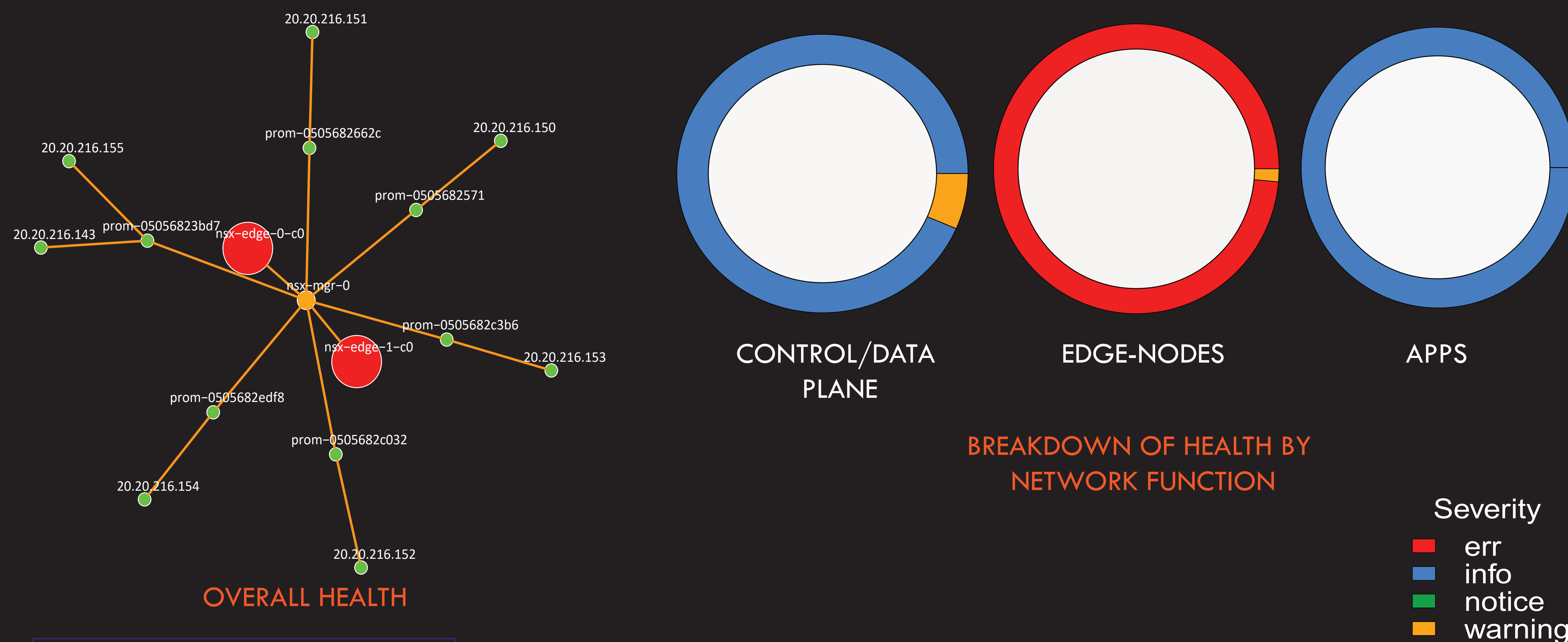# DEEP NETWORK VISUALIZATION

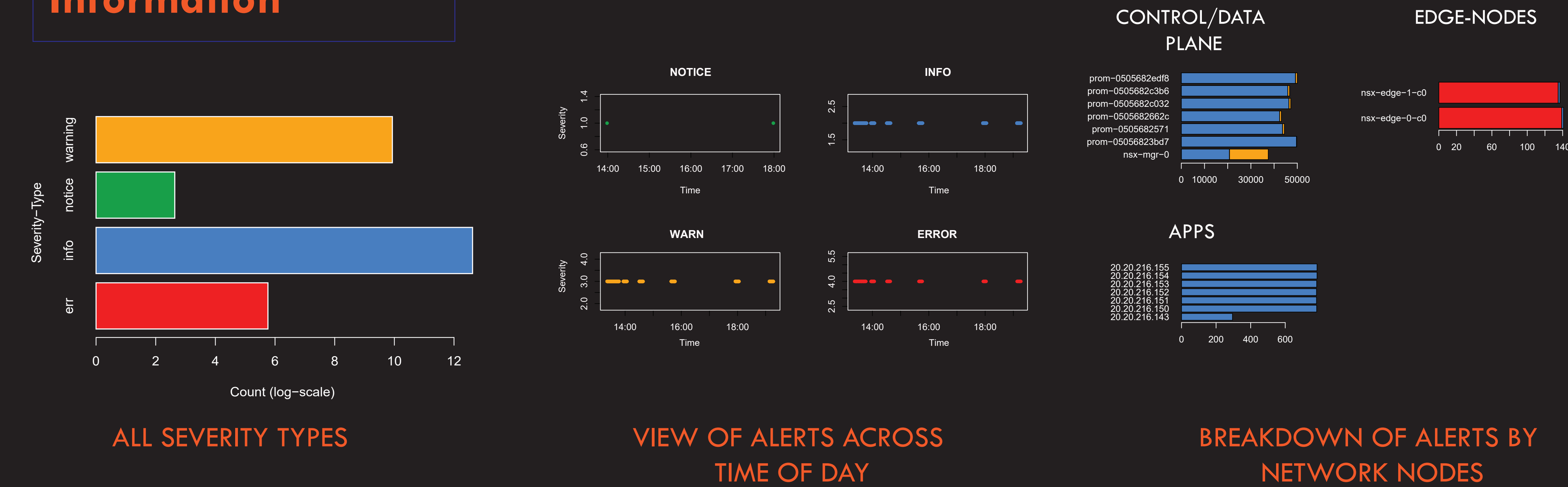## Visualizing network health for enterprise/cloud Ops

By Sharat Sripada IST-719 Spring 2022

Introduction and Health charts

Network Nodes and software components emit anamoly and health metrics via logs. Using visualizations on unstructured data, an enterprise/cloud admin can answer the following questions:

- What is the health of the network?
- Can I drill from a macro to micro view of the network?
- What severities of error categories exist?
- Is there a time of day where log volume/severities happen more?

20.20.216.151
prom-0505682662c
20.20.216.150
20.20.216.155
prom-0505682571
20.20.216.143 prom-05056823bd7
nsx-edge-0-c0
nsx-mgr-0
prom-0505682c3b6
nsx-edge-1-c0
20.20.216.153
prom-0505682edf8
prom-0505682c032
20.20.216.154
20.20.216.152

OVERALL HEALTH

CONTROL/DATA PLANE

EDGE-NODES

APPS

BREAKDOWN OF HEALTH BY NETWORK FUNCTION

Severity
- err
- info
- notice
- warning

General Information

ALL SEVERITY TYPES

Severity-Type: warning, notice, info, err
Count (log-scale): 0 2 4 6 8 10 12

VIEW OF ALERTS ACROSS TIME OF DAY

NOTICE
Severity: 0.6 1.0 1.4
Time: 14:00 15:00 16:00 17:00 18:00

INFO
Severity: 1.5 2.5
Time: 14:00 16:00 18:00

WARN
Severity: 2.0 3.0 4.0
Time: 14:00 16:00 18:00

ERROR
Severity: 2.5 4.0 5.5
Time: 14:00 16:00 18:00

CONTROL/DATA PLANE
prom-0505682edf8
prom-0505682c3b6
prom-0505682c032
prom-0505682662c
prom-0505682571
prom-05056823bd7
nsx-mgr-0
0 10000 30000 50000

EDGE-NODES
nsx-edge-1-c0
nsx-edge-0-c0
0 20 60 100 140

APPS
20.20.216.155
20.20.216.154
20.20.216.153
20.20.216.152
20.20.216.151
20.20.216.150
20.20.216.143
0 200 400 600

BREAKDOWN OF ALERTS BY NETWORK NODES

About the data

- Rows and columns: 323972 * 78
- Data was scrubbed for basic EDA and cleaned off long or repeating strings like node-names etc. for brewity in chart labels

NETWORK NODES
1   2   3
Send log data
Log-aggregator

Source: .csv/log aggregator
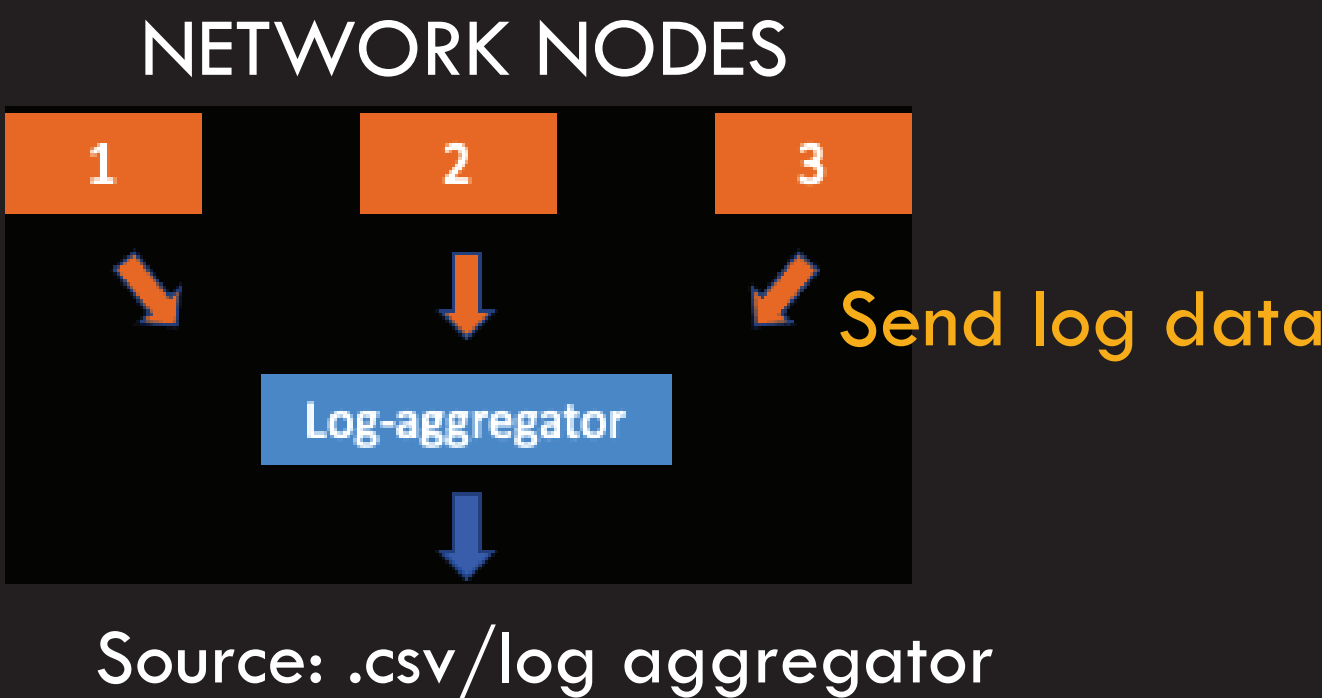
Data was exported as .csv from a centralised log aggregator where all nodes send data in the form of unstructured logs