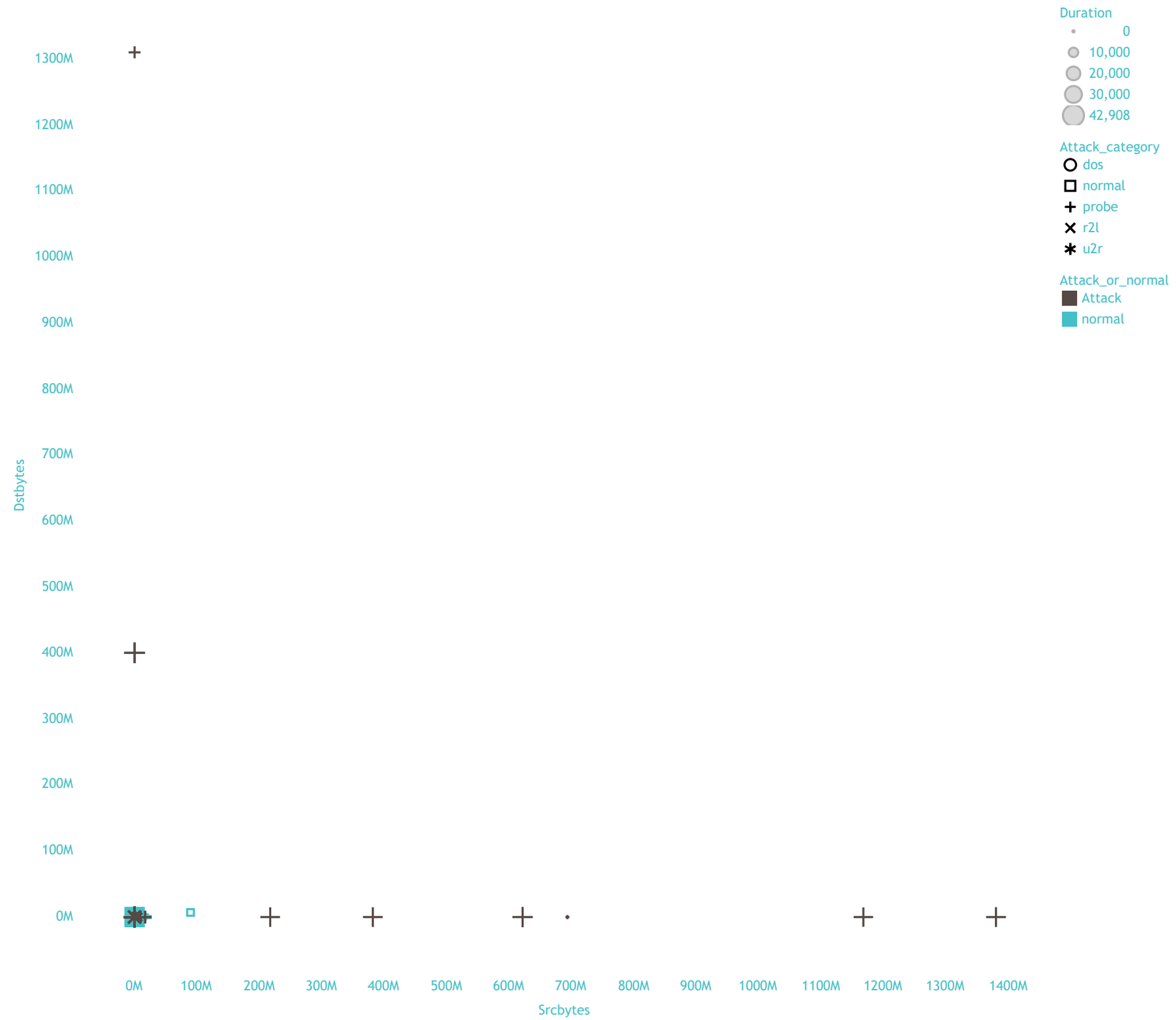
BAN-Duration

Duration
36.17M s
24.82M s attacked

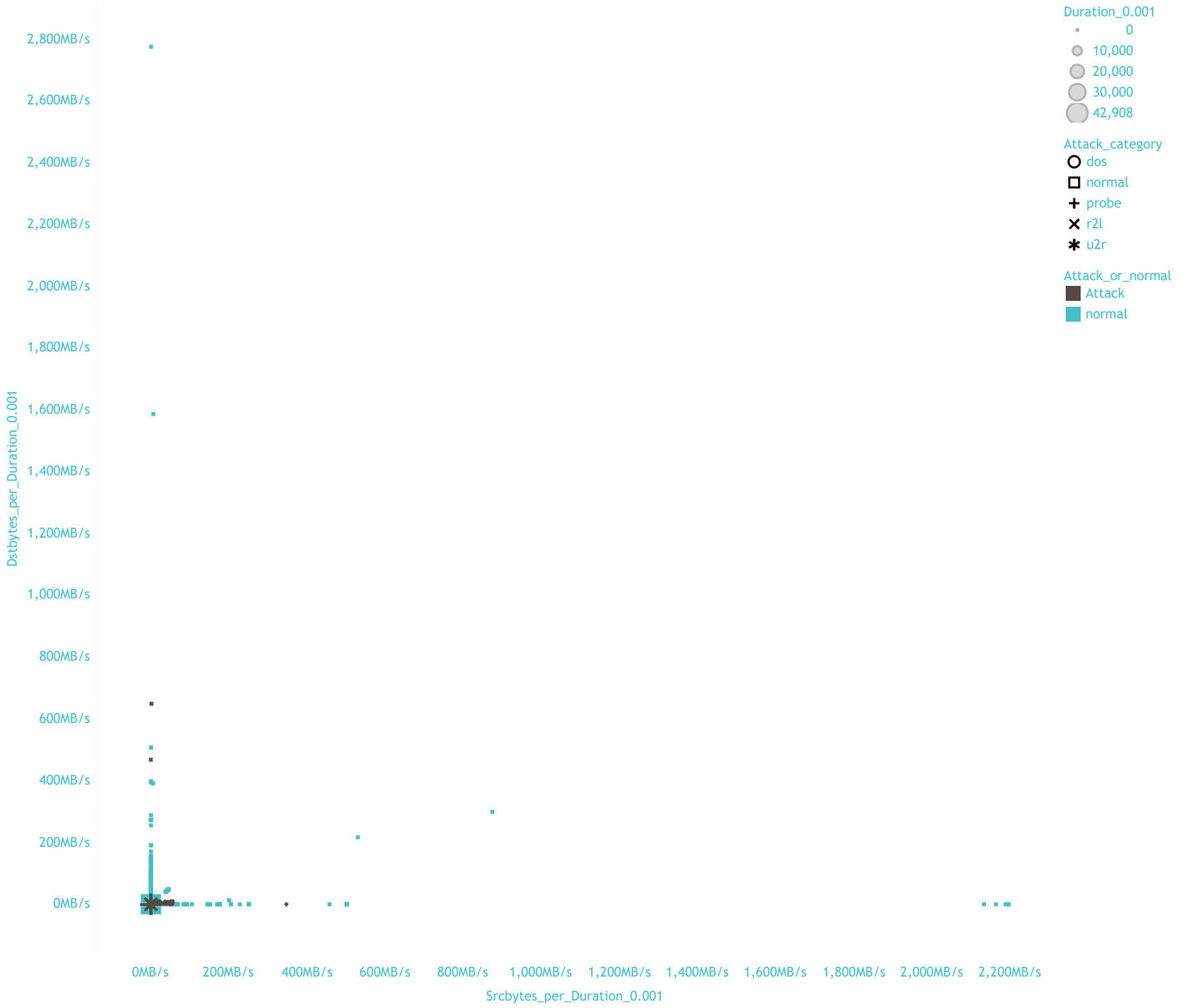
Sum of Duration and sum of Duration_attacked. The data is filtered on Action (Attack_category), which keeps 5 members.


Dstbytes & Srcbytes | Bytes per Duration
-AVG([Dstbytes])
-AVG([Srcbytes])
Avg. Dstbytes_per_Duration_0.001
Avg. Srcbytes_per_Duration_0.001
0KB
1,756KB/s
2,484KB/s
386KB
181KB
1KB/s
1KB
1KB/s
-AVG([Dstbytes]), -AVG([Srcbytes]), Avg. Dstbytes_per_Duration_0.001 and Avg. Srcbytes_per_Duration_0.001 for each Attack_category. Color shows details about -AVG([Dstbytes]), -AVG([Srcbytes]), Avg. Dstbytes_per_Duration_0.001 and Avg. Srcbytes_per_Duration_0.001. For pane -AVG([Dstbytes]): The marks are labeled by average of Dstbytes. For pane -AVG([Srcbytes]): The marks are labeled by average of Srcbytes. For pane Average of Srcbytes_per_Duration_0.001: The marks are labeled by Avg. Srcbytes_per_Duration_0.001. For pane Average of Dstbytes_per_Duration_0.001: The marks are labeled by Avg. Dstbytes_per_Duration_0.001. The data is filtered on Action (Attack_category), which keeps 5 members.

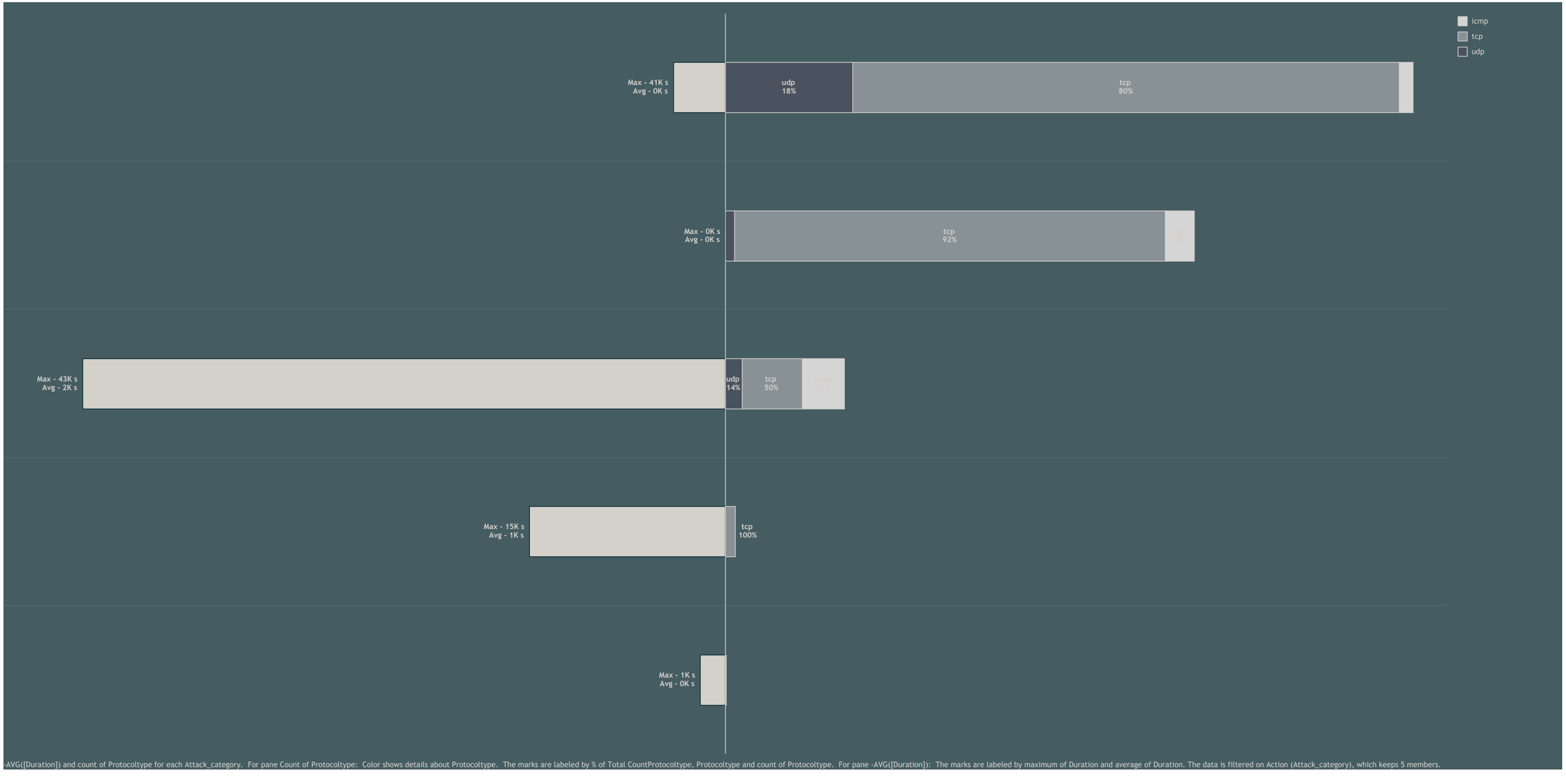

Dstbytes &
Bytes per Duration
Attack_category
dos
normal
probe
r2l
u2r
dos
36.46%
normal
53.46%
probe
9.25%
r2l
0.79%
u2r
0.04%
% of Total Count of Attack_category and Attack_category broken down by Attack_category. Color shows details about Attack_category.



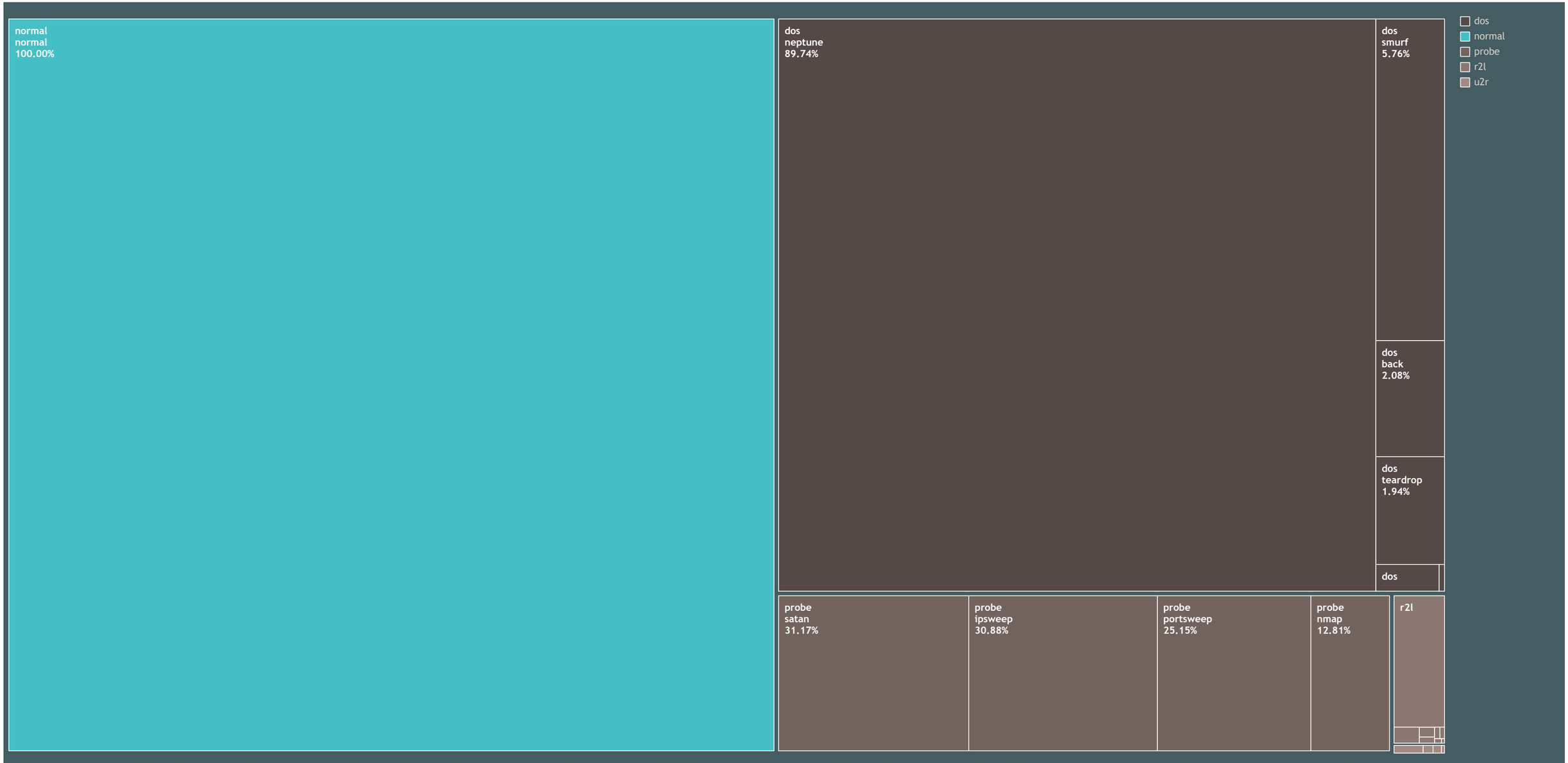
Srcbytes vs. Dstbytes. Color shows details about Attack_or_normal. Size shows Duration. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.



Srcbytes_per_Duration_0.001 vs. Dstbytes_per_Duration_0.001. Color shows details about Attack_or_normal. Size shows Duration_0.001. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.

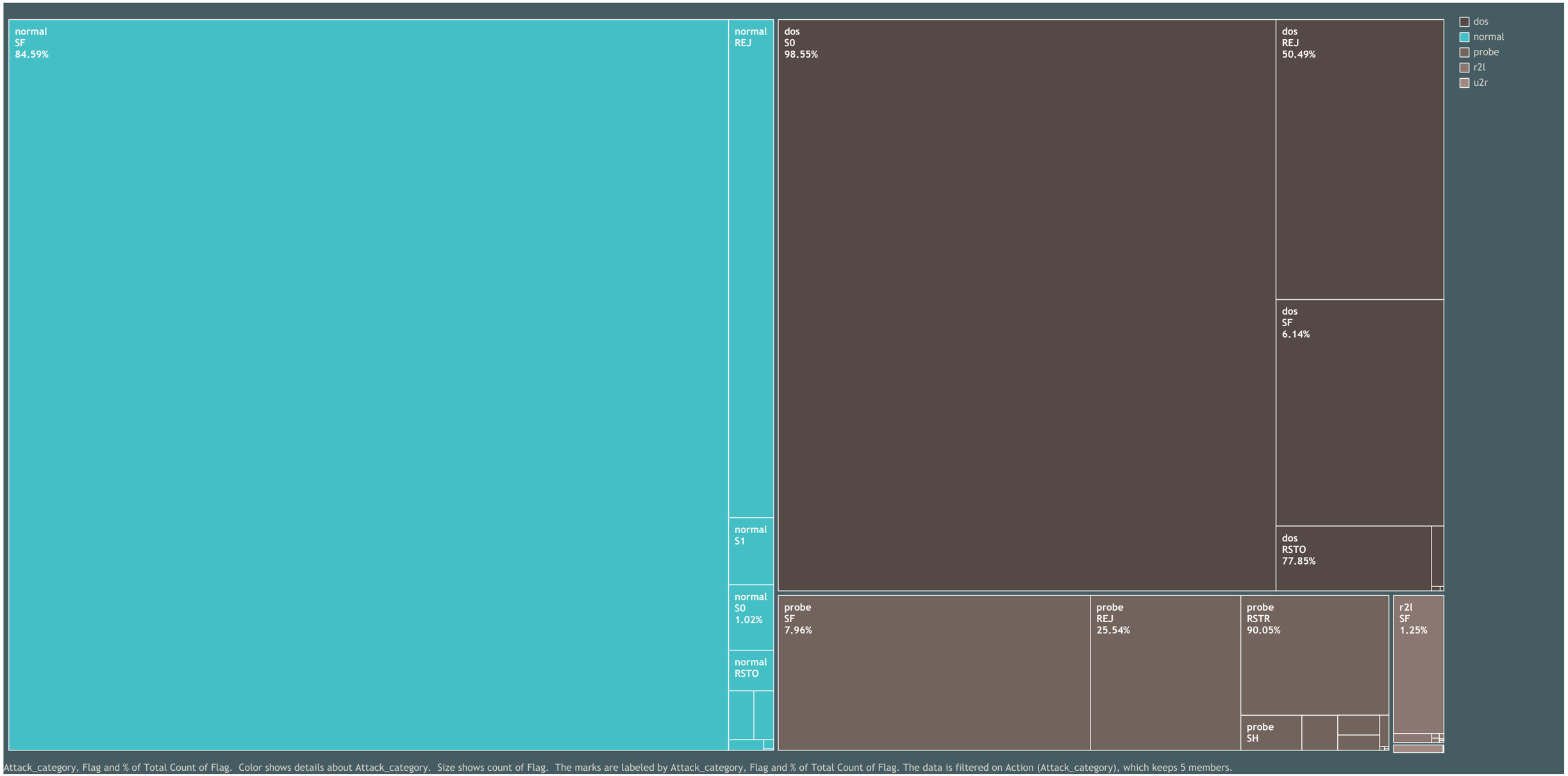


-AVG([Duration]) and count of Protocoltype for each Attack_category. For pane Count of Protocoltype: Color shows details about Protocoltype. The marks are labeled by % of Total CountProtocoltype, Protocoltype and count of Protocoltype. For pane -AVG([Duration]): The marks are labeled by maximum of Duration and average of Duration. The data is filtered on Action (Attack_category), which keeps 5 members.

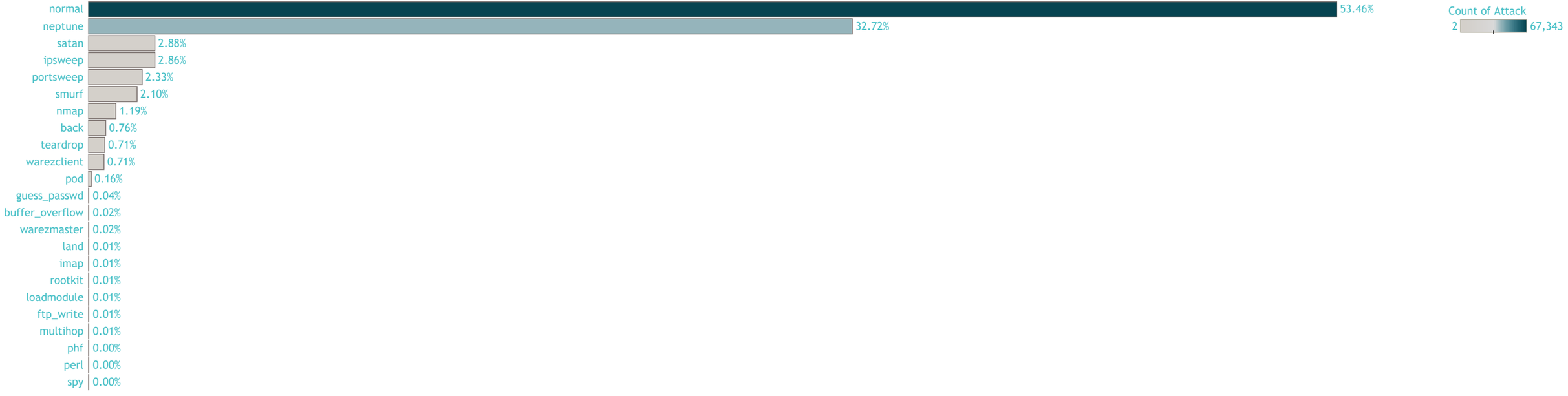


Attack_category, Attack and % of Total Count of Attack. Color shows details about Attack_category. Size shows count of Attack. The marks are labeled by Attack_category, Attack and % of Total Count of Attack. The data is filtered on Action (Attack_category), which keeps 5 members. The view is filtered on Attack_category and Attack. The Attack_category filter keeps dos, normal, probe, r2l and u2r. The Attack filter keeps 23 of 23 members.

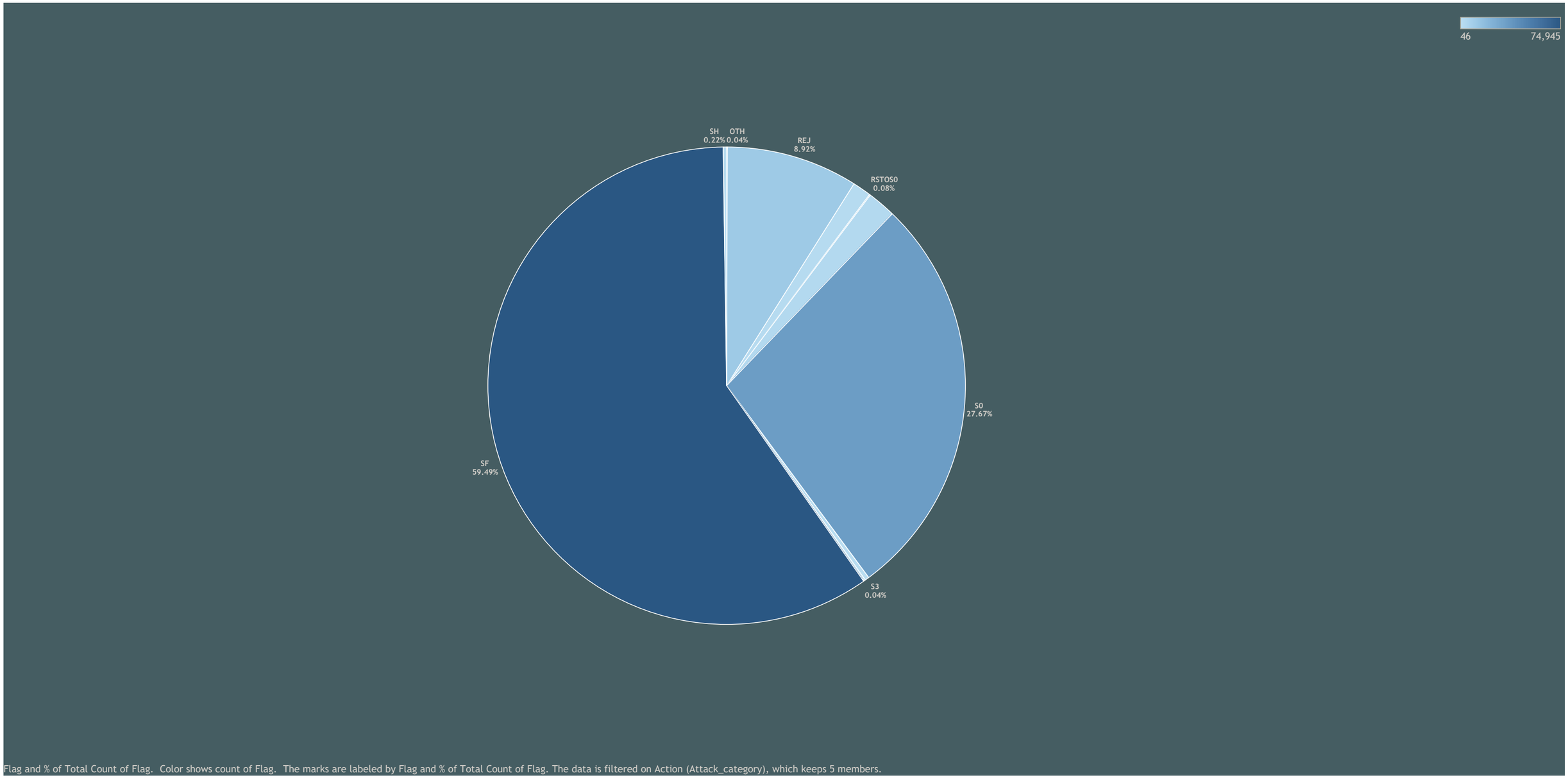
Count of Flag for each Flag. Color shows count of Flag. The marks are labeled by % of Total Count of Flag. The data is filtered on Tooltip (Attack_category,Attack), which keeps 23 members.



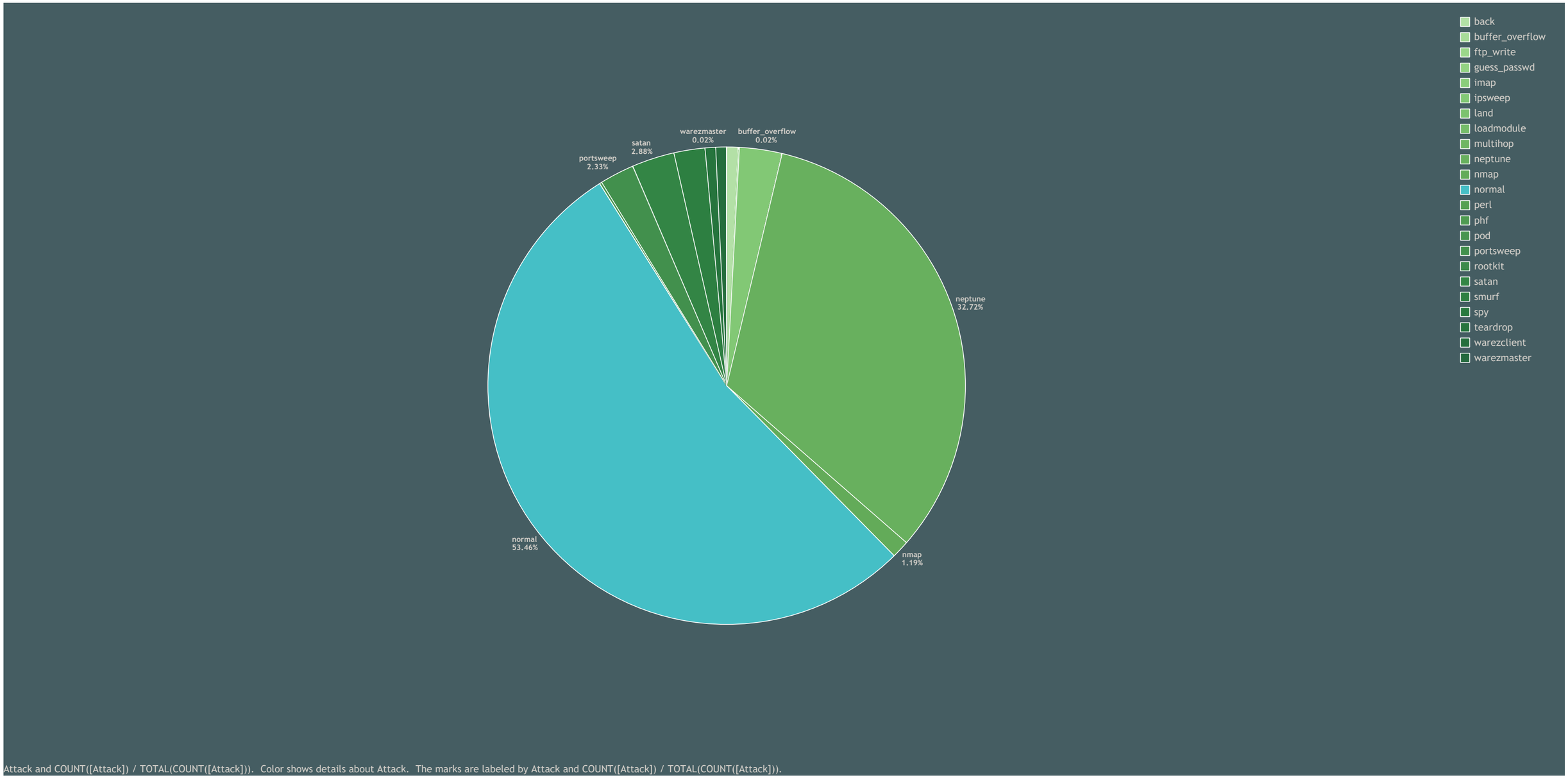
Attack_category, Flag and % of Total Count of Flag. Color shows details about Attack_category. Size shows count of Flag. The marks are labeled by Attack_category, Flag and % of Total Count of Flag. The data is filtered on Action (Attack_category), which keeps 5 members.

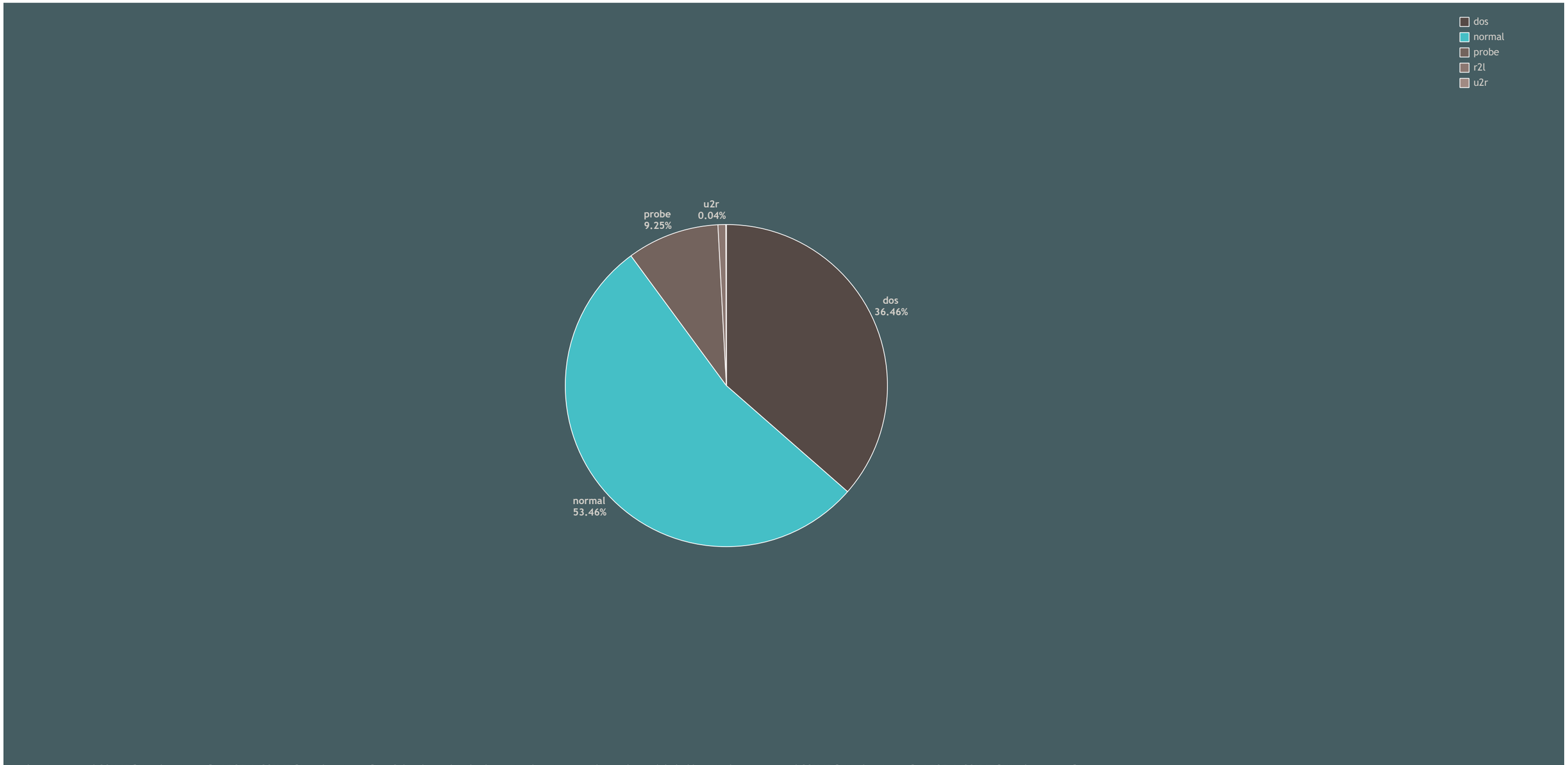


Count of Attack for each Attack. Color shows count of Attack. The marks are labeled by % of Total Count of Attack. The data is filtered on Tooltip (Attack_category,Flag), which keeps 37 members.

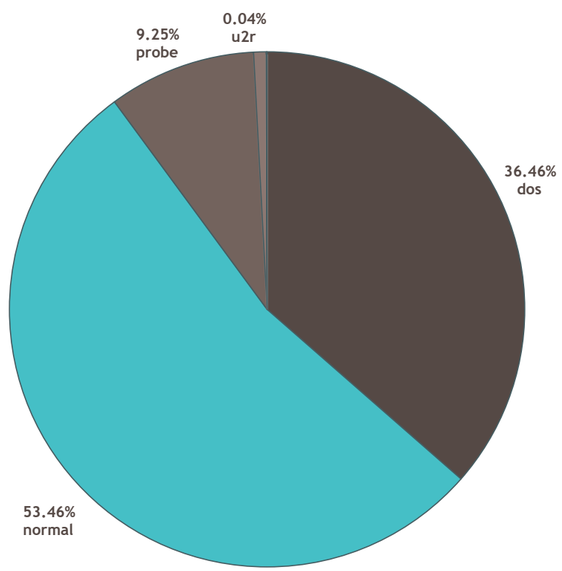


Flag and % of Total Count of Flag. Color shows count of Flag. The marks are labeled by Flag and % of Total Count of Flag. The data is filtered on Action (Attack_category), which keeps 5 members.

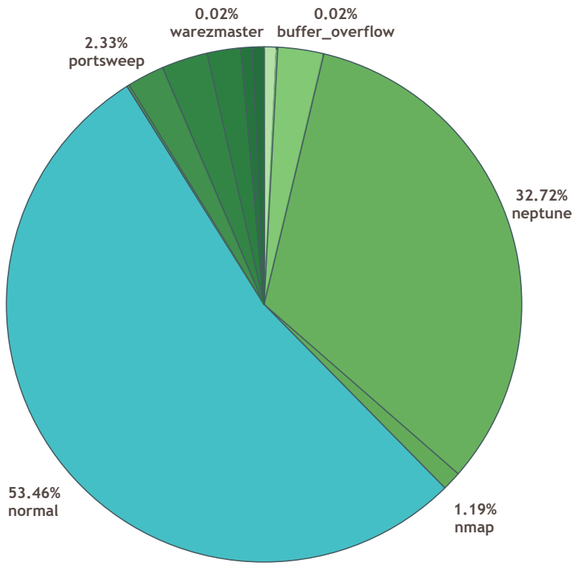

back
buffer_overflow
ftp_write
guess_passwd
imap
ipsweep
land
loadmodule
multihop
neptune
nmap
normal
perl
phf
pod
portsweep
rootkit
satan
smurf
spy
teardrop
warezclient
warezmaster
buffer_overflow
0.02%
warezmaster
0.02%
satan
2.88%
portsweep
2.33%
neptune
32.72%
nmap
1.19%
normal
53.46%
Attack and COUNT([Attack]) / TOTAL(COUNT([Attack])). Color shows details about Attack. The marks are labeled by Attack and COUNT([Attack]) / TOTAL(COUNT([Attack])).



Attack_category and COUNT([Attack_category]) / TOTAL(COUNT([Attack_category])). Color shows details about Attack_category. The marks are labeled by Attack_category and COUNT([Attack_category]) / TOTAL(COUNT([Attack_category])).

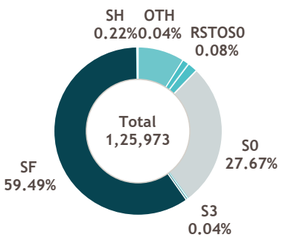


% of Total Count of Attack_category and Attack_category. Color shows details about Attack_category. The marks are labeled by % of Total Count of Attack_category and Attack_category.



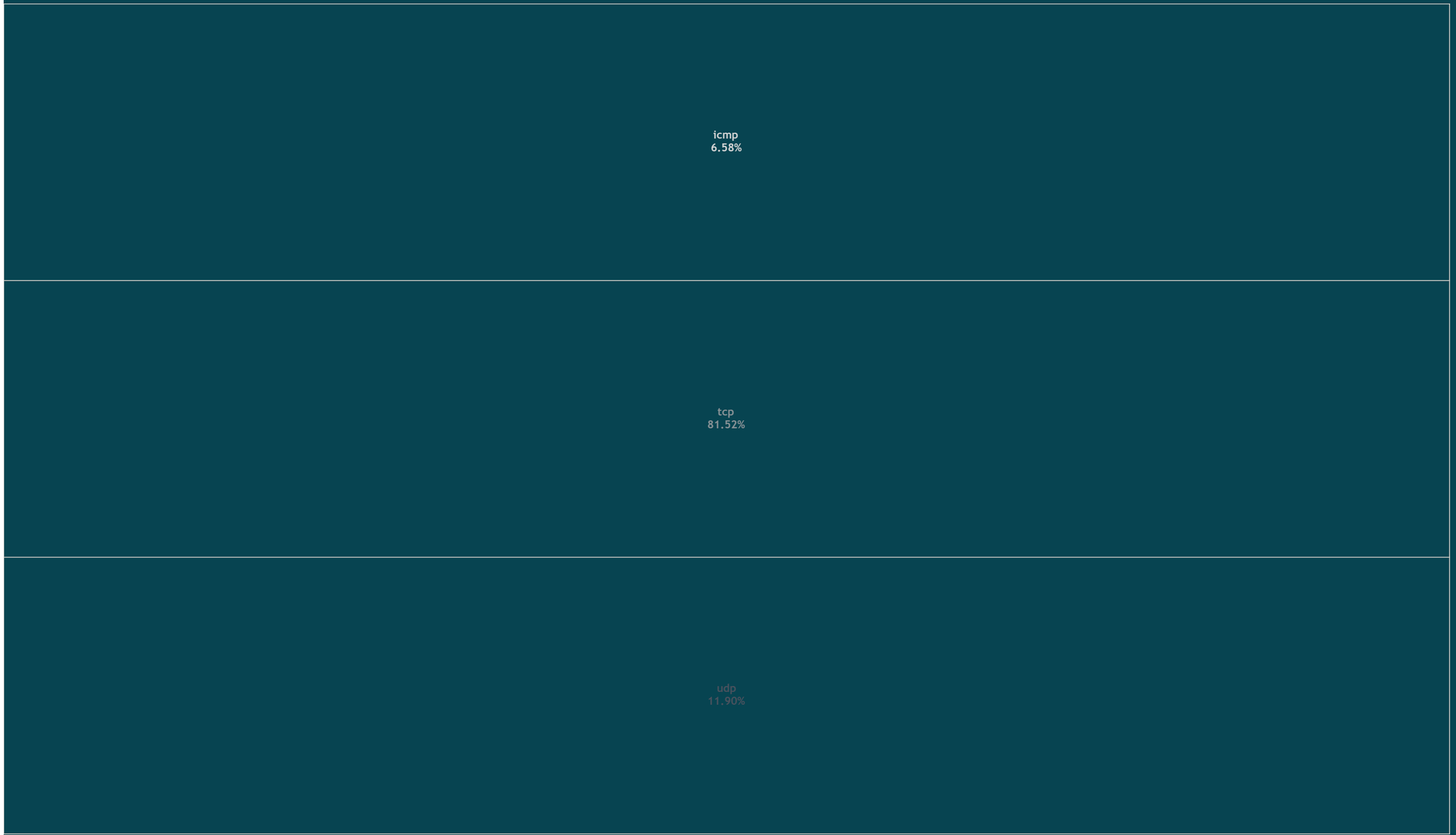
back
buffer_overflow
ftp_write
guess_passwd
imap
ipsweep
land
loadmodule
multihop
neptune
nmap
normal
perl
phf
pod
portsweep
rootkit
satan
smurf
spy
teardrop
warezclient
warezmaster

COUNT([Attack]) / TOTAL(COUNT([Attack])) and Attack. Color shows details about Attack. The marks are labeled by COUNT([Attack]) / TOTAL(COUNT([Attack])) and Attack. The data is filtered on Tooltip (Attack_category,Protocoltype), Tooltip (Attack_category), Tooltip (Flag), Tooltip (Service_category) and Tooltip (Protocoltype). The Tooltip (Attack_category,Protocoltype) filter keeps 12 members. The Tooltip (Attack_category) filter keeps 5 members. The Tooltip (Flag) filter keeps 11 members. The Tooltip (Service_category) filter keeps 8 members. The Tooltip (Protocoltype) filter keeps 3 members.



Avg(0) and Avg(0). For pane Avg(0): Color shows count of Flag. The marks are labeled by Flag and % of Total Count of Flag. For pane Avg(0) (2): The marks are labeled by count of Flag. The data is filtered on Tooltip (Attack_category,Protocoltype), Tooltip (Attack_category), Tooltip (Attack_or_normal,Protocoltype), Tooltip (Attack_or_normal,Service_category,Protocoltype), Tooltip (Service_category), Tooltip (Attack_or_normal,Service_category) and Tooltip (Protocoltype). The Tooltip (Attack_category,Protocoltype) filter keeps 12 members. The Tooltip (Attack_category) filter keeps 5 members. The Tooltip (Attack_or_normal,Protocoltype) filter keeps 6 members. The Tooltip (Attack_or_normal,Service_category,Protocoltype) filter keeps 21 members. The Tooltip (Service_category) filter keeps 8 members. The Tooltip (Attack_or_normal,Service_category) filter keeps 14 members. The Tooltip (Protocoltype) filter keeps 3 members.

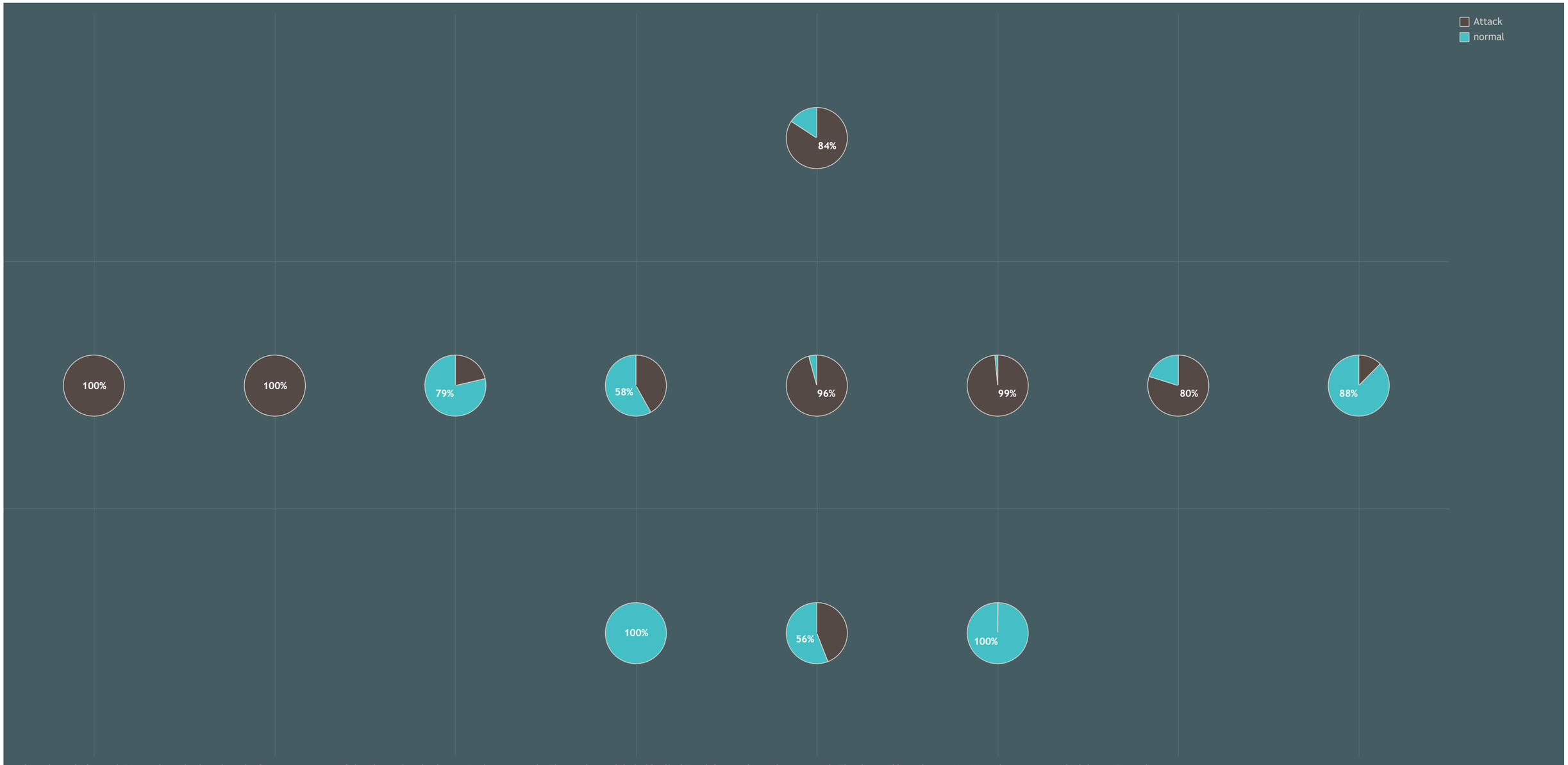
Dstbytes & | Bytes per Duration



COUNT([Protocoltype]) / TOTAL(COUNT([Protocoltype])) and Protocoltype broken down by Protocoltype. Color shows details about Protocoltype. The data is filtered on Action (Attack_category), which keeps 5 members.

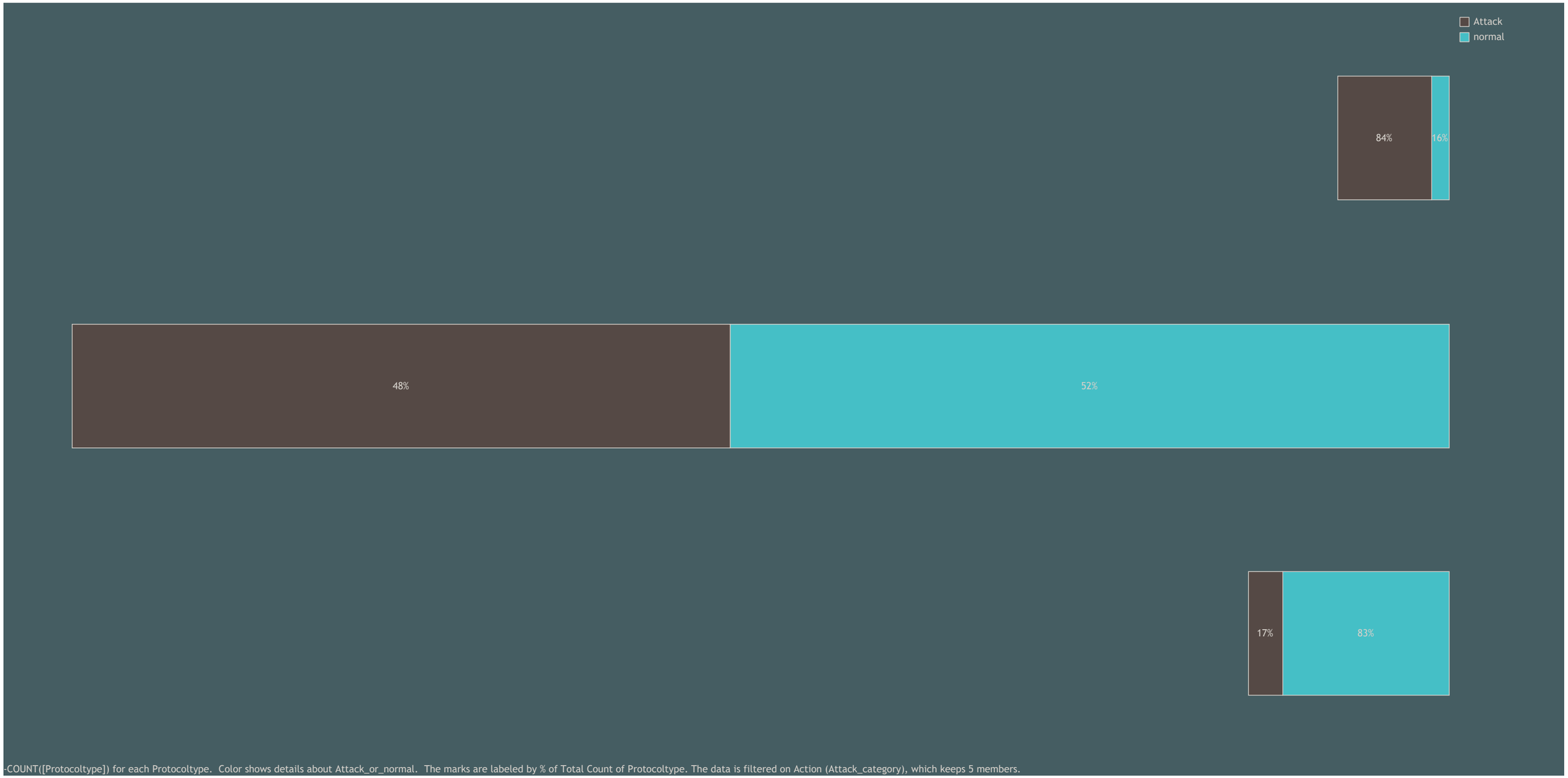
Dstbytes & | Bytes per Duration

COUNT([Service_category]) / TOTAL(COUNT([Service_category])) and Service_category broken down by Service_category. Color shows details about Service_category. The data is filtered on Action (Attack_category), which keeps 5 members.

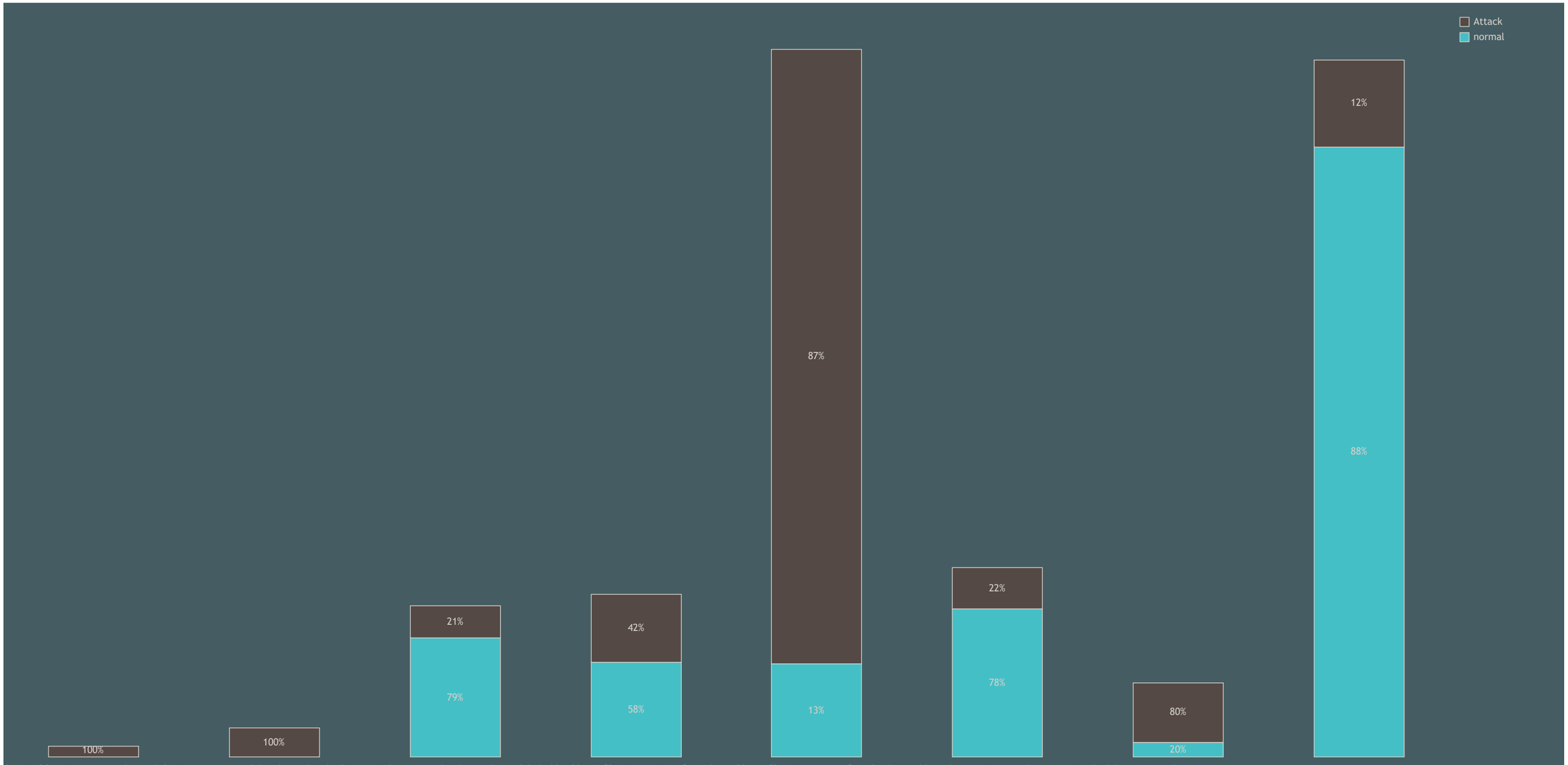


Avg(0) and Avg(0) for each Protocoltype broken down by Service_category. Color shows details about Attack_or_normal. The marks are labeled by % of Total Count of Attack_or_normal. The data is filtered on Action (Attack_category), which keeps 5 members.

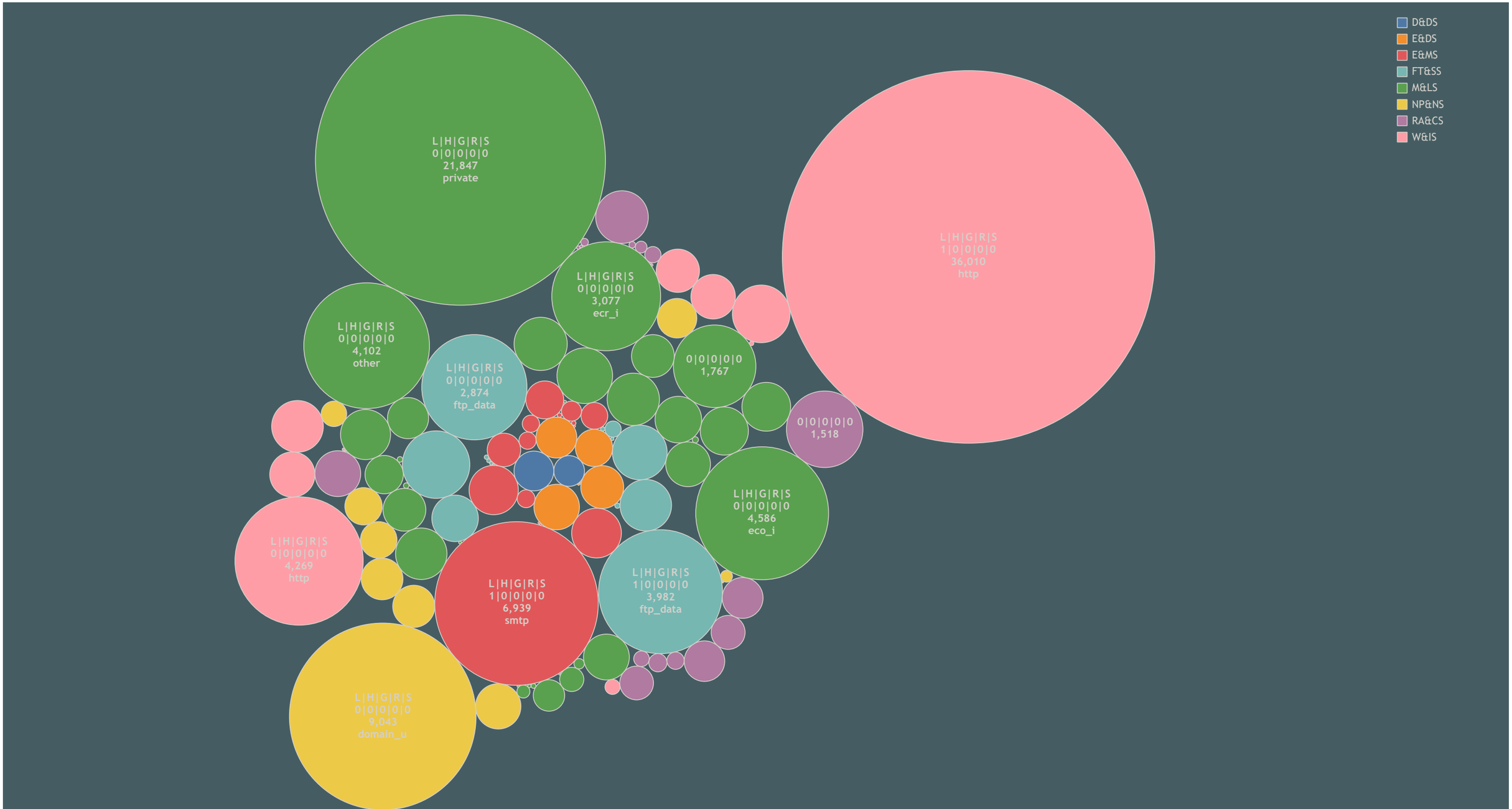
Count of Service for each Service. Color shows count of Service. The marks are labeled by COUNT([Service]) / TOTAL(COUNT([Service])). The data is filtered on Tooltip (Attack_or_normal,Service_category,Protocoltype), Tooltip (Attack_category), Tooltip (Flag), Tooltip (Service_category) and Tooltip (Protocoltype). The Tooltip (Attack_or_normal,Service_category,Protocoltype) filter keeps 21 members. The Tooltip (Attack_category) filter keeps 5 members. The Tooltip (Flag) filter keeps 11 members. The Tooltip (Service_category) filter keeps 8 members. The Tooltip (Protocoltype) filter keeps 3 members.



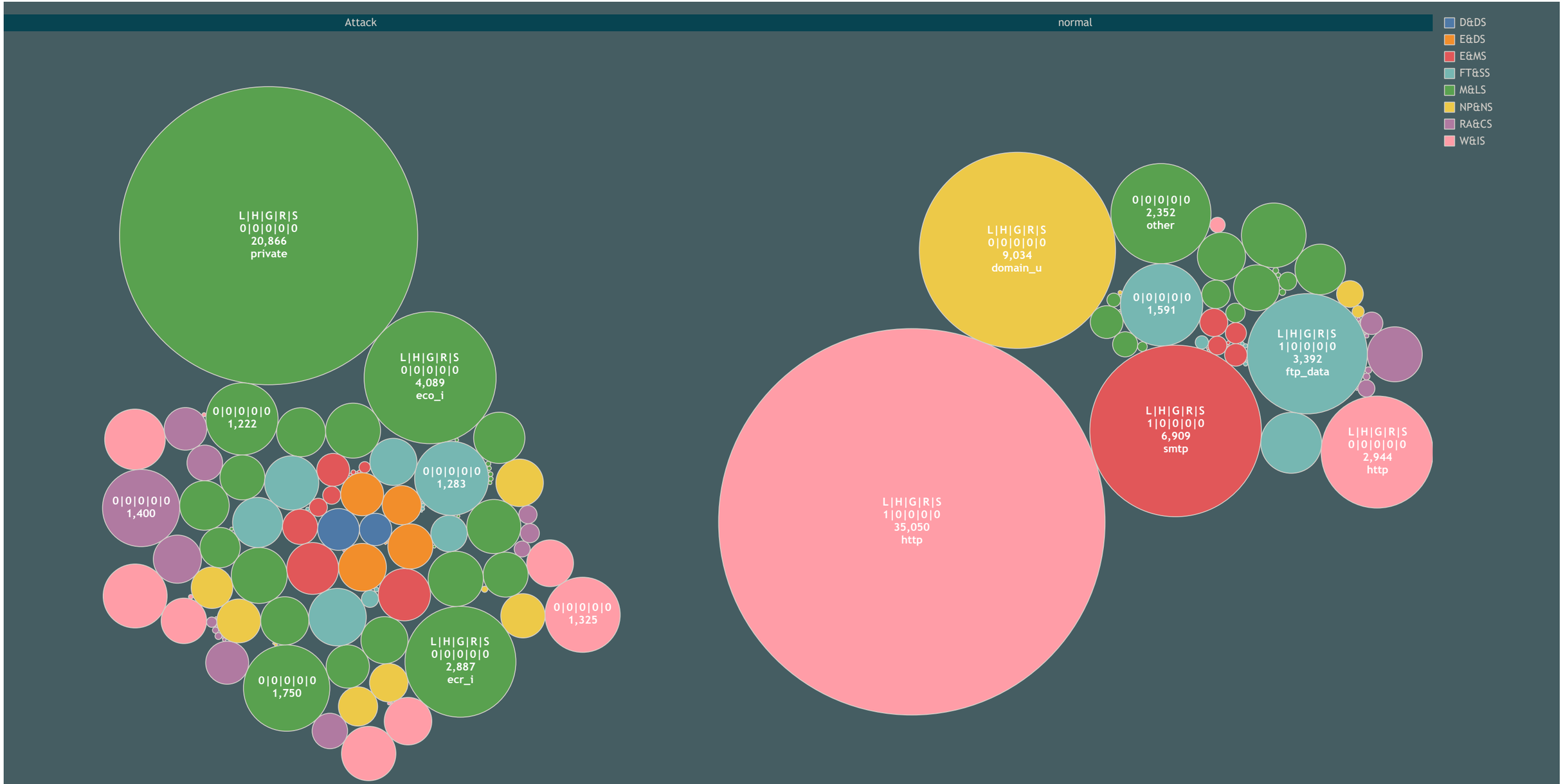
-COUNT([Protocoltype]) for each Protocoltype. Color shows details about Attack_or_normal. The marks are labeled by % of Total Count of Protocoltype. The data is filtered on Action (Attack_category), which keeps 5 members.



Count of Service_category for each Service_category. Color shows details about Attack_or_normal. The marks are labeled by COUNT([Service_category]) / TOTAL(COUNT([Service_category])). The data is filtered on Action (Attack_category), which keeps 5 members.



Ishostlogin, Isguestlogin, Loggedin, Rootshell, Suattempted_binary, count of Ishostlogin and Service. Color shows details about Service_category. Size shows count of Ishostlogin. The marks are labeled by Ishostlogin, Isguestlogin, Loggedin, Rootshell, Suattempted_binary, count of Ishostlogin and Service. The view is filtered on Loggedin, Ishostlogin, Isguestlogin, Rootshell, Suattempted_binary and Service. The Loggedin filter keeps 0 and 1. The Ishostlogin filter keeps 0 and 1. The Isguestlogin filter keeps 0 and 1. The Rootshell filter keeps 0 and 1. The Suattempted_binary filter keeps multiple members. The Service filter keeps 70 of 70 members.

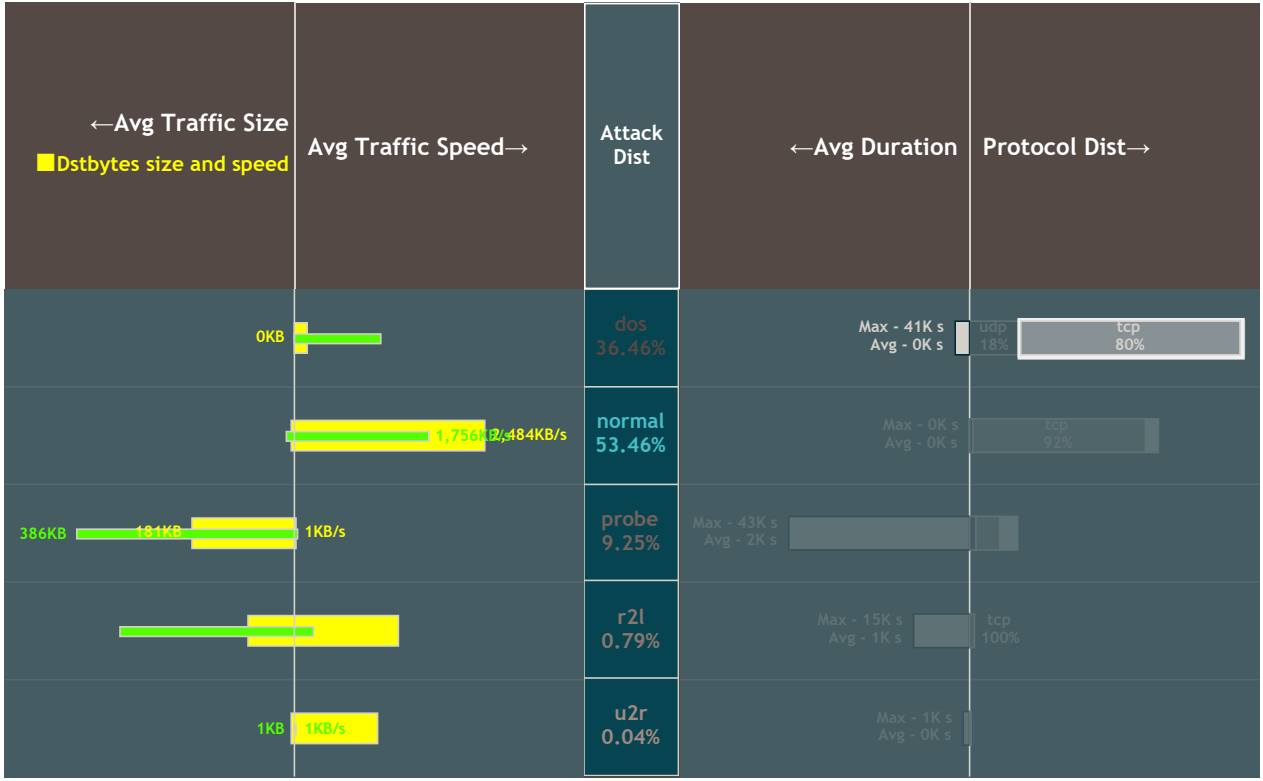


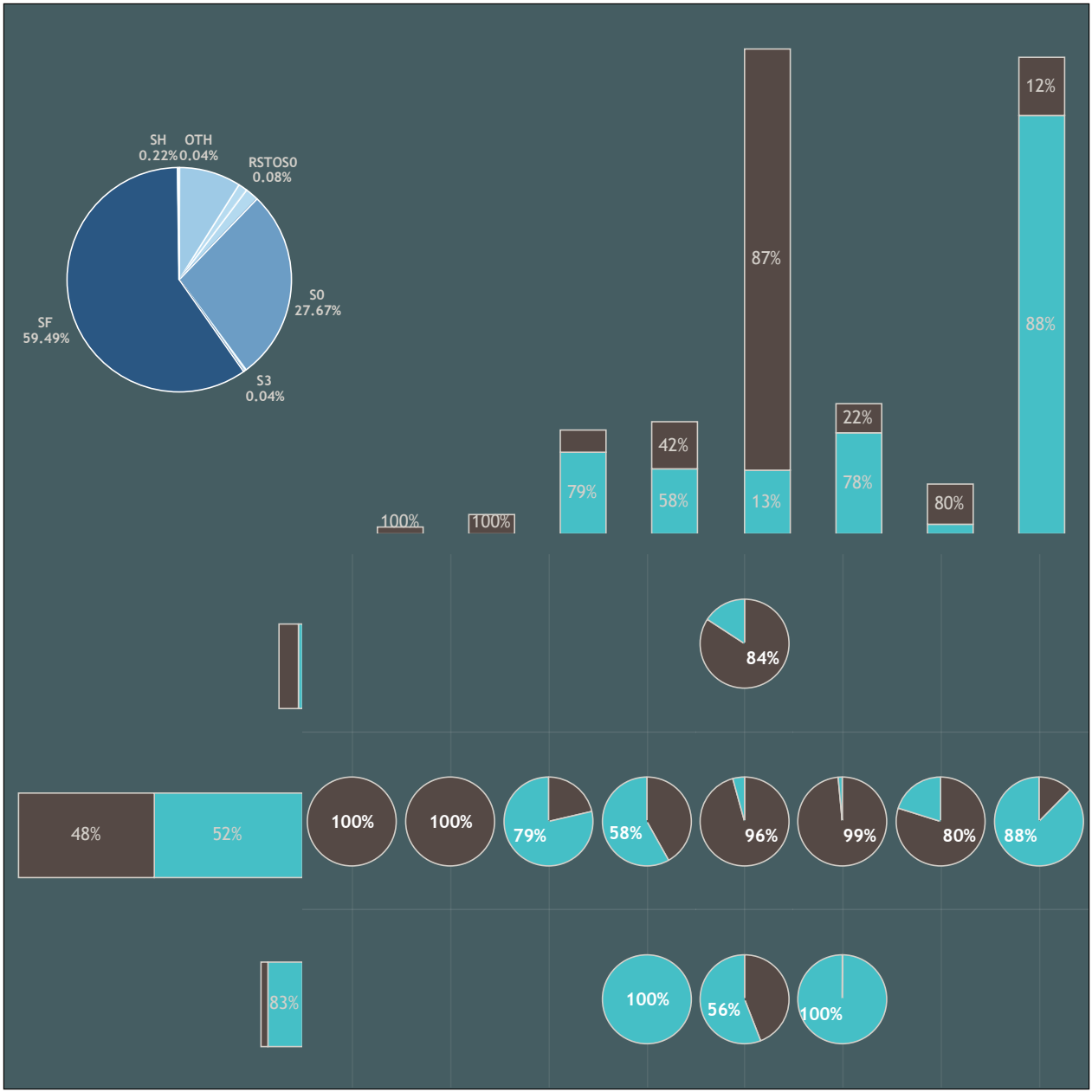
Ishostlogin, Isguestlogin, Loggedin, Rootshell, Suattempted_binary, count of Ishostlogin and Service broken down by Attack_or_normal. Color shows details about Service_category. Size shows count of Ishostlogin. The marks are labeled by Ishostlogin, Isguestlogin, Loggedin, Rootshell, Suattempted_binary, count of Ishostlogin and Service. The data is filtered on Action (Attack_category), which keeps 5 members. The view is filtered on Loggedin, Ishostlogin, Isguestlogin, Rootshell, Suattempted_binary, Service and Service_category. The Loggedin filter keeps 0 and 1. The Ishostlogin filter keeps 0 and 1. The Isguestlogin filter keeps 0 and 1. The Rootshell filter keeps 0 and 1. The Suattempted_binary filter keeps multiple members. The Service filter keeps 70 of 70 members. The Service_category filter keeps 8 of 8 members.

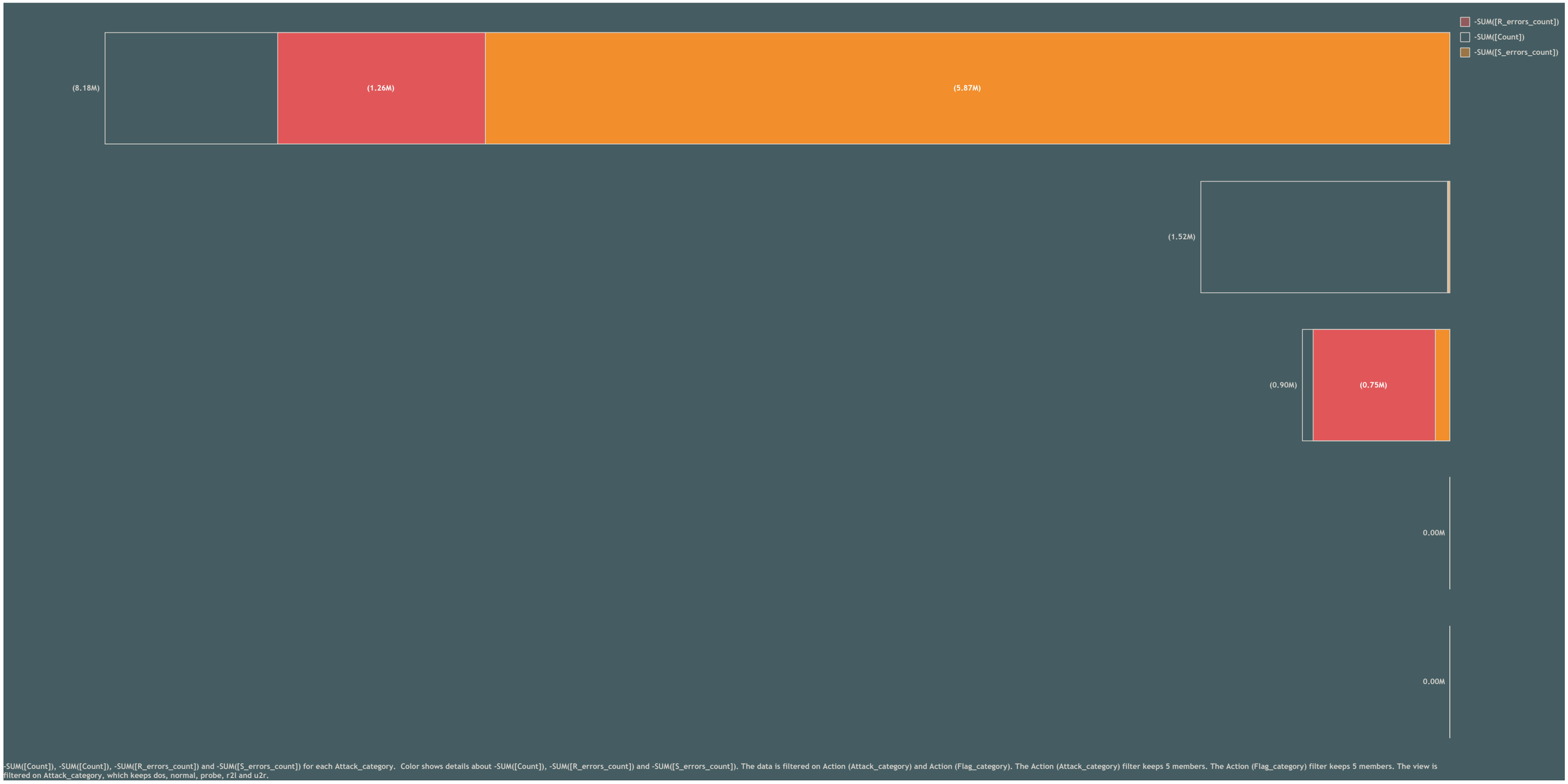
Proof that services are unique to protocol except private and other service

		Protocoltype		
		icmp	tcp	udp
1	aol		0.00%	
2	auth		0.93%	
3	bgp		0.69%	
4	courier		0.71%	
5	csnet_ns		0.53%	
6	ctf		0.55%	
7	daytime		0.51%	
8	discard		0.52%	
9	domain		0.55%	
10	domain_u			60.31%
11	echo		0.42%	
12	eco_i	55.31%		
13	ecr_i	37.11%		
14	efs		0.47%	
15	exec		0.46%	
16	finger		1.72%	
17	ftp		1.71%	
18	ftp_data		6.68%	
19	gopher		0.50%	
20	harvest		0.00%	
21	hostnames		0.45%	
22	http		39.28%	
23	http_443		0.52%	
24	http_2784		0.00%	
25	http_8001		0.00%	
26	imap4		0.63%	
27	IRC		0.18%	
28	iso_tsap		0.67%	
29	klogin		0.42%	
30	kshell		0.29%	
31	ldap		0.40%	
32	link		0.46%	
33	login		0.42%	
34	mtp		0.43%	
35	name		0.44%	
36	netbios_dgm		0.39%	
37	netbios_ns		0.34%	
38	netbios_ssn		0.35%	
39	netstat		0.35%	
40	nnsp		0.61%	
41	nntp		0.29%	
42	ntp_u			1.12%
43	other		1.82%	16.59%
44	pm_dump		0.00%	
45	pop_2		0.08%	
46	pop_3		0.26%	
47	printer		0.07%	
48	private		18.08%	21.95%
49	red_i	0.10%		
50	remote_job		0.08%	
51	rje		0.08%	
52	shell		0.06%	
53	smtp		7.12%	
54	sql_net		0.24%	
55	ssh		0.30%	
56	sunrpc		0.37%	
57	supdup		0.53%	
58	systat		0.46%	
59	telnet		2.29%	
60	tftp_u			0.02%
61	tim_i	0.10%		
62	time		0.64%	
63	urh_i	0.12%		
64	urp_i	7.26%		
65	uucp		0.76%	
66	uucp_path		0.67%	
67	vmnet		0.60%	
68	whois		0.67%	
69	X11		0.07%	
70	Z39_50		0.84%	

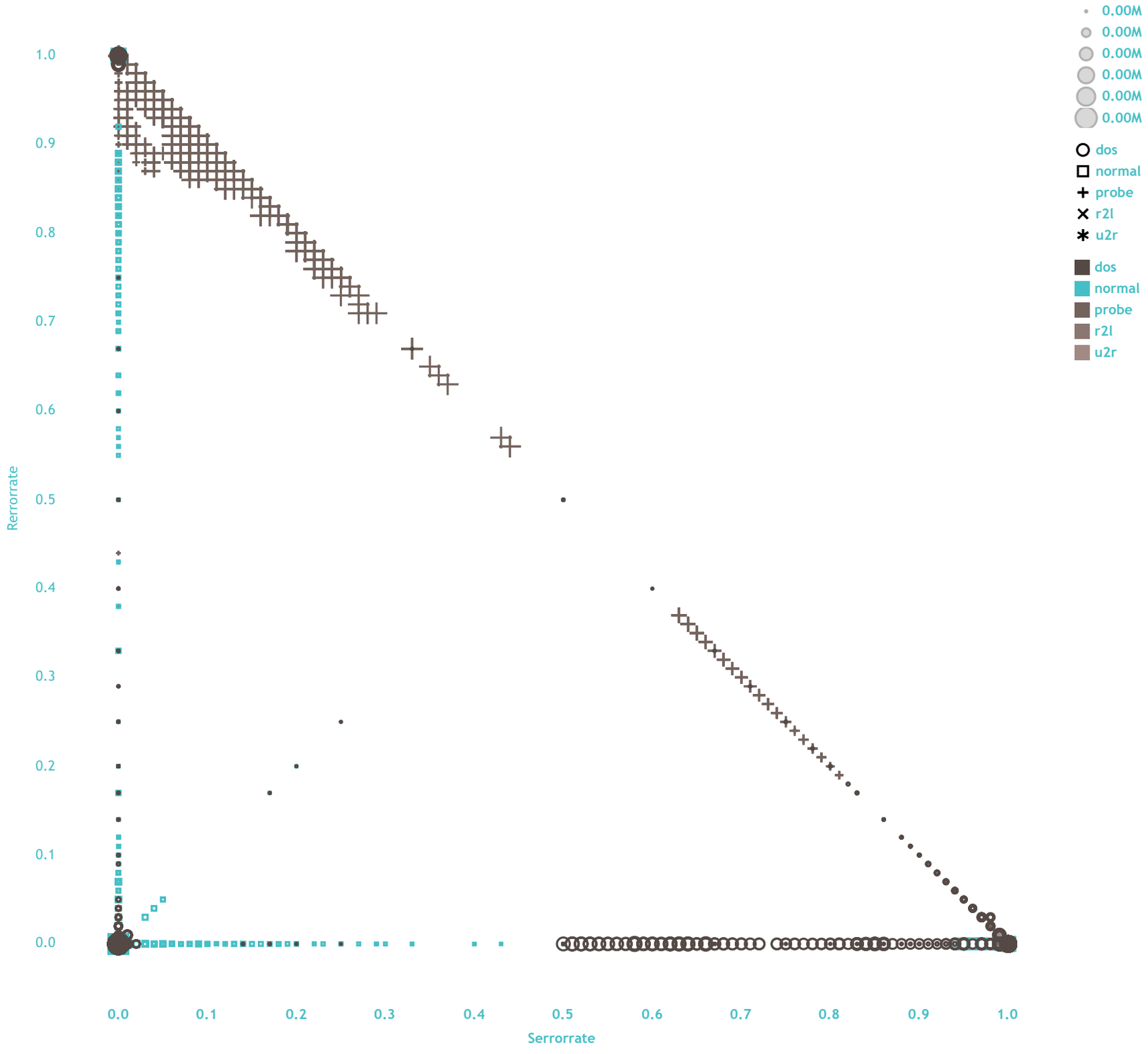
% of Total Count of Service broken down by Protocoltype vs. INDEX() and Service.


←Avg Traffic Size
Dstbytes size and speed
Avg Traffic Speed→
Attack Dist
←Avg Duration
Protocol Dist→
0KB
dos
36.46%
Max - 41K s
Avg - 0K s
udp
18%
tcp
80%
1,756KB
2,484KB/s
normal
53.46%
Max - 0K s
Avg - 0K s
tcp
92%
386KB
181KB
1KB/s
probe
9.25%
Max - 43K s
Avg - 2K s
r2l
0.79%
Max - 15K s
Avg - 1K s
tcp
100%
1KB
1KB/s
u2r
0.04%
Max - 1K s
Avg - 0K s

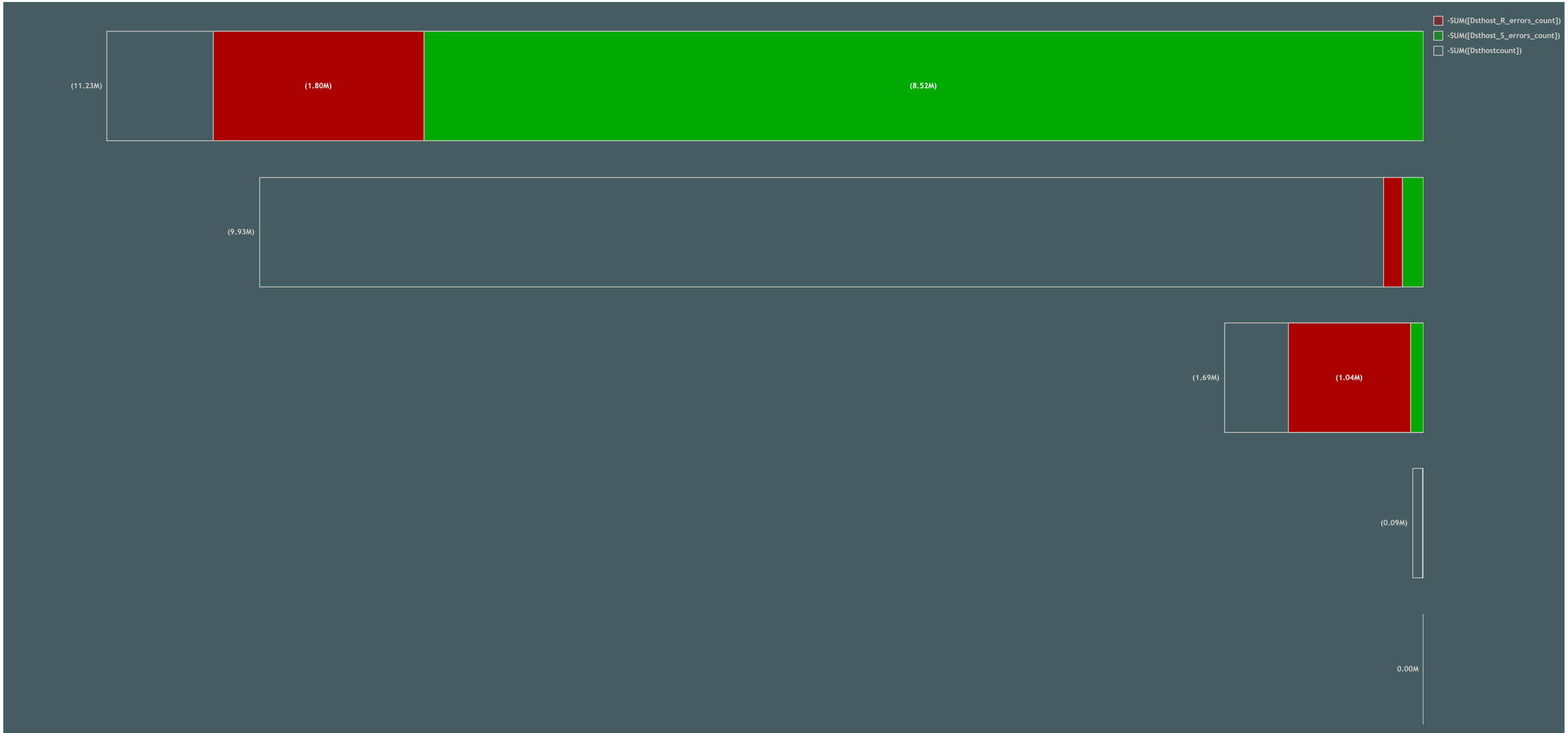

SH
0.22%
OTH
0.04%
RSTOS0
0.08%
S0
27.67%
S3
0.04%
SF
59.49%
100%
100%
79%
42%
58%
87%
13%
22%
78%
80%
12%
88%
84%
48%
52%
100%
100%
79%
58%
96%
99%
80%
88%
83%
100%
56%
100%



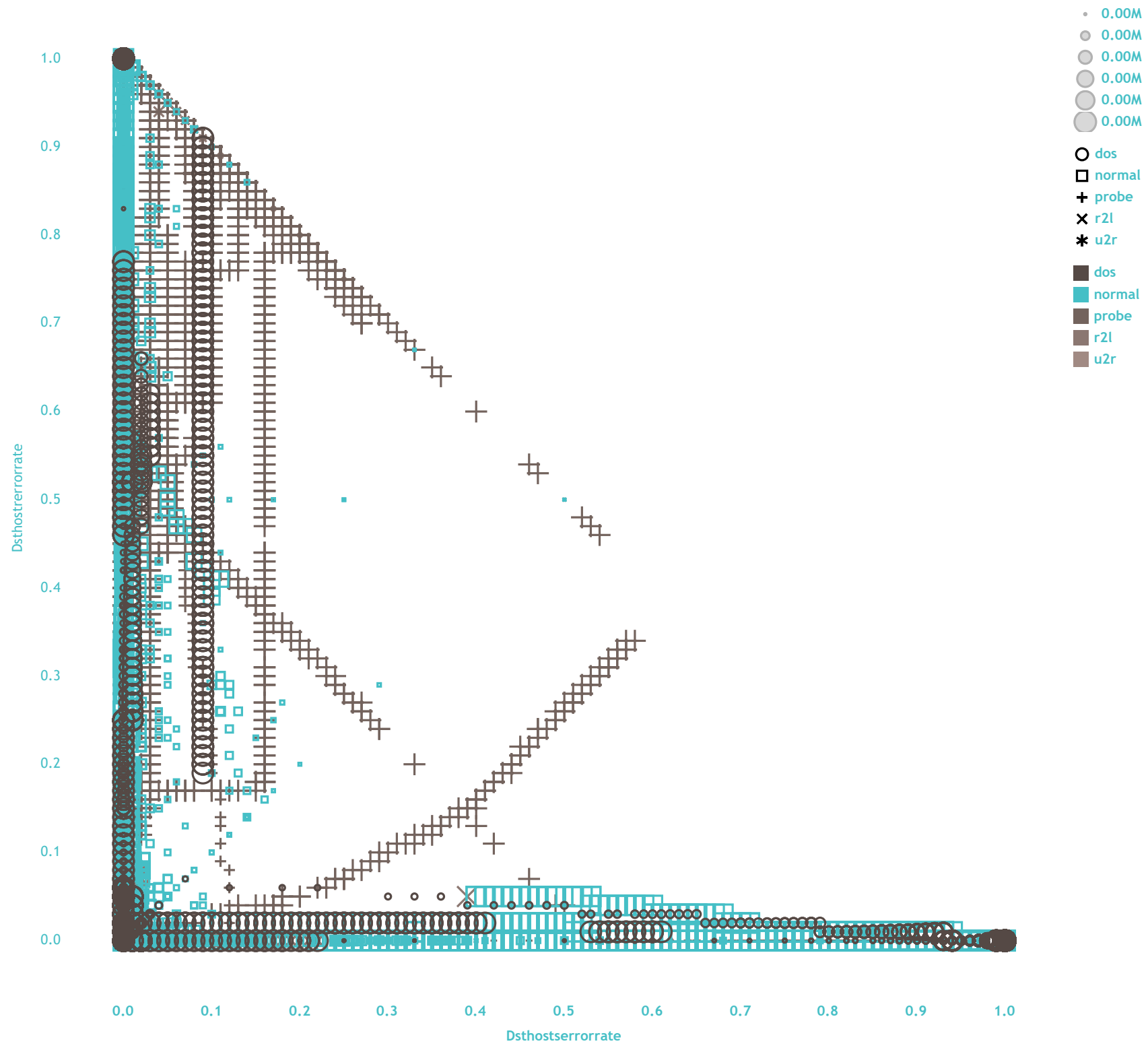
-SUM([Count]), -SUM([Count]), -SUM([R_errors_count]) and -SUM([S_errors_count]) for each Attack_category. Color shows details about -SUM([Count]), -SUM([R_errors_count]) and -SUM([S_errors_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



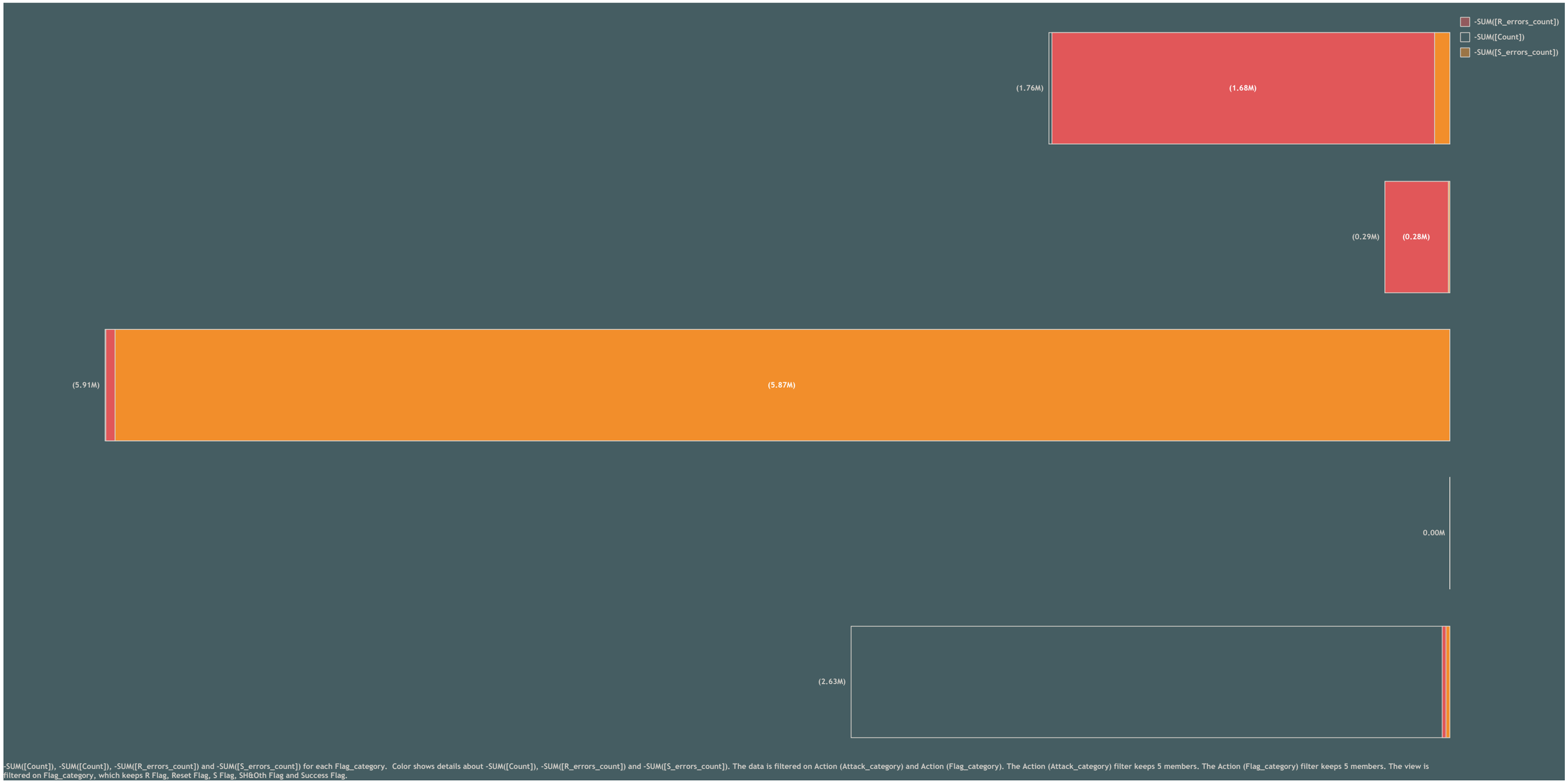
Serrorrate vs. Rerrorrate. Color shows details about Attack_category. Size shows Count. Shape shows details about Attack_category. The data is filtered on Tooltip (Flag_category) and Tooltip (Attack_category). The Tooltip (Flag_category) filter keeps 5 members. The Tooltip (Attack_category) filter keeps 5 members.



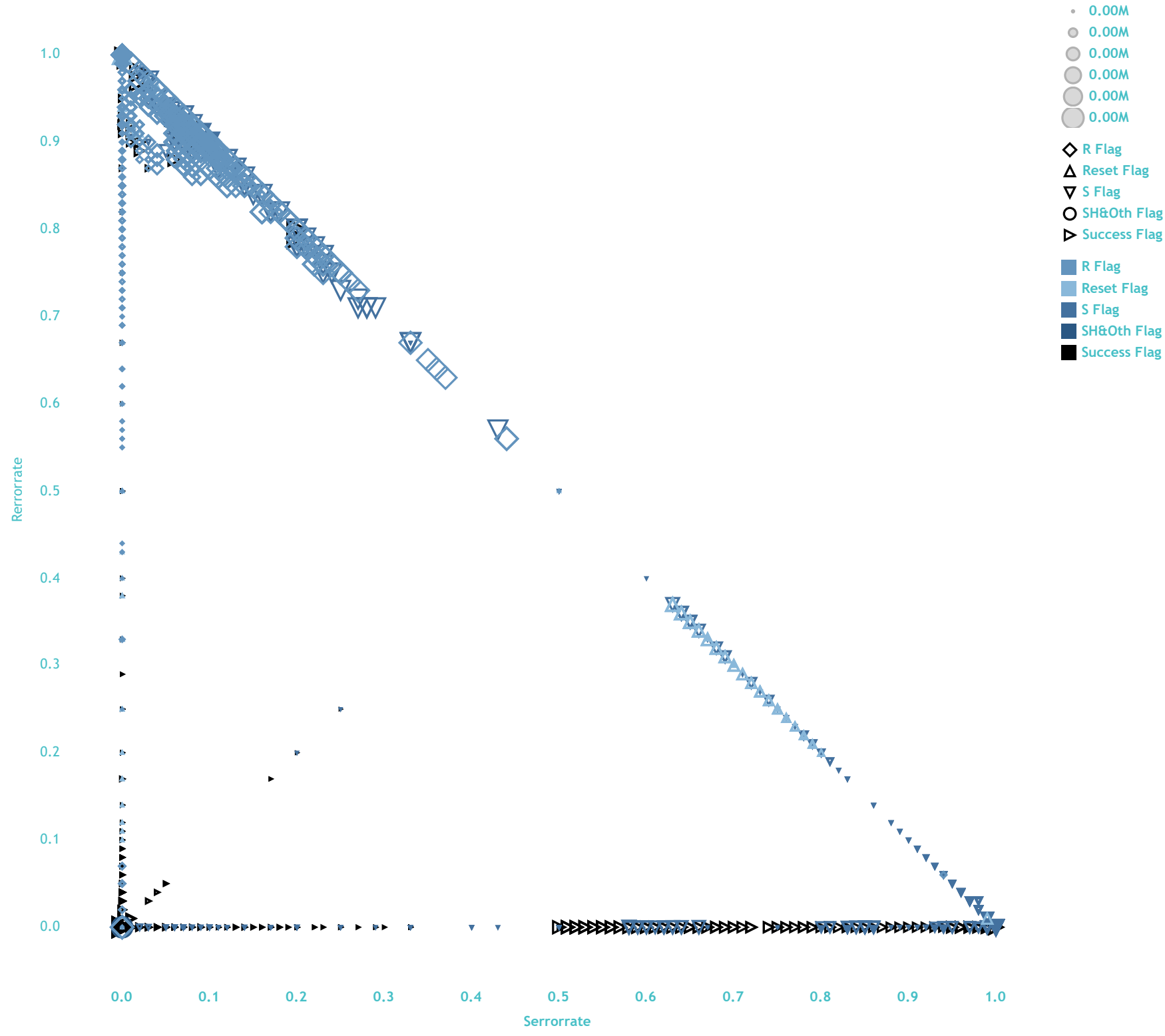
-SUM([Dsthostcount]), -SUM([Dsthostcount]), -SUM([Dsthost_R_errors_count]) and -SUM([Dsthost_S_errors_count]) for each Attack_category. Color shows details about -SUM([Dsthostcount]), -SUM([Dsthost_R_errors_count]) and -SUM([Dsthost_S_errors_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



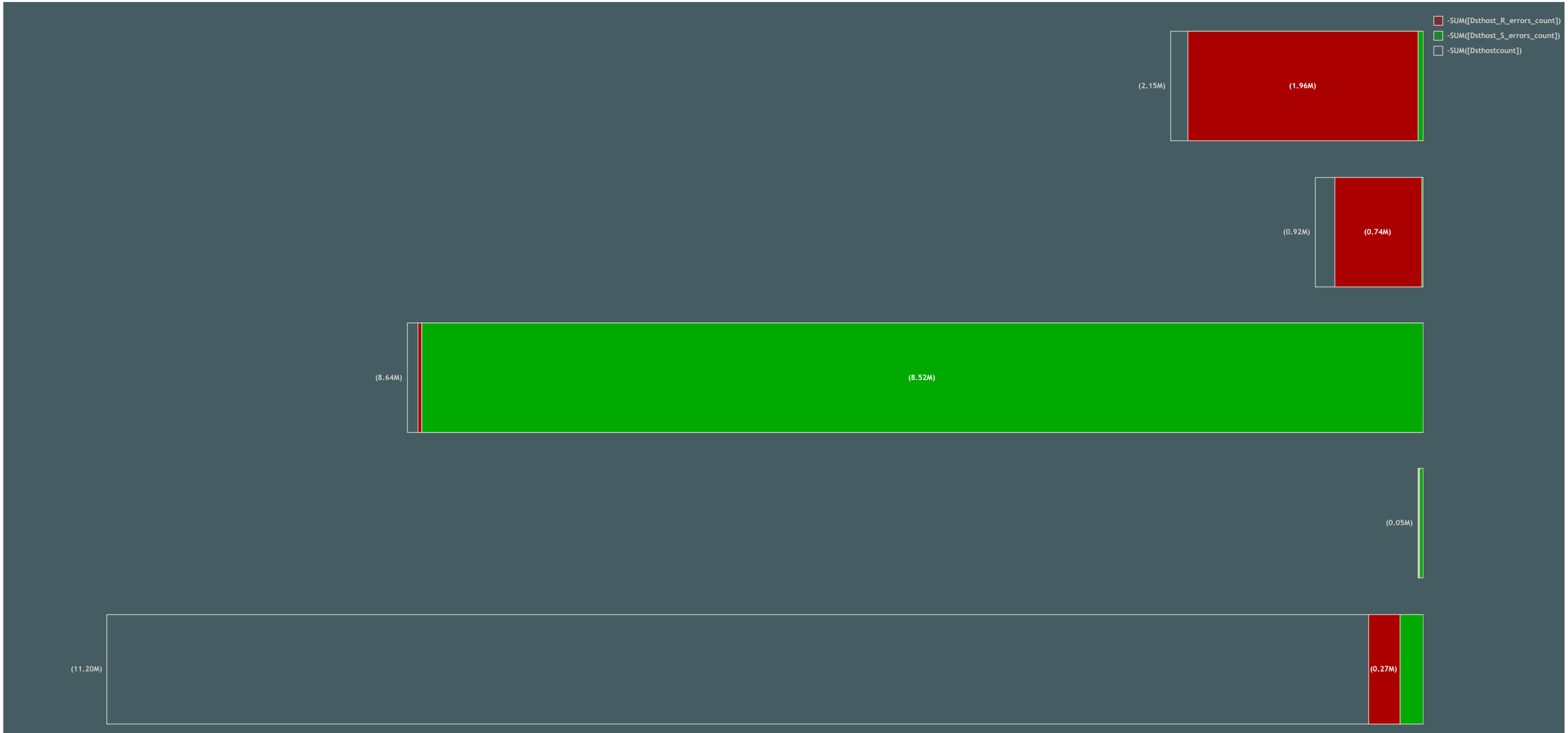
Dsthostserrorrate vs. Dsthostrerrorrate. Color shows details about Attack_category. Size shows Dsthostcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.



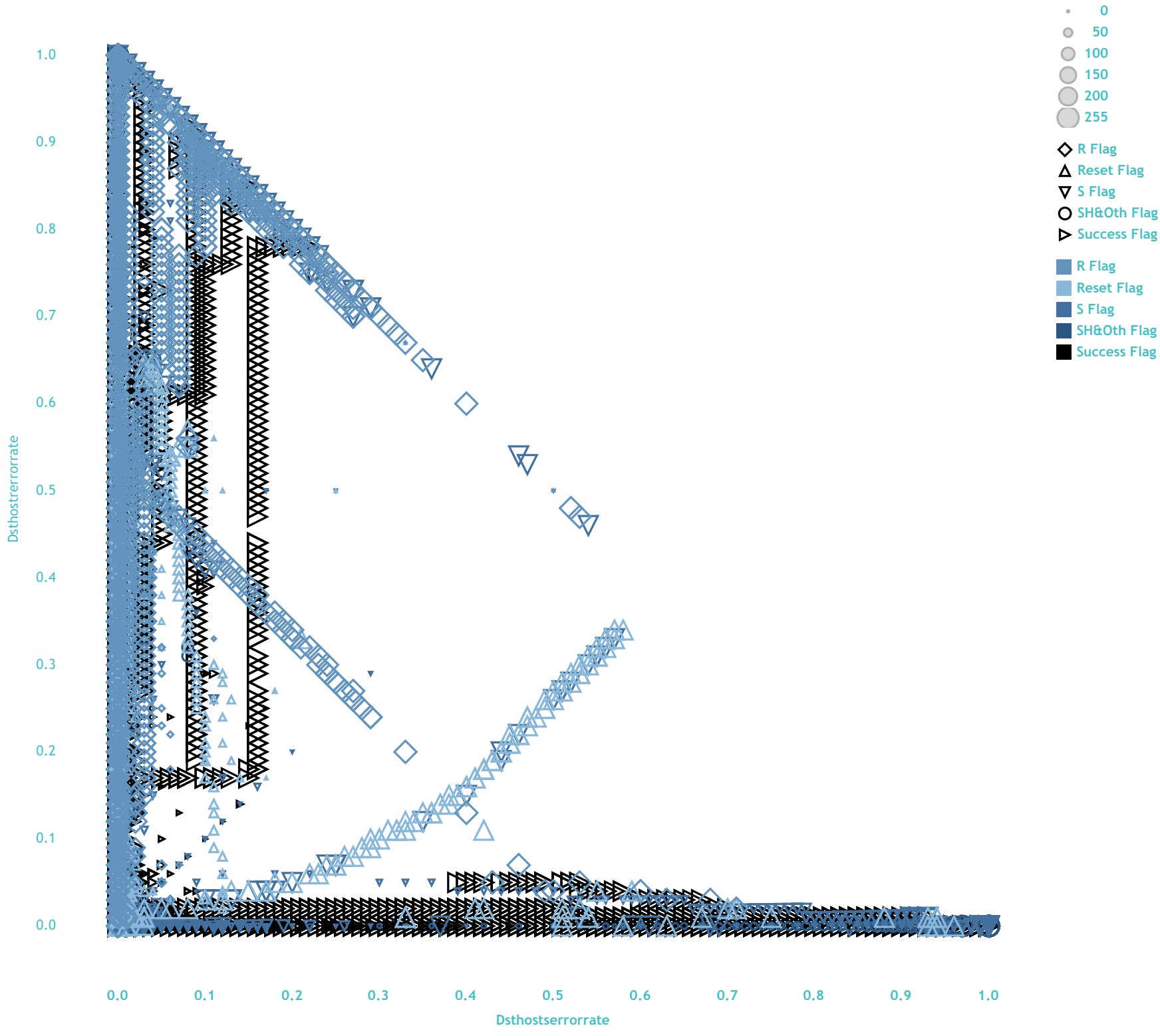
-SUM([Count]), -SUM([Count]), -SUM([R_errors_count]) and -SUM([S_errors_count]) for each Flag_category. Color shows details about -SUM([Count]), -SUM([R_errors_count]) and -SUM([S_errors_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



Serrorrate vs. Rerrorrate. Color shows details about Flag_category. Size shows Count. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

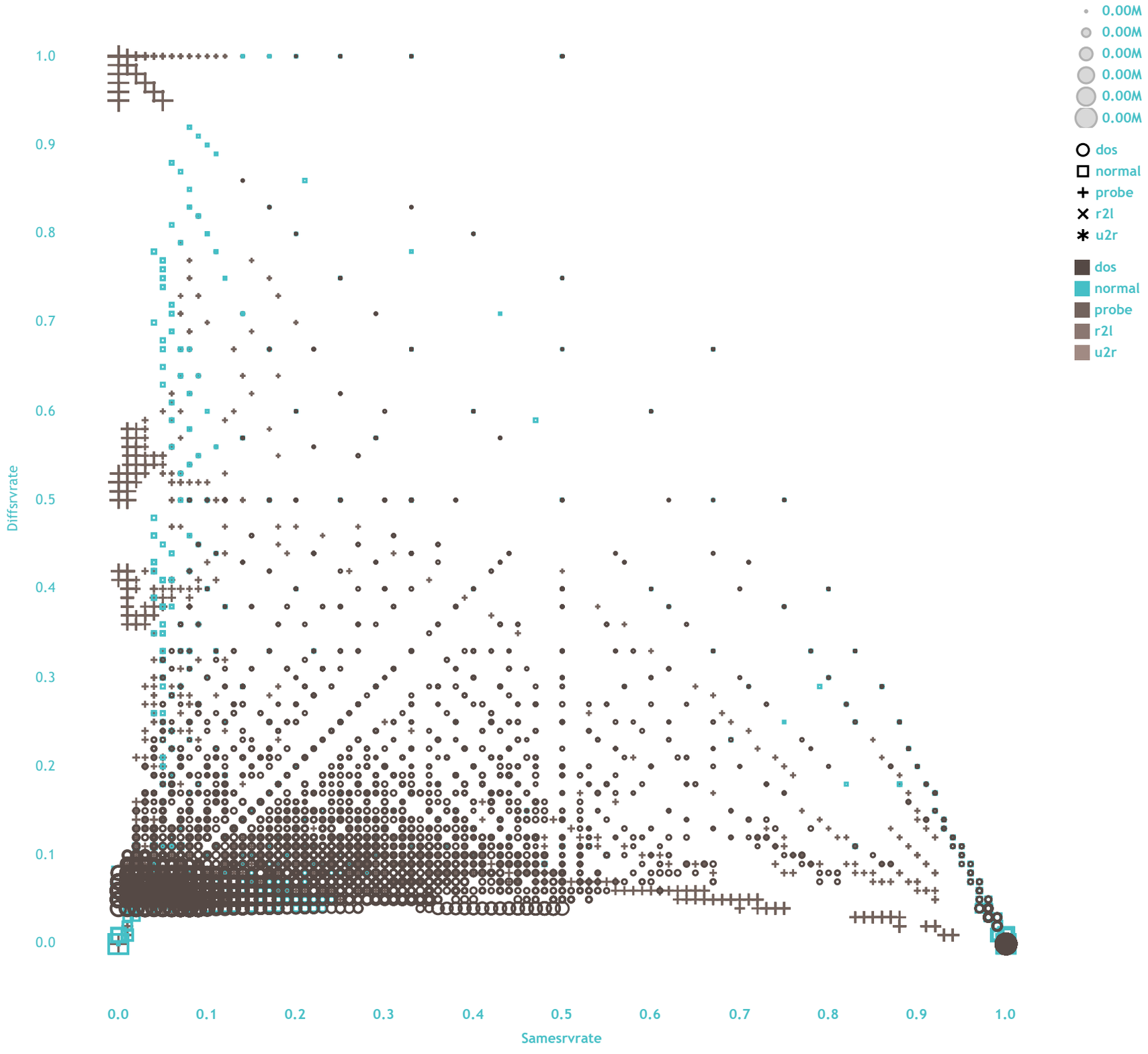


-SUM([Dsthostcount]), -SUM([Dsthostcount]), -SUM([Dsthost_R_errors_count]) and -SUM([Dsthost_S_errors_count]) for each Flag_category. Color shows details about -SUM([Dsthostcount]), -SUM([Dsthost_R_errors_count]) and -SUM([Dsthost_S_errors_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.

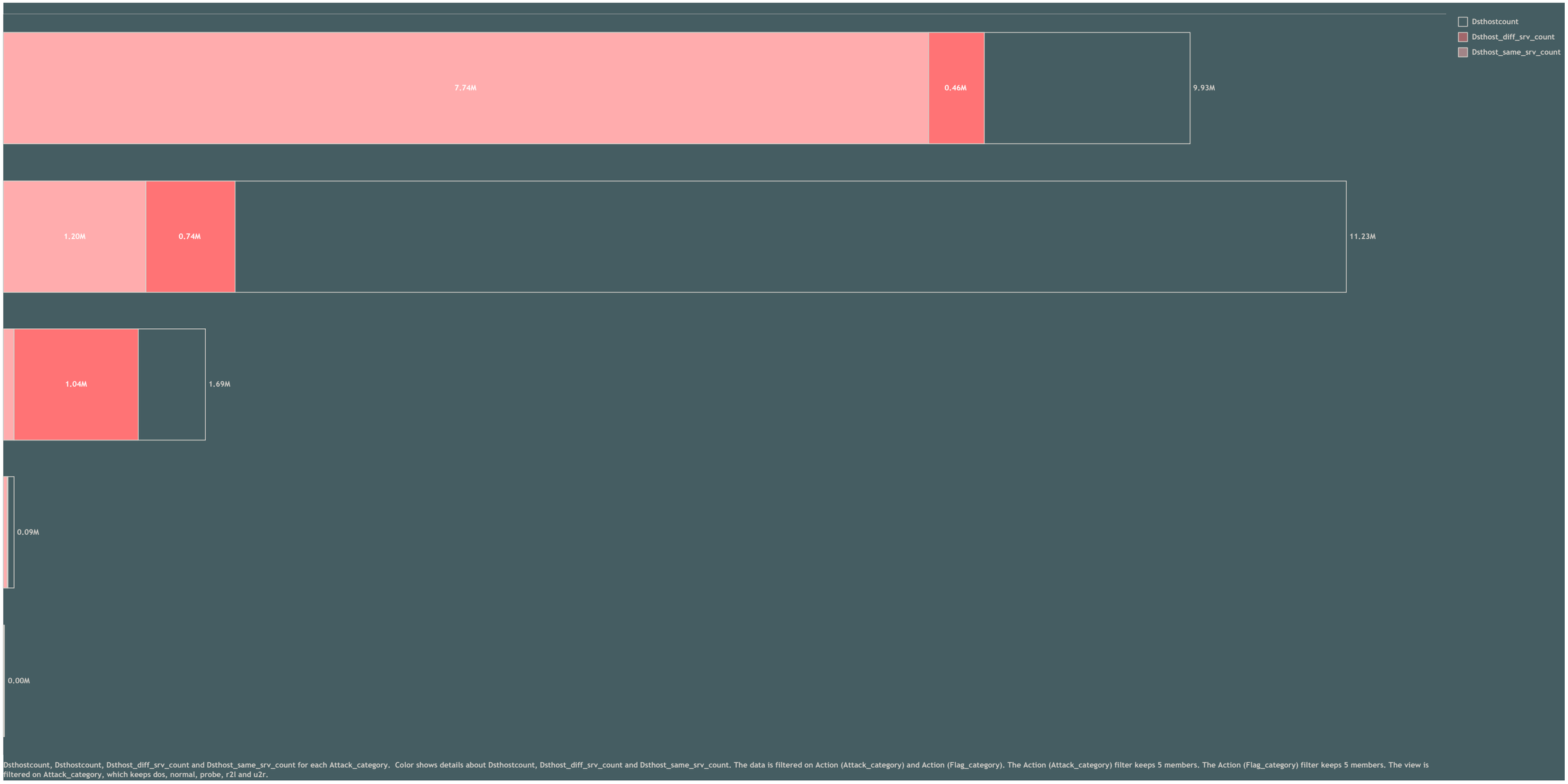


Dsthostserrorrate vs. Dsthostrerrorrate. Color shows details about Flag_category. Size shows Dsthostcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

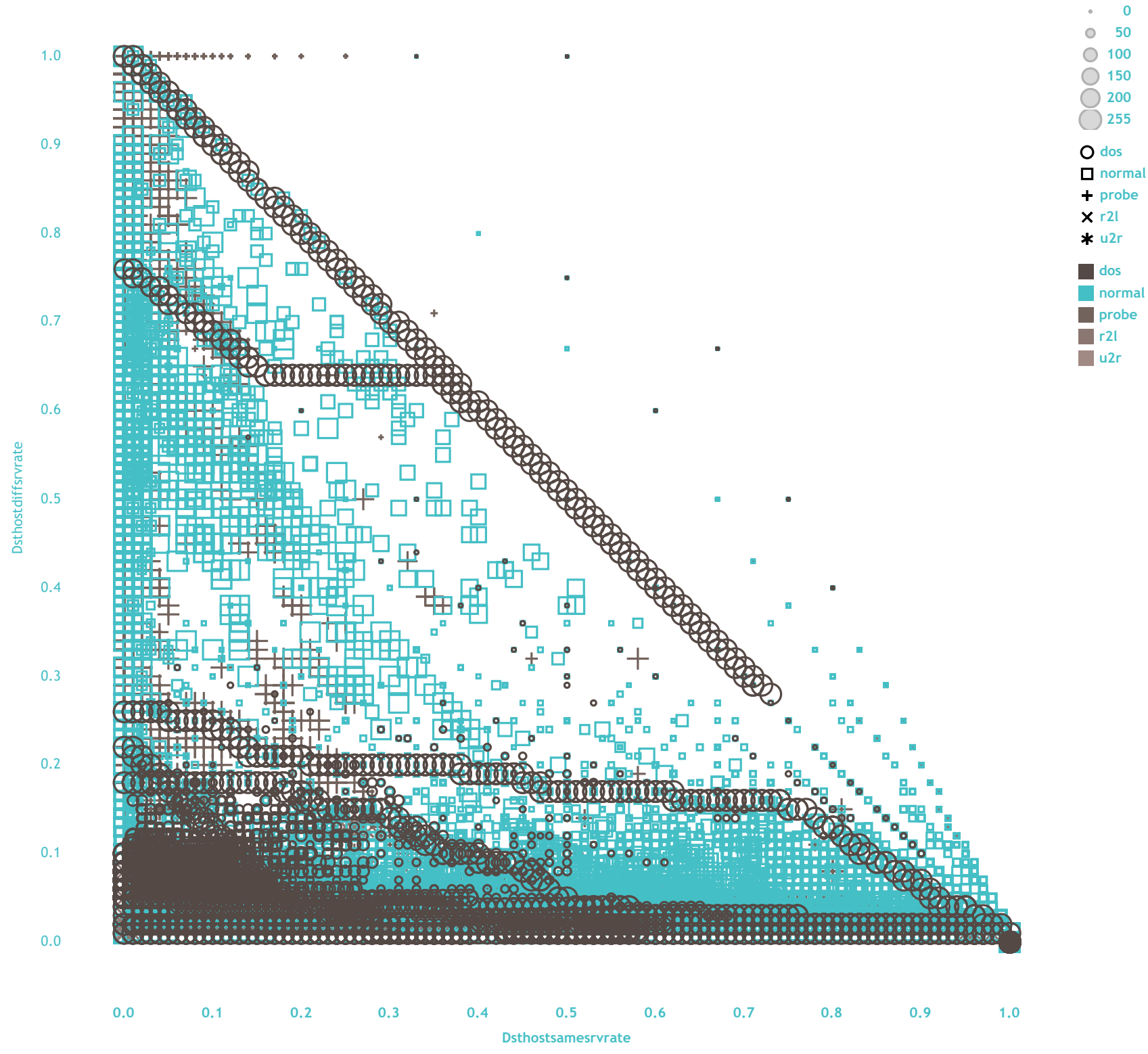
Count, Count, Diff_srv_count and Same_srv_count for each Attack_category. Color shows details about Count, Diff_srv_count and Same_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



Samesrvrate vs. Diffsrvrate. Color shows details about Attack_category. Size shows Count. Shape shows details about Attack_category. The data is filtered on Tooltip (Flag_category) and Tooltip (Attack_category). The Tooltip (Flag_category) filter keeps 5 members. The Tooltip (Attack_category) filter keeps 5 members.

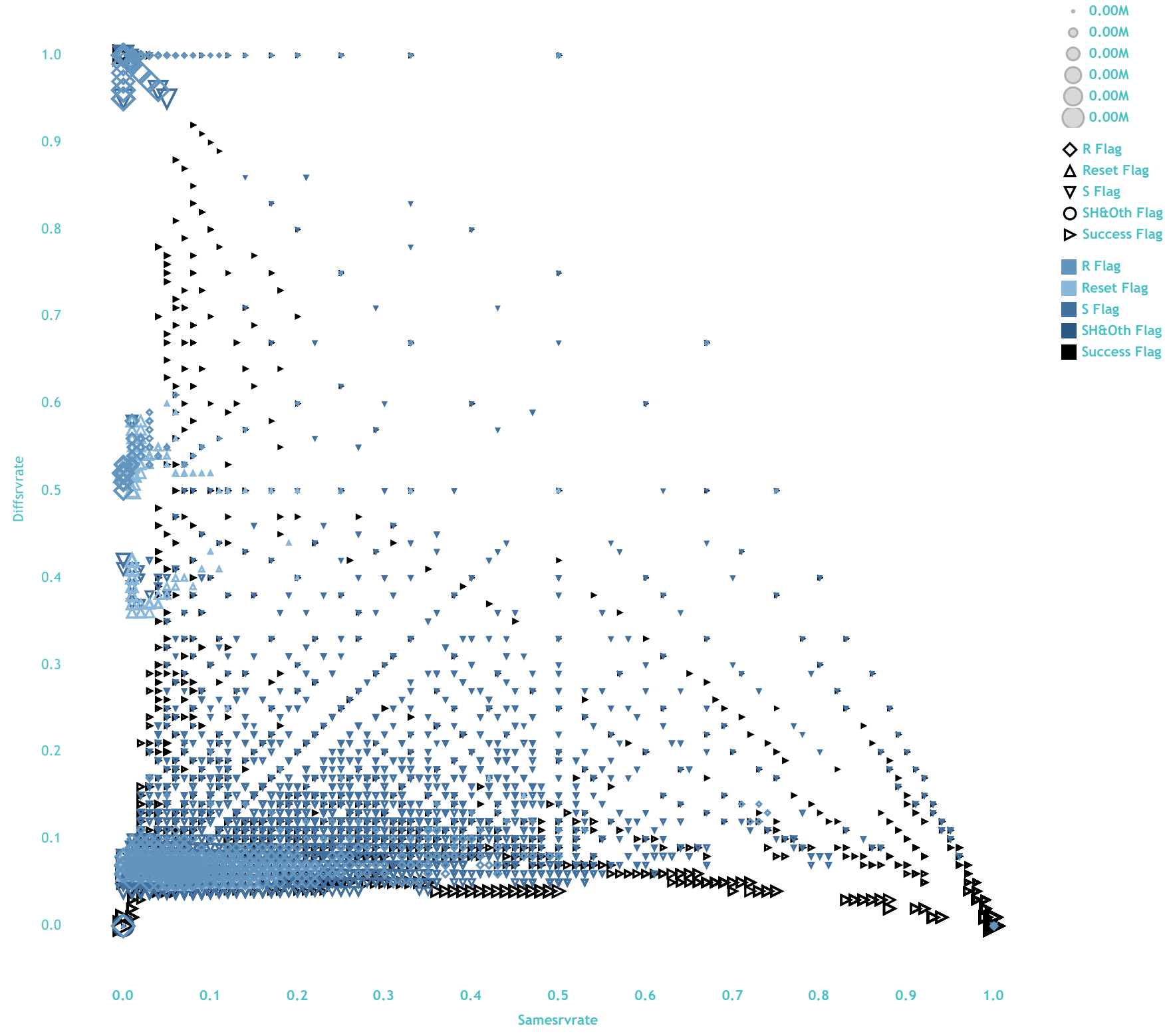


Dsthostcount, Dsthostcount, Dsthost_diff_srv_count and Dsthost_same_srv_count for each Attack_category. Color shows details about Dsthostcount, Dsthost_diff_srv_count and Dsthost_same_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.

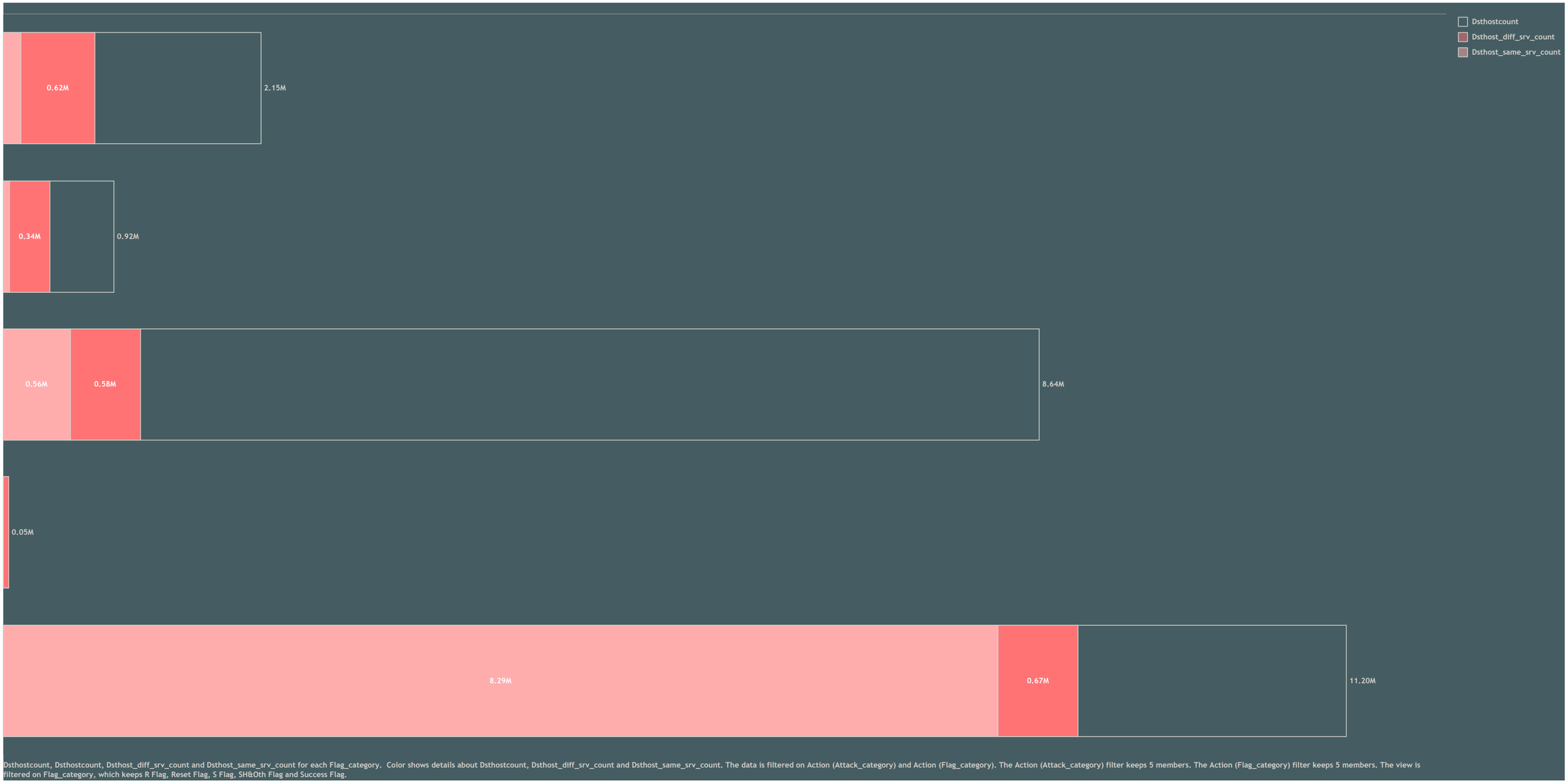


Dsthostsamesrvrate vs. Dsthostdiffsrvrate. Color shows details about Attack_category. Size shows Dsthostcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.

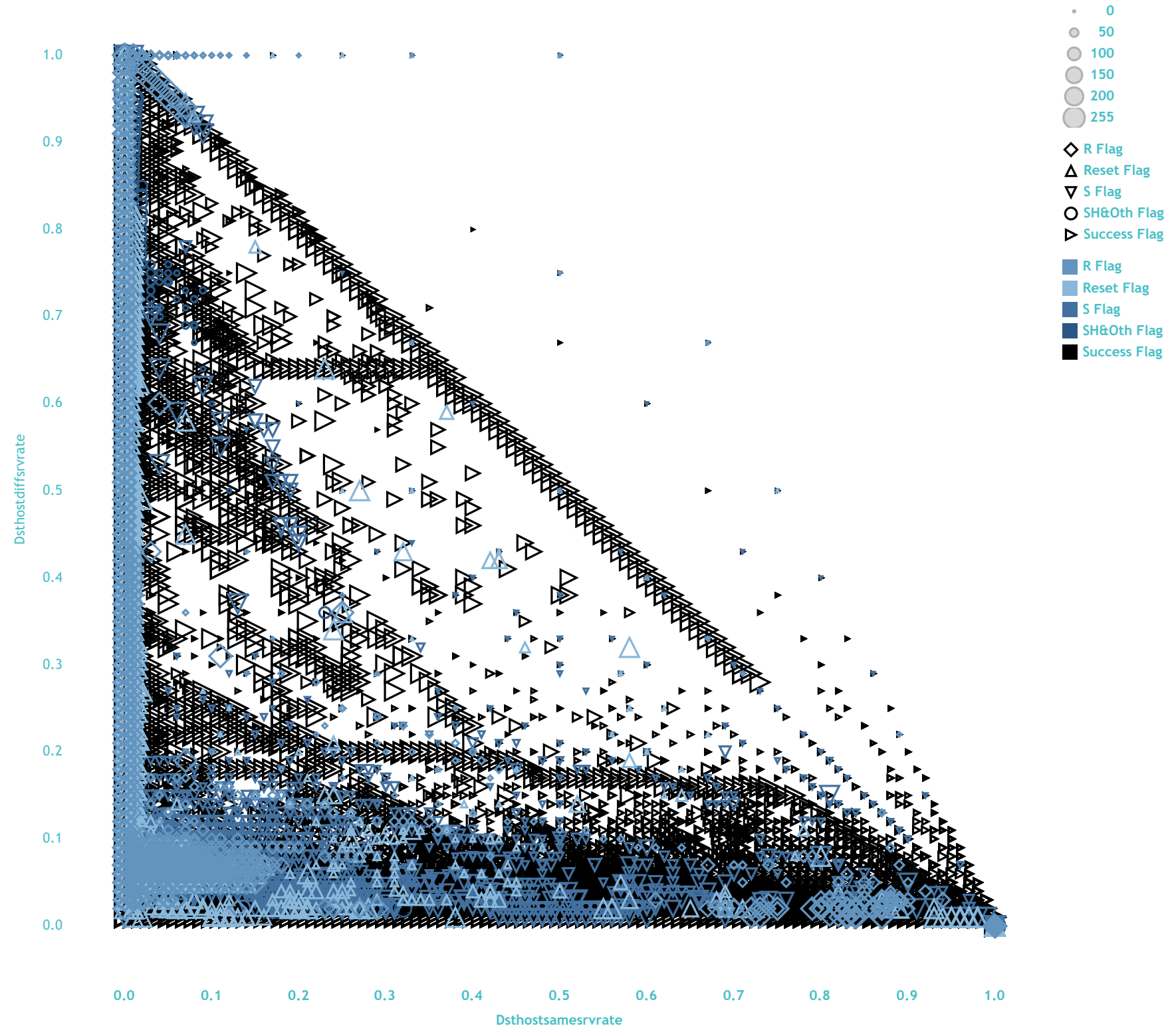
Count, Count, Diff_srv_count and Same_srv_count for each Flag_category. Color shows details about Count, Diff_srv_count and Same_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



Samesrvrate vs. Diffsrvrate. Color shows details about Flag_category. Size shows Count. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.



Dsthostcount, Dsthostcount, Dsthost_diff_srv_count and Dsthost_same_srv_count for each Flag_category. Color shows details about Dsthostcount, Dsthost_diff_srv_count and Dsthost_same_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



Dsthostsamesrvrate vs. Dsthostdiffsrvrate. Color shows details about Flag_category. Size shows Dsthostcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

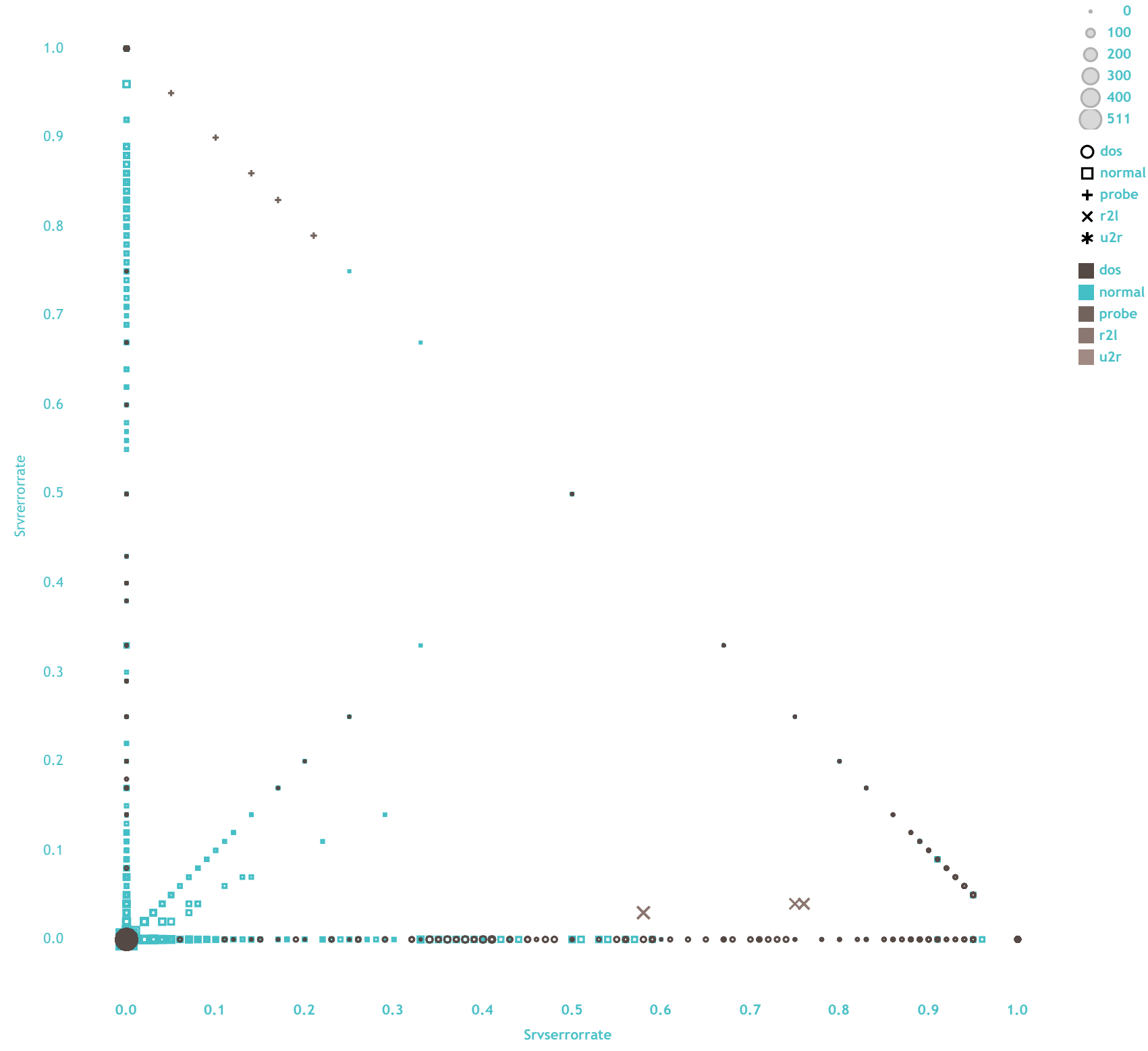

Dstbytes & Srcbytes | Bytes per Duration
normal
dos
probe
r2l
u2r
normal
14.31%
dos
77.20%
probe
8.48%
r2l
0.01%
u2r
0.00%
% of Total Count and Attack_category broken down by Attack_category. Color shows details about Attack_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

SUM([Dsthostcount]) / TOTAL(SUM([Dsthostcount])) and Attack_category broken down by Attack_category. Color shows details about Attack_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

% of Total Count and Flag_category broken down by Flag_category. Color shows details about Flag_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

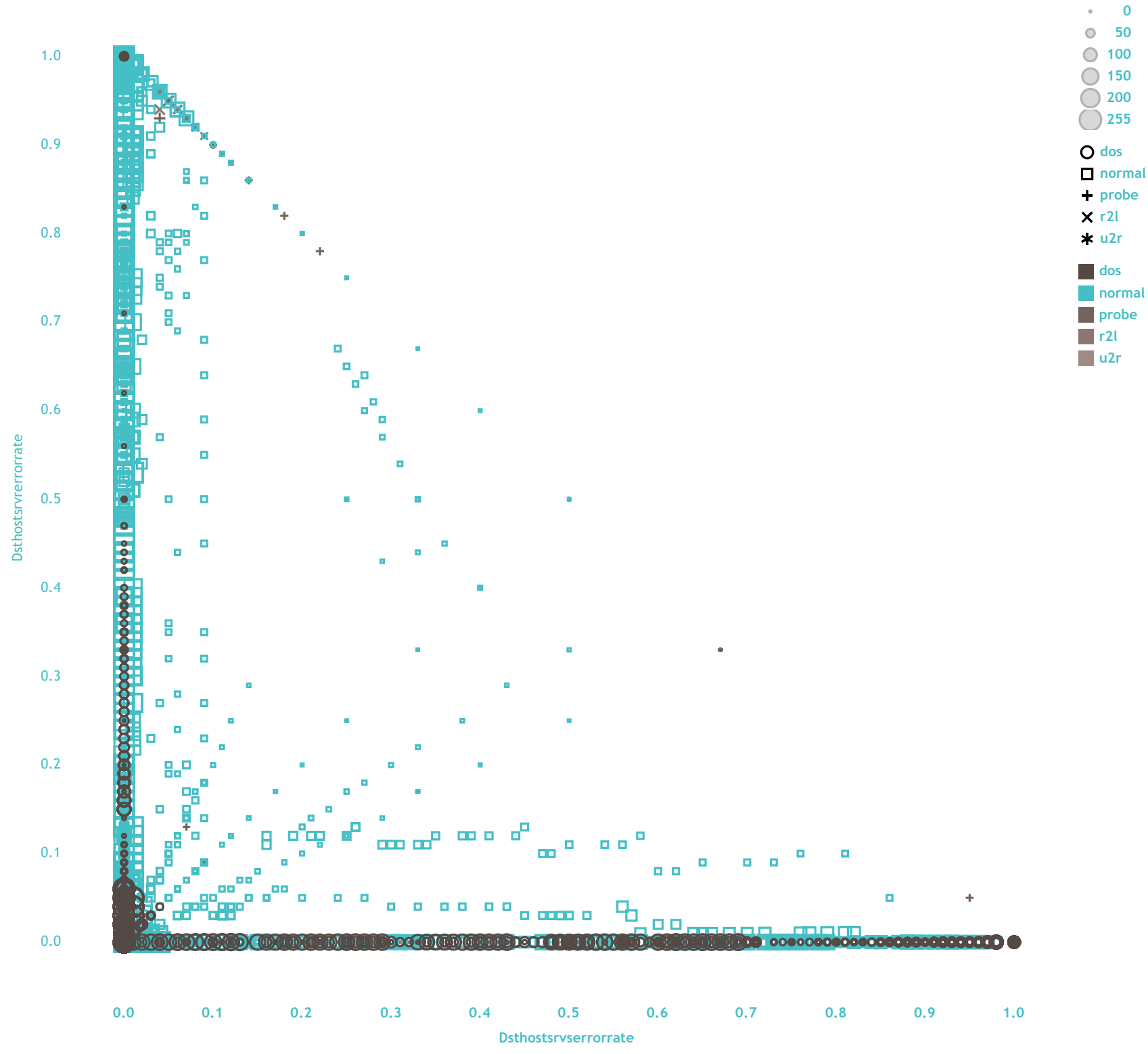
SUM([Dsthostcount]) / TOTAL(SUM([Dsthostcount])) and Flag_category broken down by Flag_category. Color shows details about Flag_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

-SUM([Srvcount]), -SUM([Srvcount]), -SUM([R_errors_srv_count]) and -SUM([S_errors_srv_count]) for each Attack_category. Color shows details about -SUM([Srvcount]), -SUM([R_errors_srv_count]) and -SUM([S_errors_srv_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



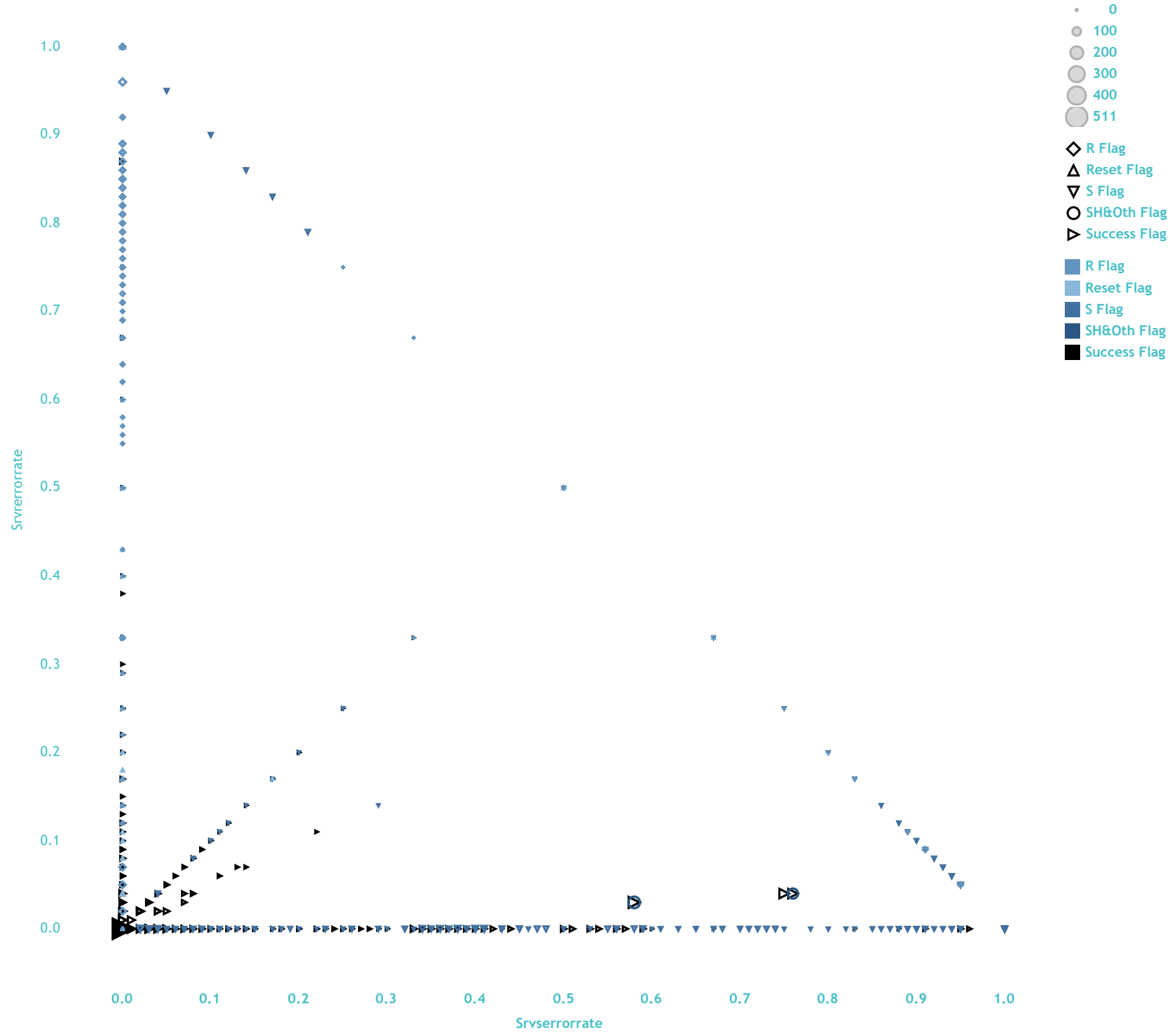
Srvserrorrate vs. Srvrerrorrate. Color shows details about Attack_category. Size shows Srvcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.

-SUM([Dsthostsrvcount]), -SUM([Dsthostsrvcount]), -SUM([Dsthost_R_errors_srv_count]) and -SUM([Dsthost_S_errors_srv_count]) for each Attack_category. Color shows details about -SUM([Dsthostsrvcount]), -SUM([Dsthost_R_errors_srv_count]) and -SUM([Dsthost_S_errors_srv_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



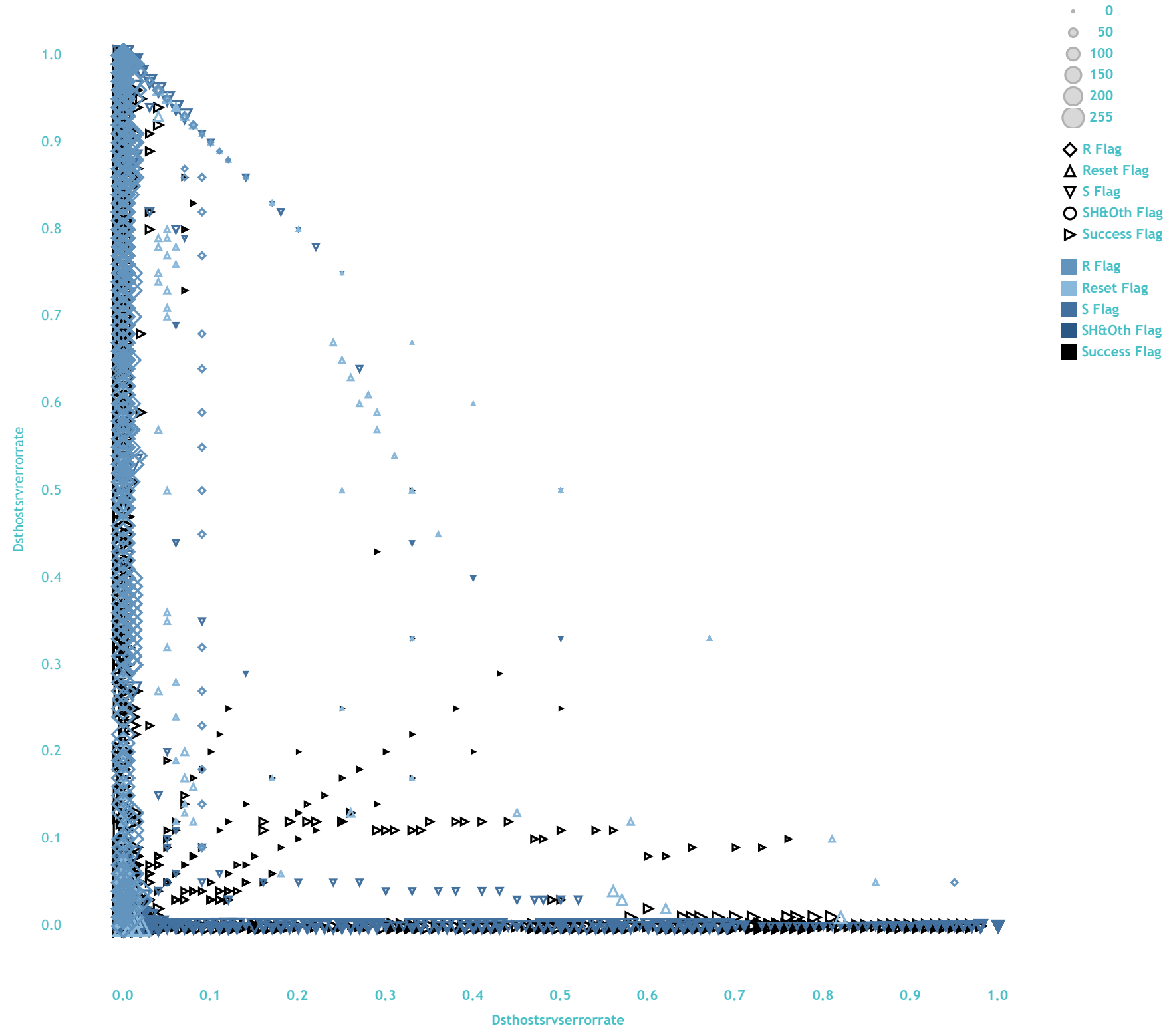
Dsthostsrvserrorrate vs. Dsthostsrvrerrorrate. Color shows details about Attack_category. Size shows Dsthostsrvcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.

-SUM([Srvcount]), -SUM([Srvcount]), -SUM([R_errors_srv_count]) and -SUM([S_errors_srv_count]) for each Flag_category. Color shows details about -SUM([Srvcount]), -SUM([R_errors_srv_count]) and -SUM([S_errors_srv_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.



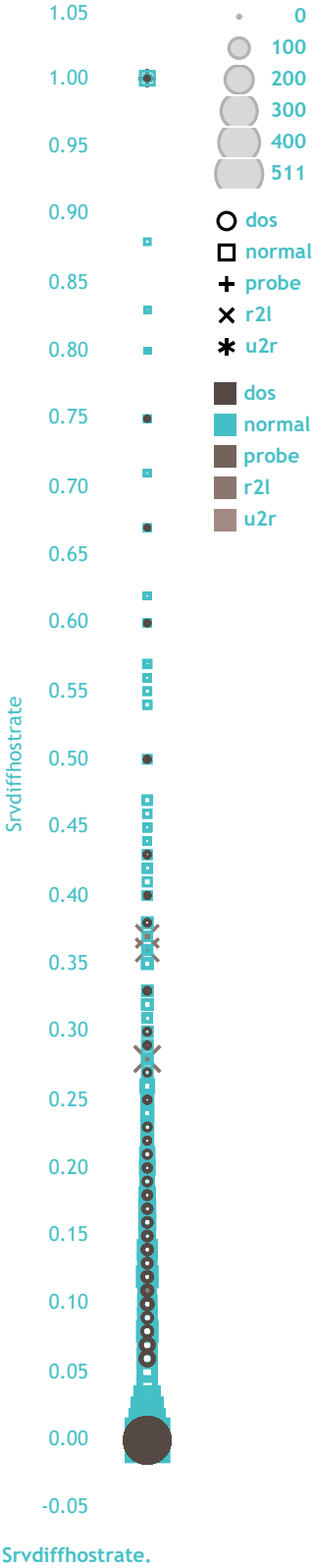
Srvserrorrate vs. Srvrerrorrate. Color shows details about Flag_category. Size shows Srvcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

-SUM([Dsthostsrvcount]), -SUM([Dsthostsrvcount]), -SUM([Dsthost_R_errors_srv_count]) and -SUM([Dsthost_S_errors_srv_count]) for each Flag_category. Color shows details about -SUM([Dsthostsrvcount]), -SUM([Dsthost_R_errors_srv_count]) and -SUM([Dsthost_S_errors_srv_count]). The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



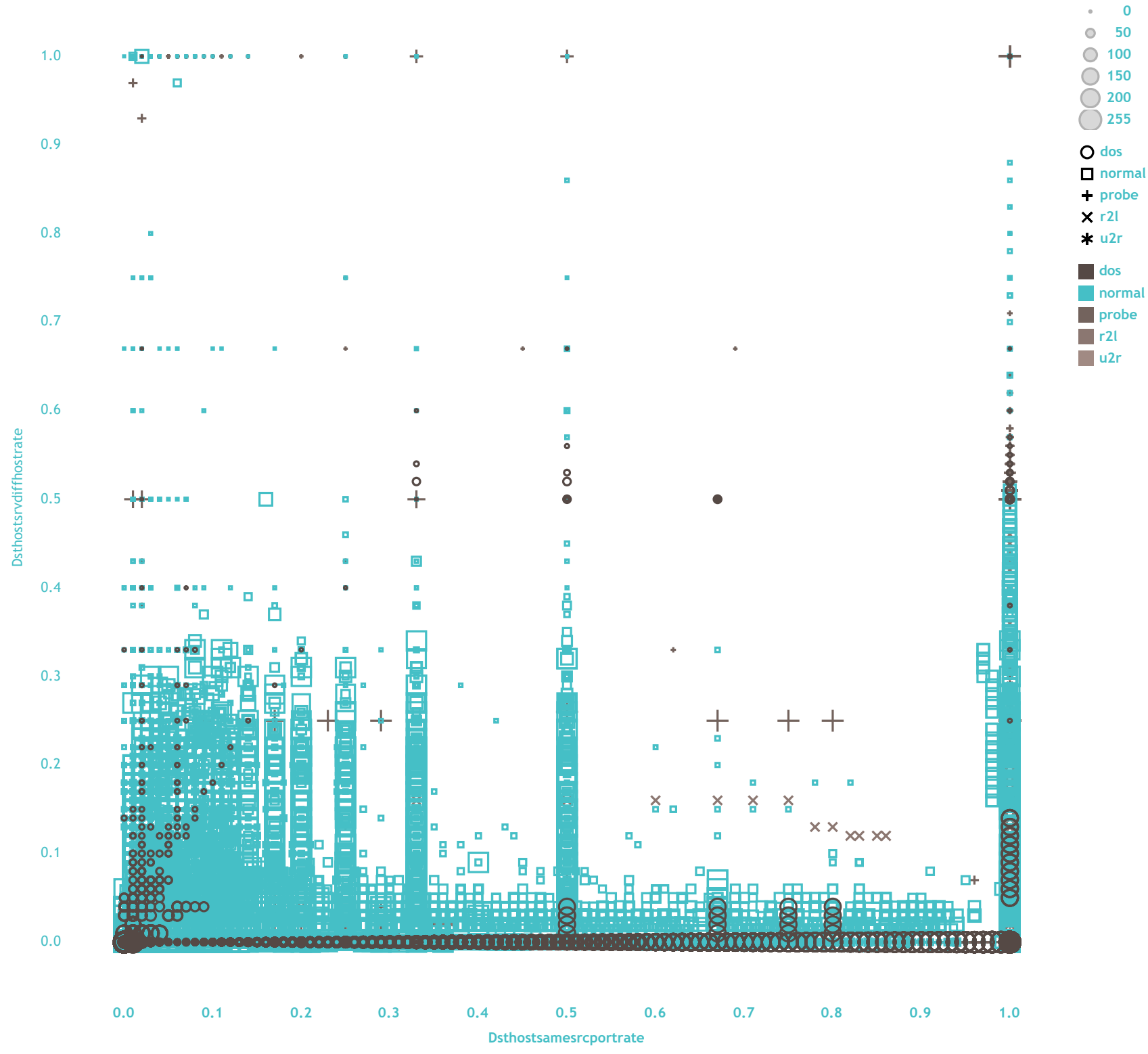
Dsthostsrvserrorrate vs. Dsthostsrvrerrorrate. Color shows details about Flag_category. Size shows Dsthostsrvcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

Srvcount and Srvdiffhost_count for each Attack_category. Color shows details about Srvcount and Srvdiffhost_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



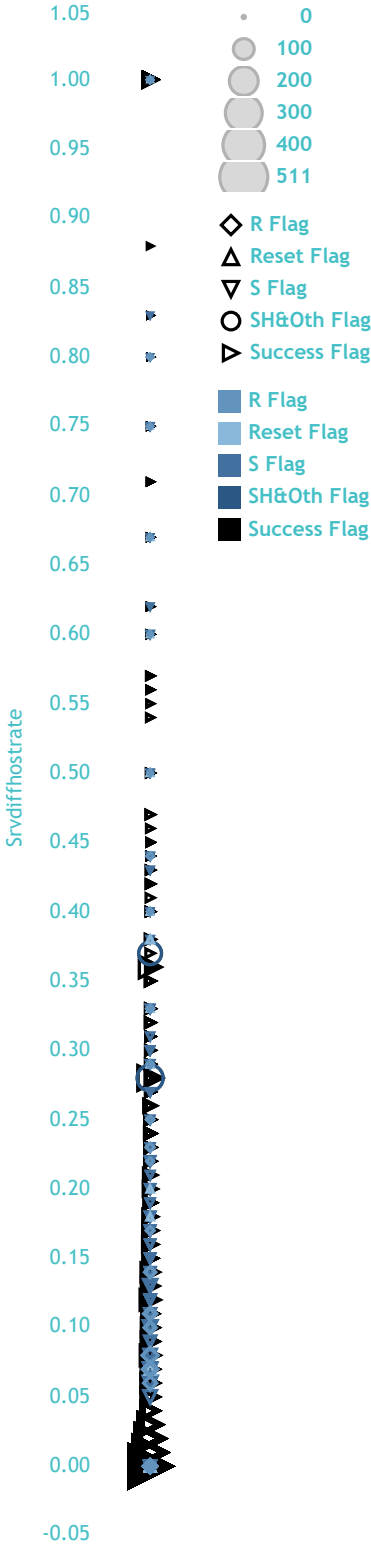
Srvdiffhostrate. Color shows details about Attack_category. Size shows Srvcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Flag_category) and Tooltip (Attack_category). The Tooltip (Flag_category) filter keeps 5 members. The Tooltip (Attack_category) filter keeps 5 members.

Dsthostsrvcount, Dsthostsrvcount, Dsthost_srv_diff_host_srv_count and Dsthost_same_src_port_srv_count for each Attack_category. Color shows details about Dsthostsrvcount, Dsthost_srv_diff_host_srv_count and Dsthost_same_src_port_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Attack_category, which keeps dos, normal, probe, r2l and u2r.



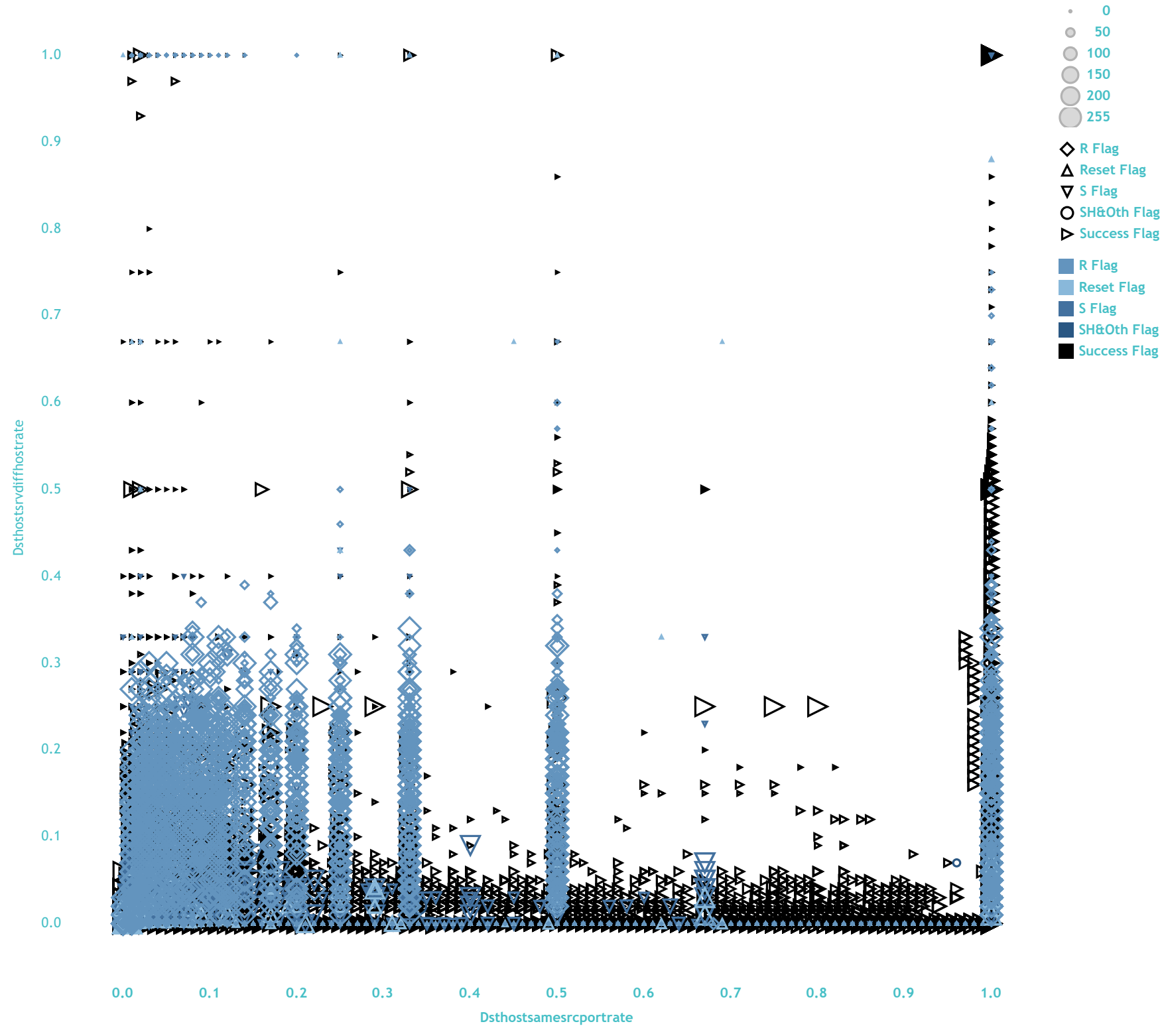
Dsthostsamesrcportrate vs. Dsthostsrvdiffhostrate. Color shows details about Attack_category. Size shows Dsthostsrvcount. Shape shows details about Attack_category. The data is filtered on Tooltip (Attack_category), which keeps 5 members.

Srvcount and Srvdiffhost_count for each Flag_category. Color shows details about Srvcount and Srvdiffhost_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



Srvdiffhostrate. Color shows details about Flag_category. Size shows Srvcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

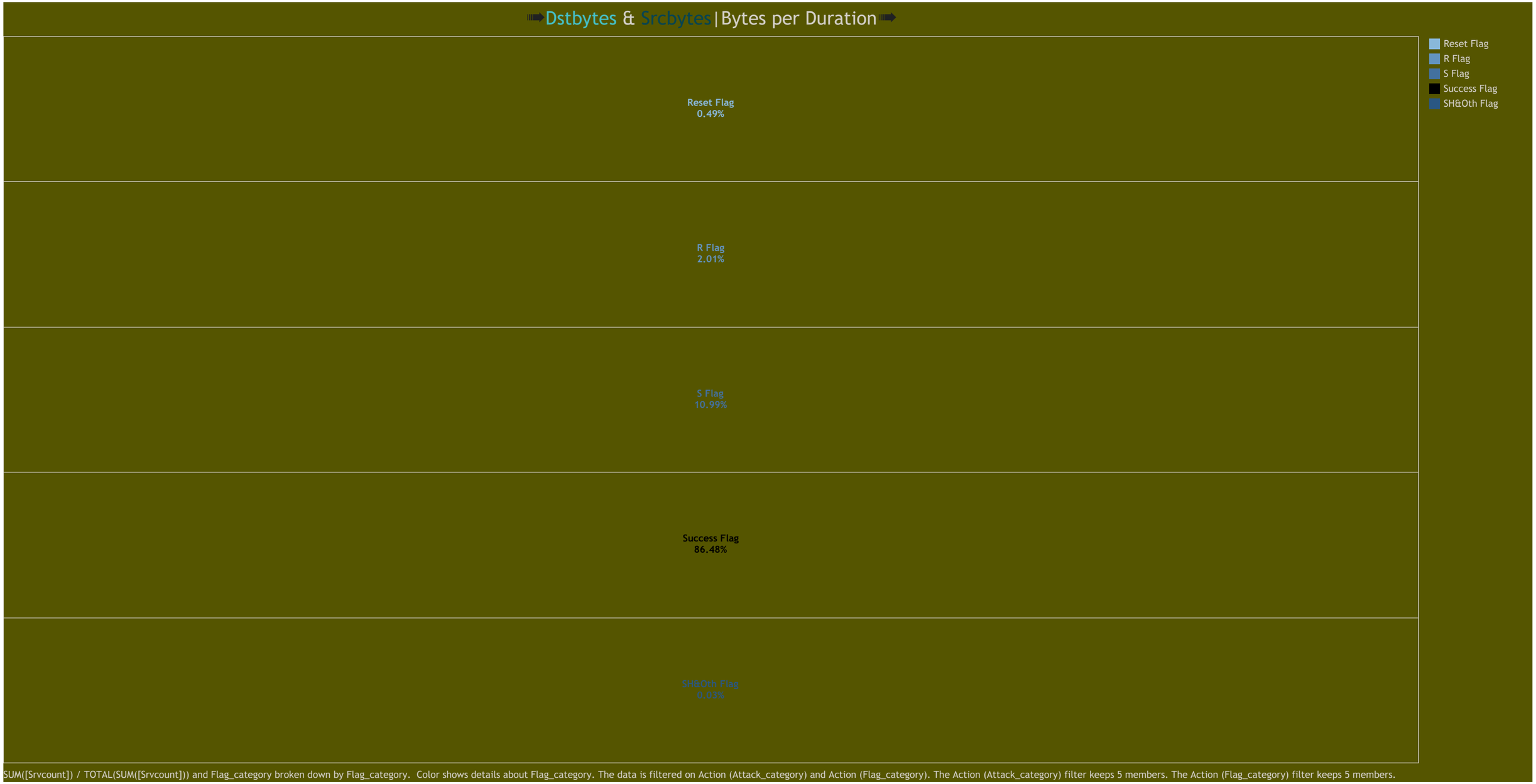
Dsthostsrvcount, Dsthostsrvcount, Dsthost_srv_diff_host_srv_count and Dsthost_same_src_port_srv_count for each Flag_category. Color shows details about Dsthostsrvcount, Dsthost_srv_diff_host_srv_count and Dsthost_same_src_port_srv_count. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members. The view is filtered on Flag_category, which keeps R Flag, Reset Flag, S Flag, SH&Oth Flag and Success Flag.



Dsthostsamesrcportrate vs. Dsthostsrvdiffhostrate. Color shows details about Flag_category. Size shows Dsthostsrvcount. Shape shows details about Flag_category. The data is filtered on Tooltip (Flag_category), which keeps 5 members.

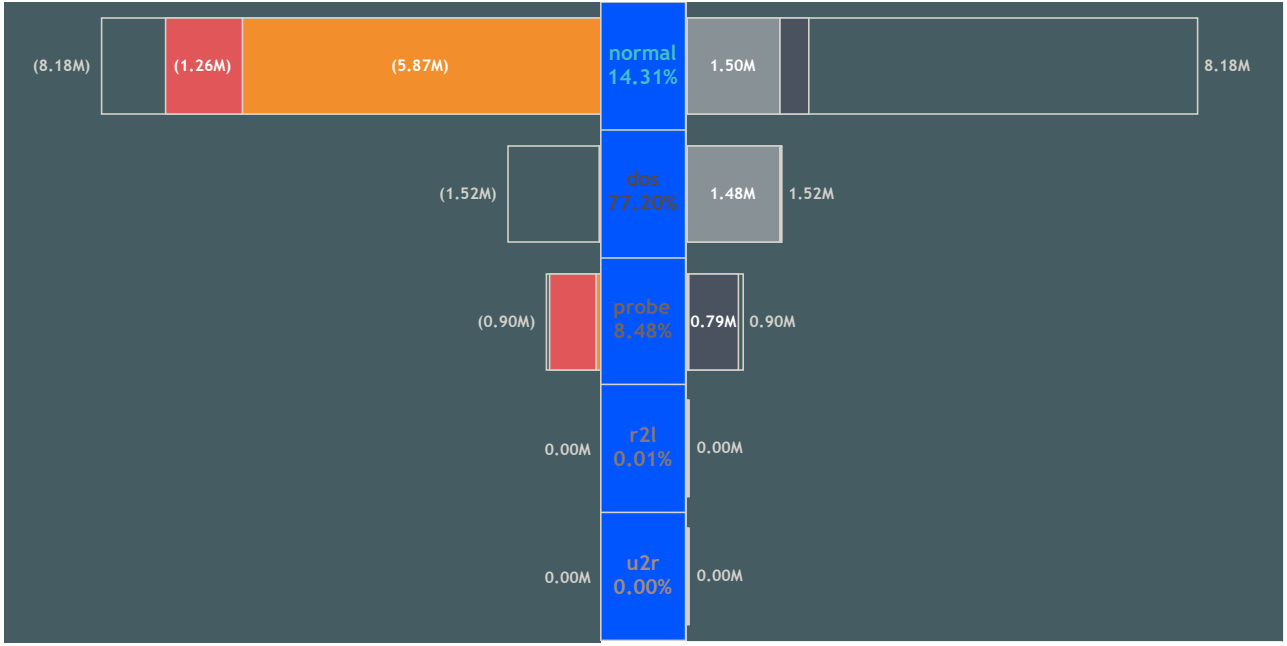
SUM([Srvcount]) / TOTAL(SUM([Srvcount])) and Attack_category broken down by Attack_category. Color shows details about Attack_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

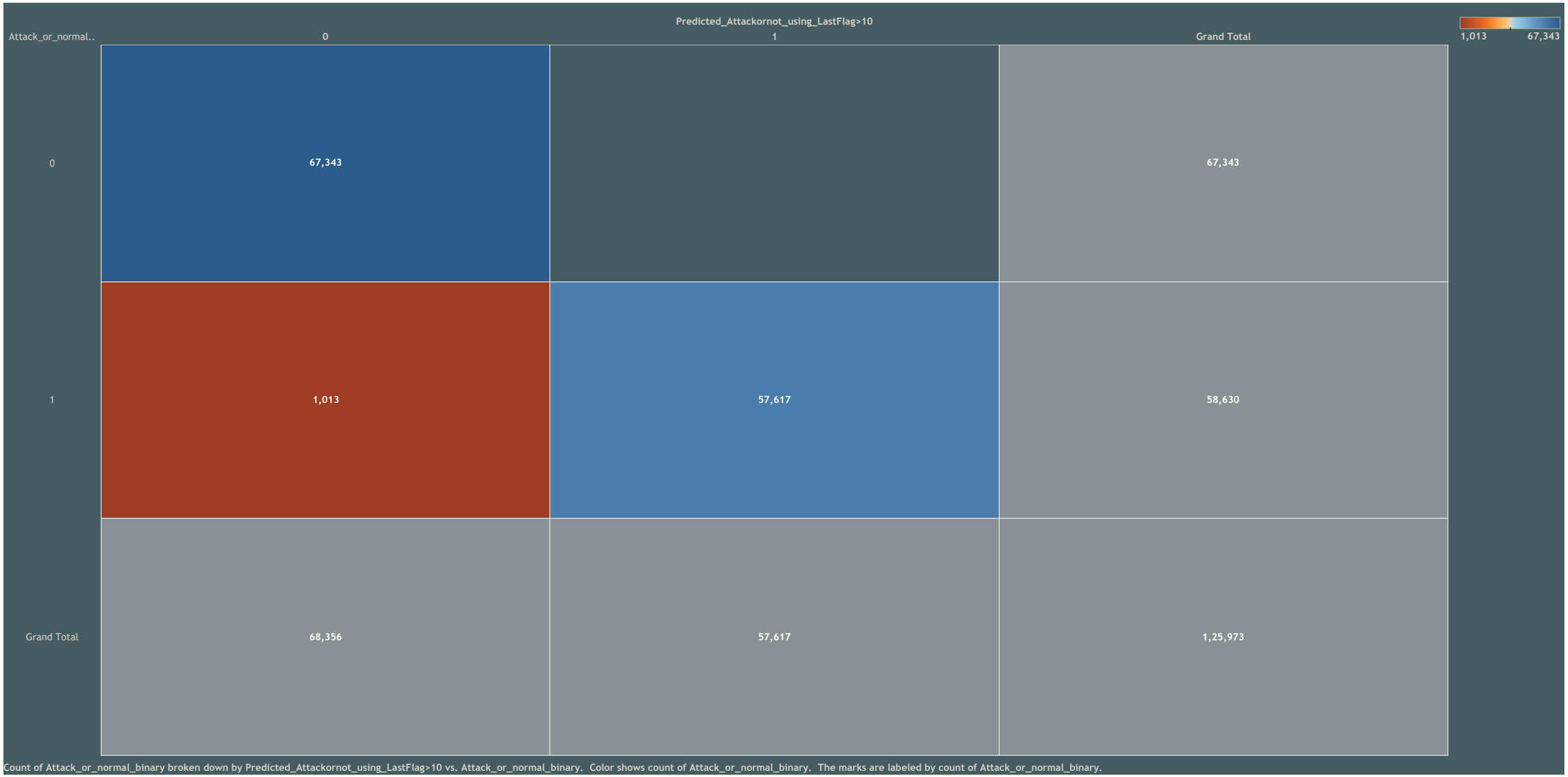
SUM([Dsthostsrvcount]) / TOTAL(SUM([Dsthostsrvcount])) and Attack_category broken down by Attack_category. Color shows details about Attack_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.



SUM([Srvcount]) / TOTAL(SUM([Srvcount])) and Flag_category broken down by Flag_category. Color shows details about Flag_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.

SUM([Dsthostsrvcount]) / TOTAL(SUM([Dsthostsrvcount])) and Flag_category broken down by Flag_category. Color shows details about Flag_category. The data is filtered on Action (Attack_category) and Action (Flag_category). The Action (Attack_category) filter keeps 5 members. The Action (Flag_category) filter keeps 5 members.


(8.18M)
(1.26M)
(5.87M)
normal
14.31%
1.50M
8.18M
(1.52M)
dos
77.20%
1.48M
1.52M
(0.90M)
probe
8.48%
0.79M
0.90M
0.00M
r2l
0.01%
0.00M
0.00M
u2r
0.00%
0.00M



Count of Attack_or_normal_binary broken down by Predicted_Attackornot_using_LastFlag>10 vs. Attack_or_normal_binary. Color shows count of Attack_or_normal_binary. The marks are labeled by count of Attack_or_normal_binary.

Predicted_values

Count of Actual_values
1 13,267

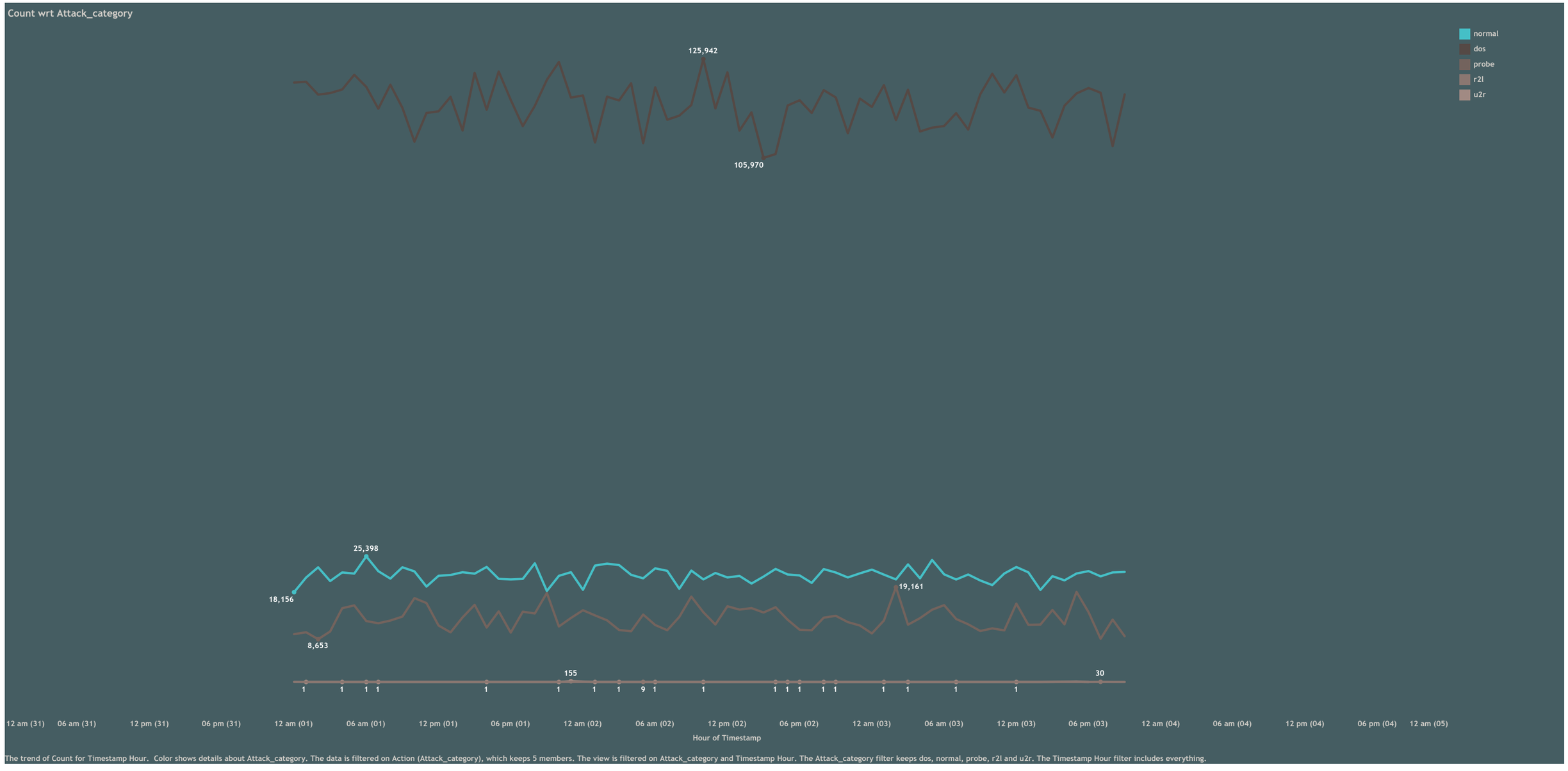
Actual_v..	dos	normal	probe	r2l	u2r
dos	9,124	55	7		
normal	61	13,267	38	73	30
probe	23	108	2,200		
r2l		129	1	69	
u2r		3	1		6

Count of Actual_values broken down by Predicted_values vs. Actual_values. Color shows count of Actual_values. The marks are labeled by count of Actual_values.

```
Test Data Accuracy: 97.90%
```

Accuracy.

Count wrt Attack_category



The trend of Count for Timestamp Hour. Color shows details about Attack_category. The data is filtered on Action (Attack_category), which keeps 5 members. The view is filtered on Attack_category and Timestamp Hour. The Attack_category filter keeps dos, normal, probe, r2l and u2r. The Timestamp Hour filter includes everything.

03-01-1999 21:48:30	dos neptune | S0	Web and Internet Services tcp | Z39_50 | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:26	dos neptune | REJ	Miscellaneous and Legacy Services tcp | bgp | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:16	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:14	dos neptune | REJ	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:12	dos neptune | REJ	Miscellaneous and Legacy Services tcp | auth | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:08	dos neptune | S0	Web and Internet Services tcp | Z39_50 | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:06	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:48:02	dos neptune | S0	Remote Access and Control Services tcp | rje | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:58	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:54	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:48	dos neptune | REJ	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:44	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:38	dos neptune | S0	Remote Access and Control Services tcp | telnet | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:36	probe satan | SF	Miscellaneous and Legacy Services udp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:34	probe nmap | SH	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:32	dos neptune | S0	Web and Internet Services tcp | http | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:30	dos neptune | S0	Miscellaneous and Legacy Services tcp | vmnet | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:26	dos smurf | SF	Miscellaneous and Legacy Services icmp | ecr_i | 1.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:24	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:10	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:06	dos neptune | S0	Remote Access and Control Services tcp | supdup | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:02	dos neptune | REJ	Miscellaneous and Legacy Services tcp | courier | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:47:00	dos neptune | REJ	File Transfer and Storage Services tcp | ftp_data | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:56	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:54	dos neptune | REJ	Email and Messaging Services tcp | nnsp | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:50	probe satan | SF	Miscellaneous and Legacy Services udp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:38	dos neptune | RSTO	Remote Access and Control Services tcp | login | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:36	dos neptune | REJ	Web and Internet Services tcp | whois | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	
03-01-1999 21:46:32	dos neptune | S0	Miscellaneous and Legacy Services tcp | sunrpc | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0	

dos
probe

dos
probe

Count
Dsthostcount
Dsthostsrvcount
Srvcount

	Attack_category [Attack_type | Flag]	Service_category [Protocol | Service | Srcbytes | Dstbytes | Duration]	Wrongfragment | Urgent | Hot | Numfailedlogins | Numcompromised | Numroot | Numfilecreations | Numshells | Numaccessfiles [Loggedin | Ishostlogin | Isguestlogin | Rootshell | Land | Suattempted]	Count (Big bar) [Srvcount(Small bar)]	Dsthostcount (Big bar) [Dsthostsrvcount (Small bar)]

Avg(-1.0), Avg(-1.0), Avg(-1.0), Count, Srvcount, Dsthostcount and Dsthostsrvcount for each Timestamp. For pane Avg(-1.0): Color shows details about Attack_category. Shape shows details about Attack_category. The marks are labeled by Attack_category, Attack and Flag. For pane Avg(-1.0) (2): The marks are labeled by Service_category_abbreviation, Protocoltype, Service, Srcbytes, Dstbytes and Duration. For pane Avg(-1.0) (3): The marks are labeled by Loggedin, Ishostlogin, Isguestlogin, Rootshell, Suattempted, Land, Wrongfragment, Urgent, Hot, Numfailedlogins, Numcompromised, Numroot, Numfilecreations, Numshells and Numaccessfiles. For pane Count: Color shows details about Count, Srvcount, Dsthostcount and Dsthostsrvcount. For pane Srvcount: Color shows details about Count, Srvcount, Dsthostcount and Dsthostsrvcount. For pane Dsthostcount: Color shows details about Count, Srvcount, Dsthostcount and Dsthostsrvcount. For pane Dsthostsrvcount: Color shows details about Count, Srvcount, Dsthostcount and Dsthostsrvcount. The data is filtered on Second of Timestamp, which ranges from 03-01-1999 21:46:32 to 03-01-1999 21:48:32. The view is filtered on Attack_category, Attack, Flag, Protocoltype and Timestamp. The Attack_category filter keeps dos, probe, r2l and u2r. The Attack filter keeps 23 of 23 members. The Flag filter keeps 11 of 11 members. The Protocoltype filter keeps icmp, tcp and udp. The Timestamp filter keeps 1,25,973 of 1,25,973 members.

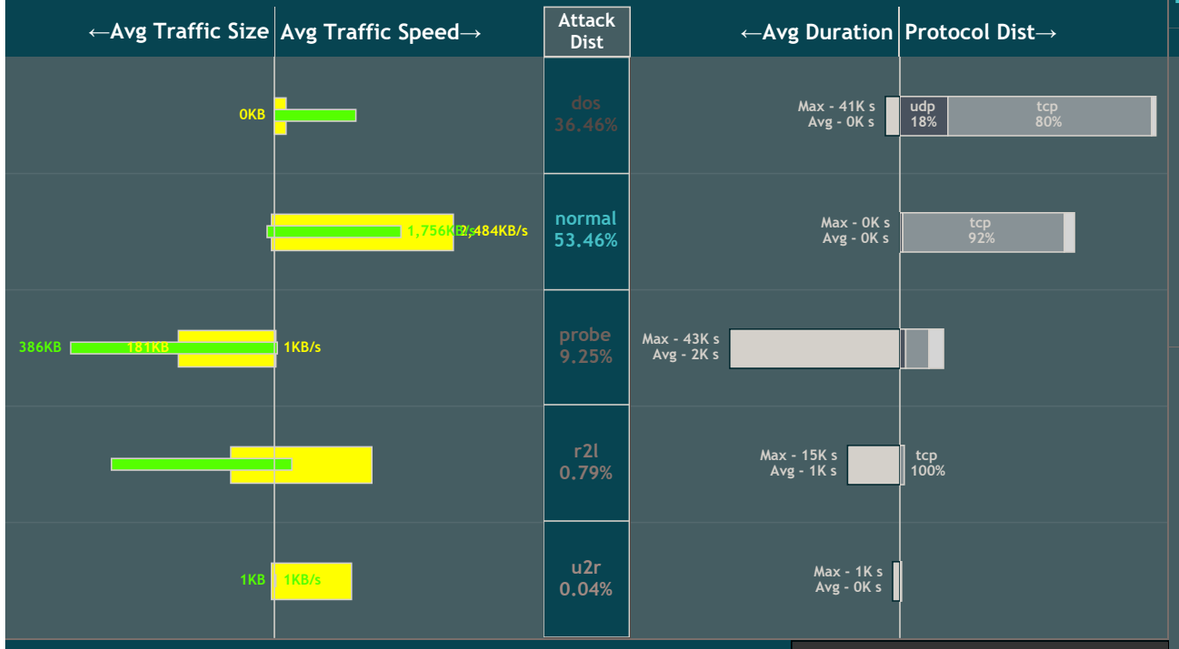
NETWORK CONNECTION METRICS DASHBOARD | Basic & Content Features

Dashboards | Export | Follow | Info | Filters

Dstbytes	Srcbytes	Duration	Attacks	Fail Logins	Wrong Frags	Urgent Pkts	Compromises	Root Accesses	File Creations	Hot Inds	Shell Prompts	Access File Ops
2.49GB	5.74GB	36.17M s	58,630	154	2,858	14	35,178	38,068	1,596	25,750	52	516
2.20GB attacked	4.86GB attacked	24.82M s attacked	1,25,973 Total	61 attacked	2,858 attacked	4 attacked	1,030 attacked	159 attacked	96 attacked	10,217 attacked	11 attacked	11 attacked

Inbound vs Outbound Traffic

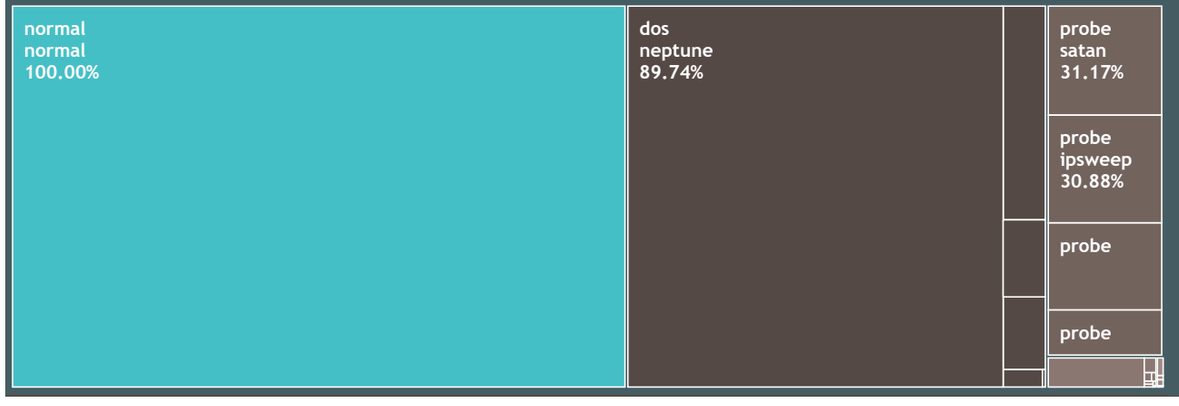
Dstbytes | Srcbytes | Duration | udp | tcp | icmp



Attack Cat Vs Type Correlation

normal | dos | probe | r2l | u2r

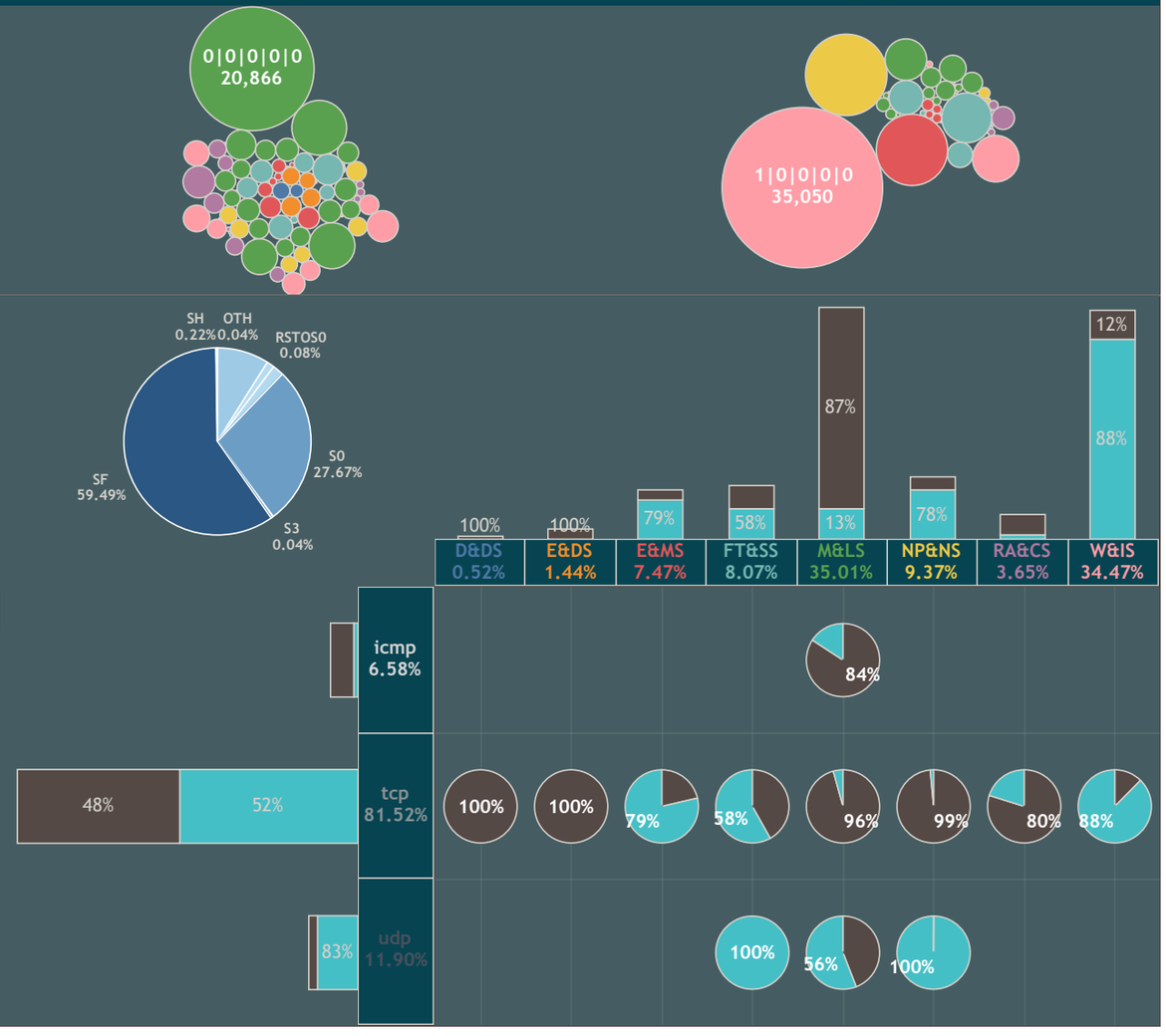
Attack Cat vs Flag (Click here)



Login | Ishost | Isguest | Root | Su_Root vs Services & Protocol

Attack | normal

Highlight Service_cat
No items highlighted



ADVANCED TRAFFIC PATTERNS DASHBOARD | Time & Host Based Features

Dashboards | Export | Follow | Info | Filters

Confusion Matrix of GBDT Model

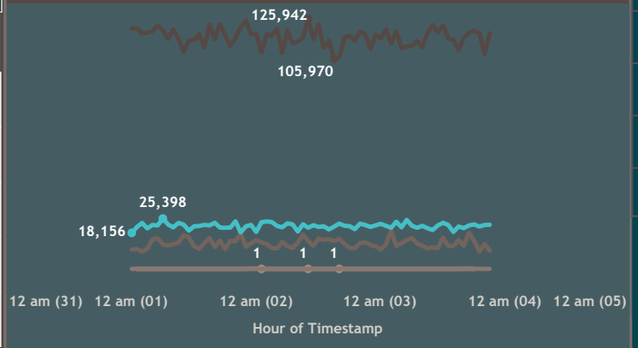
Test Data Accuracy: 97.90%

Actual_v.. \ Predicted_values	dos	normal	probe	r2l	u2r
dos	9,124	55	7		
normal	61	13,267	38	73	30
probe	23	108	2,200		
r2l		129	1	69	
u2r		3	1		6

Hourly TIme Series Plots

(Use Measure Names filter to change plot)

Count wrt Attack_category



Details of Recently Detected Anomalies

(Use filters to change table)

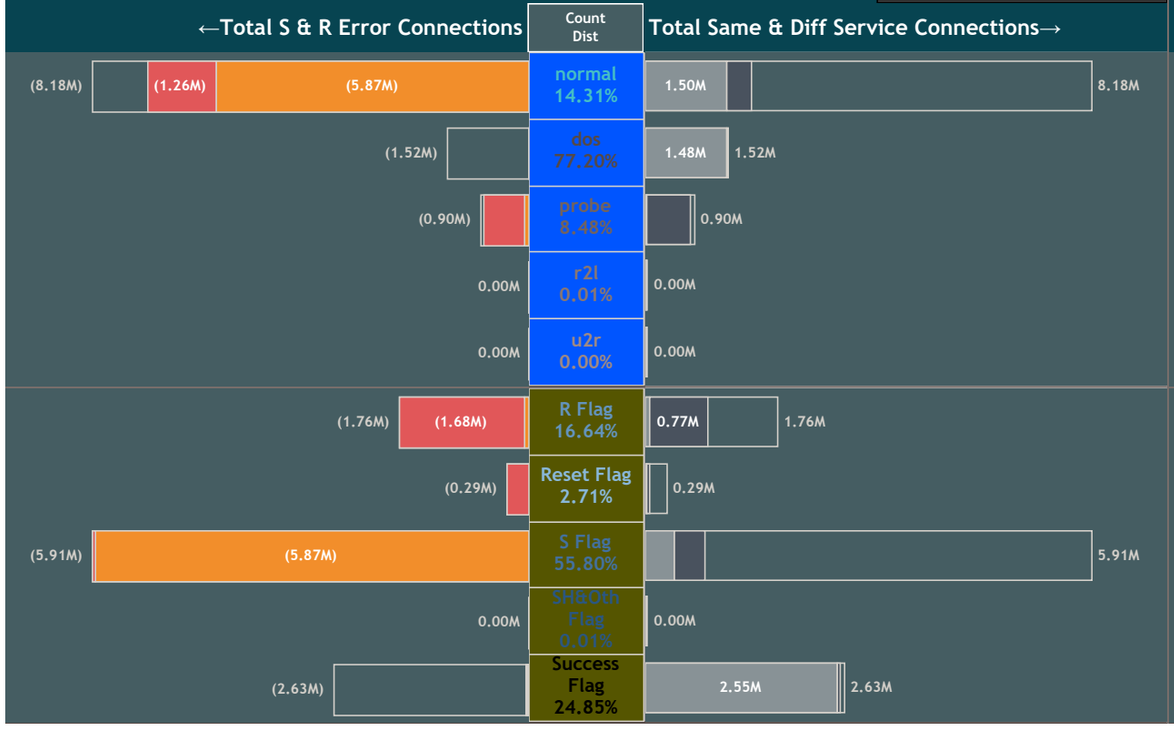
03-01-1999 21:48:30	dos neptune | S0	Web and Internet Services tcp | Z39_50 | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0
03-01-1999 21:48:26	dos neptune | REJ	Miscellaneous and Legacy Services tcp | bgp | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0
03-01-1999 21:48:16	dos neptune | S0	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0
03-01-1999 21:48:14	dos neptune | REJ	Miscellaneous and Legacy Services tcp | private | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0
03-01-1999 21:48:12	dos neptune | REJ	Miscellaneous and Legacy Services tcp | auth | 0.0KB | 0.0KB | 0.0K s	0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0

Attack_category [Attack_type | Flag] | Service_category [Protocol | Service | Srcbytes | Dstbytes| Duration] | Wrongfragment | Urgent | Hot | Numfailedlogins | Numcompromised | Numroot | Numfilecreations | Numshells | Numaccessfiles | Loggedin | Ishostlogin | Isguestlogin | Rootshell | Land | Suattempted] | Count (Big bar) [S

TIme Based Features wrt Attacks & Flags

■ S errors ■ R errors ■ Same Srv/host ■ Diff Srv/host

Srvcount charts (click here)



Host Based Features wrt Attacks & Flags

■ S errors ■ R errors ■ Same Srv/host ■ Diff Srv/host

Dst_Srvcount charts (click here)