Web and Linux System Integration

Jose Varela, Advisor: Dr. Ching-yu (Austin) Huang
School of Computer Science, Kean University, chuang@kean.edu

Abstract

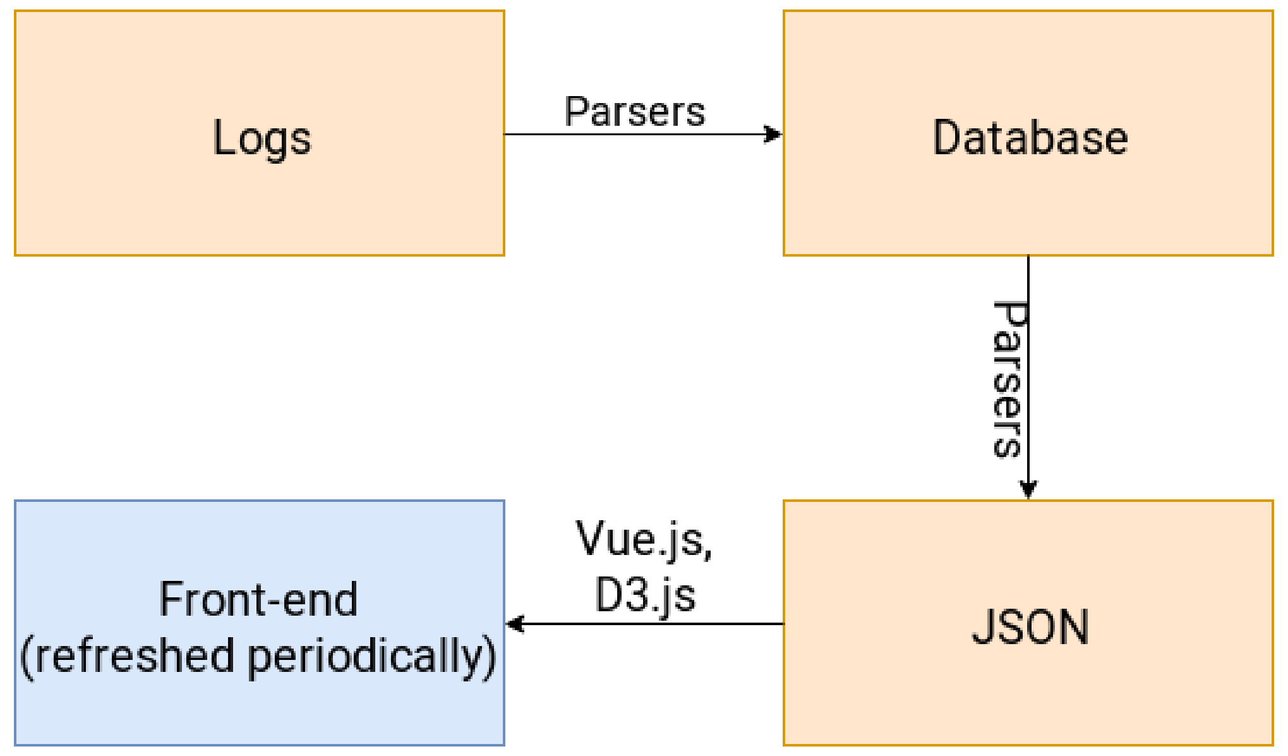
System to analyze the security posture of servers by parsing logs, inserting them into a database and displaying information visually in a front-end dashboard.

The system had to be lightweight enough to work in near real time if it was to be useful for system administrators responding to possible security incidents. Data was collected beginning from July 24, 2018.

Background

Dr. Huang had noticed suspicious activity on Computer Science department systems and wanted a tailored system to help with monitoring.

Methods



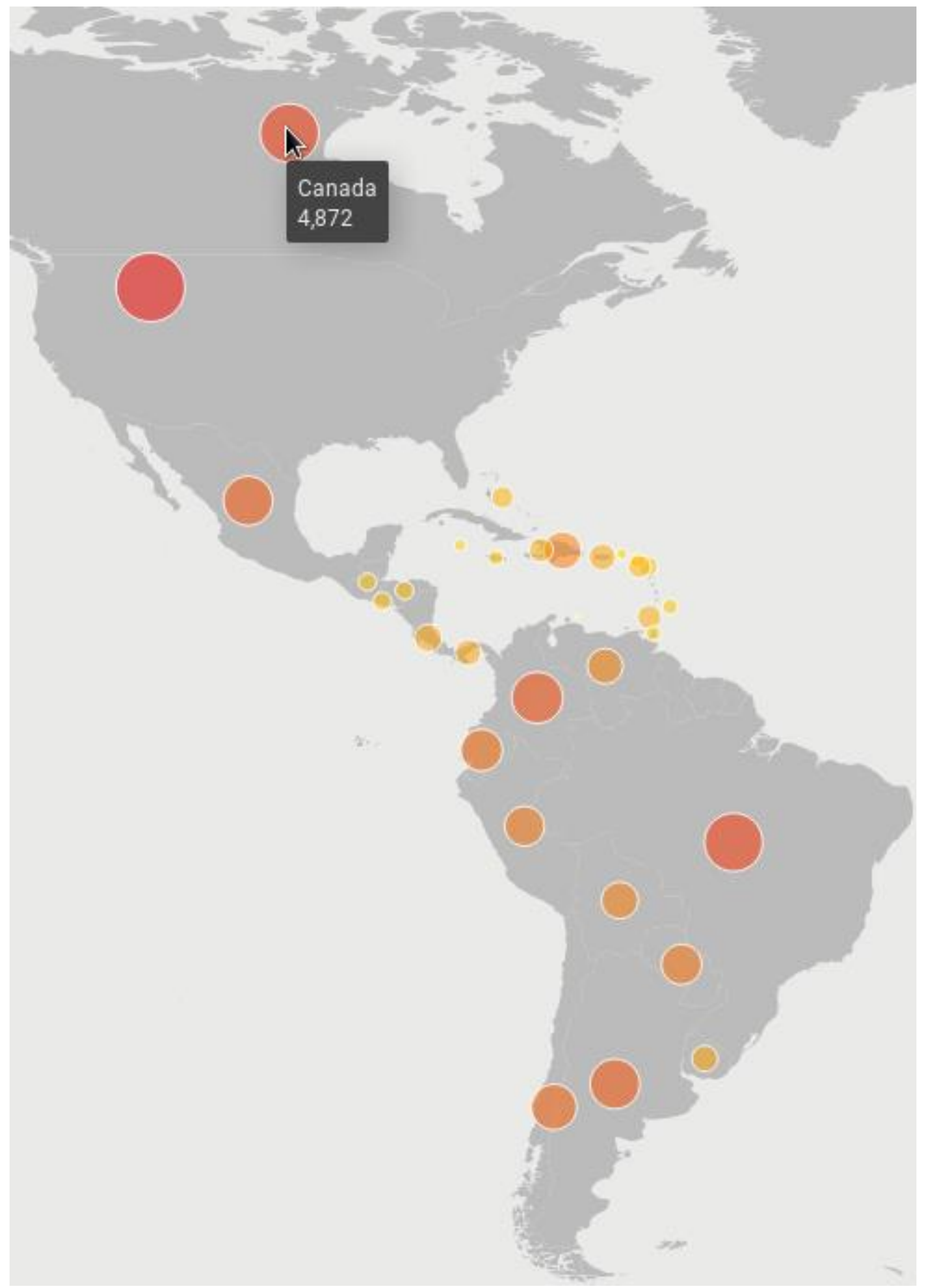
Logs
Parsers
Database
Parsers
JSON
Vue.js, D3.js
Front-end (refreshed periodically)

Materials

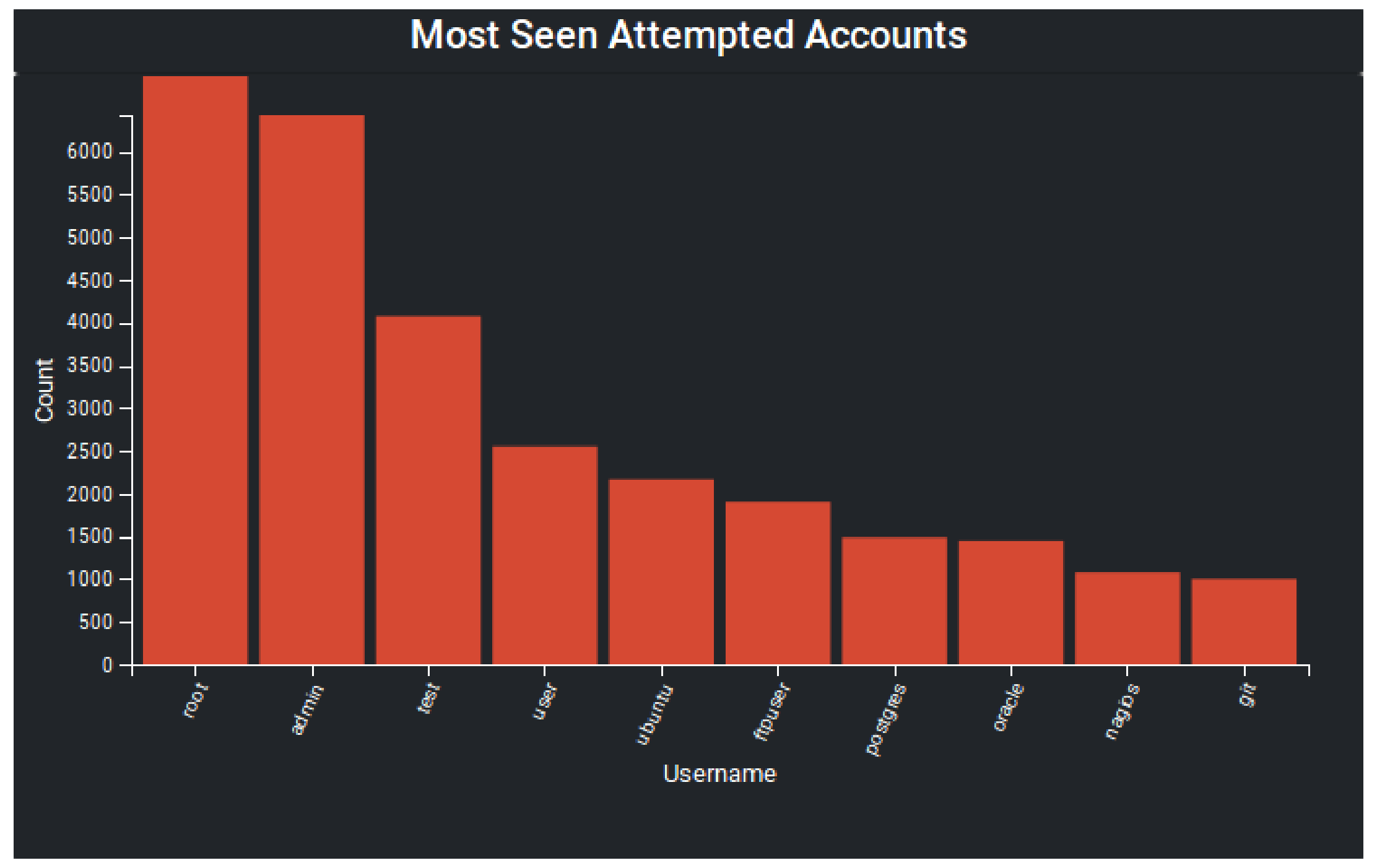
- •Programming Language: PHP, JavaScript, Bash
- •Database: MariaDB
- •Platform (OS): Fedora 28
- •Frontend: Vue.js, D3.js, Bootstrap
- •Architecture: x86
- •Server: Apache
- •Linux System Tools: cron, SSH
- •IP Geolocation DB: MaxMind Lite
- •Logs: “secure”, “access log”
- •Map Data: Natural Earth

- Geographic Information System: QGIS
- Topology Encoding: TopoJSON
- Data was collected from 7/24/2018 – 3/29/2019.
- 135,714 observations were made totaling up to 21.6 MBs in the DB.
- Most of the observations were actual attacks since the student was the only person logging into the server.
- At present, attacks occur at a rate of approximately 300 per hour.

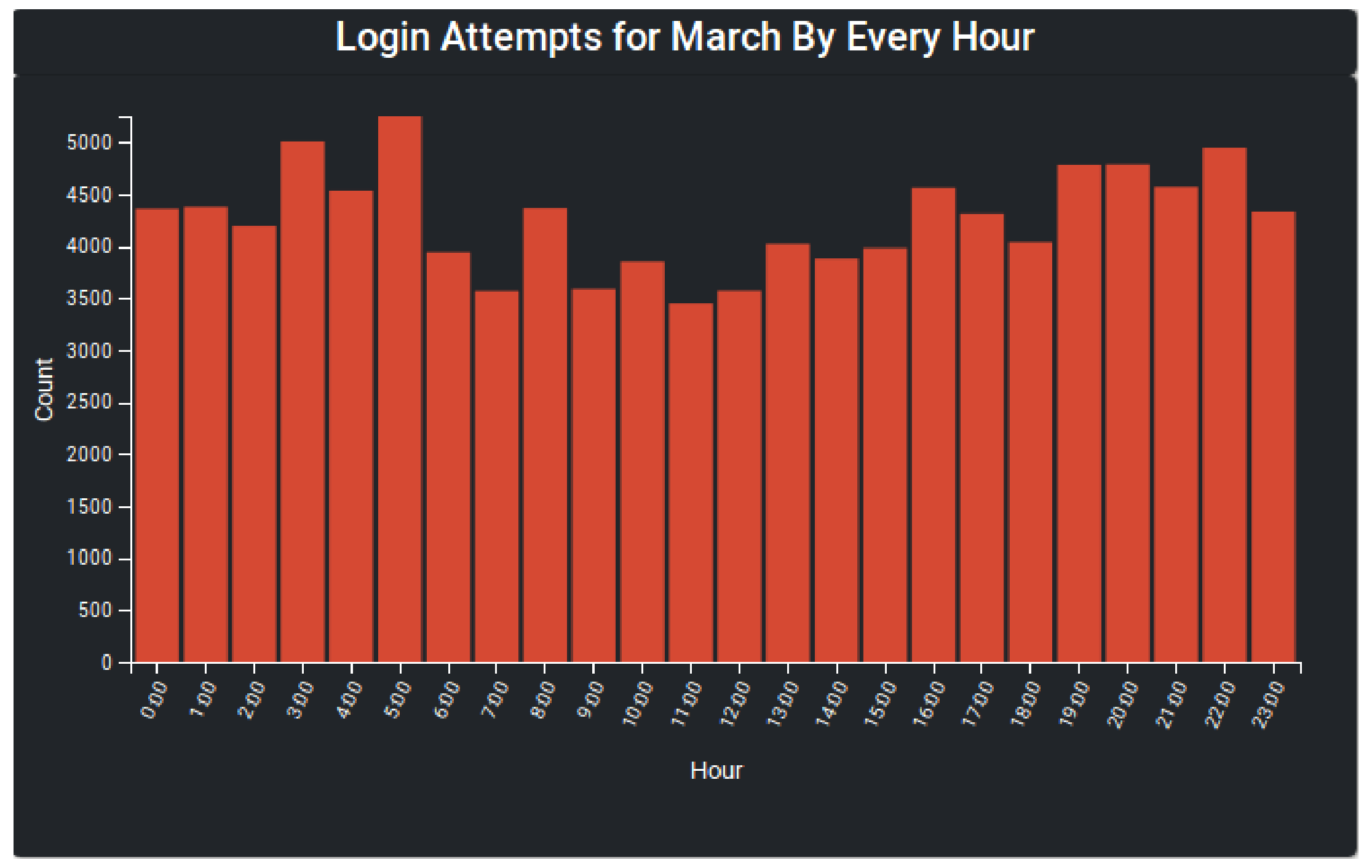
Map



Bar Graphs



Most Seen Attempted Accounts



Login Attempts for March By Every Hour

Summary

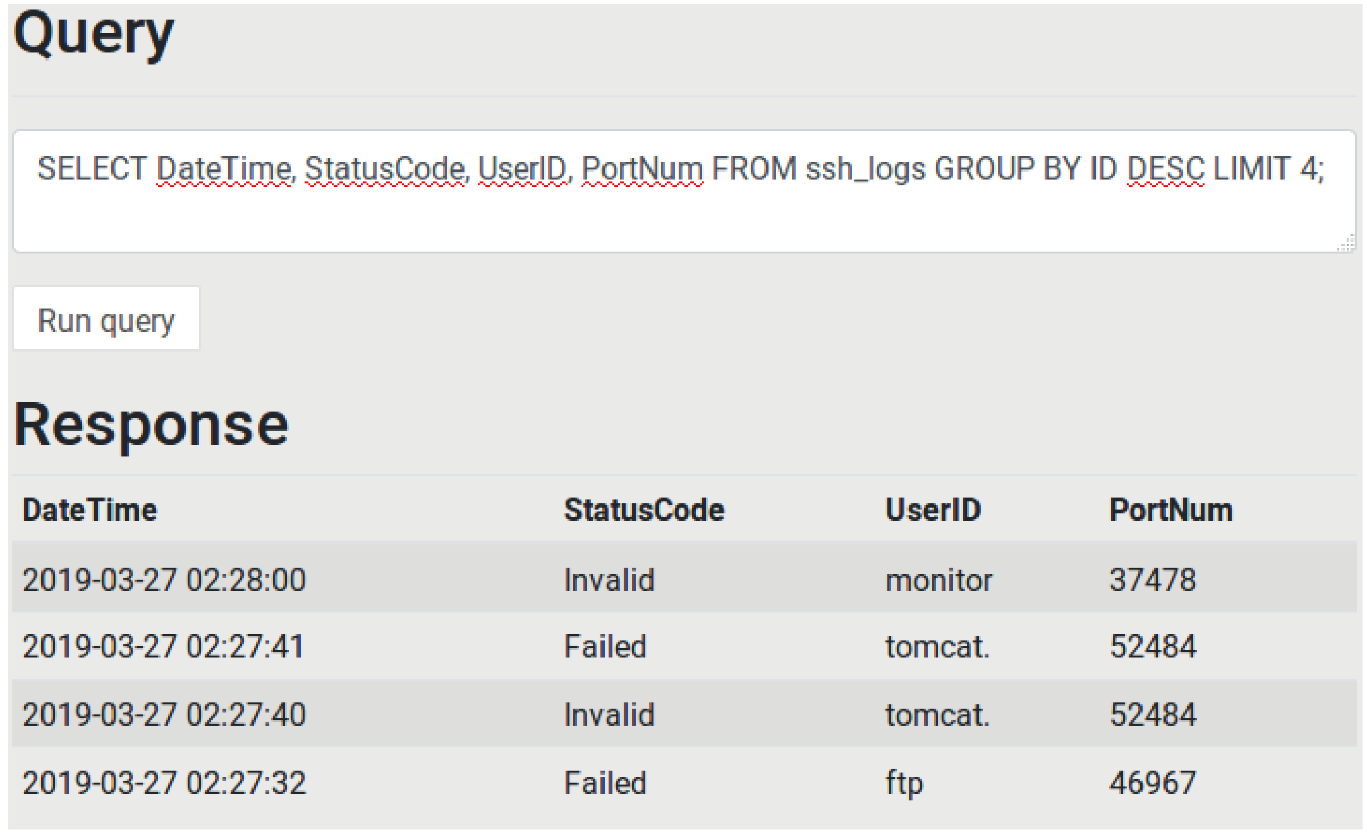
Conclusions:

- Near real time solutions require extensive optimization
- Visualizations are key to spotting anomalies

Future Work:

- Checking DB against MITRE or similar CVE databases.
- Expand logs parsed into DB (firewall, sudo, etc.)

Query Interface



Query

```
SELECT DateTime, StatusCode, UserID, PortNum FROM ssh_logs GROUP BY ID DESC LIMIT 4;
```

Response

DateTime	StatusCode	UserID	PortNum
2019-03-27 02:28:00	Invalid	monitor	37478
2019-03-27 02:27:41	Failed	tomcat.	52484
2019-03-27 02:27:40	Invalid	tomcat.	52484
2019-03-27 02:27:32	Failed	ftp	46967

Users can send SQL queries to the DB from the dashboard by switching panes.

References

1. D3.js Documentation, D3.
2. Vue.js Documentation, Vue.js.
3. Fedora System Administrator’s Guide, Red Hat, Inc.
4. PHP Manual, PHP Documentation Group.
5. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns.