CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Enhancing Cybersecurity KSATs from Cybersecurity Job Posting Data through NLP techniques

Authors: Max Douglas & Jordan Bernot
Faculty Advisor: Dan J. Kim

UNT

Homeland Security Challenge

Strengthen the overall security posture of the nation by better preparing the current and future cybersecurity workforce.

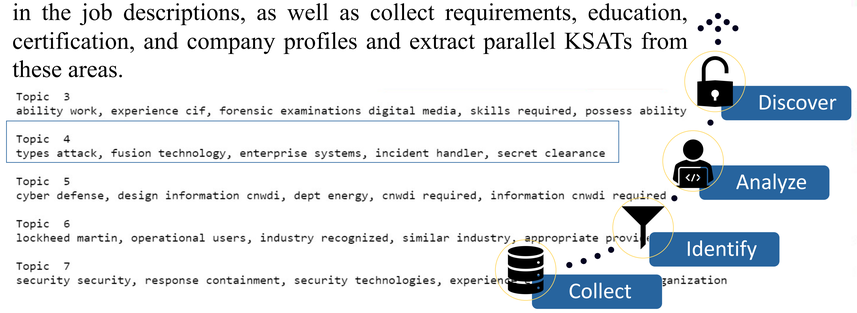
Motivation & Goal

Inconsistencies related to job posting requirements have made it difficult to identify specific skills necessary to fulfill the needs across the cybersecurity domain. Additionally, a recent revision to the NICE Framework has prompted a need to map new knowledge, skills, abilities, and tasks (KSATs) to current job posting requirements. Finally, recent national security issues has potentially revealed a gap between what KSATs have been identified by the government and what is currently needed.

The major research questions are what are the new KSATs required for current and future cybersecurity professionals and how can we identify them?

Approach / Methodology

Utilizing the Python programming language (specifically the libraries: BeautifulSoup (bs4), nltk, pandas, requests, scikit-learn, sqlite3, and TextBlob (textblob)), this project was able to collect and conduct initial text analysis on a large collection of postings and related metadata. This analysis allows us to identify prevalent topics in the job descriptions, as well as collect requirements, education, certification, and company profiles and extract parallel KSATs from these areas.



Outcomes / Results

Using exploratory and text analytics techniques, this project identified key KSATs for each job title, as defined by the NICE Framework. Additionally, utilizing Negative Matrix Factorization (NMF) topic extraction techniques allowed this project to identify possible unidentified KSATs , as well as common topics that may exist amongst the variety of job descriptions they were drawn from.

Further, the outcomes of the project will provide opportunities for additional workforce studies in other interdisciplinary fields. In the case of the NMF extraction techniques, this will allow future projects to potentially identify new and/or critical skills for training and/or cybersecurity strategy.

Below is an example of the output for the aggregated Security Analyst job postings data, after it had been cleaned, processed, and analyzed.

1.1 SECURITY TECHNICIAN/SPECIALIST

Description: - design, test, configure, and monitor security controls for systems and networks - defend systems against unauthorized access, modification, and/or destruction - perform vulnerability testing, risk analyses, and security assessments - identified system and network abnormalities and report violations - respond immediately to security incidents and provide post incident analysis, etc.
Related job titles: Information Security Specialist, Cybersecurity Specialist, Computer Security Technician, Network Security Specialist, Security Desk Specialist, IA Specialist, IT Security Specialist, Security Operations Specialist, Security Specialist, System Security Specialist, etc.
NICE relevant factors: - Category: Operation and Maintenance - Specialty Areas: installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty
Desired Knowledge/ Skills/Abilities: - TCP/IP, computer networking, routing, and switching - Windows, Unix, and Linux operating systems - IDS/IPS, penetration and vulnerability testing, DLP, and anti-malware - Understanding of ISO 27001/27002, ITIL, and COBIT frameworks - Familiarity with PCI, HIPAA, GLBA, and SOX compliance assessment
Desired Certifications: CompTIA A+, Network+, and Security+, CCNA, CEH, GIAC certifications (GSEC, GCIH, and GCIA), CISSP
Related Degree: - Associate: Computer Science - BS: Security Engineering, System Management, Computer Engineering, MIS And Cyber Security - MS/ MBA: IT Security Management, MIS, Computer Science, Digital Forensic, Cyber Security
Other Experiences: Cyber Security Analyst, Assurance Engineer, Communications Engineer, Information Security Consultant, etc.

Discussions

This project attempts to predict future workforce needs and fill the shortage of qualified cybersecurity professionals through the alignment of cybersecurity job demands with workforce supply. Additionally, it will provide important tools that continuously update the structure and common understanding of cybersecurity job components, their relationships, and career pathways.

This project provides broad impacts in several ways at different levels. For job candidates and professionals expanding their career paths, it gives a better understanding of the emerging KSATs needed for continued development. For individuals wanting to enter the field it outlines the KSATs necessary for positions and allows for better preparation regarding education and training.

Selected References

Debortoli, S., Müller, O., Junglas, I., vom Brocke, J. (2016, July) Text Mining For Information Systems Researchers: An Annotated Topic Modeling Tutorial 7-2016, Volume 39 – Article 7

Lovejoy, C. (2020, May) job-scraper (https://github.com/chris-lovejoy/job-scraper)

Elliot (2021, May) Word Clouds in Python (https://onebyzero.org.in/2021/05/17/word-clouds-in-python)

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.

ILLINOIS