Does Tenure Impact Malicious Alerts?

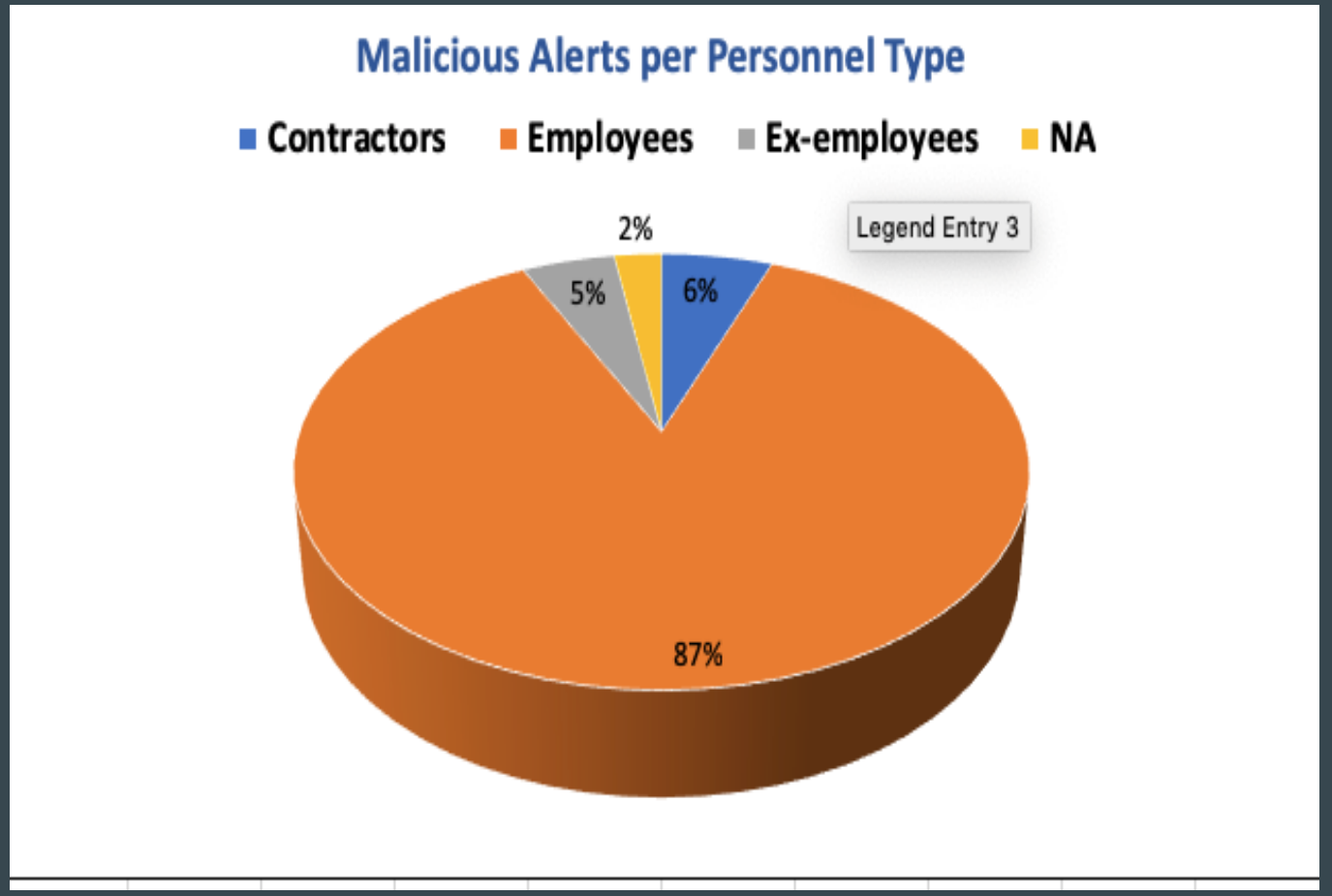
ALY6980 Spring 2019 Capstone
Instructor: Jamie Warner
Group 3: Ana Paniagua, Diana Puerta, Minyi Chen
6/19/2019

Content

- EDA
- Text Mining
- Models
- Conclusion
- References

ALERTS TRIGGERED BY DIFFERENT TYPES OF PERSONNEL

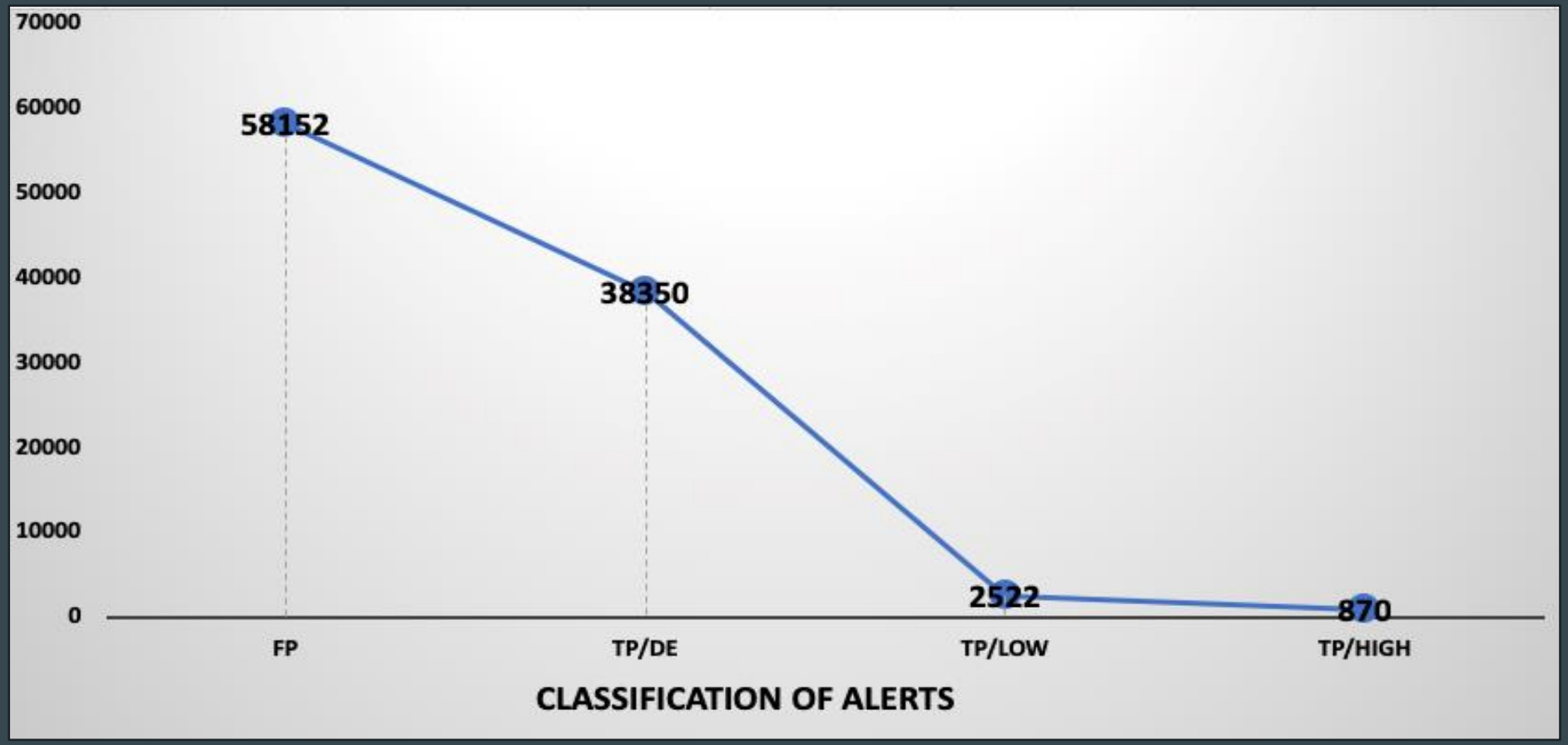
The majority of malicious alerts are caused by active employees followed by contractors and former employees.



More of the alerts triggered in the system fall under the False Positive (FP) which translate to inaccurate fired alerts

The classification of alerts are:

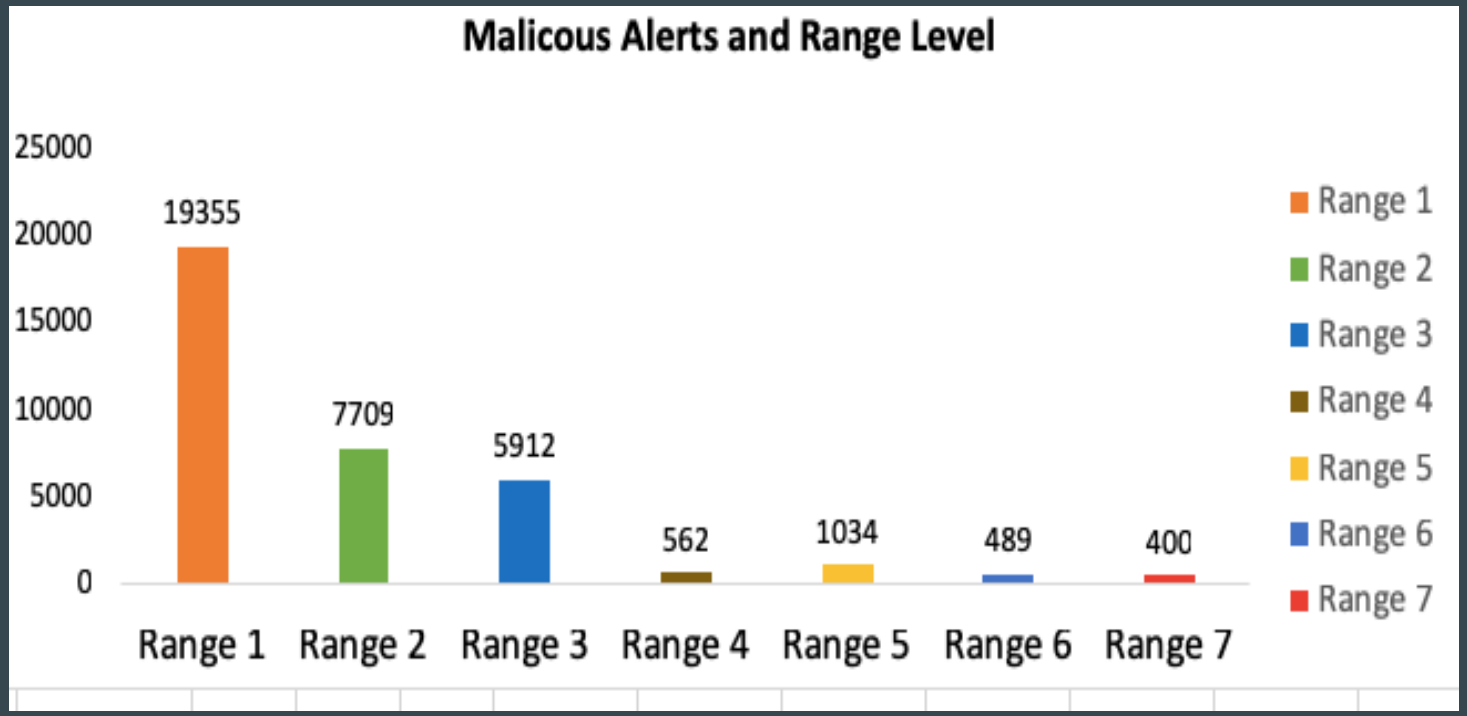
- FP: No risk
- TP/DE: Little to no risk
- TP/High: High risk
- TP/Low: Low risk involved



Which Type of Seniority level GE needs to pay attention to?

The majority of alerts are caused by employees who have been working in the company in the following ranges:

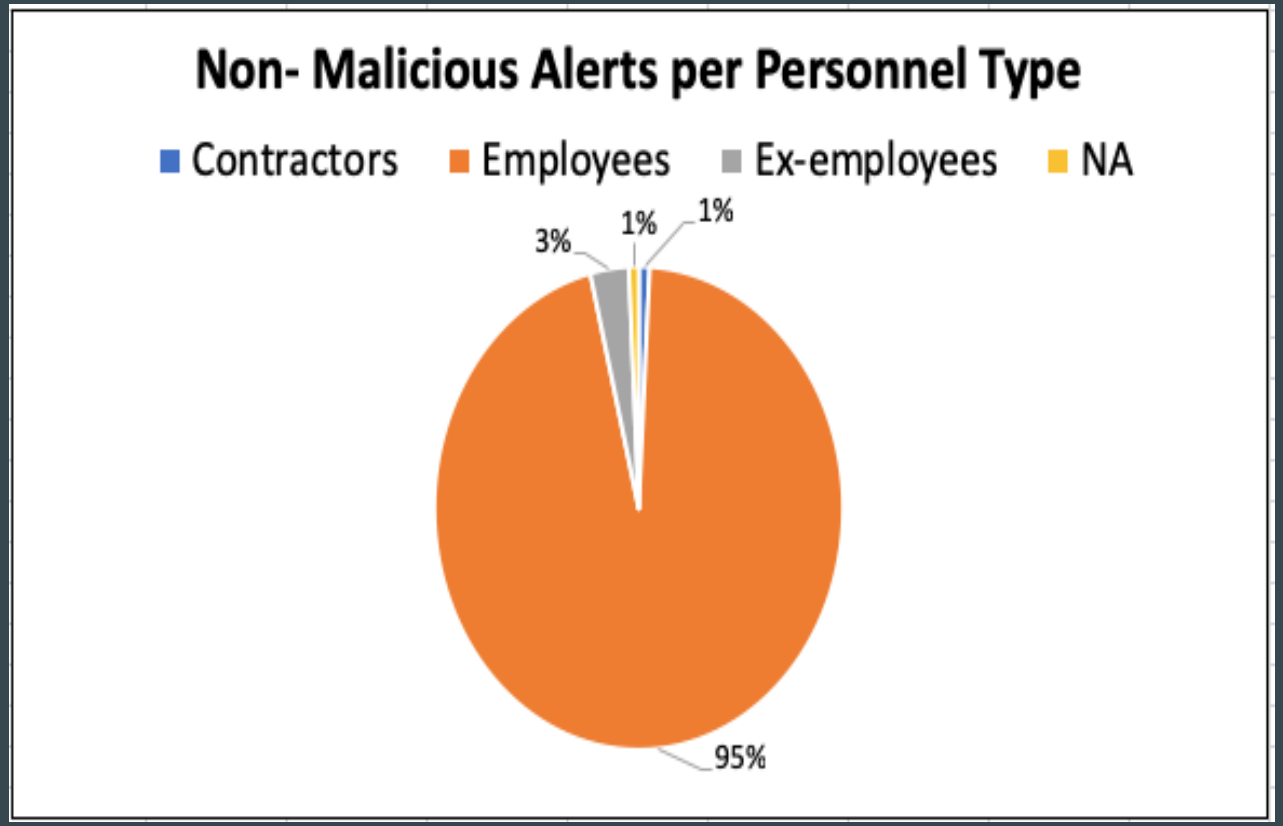
- Range 1 (0 – 3 years)
- Range 3 (13 – 18 years)
- and Range 2 (6 – 12 years)



Non-Malicious alerts based on Personnel Type

Non malicious alerts are mostly caused by active employees. The problem can be due to the indications misfired.

There is a need to take a closer look at the combination of indicators in Range 1 and Range 2.



TEXT MINING

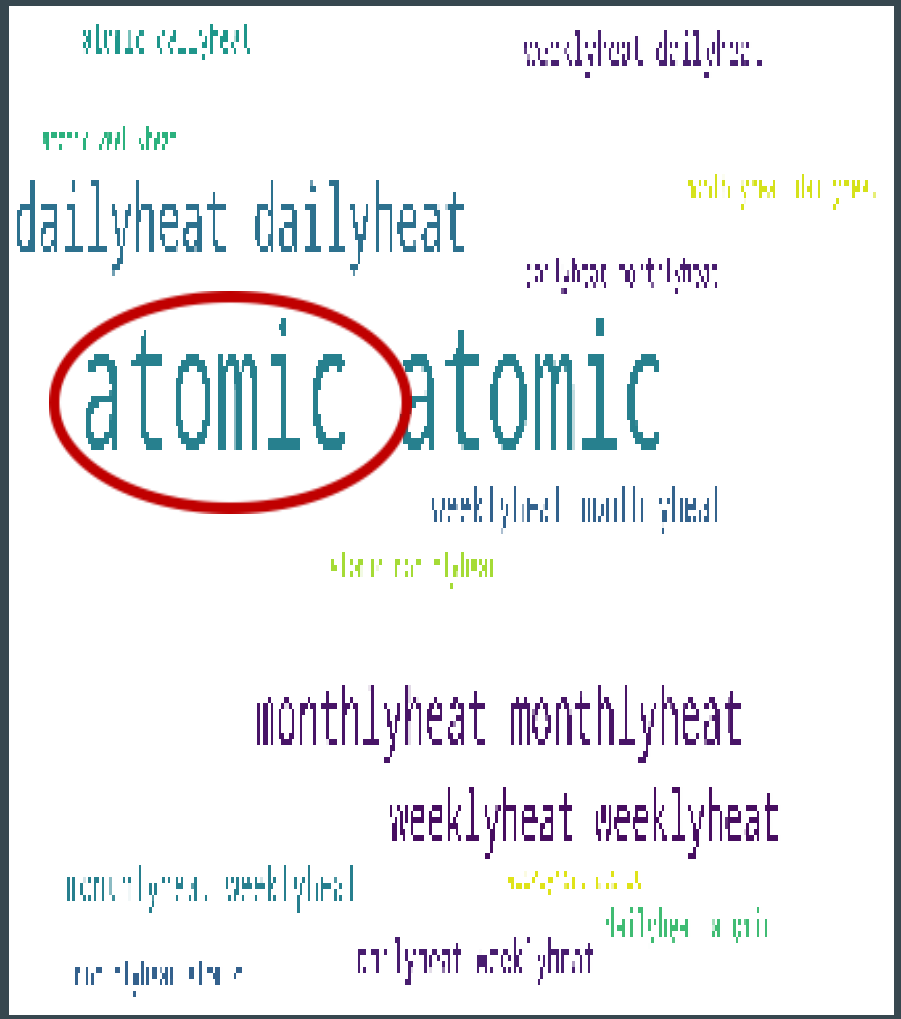
Highlight the **most frequently used keywords and** allowed the most frequently used keywords in the **alert_type** and Indicators column.

- We created word cloud by using the text mining package (*tm*) and the word cloud generator package (*wordcloud*) available in python. This step helped us to analyze texts and to visualize the keywords as a word cloud.

Takeaways

According to the **word cloud** visual representation of text data and the most frequent words of the alert_typefield were the following:

Atomic indicator, fires an alert. In addition, other common heat indicators that have a score assigned to the alerts that are also broken down into Daily, Weekly, and Monthly heat Alerts.

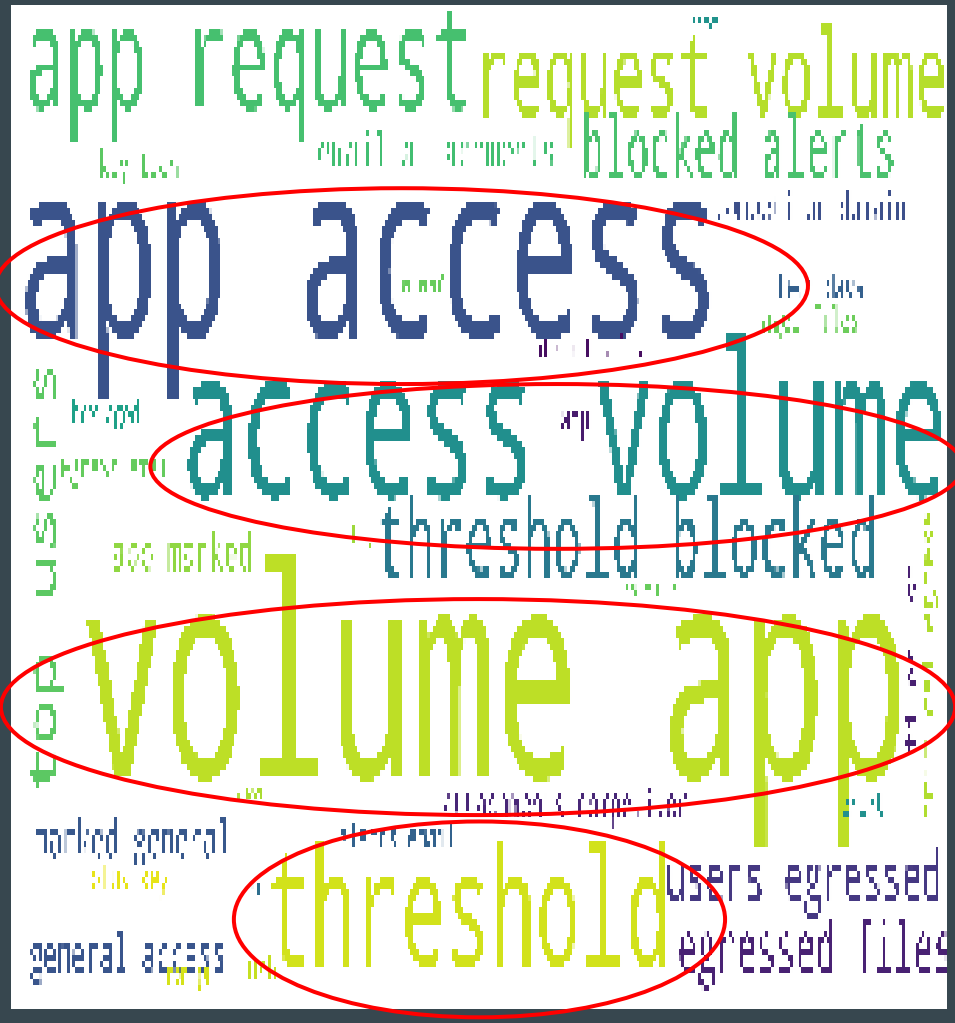


Indicators

We also decided to analyze the Indicator_field Column in the **word cloud** to have a clear visual. Therefore, the most frequent words were the following:

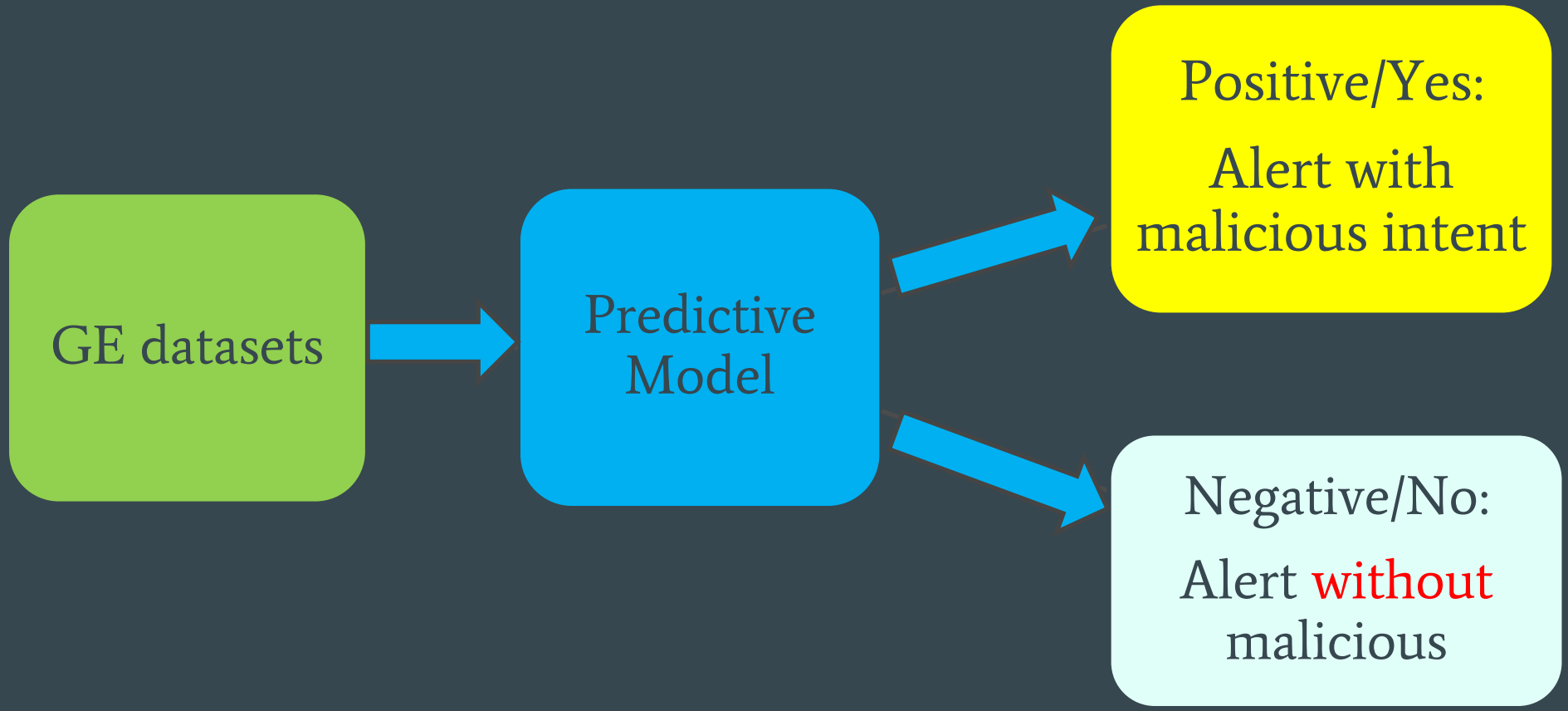
volume app, app access, access volume, threshold.

As a result, this information can be helpful since, the indicators that appear more frequently are the ones that have been triggered more times as shown in the text mining analysis shown.



The Effect of Tenure on Malicious

Predictive Models: predict if an alert has malicious intent

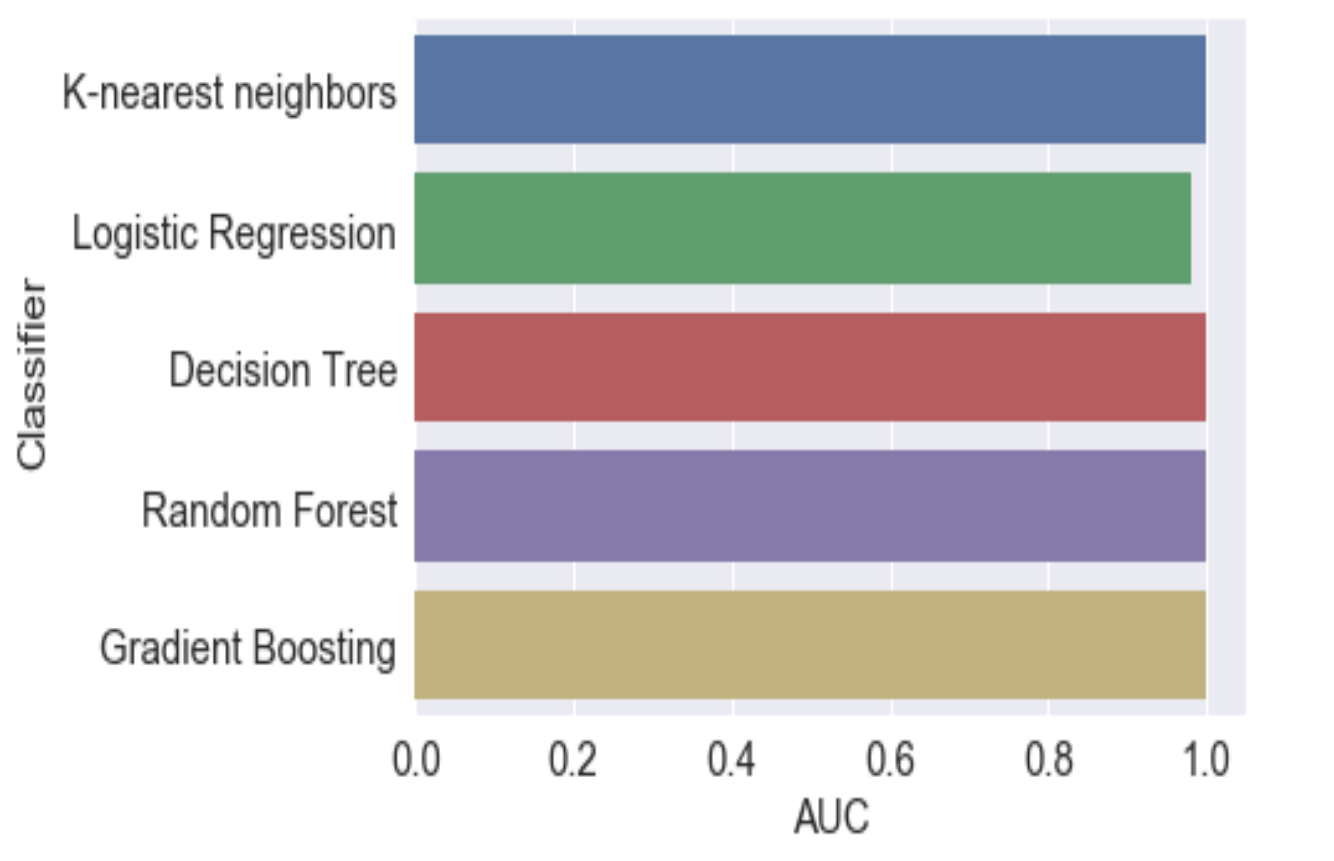


Features

	Feature	Type	Description
Output label	Malicious	Binary	1 = malicious intent (39%) 0 = no malicious
Input features	Score	Numerical	risk_factor * avg_score
	Work_years	Numerical	Tenure, how many years they have worked
	owner_name	Nominal categorical	Analysts reviewed the case
	Alert_type	Nominal categorical	Atomic, daily/weekly/monthly heat
	Function_group	Nominal categorical	Commercial, Enabling, Production
	classification	Ordinal categorical	FP, TP/DE, TP/LOW, TP/HIGH

Model Technique Comparison

All models look reasonable with AUC, but may be overfit...



	Recall (true positive rate)
KNN	0.997
LG	1
DT	1
RF	1
GBC	1

Model Results

- Logistic regression shows work_years has negative effect on malicious intent (Right graph).
- Random forest model shows work_years is the fourth important features.

Key Takeaway

This suggests that the longer the people work, the less chance they have malicious intent.

	importance
classification	2.736609
owner_name_Analyst_6	0.205341
alert_type_Daily_Heat	0.032746
alert_type_Weekly_Heat	-0.059263
work_years	-0.069765
alert_type_Monthly_Heat	-0.075134
owner_name_Analyst_4	-0.076976
score	-0.171996
owner_name_Senior_Analyst_2	-0.173662
Function_Group_Enabling	-0.174609
Function_Group_Production	-0.221388
owner_name_Analyst_5	-0.360707
owner_name_Analyst_3	-0.383597
owner_name_Senior_Analyst_1	-0.953003

Conclusion

The predictive model suggests that

"People who work longer tend to have no malicious intent."

According to the literature, the findings are mixed.

1) Long tenure leads to higher job performance and business ethics.

2) It depends on whether the employee is an executive, manager, or just employee.

3) No significant relationship between tenure and job performance.

References

- Ardichvili, A., Jondle, D., & Kowske, B. (2012). Minding the gap: Exploring differences in perceptions of ethical business cultures among executives, mid-level managers and non-managers. *Human Resource Development International*, 15(3), 337-352.
- Neswiswi, H. (2014). *Employee attitude towards business ethics in the motor industry* (Doctoral dissertation, University of Pretoria).
- Ng, T. W., & Feldman, D. C. (2013). Does longer job tenure help or hinder job performance?. *Journal of Vocational Behavior*, 83(3), 305-314.

Thank you!