CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

CIRI CyberTalent Bridge

Author: Jarod Costello
Faculty Advisor: Dr. Dipakkumar P Pravin

University of North Texas

Homeland Security Challenge

The challenge is to create a system that empowers businesses to map KSAs(Knowledge, Skills and Abilities) required to perform cybersecurity tasks to protect their business. Our goal was to provide a better matching algorithm for the CyberTalent Bridge to use for matching various TKSA's from the NICE Cybersecurity Framework to the NIST 800-53 controls in order to make the CTB a more accurate system. We focused on creating the relationship between the NICE frameworks tasks(T), knowledge(K), skills(S), and abilities(A) to the controls within the NIST 800-53 publication.

Approach / Methodology

Our team's approach was to split the work, between the tasks(T), knowledge(K), and skills(S) in the NICE framework with one member of the team working on the T;s while another focused-on K's and S's. The NICE framework also includes abilities(A) which have been deprecated in the current iteration of the framework(v1). The basis for this poster is our work with the T's.

The first approach to matching T's to given controls in the 800-53 was to use K-means clustering, which aims to cluster X number of "tasks" into Y number of clusters. Our second approach was to use a cosine similarity measure, this measures the similarity between two vectors and assigns a value to the similarity between 0 and 1. Our last approach was to use a similarity sequence matcher, and this measures the similarity between the words of two strings and the sequence in which they appear.

Outcomes / Results

Cosine Similarity

```
[('AC-2', 1.0), ('T0144', 0.296), ('T0494', 0.296), ('T0602', 0.25), ('T0660', 0.236),
 ('T1003', 0.23), ('T0907', 0.224), ('T0713', 0.213), ('T0060', 0.211), ('T0132', 0.199),
 ('T0150', 0.199), ('T0263', 0.199), ('T0587', 0.198), ('T0037', 0.196), ('T0127', 0.196)]
```

- Above shows the top 14 tasks matched with the AC-2 control.
- The closer to 1 the more similar a task is to the AC-2 control
- AC-2 shows 1 since it is being compared to itself
- AC-2 is "Account Management", T0144 is "Manage accounts, network rights, and access to systems and equipment"
- 9/10 accuracy

Similarity Sequence Matcher

```
#Top Simularity
#T0896 → 0.063492063     #T0108 → 0.062901155
#T0119 → 0.0609319       #T0862 → 0.056064073
#T0539 → 0.053265694     #T0109 → 0.052843194
#T0938 → 0.051282051     #T0355 → 0.047706422
#T0368 → 0.047405509     #T0082 → 0.045510455
#T0714 → 0.044526902     #T0454 → 0.044299674
#T1000 → 0.043617704     #T0130 → 0.042806183
#T0421 → 0.04279421
```

- Tasks are being compared to AC-2 using a similarity sequence matcher
- Above shows the top 15 tasks matched to the AC-2 control
- 3 of the top similarity tasks show up on the AC-2 control in CTB
- 7/10 accuracy

Conclusions

Our team ran 3 tests on our data; Cosine Similarity, Clustering, and Similarity Sequence, but we decided that our top 2 clustering tests with the highest accuracy were the Cosine similarity test and the similarity sequence matcher. Through the 2 clustering tests we can better the CyberTalent Bridge tool and provide a more accurate list of tasks, knowledge, skills and abilities for each control in the CTB. Our team also tried to use K-means clustering in order to sort the various TKSA's but we concluded our results were too unstable due to the fact that when we decrease the number of clusters, the same tasks did not continue to match with the same control.

References

- https://cybertalentbridge.com/projects
- https://www.cybersecuredashboard.com/
- https://towardsdatascience.com/sequencematcher-in-python-6b1e6f3915fc
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Acknowledgements

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.

UNT

ILLINOIS