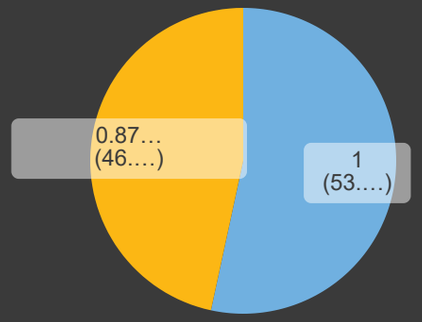
Network Intrusion Detection

Intrusion Rate By Class



class
- anomaly
- normal

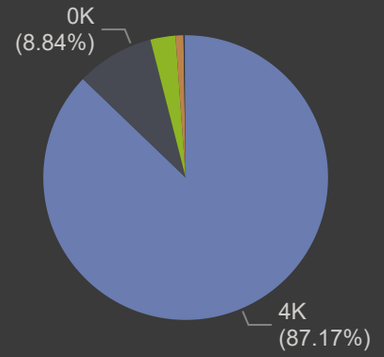
Protocol Type

icmp | tcp | udp

0.47	4989	30
Intrusion Rate	Sum of Hot Flags	Sum Failed Logins

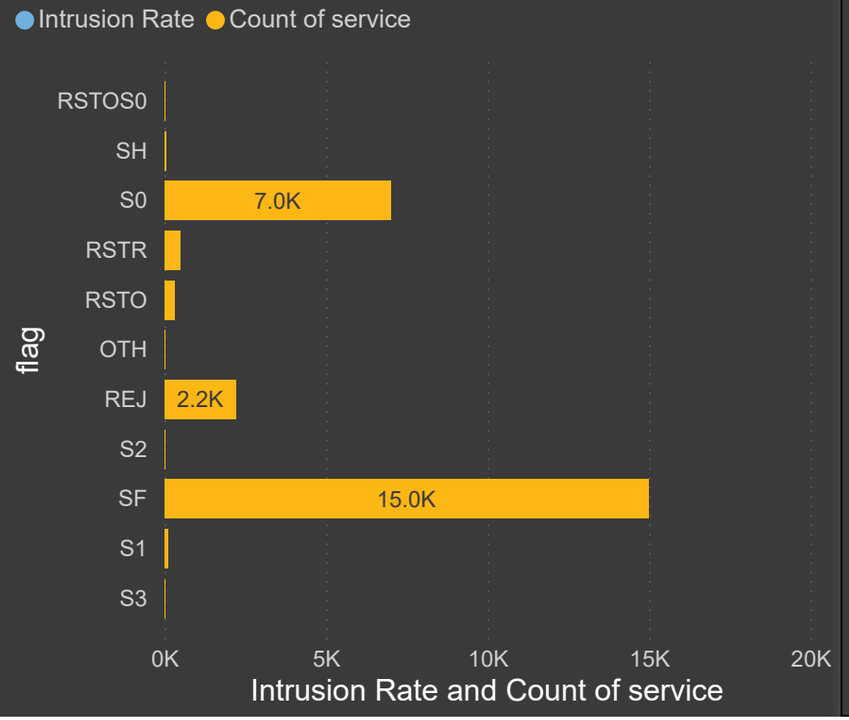
5740
Total Sum Compromised

Sum Service by Flags



service
- ftp
- http
- telnet
- ftp_data
- smtp
- imap4
- finger
- pop_3
- ssh
- sunrpc
- time
- auth
- bgp

Intrusion Rate and Count of service by flag



Key influencers | Top segments

What influences class to be normal ?

When... ....the likelihood of class being normal increases by

flag is SF	11.67x
service is http	2.79x
service is domain_u	2.01x
service is smtp	1.90x
service is urp_i	1.88x
Sum of hot is more than 28	1.88x
service is IRC	1.88x
service is ntp_u	1.88x

Sort by: **Impact** Count

protocol_type

All

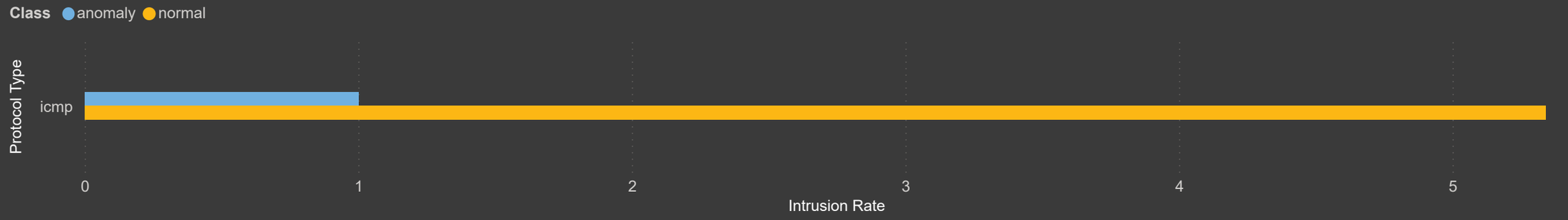
flag

All

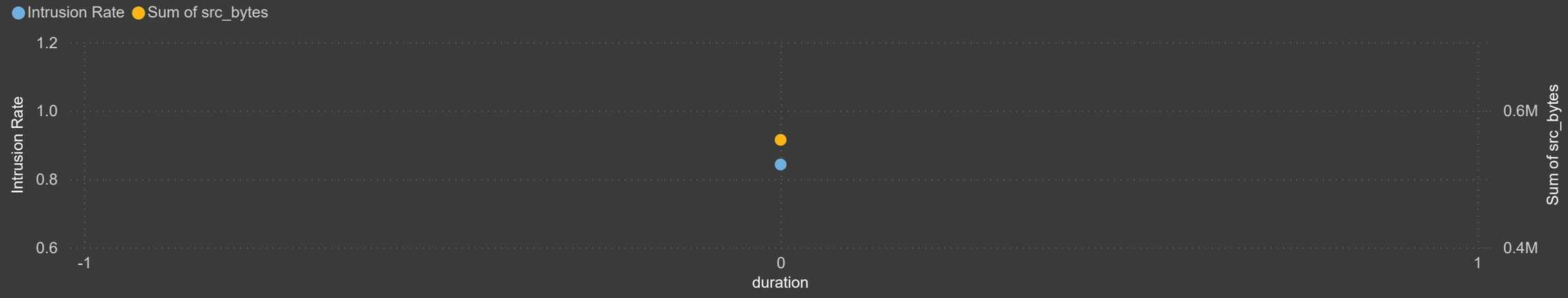
service

All

Intrusion Rate by Protocol Type



Intrusion Rate and Sum of src_bytes by duration



“Hot Flags indicate attempts to access sensitive files. A high value may suggest suspicious activity.”

Flag Definitions

- RSTOS0 **Meaning**: is a term used in the context of TCP connection establishment and termination. It refers to a situation where the originator sent a SYN followed by a RST, but never received a SYN-ACK from the responder.

- SH **Meaning**: Incomplete Handshake

- S0 **Meaning**: Connection attempt seen, no reply

- RSTR **Meaning**: Stands for "Reset by Responder." The server (responder) sent a RST (Reset) packet to terminate the connection, typically because the connection was unexpected, invalid, or not allowed. **Context**: This flag is often associated with failed connection attempts, such as when a client tries to connect to a closed port or a server detects suspicious activity and forcefully closes the connection. **Example Scenario**: A client attempts to connect to a port that is not open, and the server responds with a RST packet to terminate the attempt.

- OTH **Meaning**: The **OTH** flag indicates a TCP connection that does not fit into the standard categories of connection states (e.g., SF, S0, REJ, RSTR, etc.). It represents connections with unusual or non-standard behavior that cannot be classified under the typical TCP handshake or termination patterns. **Context**: This flag is used for connections that lack a clear SYN, ACK, RST, or FIN sequence, or where the connection state is ambiguous. It may include malformed packets, non-TCP traffic (if misclassified), or other anomalies not captured by the dataset's predefined flag categories. **Example Scenario**: A connection with incomplete or corrupted packets, or traffic that doesn't follow standard TCP protocol behavior, such as certain types of network scans or errors in packet capture.

- REJ **Meaning**: Connection attempted rejected

- S2 **Meaning**: Indicates a connection attempt where the client sent a SYN packet, received a SYN-ACK from the server, and sent an ACK, but the connection was interrupted or reset before significant data transfer (e.g., the client sent a RST after the ACK). **Context**: This flag suggests a connection that progressed further than S1 (where only SYN and SYN-ACK are exchanged) but was still terminated early, possibly due to an error or intentional reset by the client. **Example Scenario**: A client begins a connection but aborts it shortly after the handshake, perhaps due to a timeout or an intrusion attempt being detected.

- S1 **Meaning**: Normal establishment

- S3 **Meaning**: Similar to S2, but indicates a connection that progressed slightly further, where some data may have been sent after the handshake but the connection was still terminated abnormally (e.g., by a RST or timeout). **Context**: This flag represents a connection that got past the initial handshake and possibly exchanged a small amount of data before being reset or dropped, often seen in failed or malicious connection attempts. **Example Scenario**: A client establishes a connection, sends a small amount of data (e.g., part of an exploit), but the server or client terminates the connection prematurely.