Mapping Low Cost and Open Source Labs to the NICE Workforce Framework

Chris Simpson,

Director National University Center for Cybersecurity

When I find a new lab

Agenda

- Background
- Examples of free labs and how we use them
- Mapping Labs in Airtable

Background

- Hands on labs are a critical component of any cybersecurity program and a requirement to become a Center of Academic Excellence
- Several ways to deliver lab content
  - Develop and deploy labs on internal or outsourced infrastructure
  - Utilize labs from external lab providers
  - Utilize free grant resourced labs
  - Use free and open source labs
- Managing an internal lab environment is expensive

Challenges of Running an Internal Lab

- Help Desk
  - Academic vs Technical issues
  - Hours of operation
    - Student complete school work in the evening and on weekends
  - ”Ticket Management”
- Admin access to systems
- Developing lab content
- Cost

Finding Outsourced Labs

- “Word of Mouth”
- Textbook Vendors
- Vendor booths
- Google

Challenges of Free Labs

- Downtime
- Support
- Updates
- No single vendor provides everything you need
- Publicly available answers
- Course coverage of lab content
- Faculty preparation
- Vendor lab changes

Free/Freemium Providers

- Not an official endorsement from National University

Providers
(No particular order)

Immersive Labs (Free)

NICE Challenge (Free)

Over the Wire (Free)

PicoCTF (Free)

Hack The Box (Freemium)

TryHackMe.com (Freemium)

Blue Team Labs (Freemium)

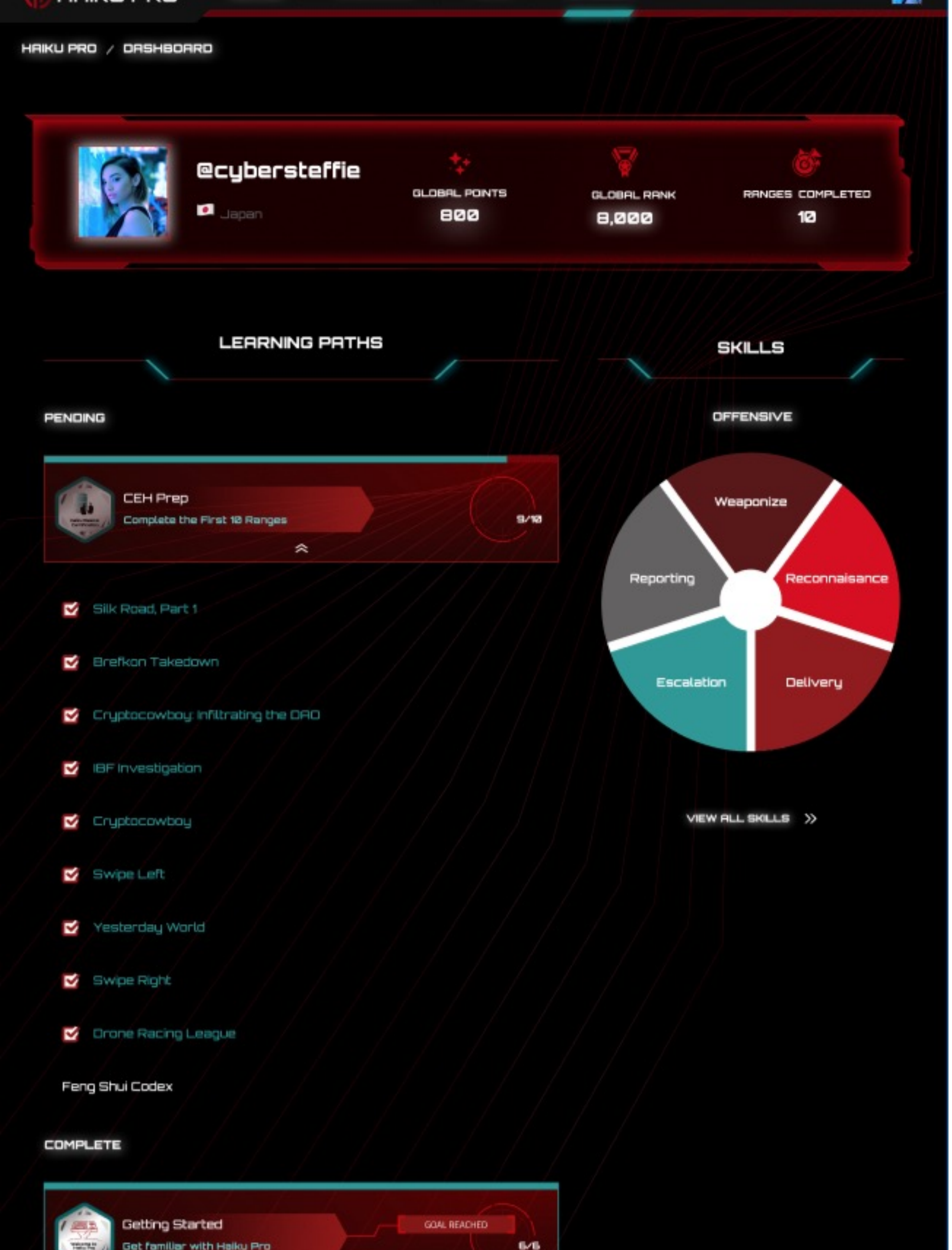
Haiku Pro

(Freemium)

Deploy in the Cloud

- Use Devops tools to deploy labs in the cloud
- Examples
  - Detection Lab
  - Mordor
  - CyberRange

Mapping to Certs



HAIKU PRO / DASHBOARD

@cybersteffie
Japan

GLOBAL POINTS 800

GLOBAL RANK 8,000

RANGES COMPLETED 10

LEARNING PATHS

PENDING

CEH Prep
Complete the First 10 Ranges
9/10

☑ Silk Road, Part 1

☑ Brefkon Takedown

☑ Cryptocowboy: Infiltrating the DAO

☑ IBF Investigation

☑ Cryptocowboy

☑ Swipe Left

☑ Yesterday World

☑ Swipe Right

☑ Drone Racing League

Feng Shui Codex

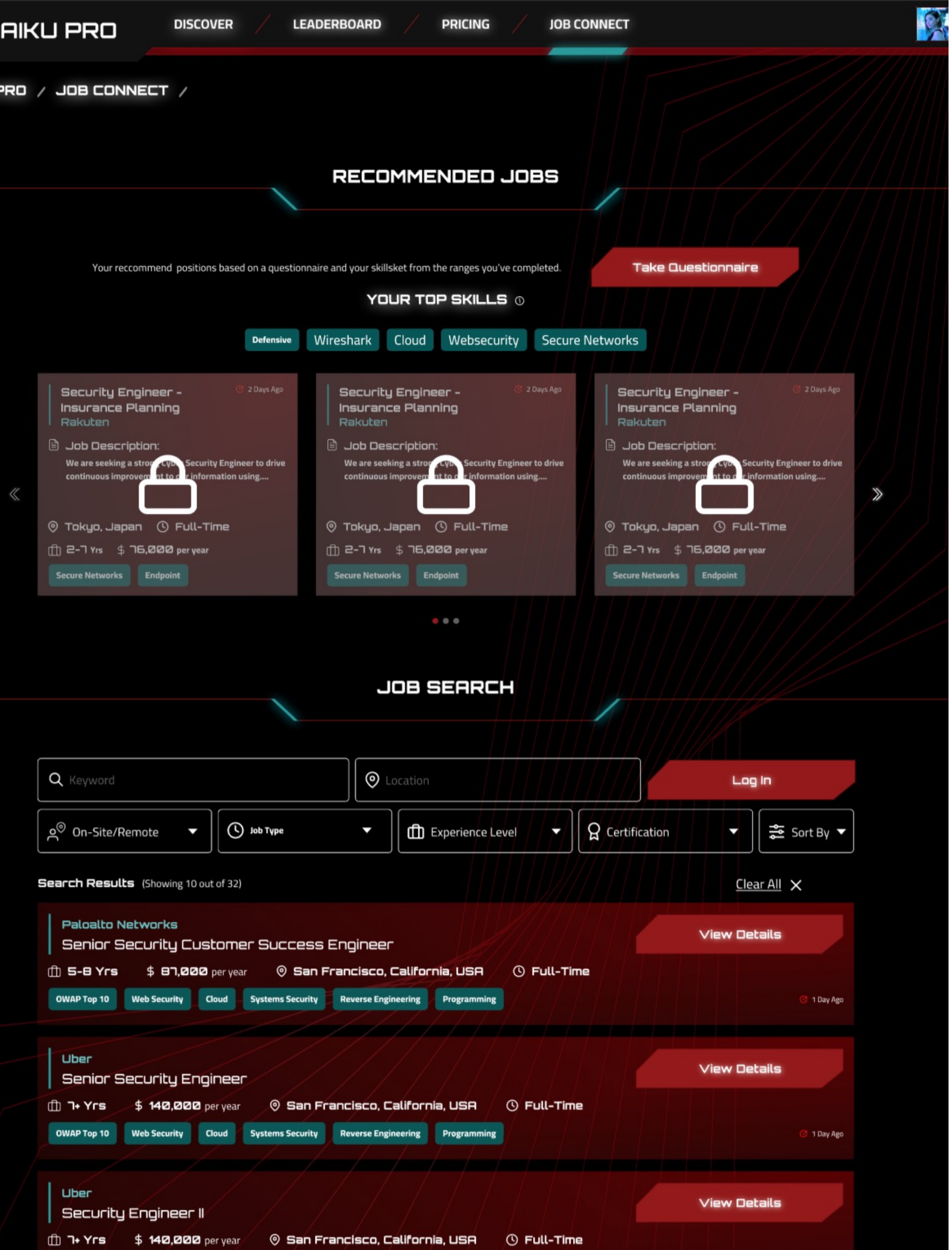
COMPLETE

Getting Started
Get familiar with Haiku Pro
GOAL REACHED
6/6

SKILLS

OFFENSIVE

VIEW ALL SKILLS »



AIKU PRO DISCOVER / LEADERBOARD / PRICING / JOB CONNECT

PRO / JOB CONNECT /

RECOMMENDED JOBS

Your reccommend positions based on a questionnaire and your skillsket from the ranges you've completed.

Take Questionnaire

YOUR TOP SKILLS

Defensive | Wireshark | Cloud | Websecurity | Secure Networks

Security Engineer - Insurance Planning
Rakuten
2 Days Ago
Job Description:
We are seeking a strong Cyber Security Engineer to drive continuous improvement to our information using....
Tokyo, Japan | Full-Time
2-7 Yrs | $ 76,000 per year
Secure Networks | Endpoint

Security Engineer - Insurance Planning
Rakuten
2 Days Ago
Job Description:
We are seeking a strong Cyber Security Engineer to drive continuous improvement to our information using....
Tokyo, Japan | Full-Time
2-7 Yrs | $ 76,000 per year
Secure Networks | Endpoint

Security Engineer - Insurance Planning
Rakuten
2 Days Ago
Job Description:
We are seeking a strong Cyber Security Engineer to drive continuous improvement to our information using....
Tokyo, Japan | Full-Time
2-7 Yrs | $ 76,000 per year
Secure Networks | Endpoint

JOB SEARCH

Keyword | Location | Log In

On-Site/Remote | Job Type | Experience Level | Certification | Sort By

Search Results (Showing 10 out of 32) Clear All ×

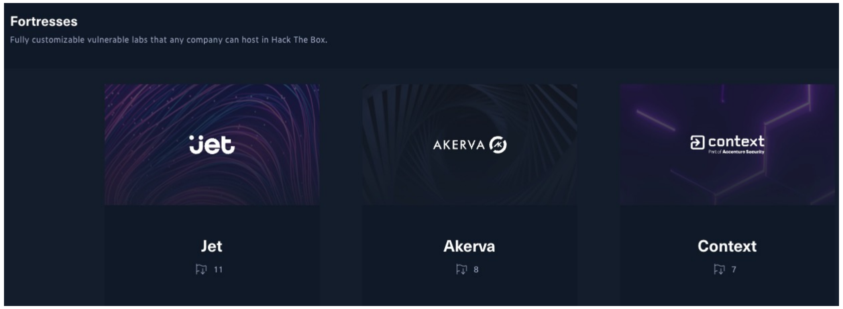
Paloalto Networks
Senior Security Customer Success Engineer
View Details
5-8 Yrs | $ 87,000 per year | San Francisco, California, USA | Full-Time
OWAP Top 10 | Web Security | Cloud | Systems Security | Reverse Engineering | Programming
1 Day Ago

Uber
Senior Security Engineer
View Details
7+ Yrs | $ 140,000 per year | San Francisco, California, USA | Full-Time
OWAP Top 10 | Web Security | Cloud | Systems Security | Reverse Engineering | Programming
1 Day Ago

Uber
Security Engineer II
View Details
7+ Yrs | $ 140,000 per year | San Francisco, California, USA | Full-Time

- Mapping to Jobs

Working with Companies
Hack the Box



Fortresses

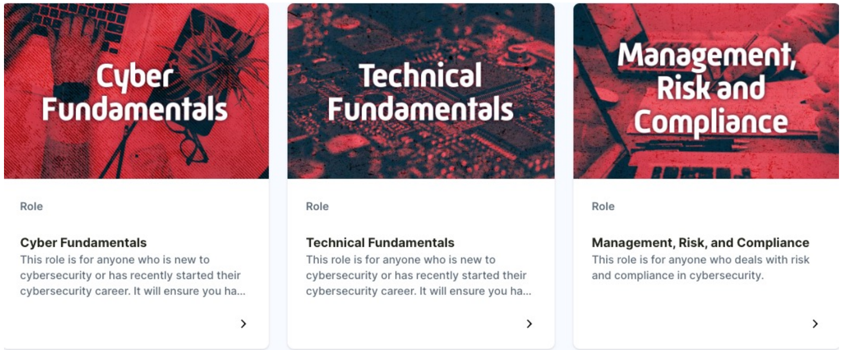
Fully customizable vulnerable labs that any company can host in Hack The Box.

Jet 11

Akerva 8

Context 7

Mapping to Roles
Immersive Labs



Role

Cyber Fundamentals

This role is for anyone who is new to cybersecurity or has recently started their cybersecurity career. It will ensure you ha...

Role

Technical Fundamentals

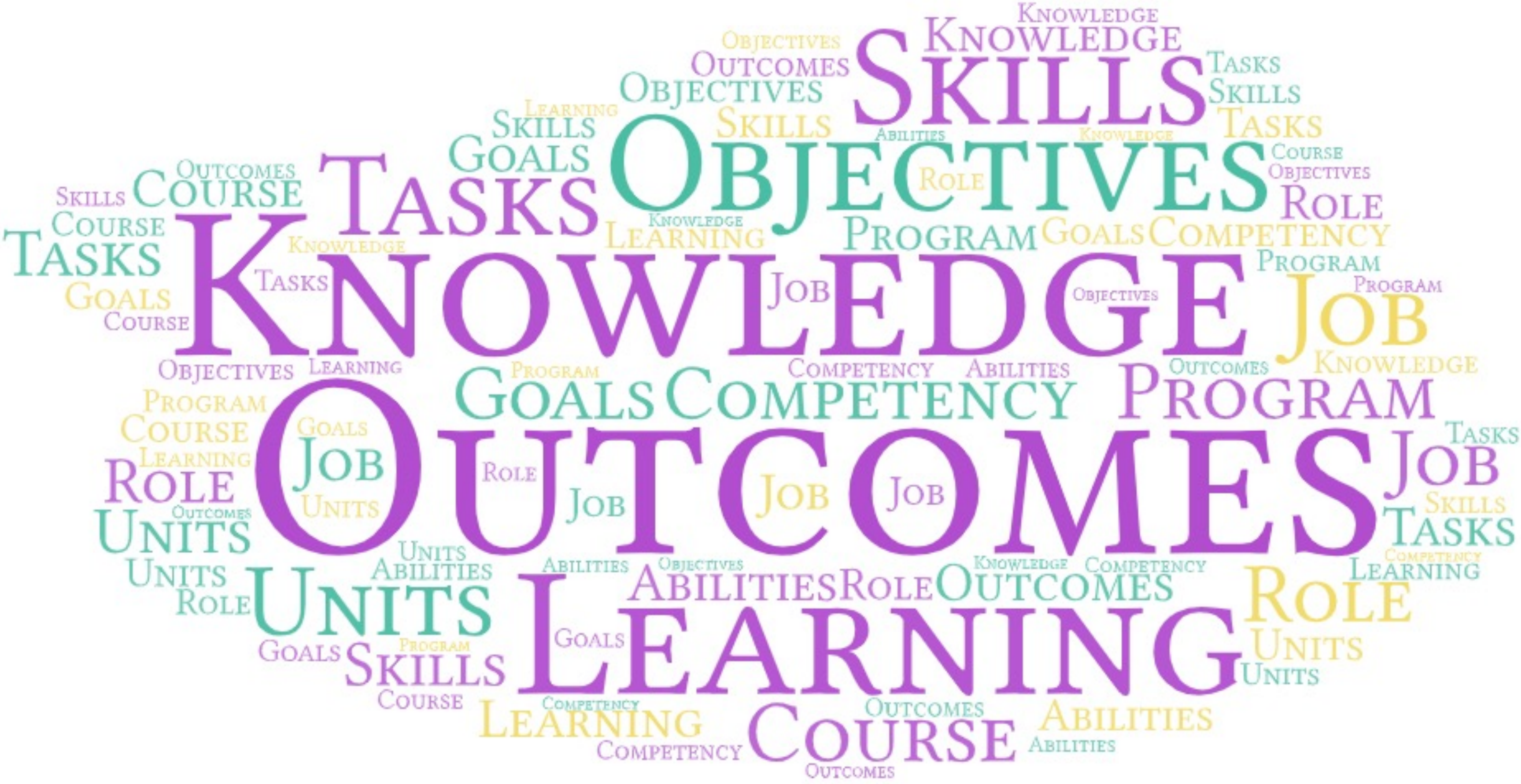
This role is for anyone who is new to cybersecurity or has recently started their cybersecurity career. It will ensure you ha...

Role

Management, Risk, and Compliance

This role is for anyone who deals with risk and compliance in cybersecurity.

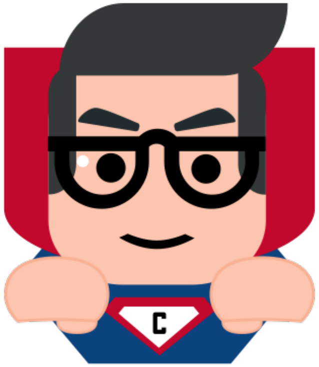
So What?


Knowledge
Objectives
Knowledge
Outcomes
Skills
Tasks
Objectives
Skills
Learning
Skills
Abilities
Knowledge
Tasks
Skills
Goals
Objectives
Course
Outcomes
Role
Objectives
Skills
Course
Tasks
Role
Course
Knowledge
Program
Goals
Competency
Tasks
Knowledge
Learning
Program
Tasks
Knowledge
Job
Objectives
Program
Goals
Job
Course
Objectives
Learning
Program
Competency
Abilities
Outcomes
Knowledge
Goals
Competency
Program
Program
Course
Goals
Outcomes
Tasks
Learning
Job
Job
Role
Role
Job
Job
Job
Outcomes
Units
Skills
Units
Tasks
Units
Competency
Units
Abilities
Abilities
Objectives
Knowledge
Competency
Learning
Role
Abilities
Role
Outcomes
Role
Units
Units
Goals
Program
Skills
Goals
Learning
Course
Units
Competency
Outcomes
Abilities
Learning
Course
Competency
Abilities
Outcomes

HELP

Airtable

+



Max Power Collection

Mapping Labs To Objectives

Build a catalog of labs mapped to the NICE Framework and CAE KU’s

Student project mapping TryHackMe

Using AirTable

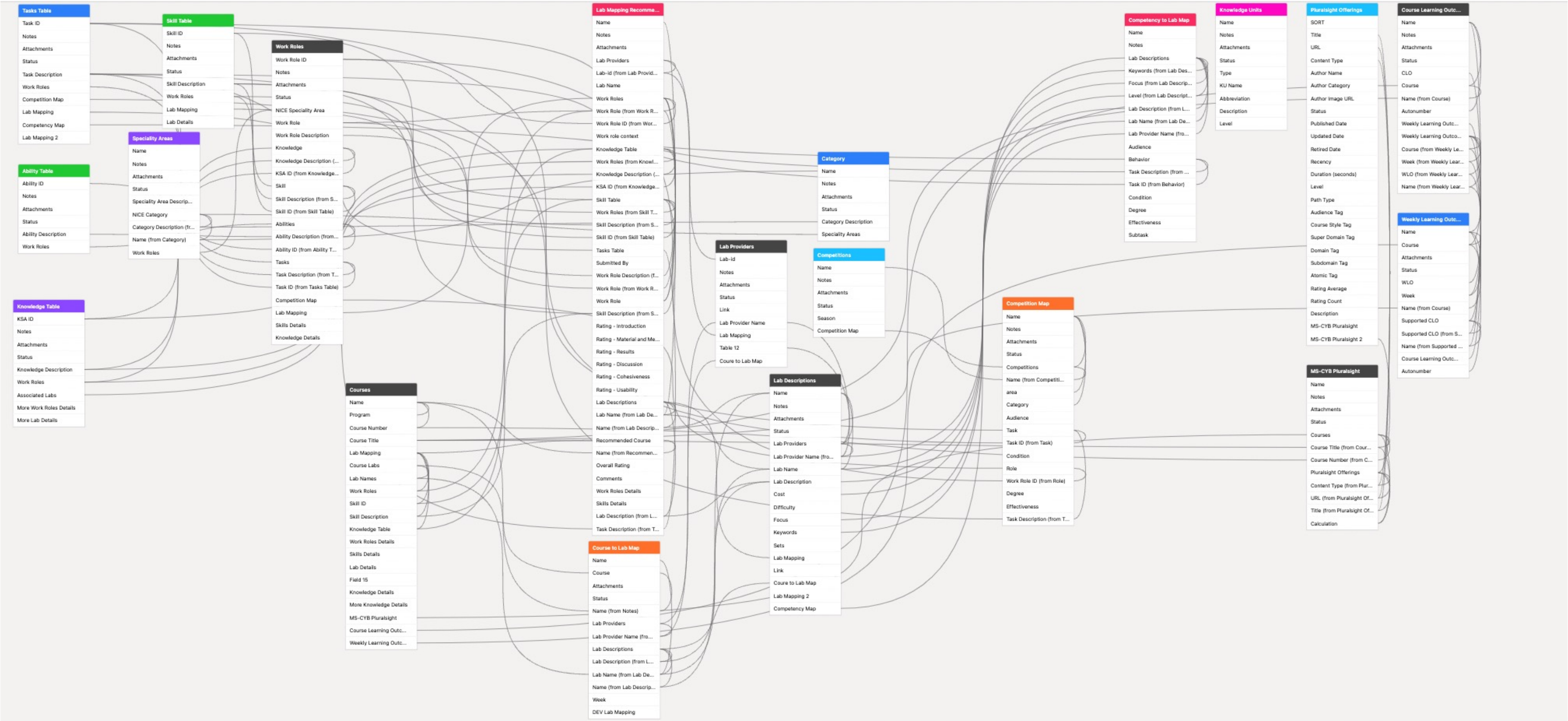
What is Airtable

- “Our powerful, visual platform connects data, people and workflows across the organization, so everyone's using the same source of truth. It's easy to start building on Airtable, and endlessly extensible: anyone can create and automate apps that perfectly fit their needs.”
- Airtable About Page

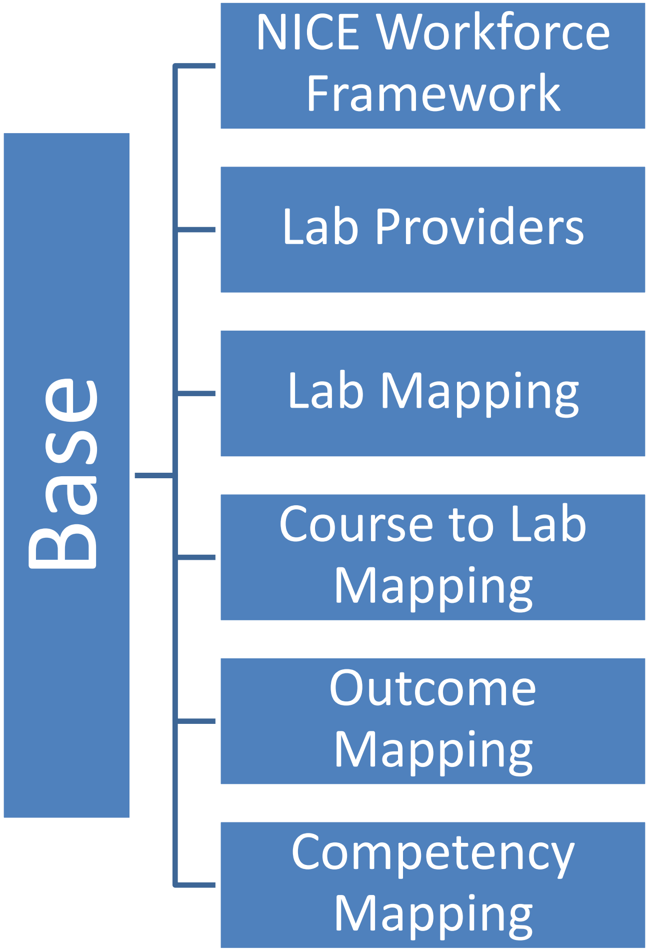
Airtable

- Visual way to build complex databases and easily display the data
- Easy to connect data and join tables
- Easy import

Structure


Tasks Table
Task ID
Notes
Attachments
Status
Task Description
Work Roles
Competition Map
Lab Mapping
Competency Map
Lab Mapping 2
Skill Table
Skill ID
Notes
Attachments
Status
Skill Description
Work Roles
Lab Mapping
Lab Details
Work Roles
Work Role ID
Notes
Attachments
Status
NICE Speciality Area
Work Role
Work Role Description
Knowledge
Knowledge Description (...
KSA ID (from Knowledge...
Skill
Skill Description (from S...
Skill ID (from Skill Table)
Abilities
Ability Description (from...
Ability ID (from Ability T...
Tasks
Task Description (from T...
Task ID (from Tasks Table)
Competition Map
Lab Mapping
Skills Details
Knowledge Details
Speciality Areas
Name
Notes
Attachments
Status
Speciality Area Descrip...
NICE Category
Category Description (fr...
Name (from Category)
Work Roles
Ability Table
Ability ID
Notes
Attachments
Status
Ability Description
Work Roles
Knowledge Table
KSA ID
Notes
Attachments
Status
Knowledge Description
Work Roles
Associated Labs
More Work Roles Details
More Lab Details
Courses
Name
Program
Course Number
Course Title
Lab Mapping
Course Labs
Lab Names
Work Roles
Skill ID
Skill Description
Knowledge Table
Work Roles Details
Skills Details
Lab Details
Field 15
Knowledge Details
More Knowledge Details
MS-CYB Pluralsight
Course Learning Outc...
Weekly Learning Outc...
Lab Mapping Recomme...
Name
Notes
Attachments
Lab Providers
Lab-id (from Lab Provid...
Lab Name
Work Roles
Work Role (from Work R...
Work Role ID (from Wor...
Work role context
Knowledge Table
Work Roles (from Knowl...
Knowledge Description (...
KSA ID (from Knowledge...
Skill Table
Work Roles (from Skill T...
Skill Description (from S...
Skill ID (from Skill Table)
Tasks Table
Submitted By
Work Role Description (f...
Work Role (from Work R...
Work Role
Skill Description (from S...
Rating - Introduction
Rating - Material and Me...
Rating - Results
Rating - Discussion
Rating - Cohesiveness
Rating - Usability
Lab Descriptions
Lab Name (from Lab De...
Name (from Lab Descrip...
Recommended Course
Name (from Recommen...
Overall Rating
Comments
Work Roles Details
Skills Details
Lab Description (from L...
Task Description (from T...
Course to Lab Map
Name
Course
Attachments
Status
Name (from Notes)
Lab Providers
Lab Provider Name (fro...
Lab Descriptions
Lab Description (from L...
Lab Name (from Lab De...
Name (from Lab Descrip...
Week
DEV Lab Mapping
Lab Providers
Lab-id
Notes
Attachments
Status
Link
Lab Provider Name
Lab Mapping
Table 12
Coure to Lab Map
Category
Name
Notes
Attachments
Status
Category Description
Speciality Areas
Competitions
Name
Notes
Attachments
Status
Season
Competition Map
Lab Descriptions
Name
Notes
Attachments
Status
Lab Providers
Lab Provider Name (fro...
Lab Name
Lab Description
Cost
Difficulty
Focus
Keywords
Sets
Lab Mapping
Link
Coure to Lab Map
Lab Mapping 2
Competency Map
Competition Map
Name
Notes
Attachments
Status
Competitions
Name (from Competiti...
area
Category
Audience
Task
Task ID (from Task)
Condition
Role
Work Role ID (from Role)
Degree
Effectiveness
Task Description (from T...
Competency to Lab Map
Name
Notes
Lab Descriptions
Keywords (from Lab Des...
Focus (from Lab Descrip...
Level (from Lab Descript...
Lab Description (from L...
Lab Name (from Lab De...
Lab Provider Name (fro...
Audience
Behavior
Task Description (from ...
Task ID (from Behavior)
Condition
Degree
Effectiveness
Subtask
Knowledge Units
Name
Notes
Attachments
Status
Type
KU Name
Abbreviation
Description
Level
Pluralsight Offerings
SORT
Title
URL
Content Type
Author Name
Author Category
Author Image URL
Status
Published Date
Updated Date
Retired Date
Recency
Duration (seconds)
Level
Path Type
Audience Tag
Course Style Tag
Super Domain Tag
Domain Tag
Subdomain Tag
Atomic Tag
Rating Average
Rating Count
Description
MS-CYB Pluralsight
MS-CYB Pluralsight 2
MS-CYB Pluralsight
Name
Notes
Attachments
Status
Courses
Course Title (from Cour...
Course Number (from C...
Pluralsight Offerings
Content Type (from Plur...
URL (from Pluralsight Of...
Title (from Pluralsight Of...
Calculation
Course Learning Outc...
Name
Notes
Attachments
Status
CLO
Course
Name (from Course)
Autonumber
Weekly Learning Outc...
Weekly Learning Outco...
Course (from Weekly Le...
Week (from Weekly Lear...
WLO (from Weekly Lear...
Name (from Weekly Lear...
Weekly Learning Outc...
Name
Course
Attachments
Status
WLO
Week
Name (from Course)
Supported CLO
Supported CLO (from S...
Name (from Supported ...
Course Learning Outc...
Autonumber

Structure



Base

NICE Workforce Framework

Lab Providers

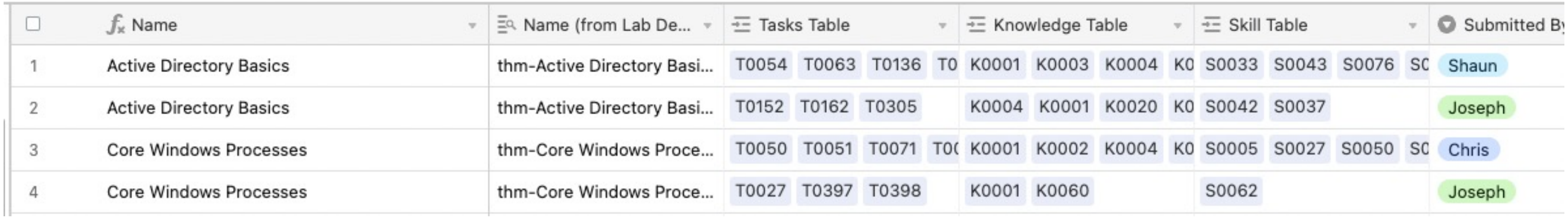
Lab Mapping

Course to Lab Mapping

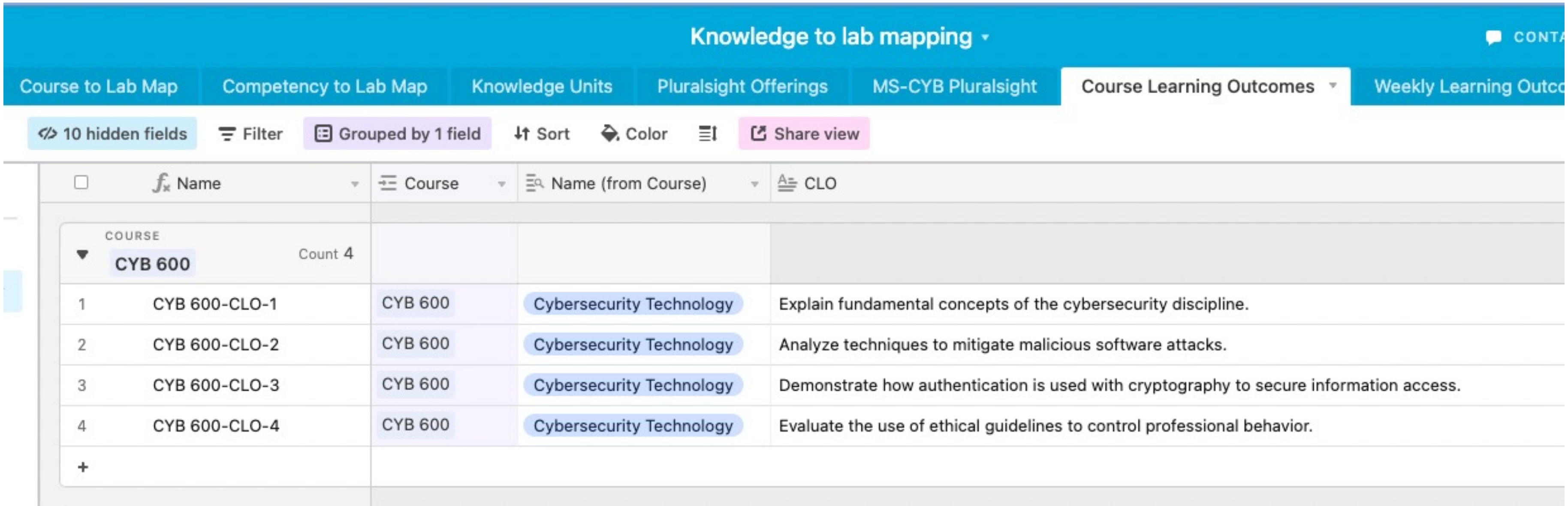
Outcome Mapping

Competency Mapping

Student Mapping to NICE Framework



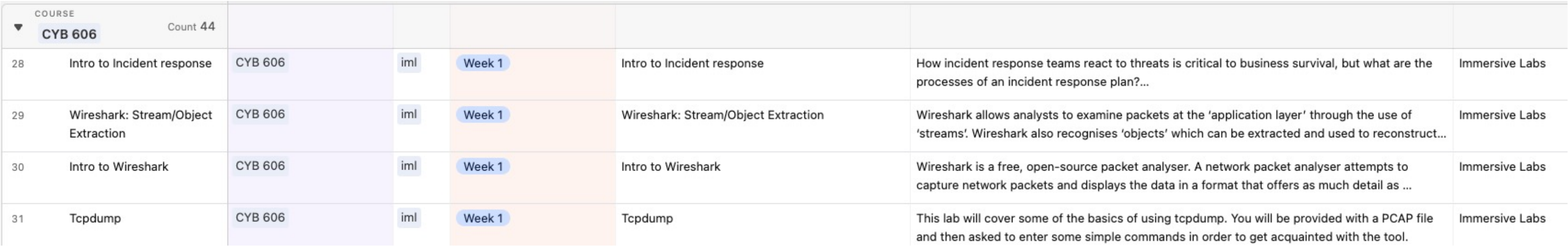
☐	Name	Name (from Lab De...	Tasks Table	Knowledge Table	Skill Table	Submitted B
1	Active Directory Basics	thm-Active Directory Basi...	T0054 T0063 T0136 T0	K0001 K0003 K0004 K0	S0033 S0043 S0076 S0	Shaun
2	Active Directory Basics	thm-Active Directory Basi...	T0152 T0162 T0305	K0004 K0001 K0020 K0	S0042 S0037	Joseph
3	Core Windows Processes	thm-Core Windows Proce...	T0050 T0051 T0071 T0	K0001 K0002 K0004 K0	S0005 S0027 S0050 S0	Chris
4	Core Windows Processes	thm-Core Windows Proce...	T0027 T0397 T0398	K0001 K0060	S0062	Joseph



	Name	Course	Name (from Course)	CLO
1	CYB 600-CLO-1	CYB 600	Cybersecurity Technology	Explain fundamental concepts of the cybersecurity discipline.
2	CYB 600-CLO-2	CYB 600	Cybersecurity Technology	Analyze techniques to mitigate malicious software attacks.
3	CYB 600-CLO-3	CYB 600	Cybersecurity Technology	Demonstrate how authentication is used with cryptography to secure information access.
4	CYB 600-CLO-4	CYB 600	Cybersecurity Technology	Evaluate the use of ethical guidelines to control professional behavior.

Course Learning Outcomes

Lab to Course Mapping

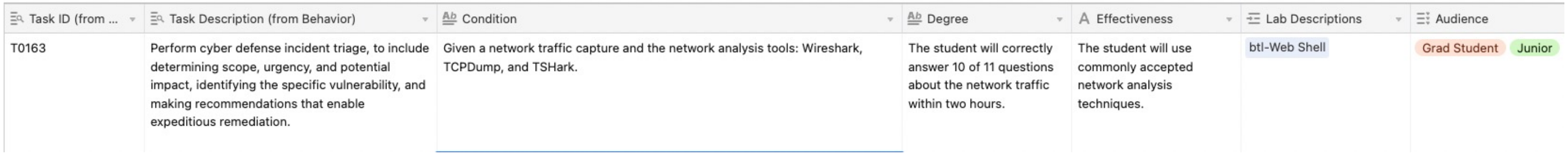


COURSE

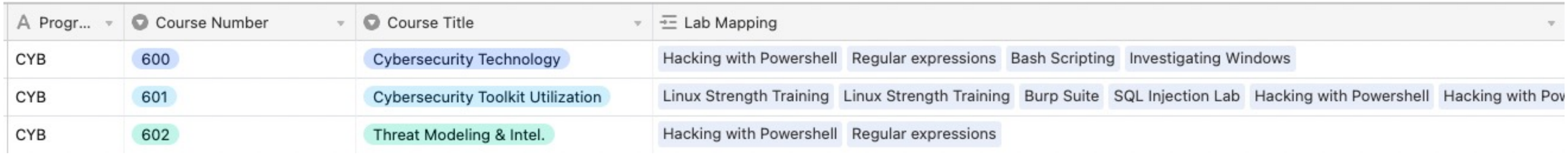
CYB 606 Count 44

28	Intro to Incident response	CYB 606	iml	Week 1	Intro to Incident response	How incident response teams react to threats is critical to business survival, but what are the processes of an incident response plan?...	Immersive Labs
29	Wireshark: Stream/Object Extraction	CYB 606	iml	Week 1	Wireshark: Stream/Object Extraction	Wireshark allows analysts to examine packets at the 'application layer' through the use of 'streams'. Wireshark also recognises 'objects' which can be extracted and used to reconstruct...	Immersive Labs
30	Intro to Wireshark	CYB 606	iml	Week 1	Intro to Wireshark	Wireshark is a free, open-source packet analyser. A network packet analyser attempts to capture network packets and displays the data in a format that offers as much detail as ...	Immersive Labs
31	Tcpdump	CYB 606	iml	Week 1	Tcpdump	This lab will cover some of the basics of using tcpdump. You will be provided with a PCAP file and then asked to enter some simple commands in order to get acquainted with the tool.	Immersive Labs

Competency Example



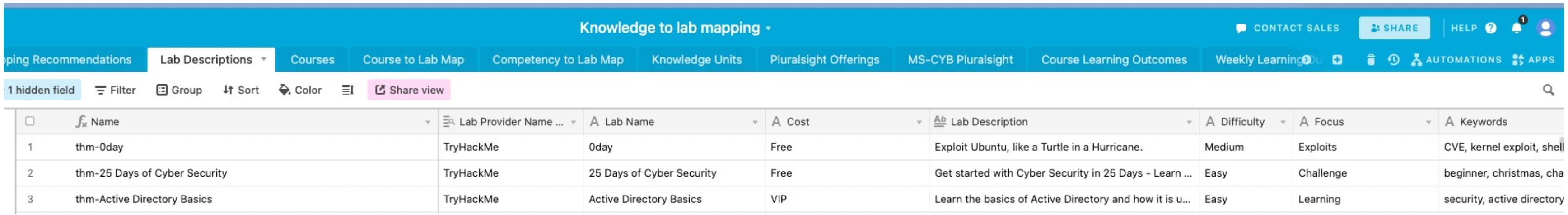
Task ID (from ...	Task Description (from Behavior)	Condition	Degree	Effectiveness	Lab Descriptions	Audience
T0163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.	Given a network traffic capture and the network analysis tools: Wireshark, TCPDump, and TSHark.	The student will correctly answer 10 of 11 questions about the network traffic within two hours.	The student will use commonly accepted network analysis techniques.	btl-Web Shell	Grad Student Junior



Progr...	Course Number	Course Title	Lab Mapping
CYB	600	Cybersecurity Technology	Hacking with Powershell Regular expressions Bash Scripting Investigating Windows
CYB	601	Cybersecurity Toolkit Utilization	Linux Strength Training Linux Strength Training Burp Suite SQL Injection Lab Hacking with Powershell Hacking with Pow
CYB	602	Threat Modeling & Intel.	Hacking with Powershell Regular expressions

Course Labs

Lab List



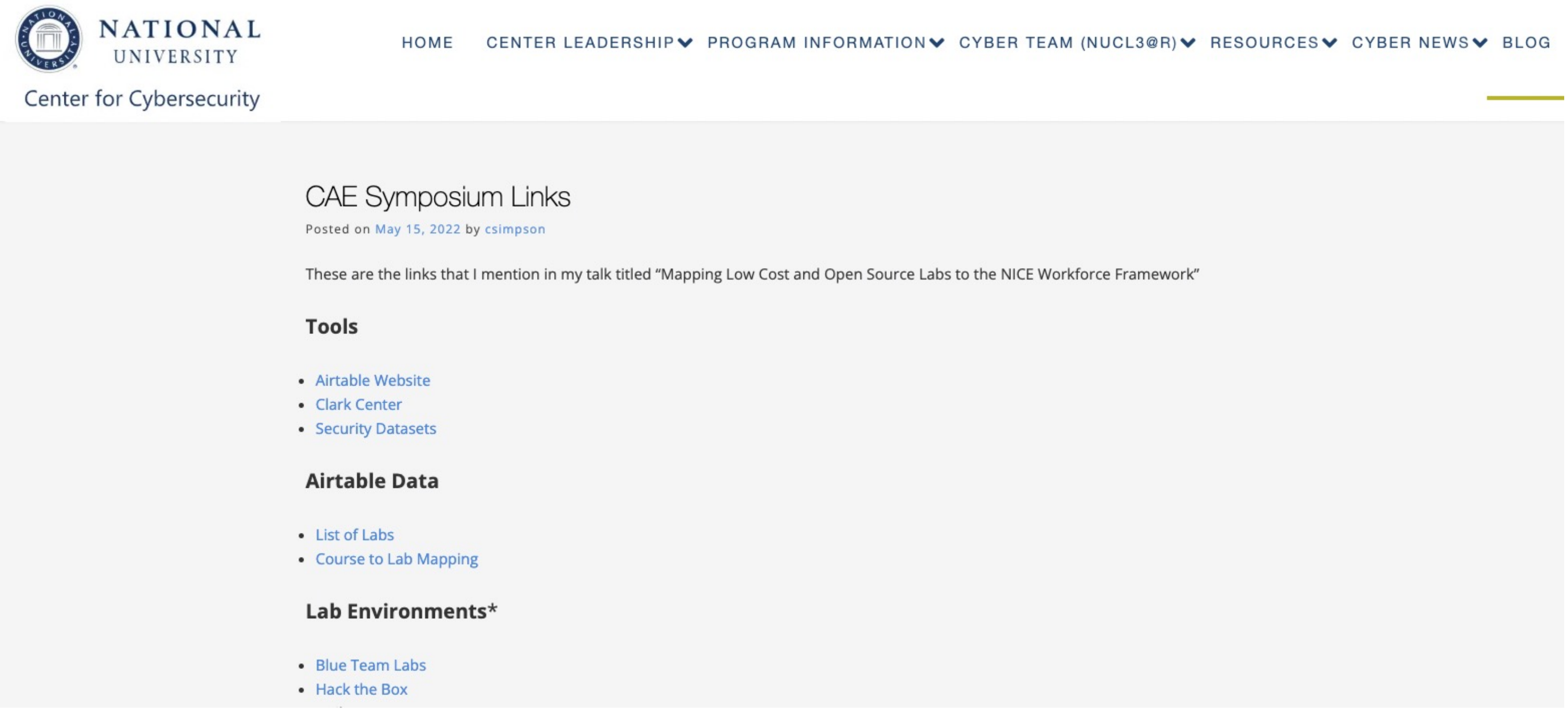
□	Name	Lab Provider Name ...	Lab Name	Cost	Lab Description	Difficulty	Focus	Keywords
1	thm-0day	TryHackMe	0day	Free	Exploit Ubuntu, like a Turtle in a Hurricane.	Medium	Exploits	CVE, kernel exploit, shell
2	thm-25 Days of Cyber Security	TryHackMe	25 Days of Cyber Security	Free	Get started with Cyber Security in 25 Days - Learn ...	Easy	Challenge	beginner, christmas, cha
3	thm-Active Directory Basics	TryHackMe	Active Directory Basics	VIP	Learn the basics of Active Directory and how it is u...	Easy	Learning	security, active directory

How much data in Airtable

- 607 Labs with descriptions
- 200 Weekly Learning Outcomes
- 16 classes
- NICE Workforce Framework
  - Roles
  - Knowledge
  - Skills
  - Tasks

Links and Videos

https://www.nucsia.org/2022/05/cae-symposium-links/



CAE Symposium Links

Posted on May 15, 2022 by csimpson

These are the links that I mention in my talk titled "Mapping Low Cost and Open Source Labs to the NICE Workforce Framework"

Tools

- Airtable Website
- Clark Center
- Security Datasets

Airtable Data

- List of Labs
- Course to Lab Mapping

Lab Environments*

- Blue Team Labs
- Hack the Box

Collaboration

- Happy to share access
- Welcome to enter data
- Evidencing Competency Working Group 2
  - Evaluating Tools

Questions?

- Email: csimpson@nu.edu

CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY
CAE
COMMUNITY