NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Webinar: Witnessing an Evolution- The NICE Framework and its Role in Building a Better Cybersecurity Workforce

December 15, 2021

CALL FOR COMMENTS – *due by January 31, 2022*

- Proposed NICE Framework Data Update Process
- Refactored NICE Framework Ability Statements
- NICE Framework Competencies, NISTIR 8355 (Second Draft)

NEW RESOURCE

- NICE Framework in machine-readable JSON Format

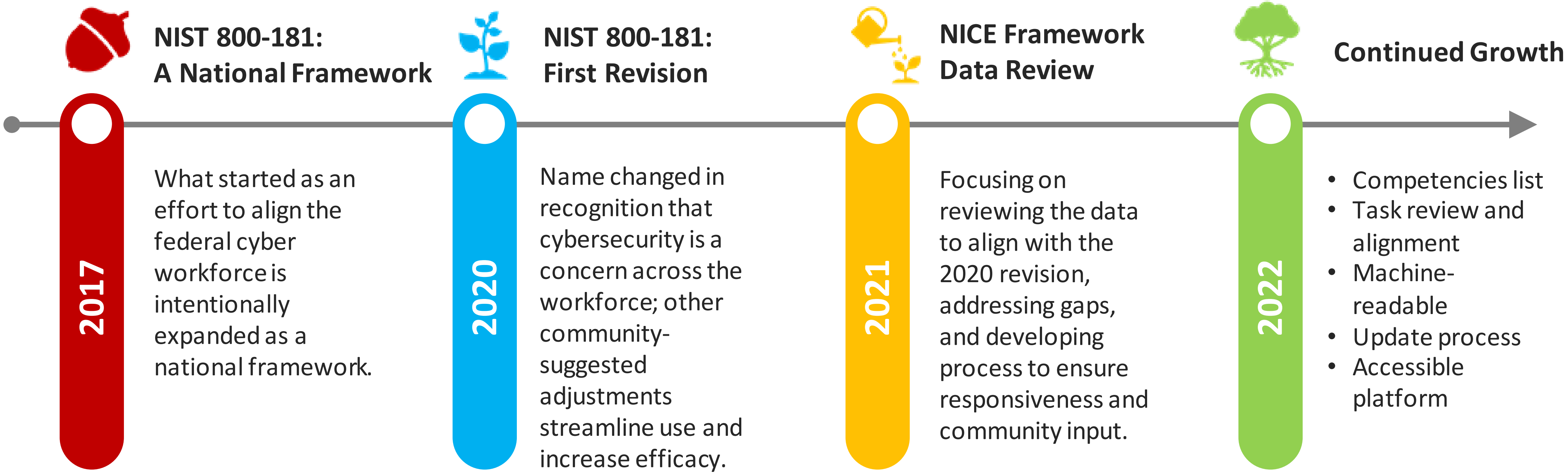
JUST ANNOUNCED

The NICE Framework: Evolution and Growth

Karen Wetzel, Manager of the NICE Framework

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Evolution: A Quick Recap



NIST 800-181:
A National Framework

2017

What started as an effort to align the federal cyber workforce is intentionally expanded as a national framework.

NIST 800-181:
First Revision

2020

Name changed in recognition that cybersecurity is a concern across the workforce; other community-suggested adjustments streamline use and increase efficacy.

NICE Framework
Data Review

2021

Focusing on reviewing the data to align with the 2020 revision, addressing gaps, and developing process to ensure responsiveness and community input.

Continued Growth

2022

- Competencies list
- Task review and alignment
- Machine-readable
- Update process
- Accessible platform

2020 Revision

- Stakeholder community feedback gathered since 2017 and during 2019 comment period
- National Framework: Government, Private Industry, and Academia
- Most significant changes:
  - Deprecation of Specialty Areas
  - Deprecation of Ability Statements
  - Addition of Competencies

NICE Framework Attributes

Agility
Keep pace with a constantly evolving ecosystem.

Flexibility
Account for your organization’s unique operating context.

Interoperability
Exchange workforce information using a common language and framework model.

Modularity
Communicate about other enterprise risks and workforces (e.g., privacy) within and across organizations and sectors.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Evolution and Transformation

Data Review: Ability Statement Refactoring

- Mostly skills, a handful of knowledge and task statements, e.g.:
  - A0016: Ability to facilitate small group discussions.
  - *Becomes:* Skill in facilitating small group discussions.
- Addressing redundancies and duplicates, e.g.:
  - A0010: Ability to analyze malware.
  - S0131 Skill in analyzing malware.
- Alignment with TKS Authoring Guide, e.g.,
  - A0061: Ability to design architectures and frameworks.
  - Skill: Skill in designing architectures
  - Skill: Skill in designing frameworks

178 Ability Statements…

- 42 Knowledge Statements
- 93 Skill Statements
- 6 Task Statements

14
1

TKS Authoring Guide General Principles

- Flexible
- Consistent
- Clear
- Affirmative
- Discrete

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Data Review: Skill Statements Review

TKS Authoring Guide alignment:

- **Consistent phrasing, e.g.,**
  - Skill in performing sensitivity analysis
  - Skill in performing fusion analysis
    (vs. the original "Skill in fusion analysis")
- **Observable actions, e.g.,**
  - Skill in recognizing relevance of information.
    - vs.
  - Skill in encrypting network communications.
- **Include only one skill, e.g.,**
  - Skill in identifying and extracting data of forensic interest in diverse media
    - becomes
  - Skill in identifying forensic data in diverse media *and* Skill in extracting forensic data in diverse media.

Also addresses:

- **Redundancies or duplicates:**
  - Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.
  - Skill in applying various analytical methods, tools, and techniques
- **Verbs, e.g.,** using, utilizing, use ("Skill in using PKI" becomes "Skill in implementing PKI")

Skill: The capacity to perform an observable action.
Skill Statements

- Begin with "Skill in" followed by a verb
- Represent observable actions
- Include only one skill in a single statement

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Data Review: Knowledge Statements

- Limited to a single concept
  - Possible exceptions to the rule (e.g., “Knowledge of performance tuning tools and techniques.”)
- Removal of parentheticals
  - Will introduce usage guidance field
  - Ex: Knowledge of key concepts in security management. (e.g., Release Management, Patch Management)

Knowledge: A retrievable set of concepts within memory.
Knowledge Statements

- Begin with “Knowledge of” followed by a concept
- Are limited to one concept in a single statement

Data Review: Competencies & Update Process

- NICE Framework Competencies NISTIR: Second Draft
  - Clearer definition
  - More clarity on Competencies vs. Work Roles
  - More application information

- NICE Framework Data Review and Update Process
  - Aim to implement in 2022
  - Provides insight into the proposed process
  - Answers questions

NICE Framework: Ongoing Improvements

- **Content Review & Updates**
  - December 2021:
    - Ability statement refactoring
    - Knowledge & Skill statements
    - NICE Framework Competencies (2nd draft)
  - 2022:
    - Task statements
    - Competencies List
- **NICE Framework Update Process**
  - December 2021: Overview release
  - 2022 Launch

- **Machine-readable format**
  - December 2021: JSON & Schema
- **2022: Web access, tools, resources**
  - Framework in Focus
  - Success Stories
  - Guides
  - Filling gaps (OT, Cybersecurity Awareness, etc.)

NICE Framework: Ongoing Improvements

- **Content Review & Updates**
  - December 2021:
    - Ability statement refactoring
    - Knowledge & Skill statements
    - NICE Framework Competencies (2nd draft)
  - 2022:
    - Task statements
    - Competencies List
- **NICE Framework Update Process**
  - December 2021: Overview release
  - 2022 Launch

ema

esources

y Awareness, etc.)

Strategic Plan: Expand Use of the NICE Framework

Document and disseminate uses

Align with other frameworks and publications

Establish regular review and update process

Explore tool development

Highlight areas that could be performed by automated techniques

Expand international outreach

For More Information

nist.gov/nice/framework

NICEFramework@nist.gov

nist.gov/nice/community

@NISTcyber

Karen Wetzel
Manager, NICE Framework
karen.wetzel@nist.gov

Q & A

Witnessing an Evolution - The NICE Framework and its Role in Building a Better Cybersecurity Workforce at Nova Southeastern University

Yair Levy, Ph.D.

Nova Southeastern University

College of Computing and Engineering

Professor of IS and Cybersecurity

Director of Center for Information Protection, Education, and Research (CIPhER) - https://InfoSec.nova.edu/

Proud NSA National Center of Academic Excellence (NCAE) in Cybersecurity - Cyber Defense (CD) since 2005!

NSU
Florida

Nova Southeastern University (NSU) - Florida

nova.edu

Nova Southeastern University (NSU) - Florida

College of Computing and Engineering

PREPARE FOR NEXT SEMESTER

computing.nova.edu

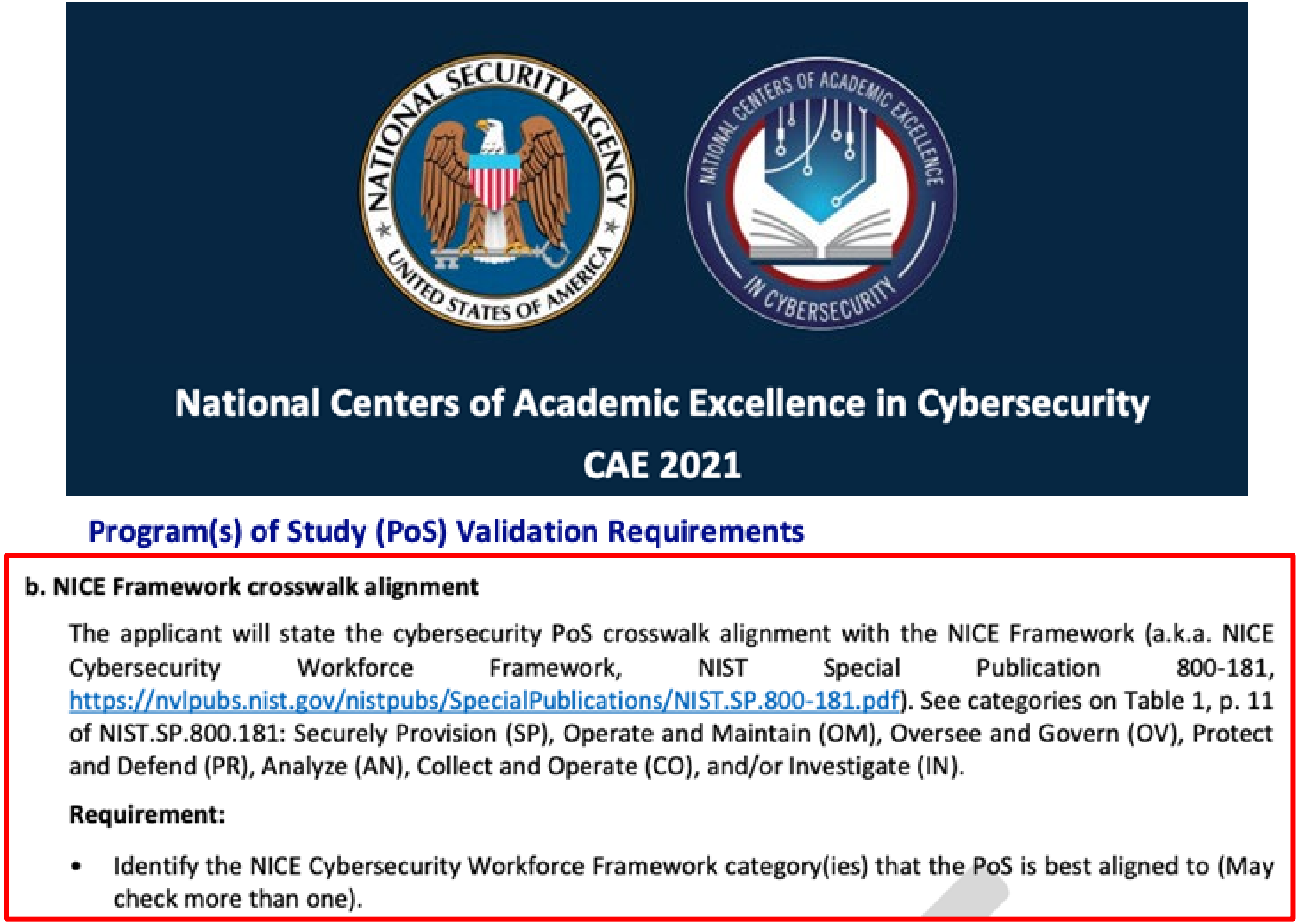
Nova Southeastern University (NSU) - Florida

- NSU's **College of Computing and Engineering** (https://computing.nova.edu/) is recognized as a national leader in Computer Science, Information Technology, and Cybersecurity Education.
  - BS in Computer Science – ABET Accredited
  - BS in Information Technology
  - BS minors in Cybersecurity or Data Analytics
  - MS in Cybersecurity Management – NSA NCAE-C Designated Program
  - MS in IA & Cybersecurity – NSA NCAE-C Designated Program
  - MS in Computer Science
  - MS programs in Information Technology, Data Analytics, Tech Leadership, and Information Systems
  - Ph.D. in Cybersecurity Management, Computer Science, and Information Systems

Nova Southeastern University (NSU) - Florida

- NSU was among the first in the State of Florida to be designated as a CAE in March 2005 and received CAE re-designation in 2009, 2014, and 2021 (https://infosec.nova.edu/)
- Cybersecurity Programs:
  - ***Ph.D. in Cybersecurity Management***
  - ***MS in Information Assurance and Cybersecurity*** (30cr)
    - Focus on “Network Security Engineering”
      ⍰ **NICE WF Cat: Protect and Defend**
  - ***MS in Cybersecurity Management*** (30cr)
    - Focus on “Security Policy Development and Compliance”
      ⍰ **NICE WF Cat: Oversee and Govern**

The NCAE-C & NICE Framework



National Centers of Academic Excellence in Cybersecurity

CAE 2021

Program(s) of Study (PoS) Validation Requirements

b. NICE Framework crosswalk alignment

The applicant will state the cybersecurity PoS crosswalk alignment with the NICE Framework (a.k.a. NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf). See categories on Table 1, p. 11 of NIST.SP.800.181: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and/or Investigate (IN).

Requirement:

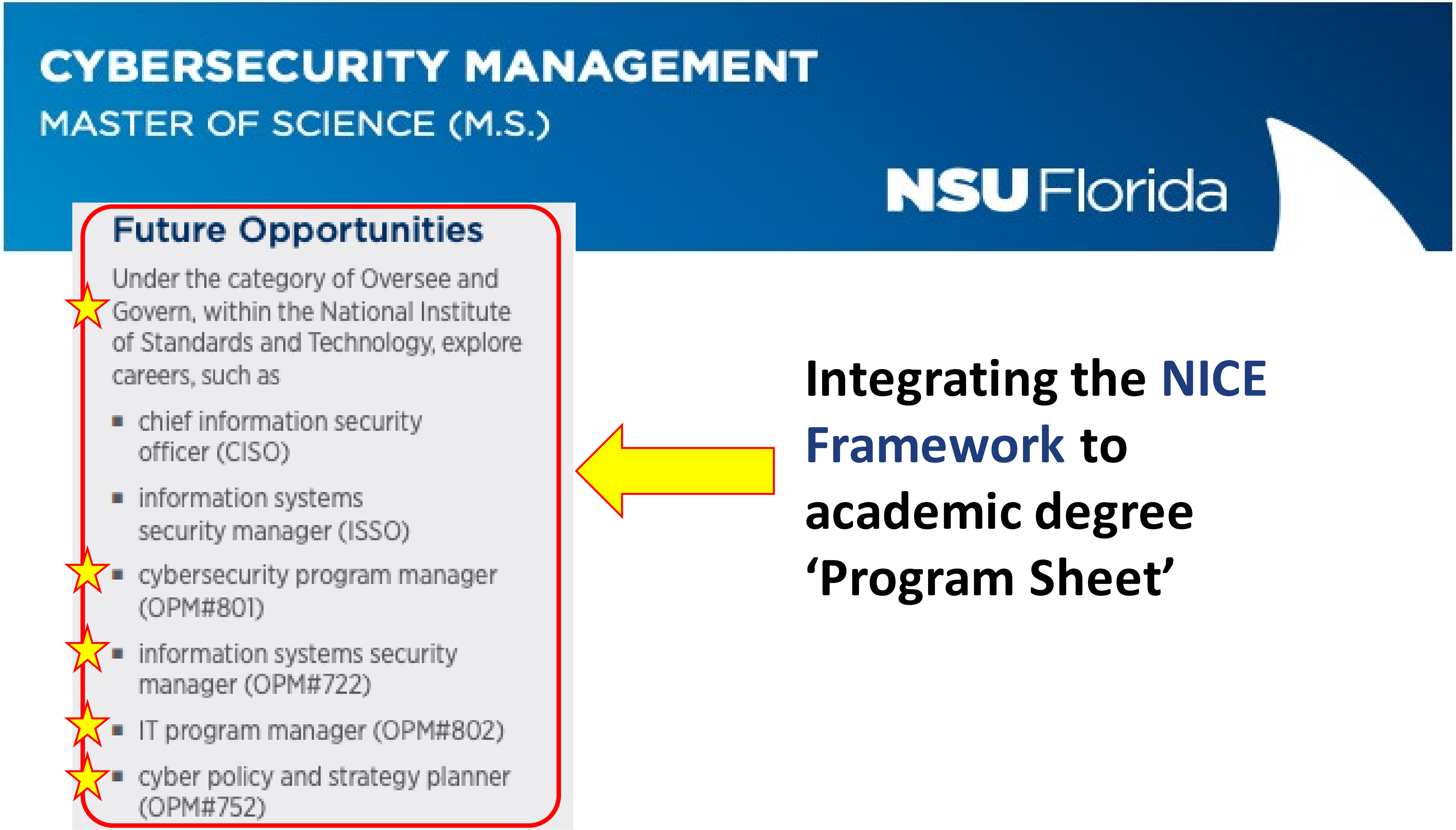
- Identify the NICE Cybersecurity Workforce Framework category(ies) that the PoS is best aligned to (May check more than one).

Source: https://public.cyber.mil/ncae-c/documents-library/

Nova Southeastern University (NSU)

- Faculty and staff of College of Computing and Engineering (CCE) at NSU and NSU Career Development Office (CDO) staff (https://www.nova.edu/career/) collaboration
- Integration of the NCWF into the student advising process
    - Relevant job roles for the NSA NCAE-C designated programs
    - Identifying and listing NCWF Job Roles for each program
    - Exposure of the framework to the career advisors
    - Creation of a focused Career Development Newsletter
    - Development of sample student resumes
        - Entry level, five, and 10 Years of Experience resume samples

Nova Southeastern University (NSU)



CYBERSECURITY MANAGEMENT

MASTER OF SCIENCE (M.S.)

NSU Florida

Future Opportunities

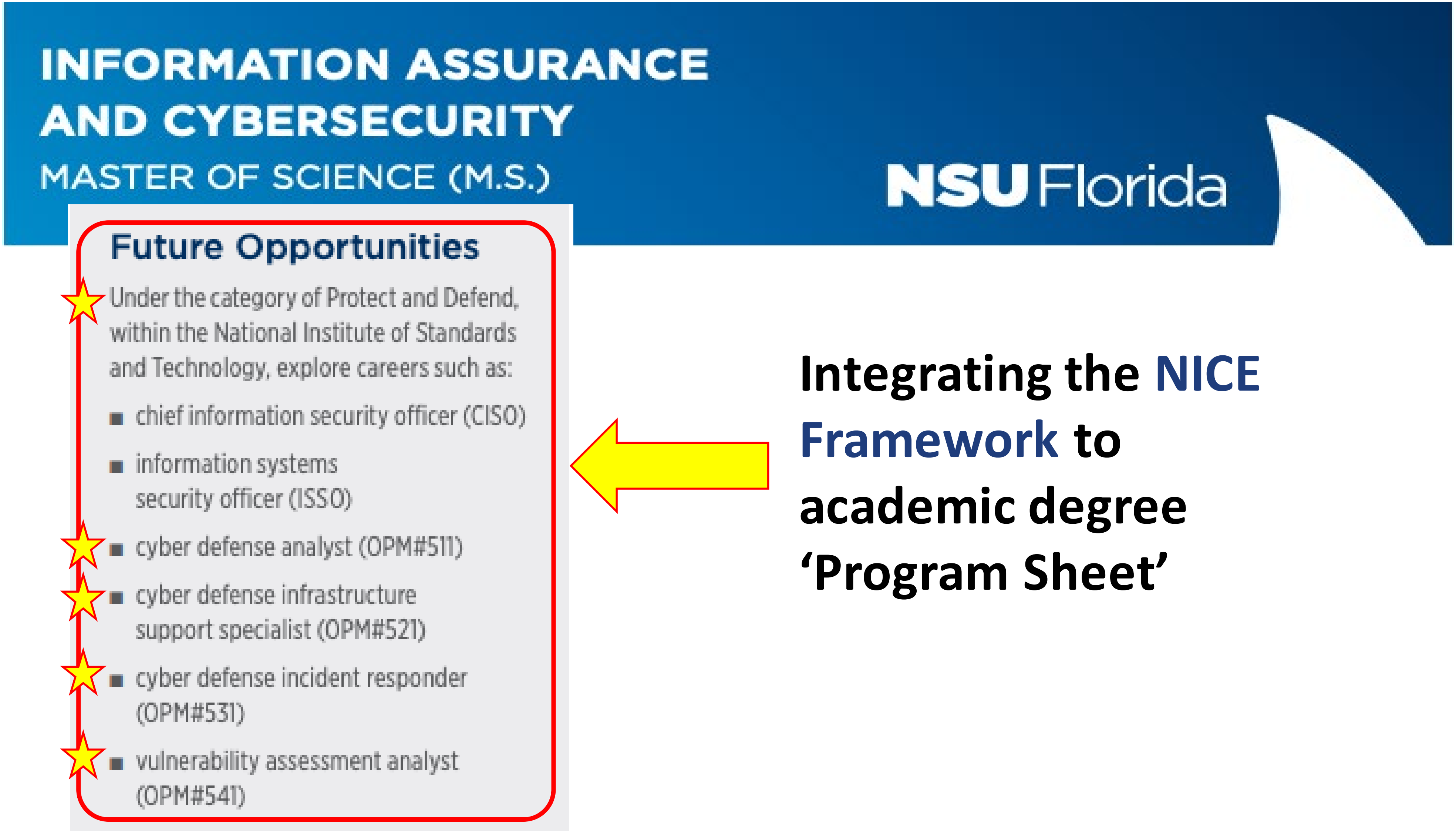
Under the category of Oversee and Govern, within the National Institute of Standards and Technology, explore careers, such as

- chief information security officer (CISO)
- information systems security manager (ISSO)
- cybersecurity program manager (OPM#801)
- information systems security manager (OPM#722)
- IT program manager (OPM#802)
- cyber policy and strategy planner (OPM#752)

Integrating the NICE Framework to academic degree ‘Program Sheet’

Source: https://computing.nova.edu/masters/documents/ms-cybersec-mgmt.pdf

Nova Southeastern University (NSU)



INFORMATION ASSURANCE
AND CYBERSECURITY
MASTER OF SCIENCE (M.S.)

NSU Florida

Future Opportunities

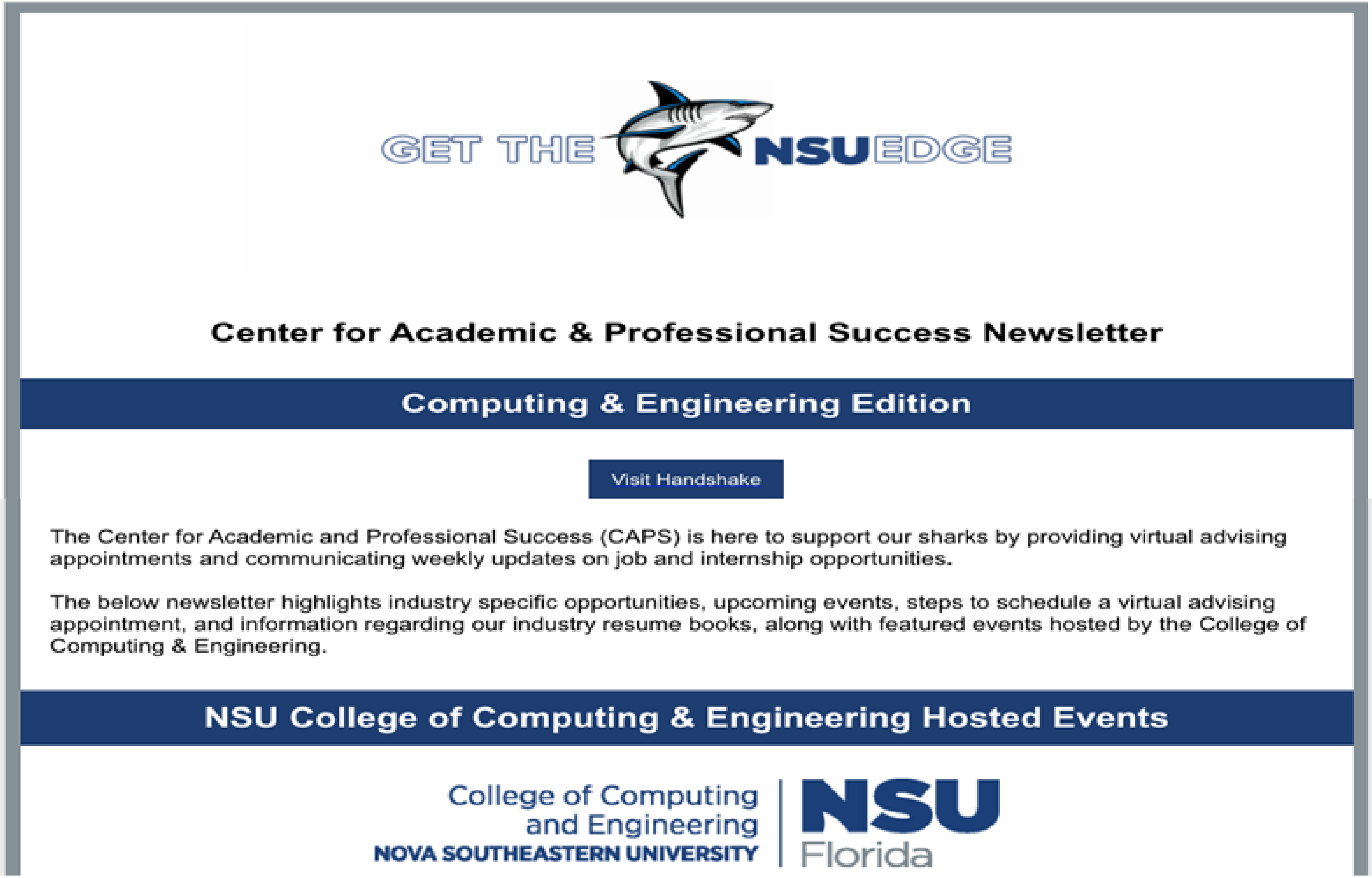
Under the category of Protect and Defend, within the National Institute of Standards and Technology, explore careers such as:

- chief information security officer (CISO)
- information systems security officer (ISSO)
- cyber defense analyst (OPM#511)
- cyber defense infrastructure support specialist (OPM#521)
- cyber defense incident responder (OPM#531)
- vulnerability assessment analyst (OPM#541)

Integrating the NICE Framework to academic degree ‘Program Sheet’

Source: https://computing.nova.edu/computing/documents/ms-info_assurance_cybersecurity.pdf

Nova Southeastern University (NSU)



Center for Academic & Professional Success Newsletter

Computing & Engineering Edition

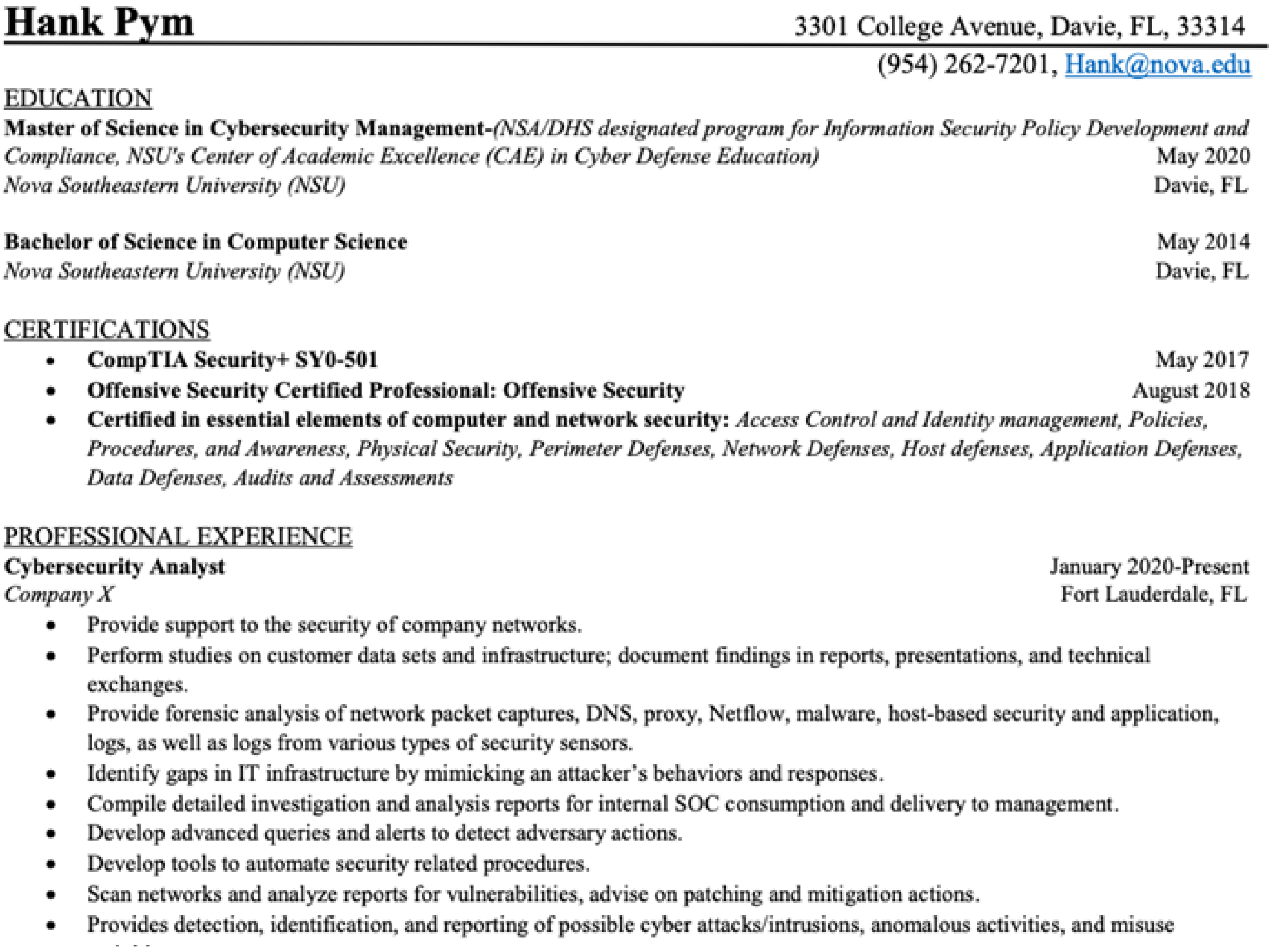
The Center for Academic and Professional Success (CAPS) is here to support our sharks by providing virtual advising appointments and communicating weekly updates on job and internship opportunities.

The below newsletter highlights industry specific opportunities, upcoming events, steps to schedule a virtual advising appointment, and information regarding our industry resume books, along with featured events hosted by the College of Computing & Engineering.

NSU College of Computing & Engineering Hosted Events

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU Florida

Nova Southeastern University (NSU)



Hank Pym

3301 College Avenue, Davie, FL, 33314
(954) 262-7201, Hank@nova.edu

EDUCATION

Master of Science in Cybersecurity Management-*(NSA/DHS designated program for Information Security Policy Development and Compliance, NSU's Center of Academic Excellence (CAE) in Cyber Defense Education)* May 2020
Nova Southeastern University (NSU) Davie, FL

Bachelor of Science in Computer Science May 2014
Nova Southeastern University (NSU) Davie, FL

CERTIFICATIONS

- **CompTIA Security+ SY0-501** May 2017
- **Offensive Security Certified Professional: Offensive Security** August 2018
- **Certified in essential elements of computer and network security:** *Access Control and Identity management, Policies, Procedures, and Awareness, Physical Security, Perimeter Defenses, Network Defenses, Host defenses, Application Defenses, Data Defenses, Audits and Assessments*

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst January 2020-Present
Company X Fort Lauderdale, FL

- Provide support to the security of company networks.
- Perform studies on customer data sets and infrastructure; document findings in reports, presentations, and technical exchanges.
- Provide forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and application, logs, as well as logs from various types of security sensors.
- Identify gaps in IT infrastructure by mimicking an attacker's behaviors and responses.
- Compile detailed investigation and analysis reports for internal SOC consumption and delivery to management.
- Develop advanced queries and alerts to detect adversary actions.
- Develop tools to automate security related procedures.
- Scan networks and analyze reports for vulnerabilities, advise on patching and mitigation actions.
- Provides detection, identification, and reporting of possible cyber attacks/intrusions, anomalous activities, and misuse

NICE Framework – Core

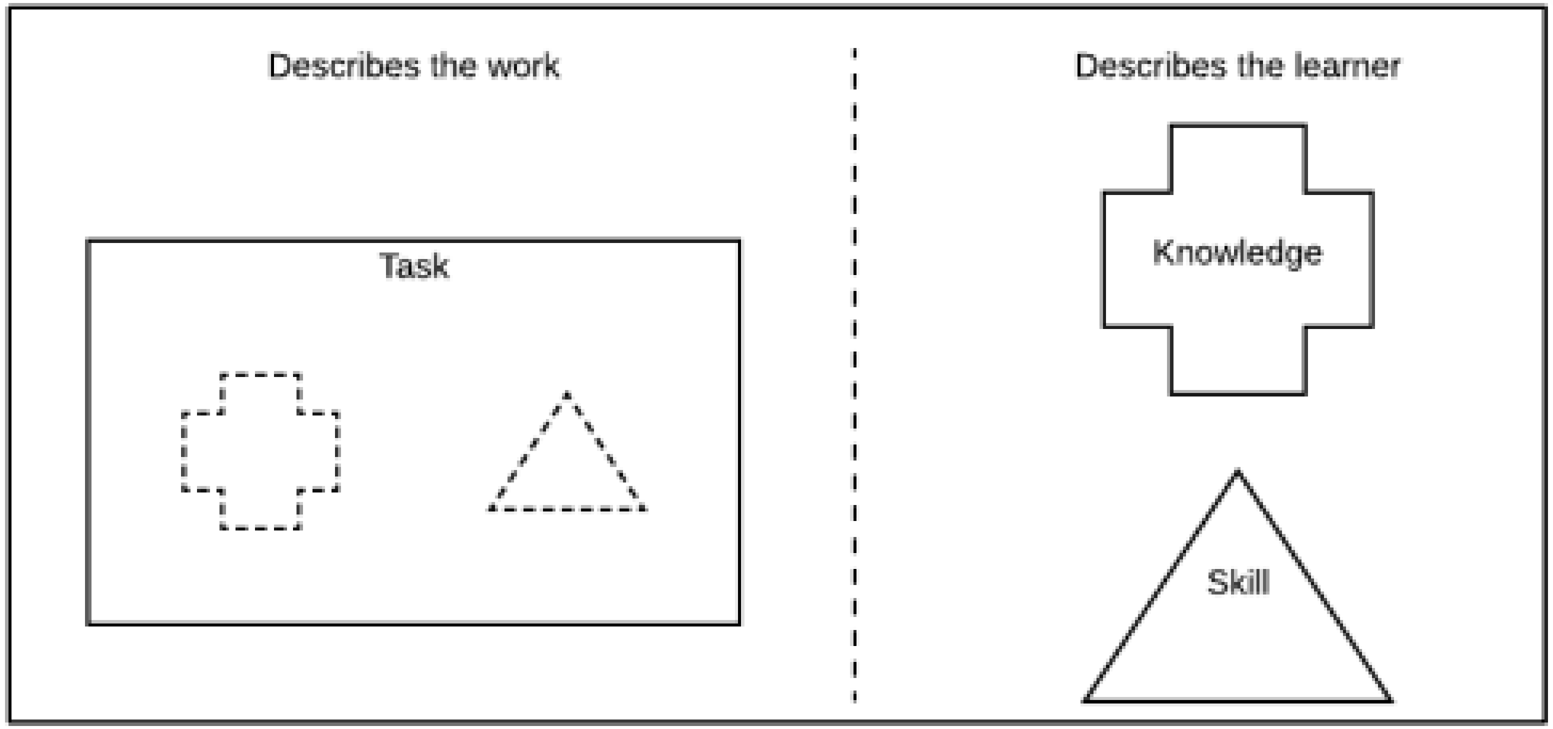


Figure 1 - NICE Framework Approach

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1-draft.pdf

Skill Development and Competencies

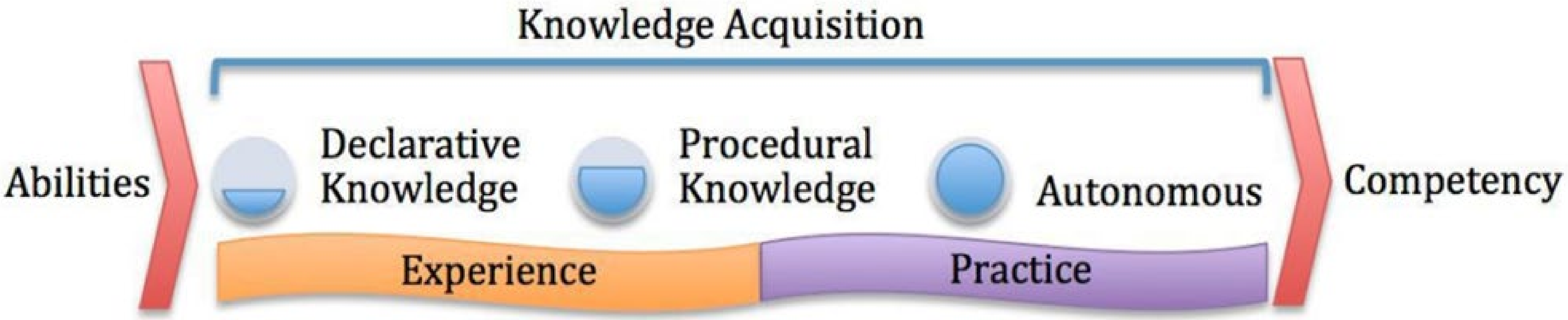
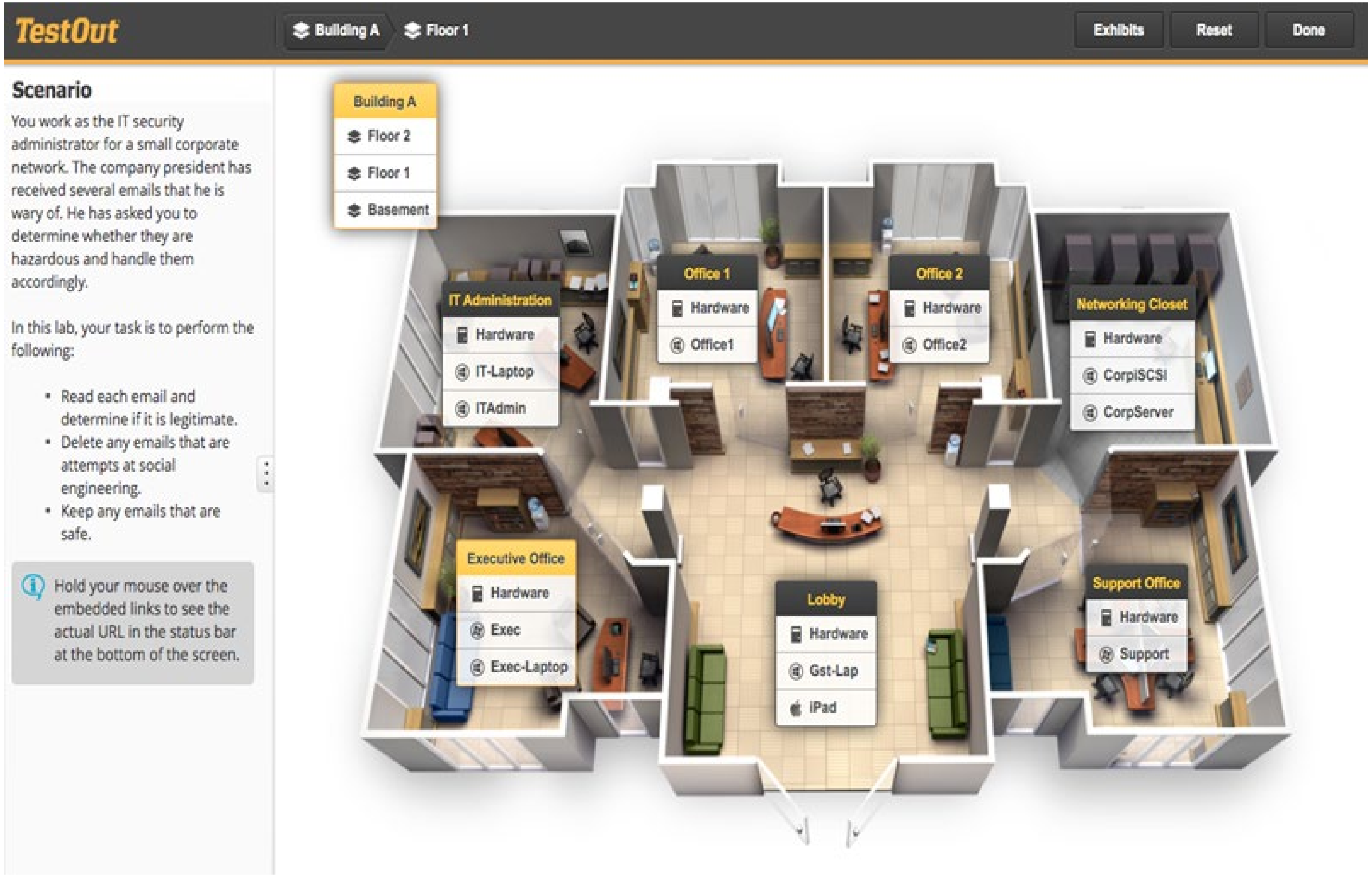


Figure 1. The Stages of Skill Development and Competency Attainment

Carlton, M., Levy, Y., & Ramim, M. M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security, 27*(1), 101-121. https://doi.org/10.1108/ICS-11-2016-0088

Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. *Online Journal of Applied Knowledge Management, 6*(1), 107-118. https://doi.org/10.36965/OJAKM.2018.6(1)107-118

Skill Development and Competencies



Scenario

You work as the IT security administrator for a small corporate network. The company president has received several emails that he is wary of. He has asked you to determine whether they are hazardous and handle them accordingly.

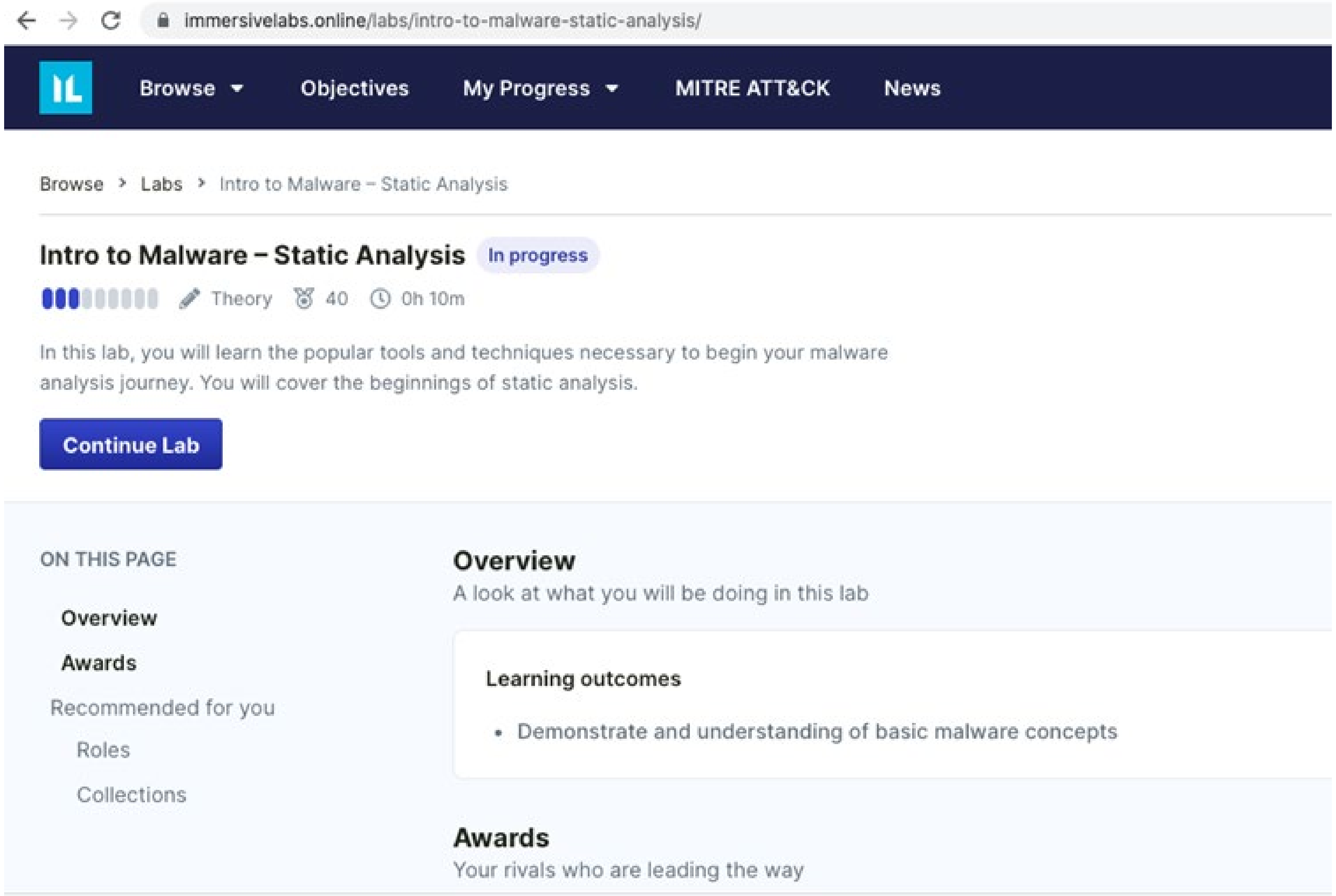
In this lab, your task is to perform the following:

- Read each email and determine if it is legitimate.
- Delete any emails that are attempts at social engineering.
- Keep any emails that are safe.

Hold your mouse over the embedded links to see the actual URL in the status bar at the bottom of the screen.

TestOut – LabSim SecurityPro

Skill Development and Competencies



immersivelabs.online/labs/intro-to-malware-static-analysis/
IL
Browse
Objectives
My Progress
MITRE ATT&CK
News
Browse › Labs › Intro to Malware – Static Analysis

Intro to Malware – Static Analysis

In progress

Theory 40 0h 10m

In this lab, you will learn the popular tools and techniques necessary to begin your malware analysis journey. You will cover the beginnings of static analysis.

Overview

A look at what you will be doing in this lab

Learning outcomes

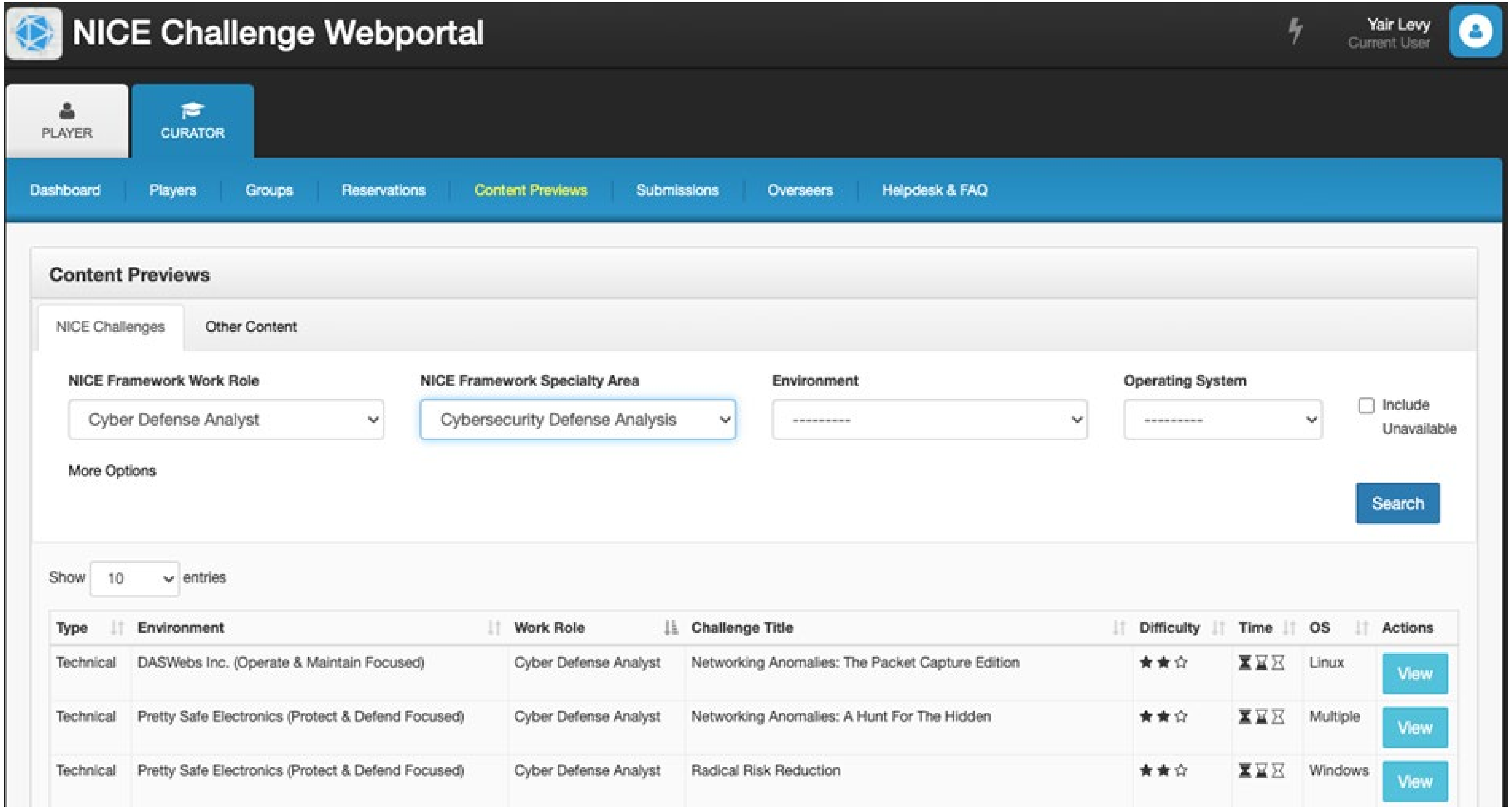
- Demonstrate and understanding of basic malware concepts

Awards

Your rivals who are leading the way

ImmersiveLabs.com - Digital Cyber Academy (DCA)

Skill Development and Competencies



Content Previews

NICE Challenges | Other Content

NICE Framework Work Role: Cyber Defense Analyst

NICE Framework Specialty Area: Cybersecurity Defense Analysis

Environment: ----------

Operating System: ----------

☐ Include Unavailable

More Options

Show 10 entries

Type	Environment	Work Role	Challenge Title	Difficulty	Time	OS	Actions
Technical	DASWebs Inc. (Operate & Maintain Focused)	Cyber Defense Analyst	Networking Anomalies: The Packet Capture Edition	★★☆	⧗⧗⧖	Linux	View
Technical	Pretty Safe Electronics (Protect & Defend Focused)	Cyber Defense Analyst	Networking Anomalies: A Hunt For The Hidden	★★☆	⧗⧗⧖	Multiple	View
Technical	Pretty Safe Electronics (Protect & Defend Focused)	Cyber Defense Analyst	Radical Risk Reduction	★★☆	⧗⧗⧖	Windows	View

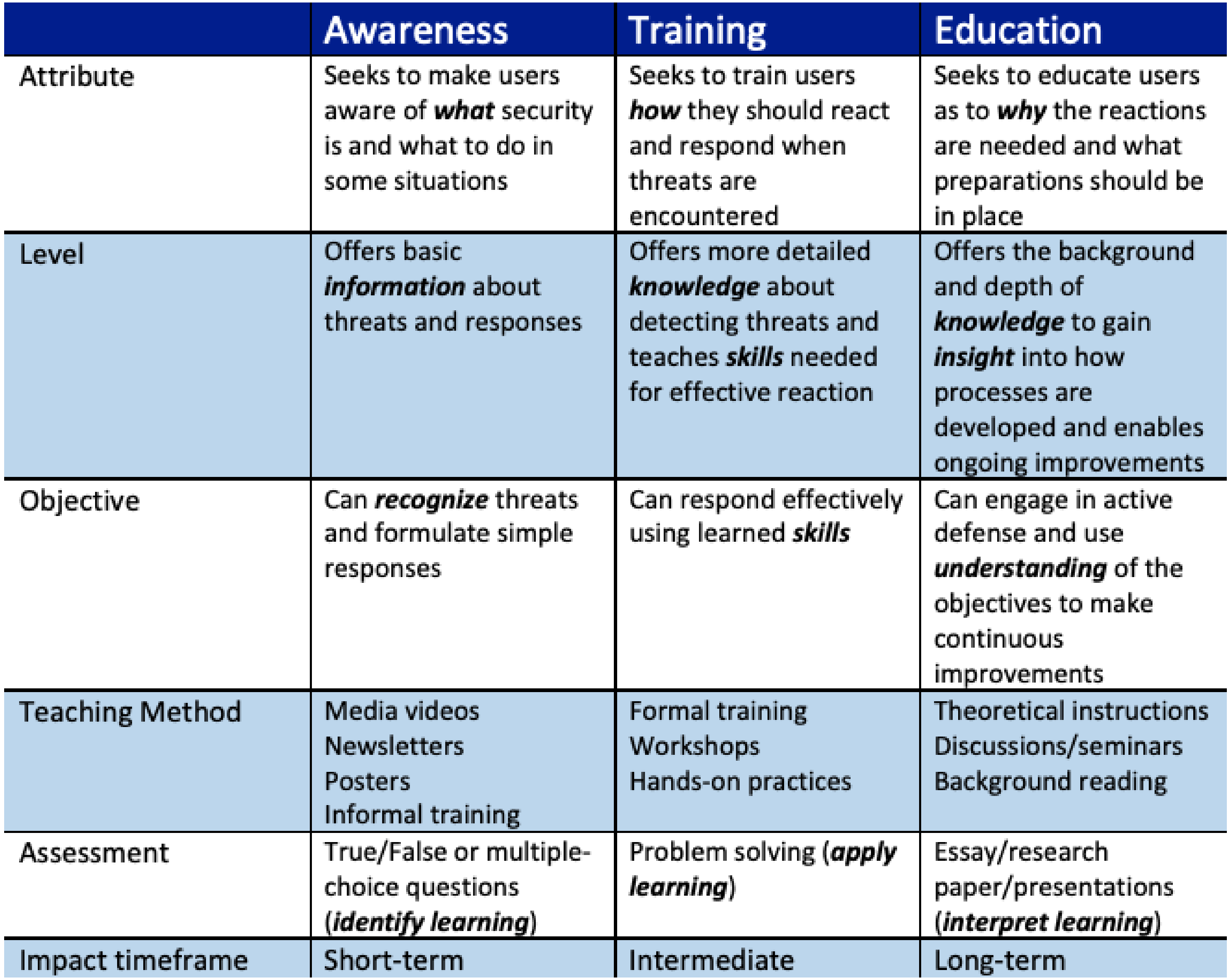
https://nice-challenge.com/

Witnessing an Evolution - The NICE Framework and its Role in Building a Better Cybersecurity Workforce

at Nova Southeastern University (NSU)

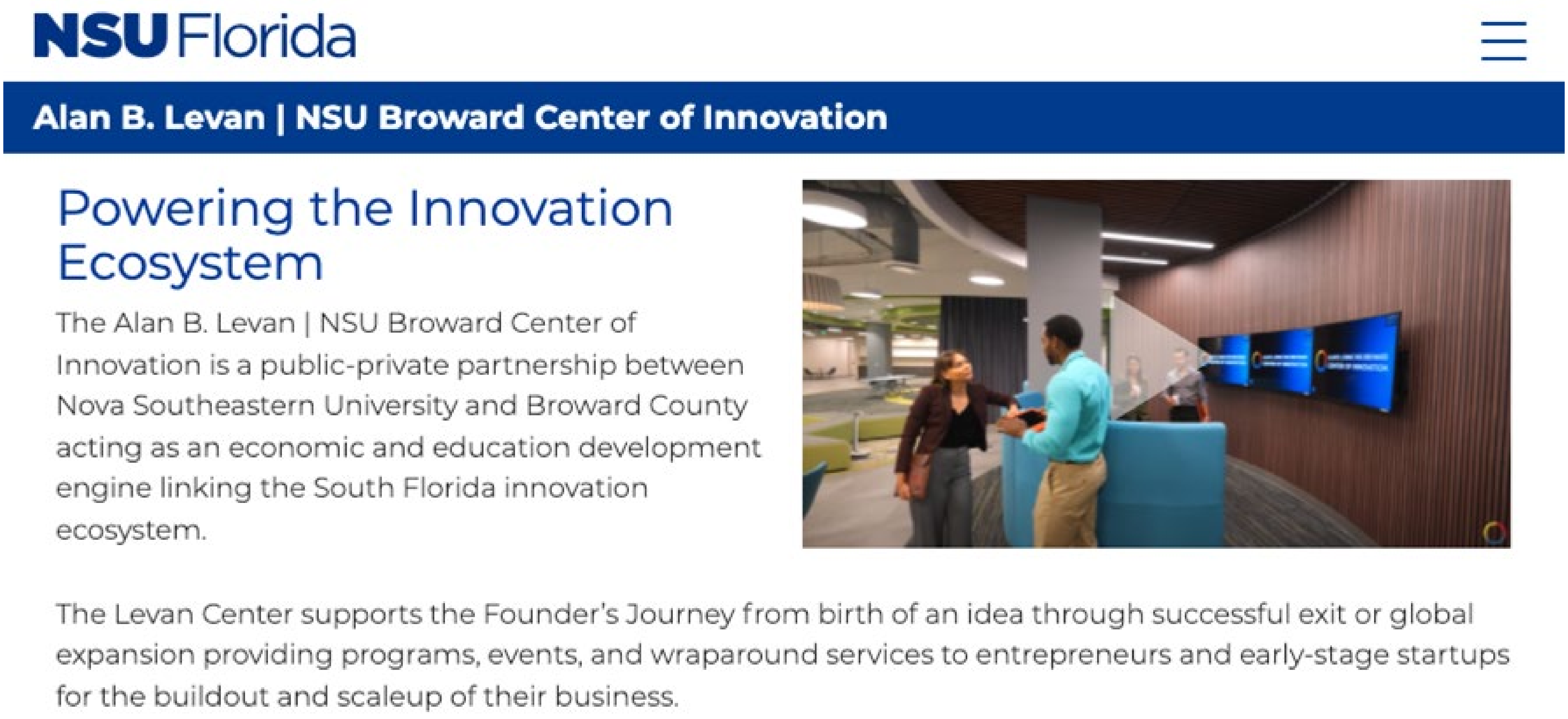
- The future?

Future in Skills and Competency Assessments



	Awareness	Training	Education
Attribute	Seeks to make users aware of ***what*** security is and what to do in some situations	Seeks to train users ***how*** they should react and respond when threats are encountered	Seeks to educate users as to ***why*** the reactions are needed and what preparations should be in place
Level	Offers basic ***information*** about threats and responses	Offers more detailed ***knowledge*** about detecting threats and teaches ***skills*** needed for effective reaction	Offers the background and depth of ***knowledge*** to gain ***insight*** into how processes are developed and enables ongoing improvements
Objective	Can ***recognize*** threats and formulate simple responses	Can respond effectively using learned ***skills***	Can engage in active defense and use ***understanding*** of the objectives to make continuous improvements
Teaching Method	Media videos Newsletters Posters Informal training	Formal training Workshops Hands-on practices	Theoretical instructions Discussions/seminars Background reading
Assessment	True/False or multiple-choice questions (***identify learning***)	Problem solving (***apply learning***)	Essay/research paper/presentations (***interpret learning***)
Impact timeframe	Short-term	Intermediate	Long-term

Source: *Whitman, M., & Mattord, H. (2021). Principles of information security (7th ed.). Cengage Learning.*



NSU Florida

Alan B. Levan | NSU Broward Center of Innovation

Powering the Innovation Ecosystem

The Alan B. Levan | NSU Broward Center of Innovation is a public-private partnership between Nova Southeastern University and Broward County acting as an economic and education development engine linking the South Florida innovation ecosystem.

The Levan Center supports the Founder's Journey from birth of an idea through successful exit or global expansion providing programs, events, and wraparound services to entrepreneurs and early-stage startups for the buildout and scaleup of their business.

https://www.nova.edu/innovation/

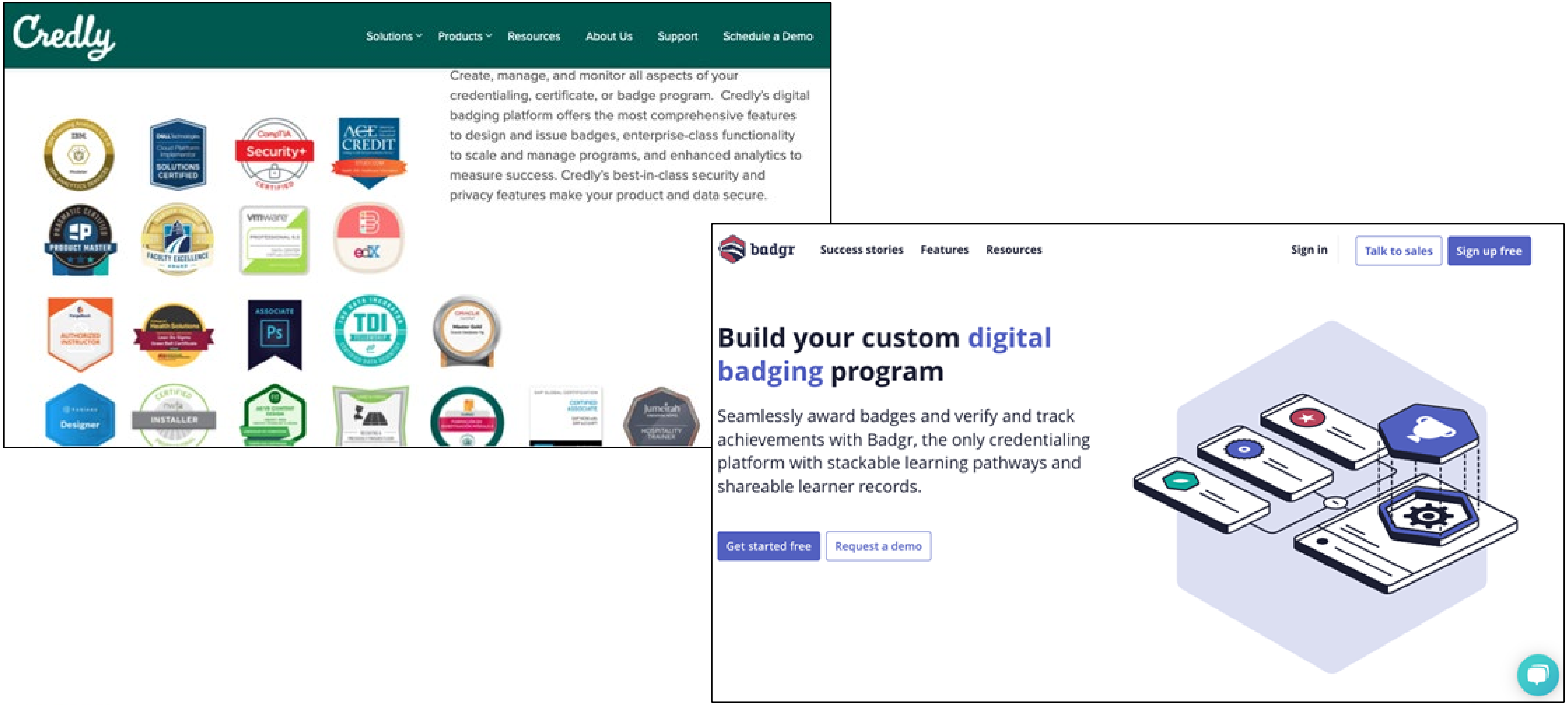
NSU Florida

Alan B. Levan | NSU Broward Center of Innovation

Levan Center Cybersecurity overview

https://www.nova.edu/innovation/

Future in Skills and Competency Assessments



Create, manage, and monitor all aspects of your credentialing, certificate, or badge program. Credly's digital badging platform offers the most comprehensive features to design and issue badges, enterprise-class functionality to scale and manage programs, and enhanced analytics to measure success. Credly's best-in-class security and privacy features make your product and data secure.

Build your custom digital badging program

Seamlessly award badges and verify and track achievements with Badgr, the only credentialing platform with stackable learning pathways and shareable learner records.

Thank you!

Contact:

levyy@nova.edu

https://www.caecommunity.org/community-of-practice/cyber-defense

Q & A

EC-Council

BUILDING AND MEASURING CYBERSECURITY SKILLS

CyberQ

Mapping Cyber Range activities to the NICE Framework

Steve Graham – Sr. Vice President

ABOUT EC-COUNCIL

2001: EC-Council was founded.

2003: Launched the Certified Ethical Hacker (CEH) course and certification.

2005: EC-Council's first federal customer – Federal Bureau of Investigation (FBI).

2010: Achieve first U.S. Department of Defense (DoD) Accreditation for CEH.

2004-21: Developed over 20 hands-on, tactical Cybersecurity certification courses along with several leading cybersecurity education brands. 4 Courses accredited by the U.S. Department of Defense (DoD).

EC-Council Global Brands

EC-Council Hackers are here. Where are you?
EC-COUNCIL | ACADEMIA
CyberQ
codered FROM EC-COUNCIL
OHPHISH Fortifying Front Lines
CISO MAG
Hacker Halted
EC-COUNCIL UNIVERSITY
EC-Council | iClass
EC-Council CISO PROGRAM
IIB COUNCIL
GLOBAL CYBERLYMPICS
CEH Certified Ethical Hacker
Accredited Training Center EC-Council
STORM

EC-Council

Teaching Cybersecurity for Over 20 Years

Accreditations / Mapping

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

ANSI ACCREDITED ISO/IEC 17024 Personnel Certification Program #0937

CNSS

nicf National Infocomm Competency Framework

MSC MALAYSIA

ACE American Council on Education

Accepted and Trusted Globally By

pwc

accenture

Microsoft

KPMG

DELL

Deloitte.

L&T Infotech

EY

tcs

AtoS

wipro

Capgemini

FUJITSU

genpact

PayPal

pepsi

Reliance

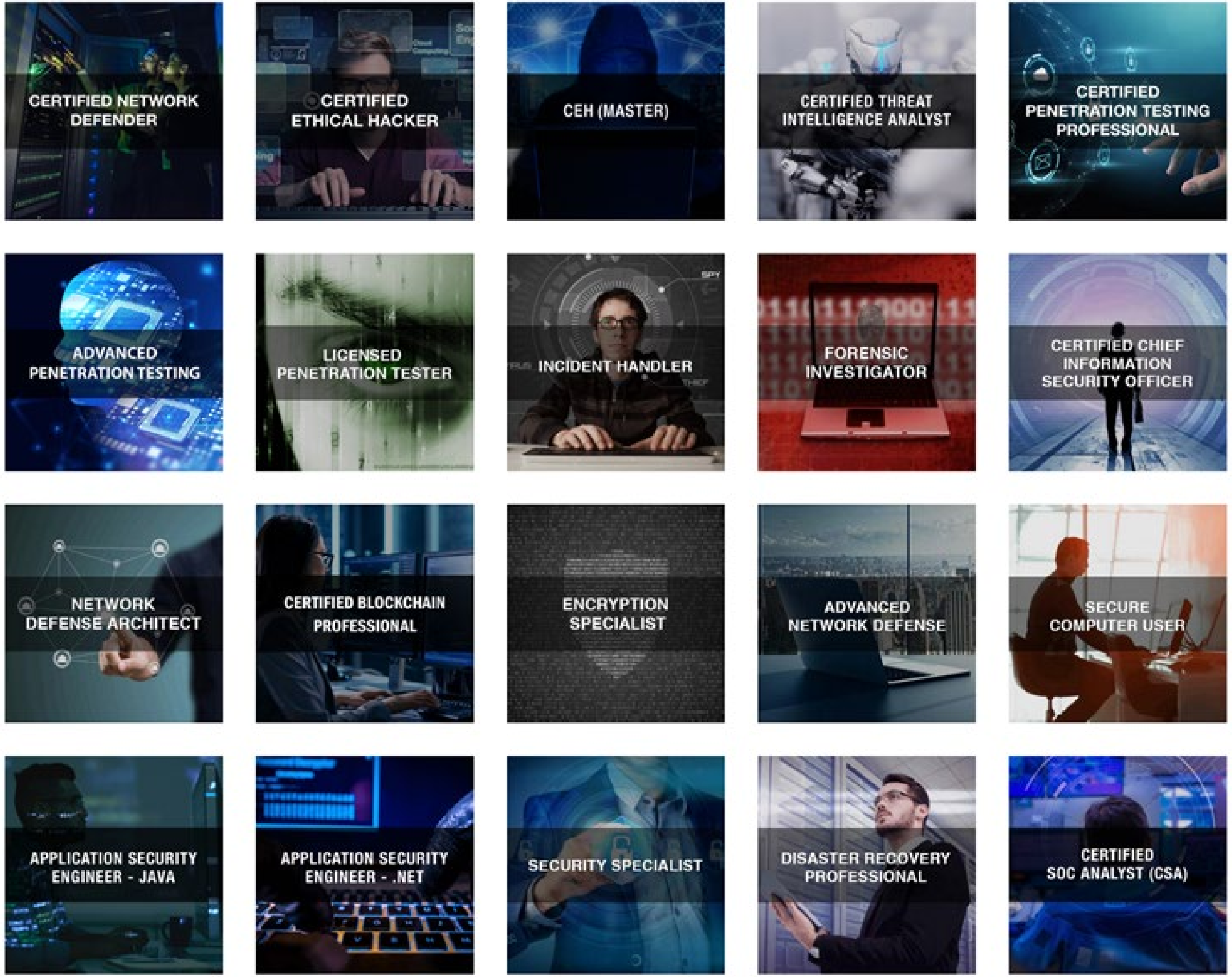
أرامكو السعودية Saudi Aramco

paloalto

And many more...

CyberQ

Our Programs



CERTIFIED NETWORK DEFENDER

CERTIFIED ETHICAL HACKER

CEH (MASTER)

CERTIFIED THREAT INTELLIGENCE ANALYST

CERTIFIED PENETRATION TESTING PROFESSIONAL

ADVANCED PENETRATION TESTING

LICENSED PENETRATION TESTER

INCIDENT HANDLER

FORENSIC INVESTIGATOR

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

NETWORK DEFENSE ARCHITECT

CERTIFIED BLOCKCHAIN PROFESSIONAL

ENCRYPTION SPECIALIST

ADVANCED NETWORK DEFENSE

SECURE COMPUTER USER

APPLICATION SECURITY ENGINEER - JAVA

APPLICATION SECURITY ENGINEER - .NET

SECURITY SPECIALIST

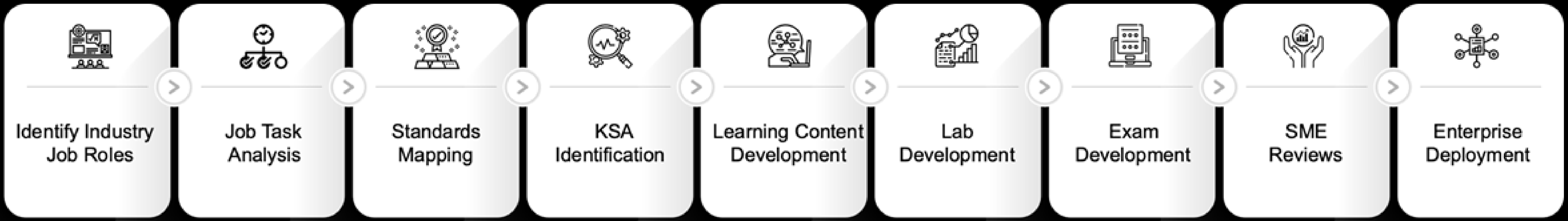
DISASTER RECOVERY PROFESSIONAL

CERTIFIED SOC ANALYST (CSA)

How Do We Do It?

ANSI Accredited 17024

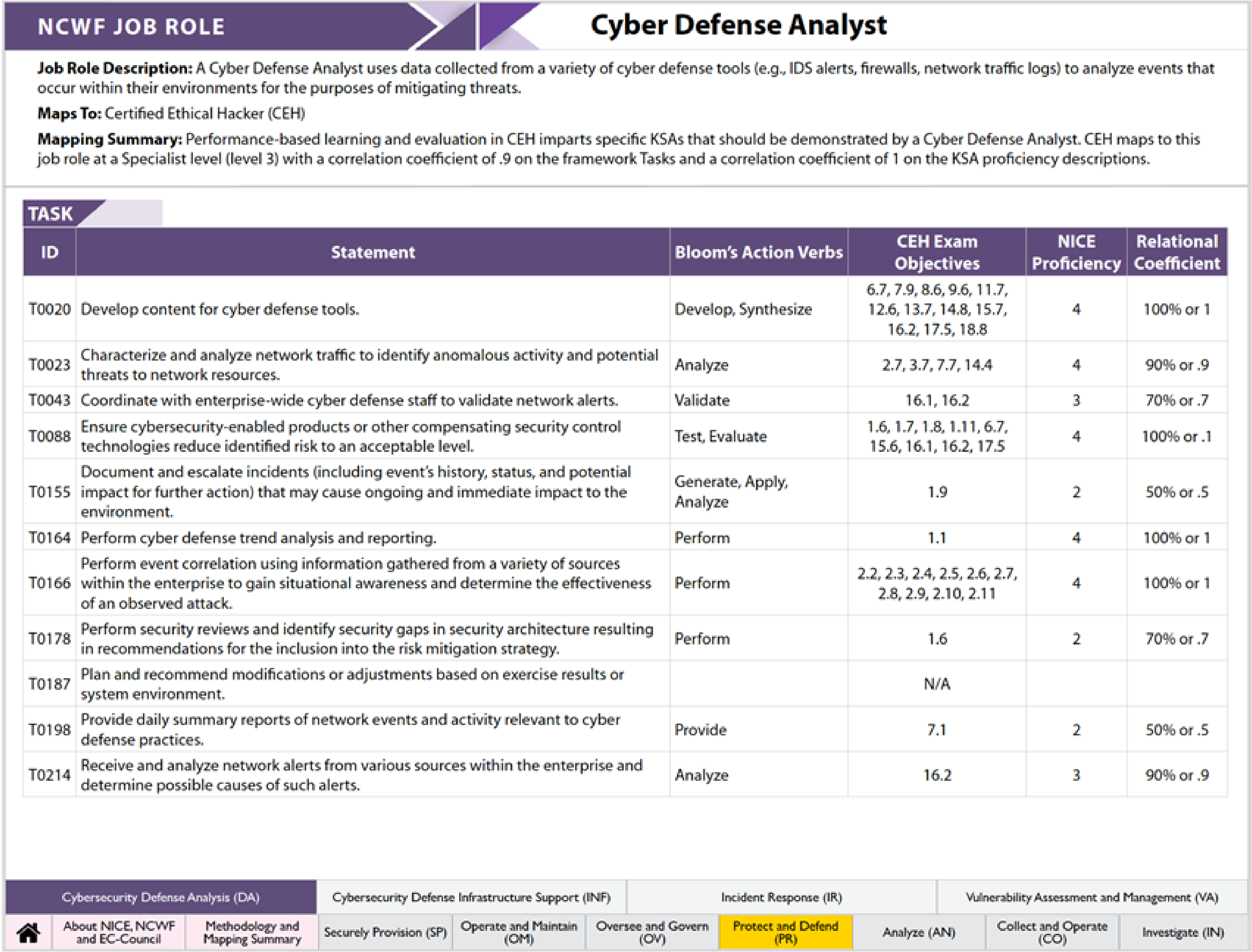
THE EC-COUNCIL CONTINUOUS SKILL DEVELOPMENT CAPABILITY



Identify Industry Job Roles > Job Task Analysis > Standards Mapping > KSA Identification > Learning Content Development > Lab Development > Exam Development > SME Reviews > Enterprise Deployment

EC-Council

Program Level NICE Framework Mapping



Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

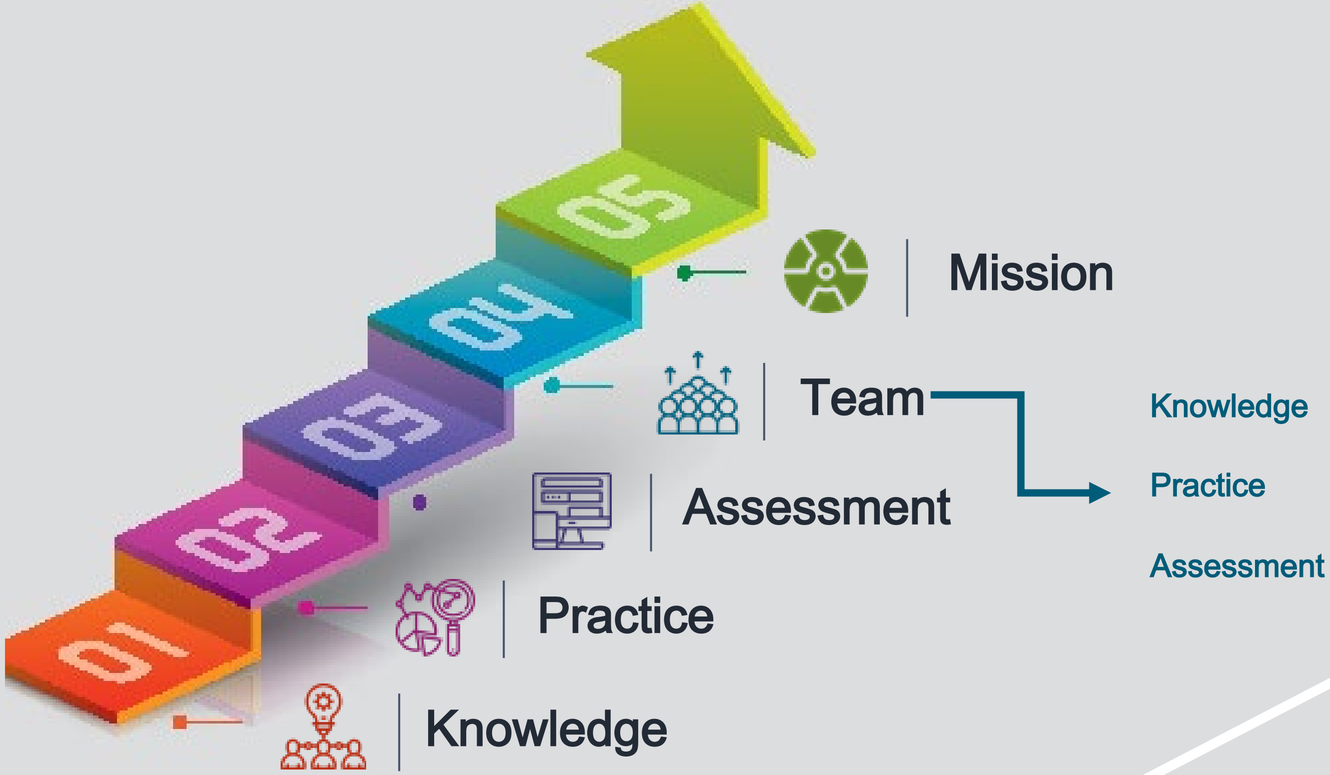
TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0020	Develop content for cyber defense tools.	Develop, Synthesize	6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8	4	100% or 1
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Analyze	2.7, 3.7, 7.7, 14.4	4	90% or .9
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Validate	16.1, 16.2	3	70% or .7
T0088	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Test, Evaluate	1.6, 1.7, 1.8, 1.11, 6.7, 15.6, 16.1, 16.2, 17.5	4	100% or .1
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Generate, Apply, Analyze	1.9	2	50% or .5
T0164	Perform cyber defense trend analysis and reporting.	Perform	1.1	4	100% or 1
T0166	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	Perform	2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11	4	100% or 1
T0178	Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.	Perform	1.6	2	70% or .7
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.		N/A		
T0198	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Provide	7.1	2	50% or .5
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Analyze	16.2	3	90% or .9

Cybersecurity Defense Analysis (DA)
Cybersecurity Defense Infrastructure Support (INF)
Incident Response (IR)
Vulnerability Assessment and Management (VA)
About NICE, NCWF and EC-Council
Methodology and Mapping Summary
Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Applied Skill Mastery in Education with a Cyber Range

Redefining Skill Mastery with CyberQ



Mission

Team

Assessment

Practice

Knowledge

Knowledge

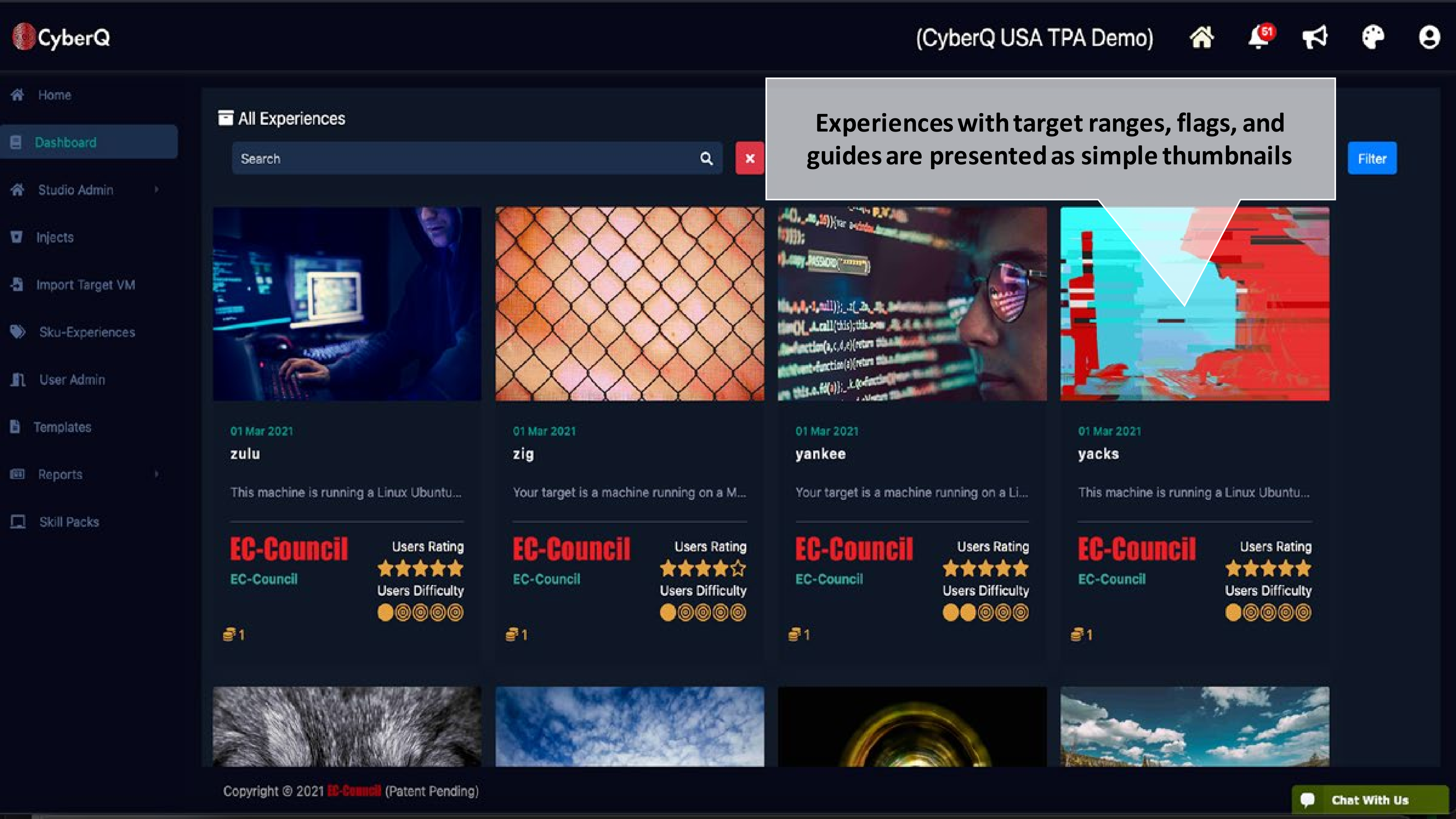
Practice

Assessment

Knowledge gained from realworld experience that updates the process over time.

TRAIN | PRACTICE | ASSESS | COMPETE | EXECUTE

Experiences with target ranges, flags, and guides are presented as simple thumbnails



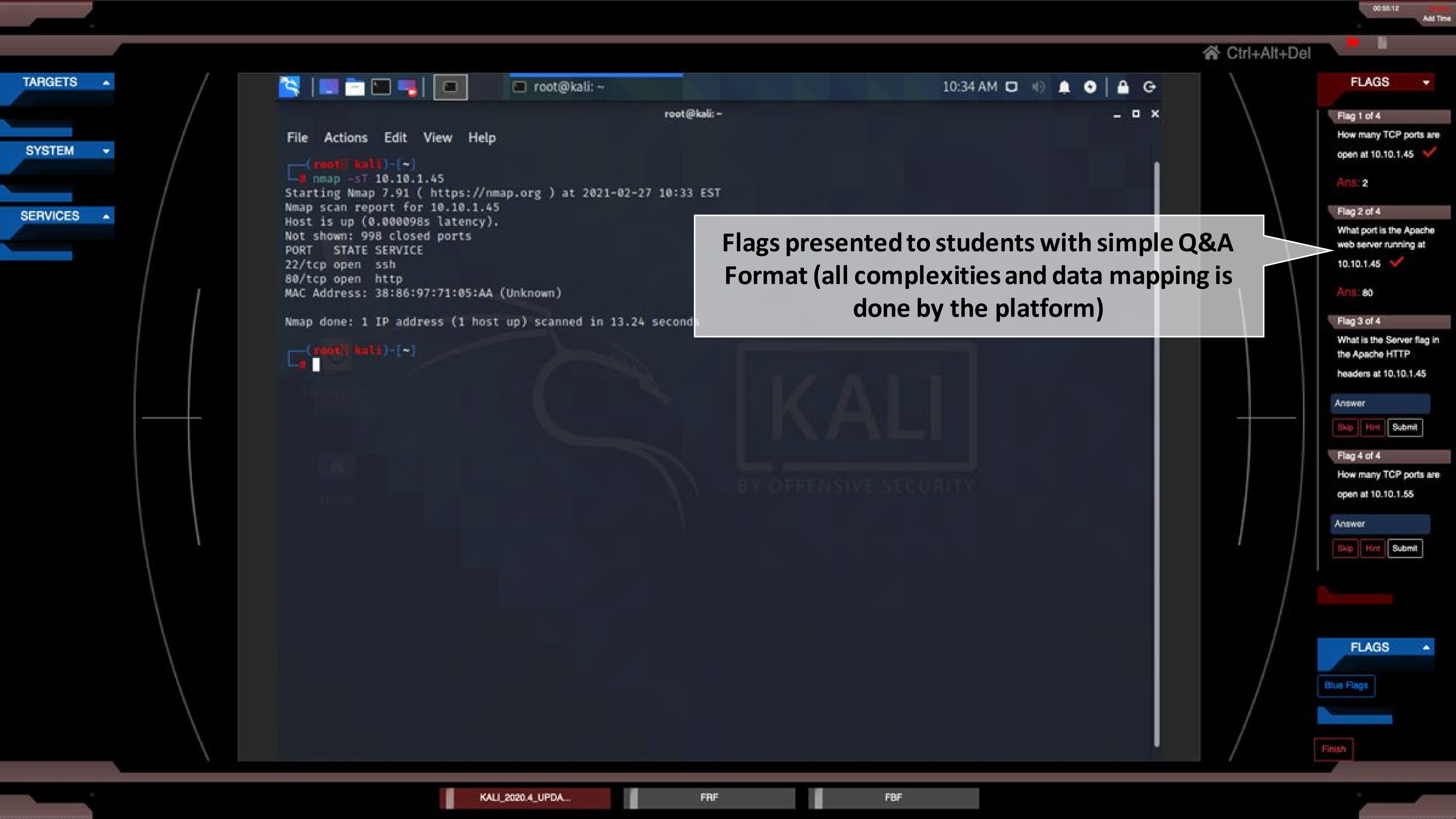
01 Mar 2021
zulu
This machine is running a Linux Ubuntu...
EC-Council
EC-Council
Users Rating ★★★★★
Users Difficulty ●○○○○
1

01 Mar 2021
zig
Your target is a machine running on a M...
EC-Council
EC-Council
Users Rating ★★★★☆
Users Difficulty ●○○○○
1

01 Mar 2021
yankee
Your target is a machine running on a Li...
EC-Council
EC-Council
Users Rating ★★★★★
Users Difficulty ●●○○○
1

01 Mar 2021
yacks
This machine is running a Linux Ubuntu...
EC-Council
EC-Council
Users Rating ★★★★★
Users Difficulty ●○○○○
1

Copyright © 2021 EC-Council (Patent Pending)



```
┌──(root💀 kali)-[~]
└─# nmap -sT 10.10.1.45
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-27 10:33 EST
Nmap scan report for 10.10.1.45
Host is up (0.000098s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 38:86:97:71:05:AA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds

┌──(root💀 kali)-[~]
└─#
```

FLAGS

Flag 1 of 4

How many TCP ports are open at 10.10.1.45 ✓

Ans: 2

Flag 2 of 4

What port is the Apache web server running at 10.10.1.45 ✓

Ans: 80

Flag 3 of 4

What is the Server flag in the Apache HTTP headers at 10.10.1.45

Answer

Skip Hint Submit

Flag 4 of 4

How many TCP ports are open at 10.10.1.55

Answer

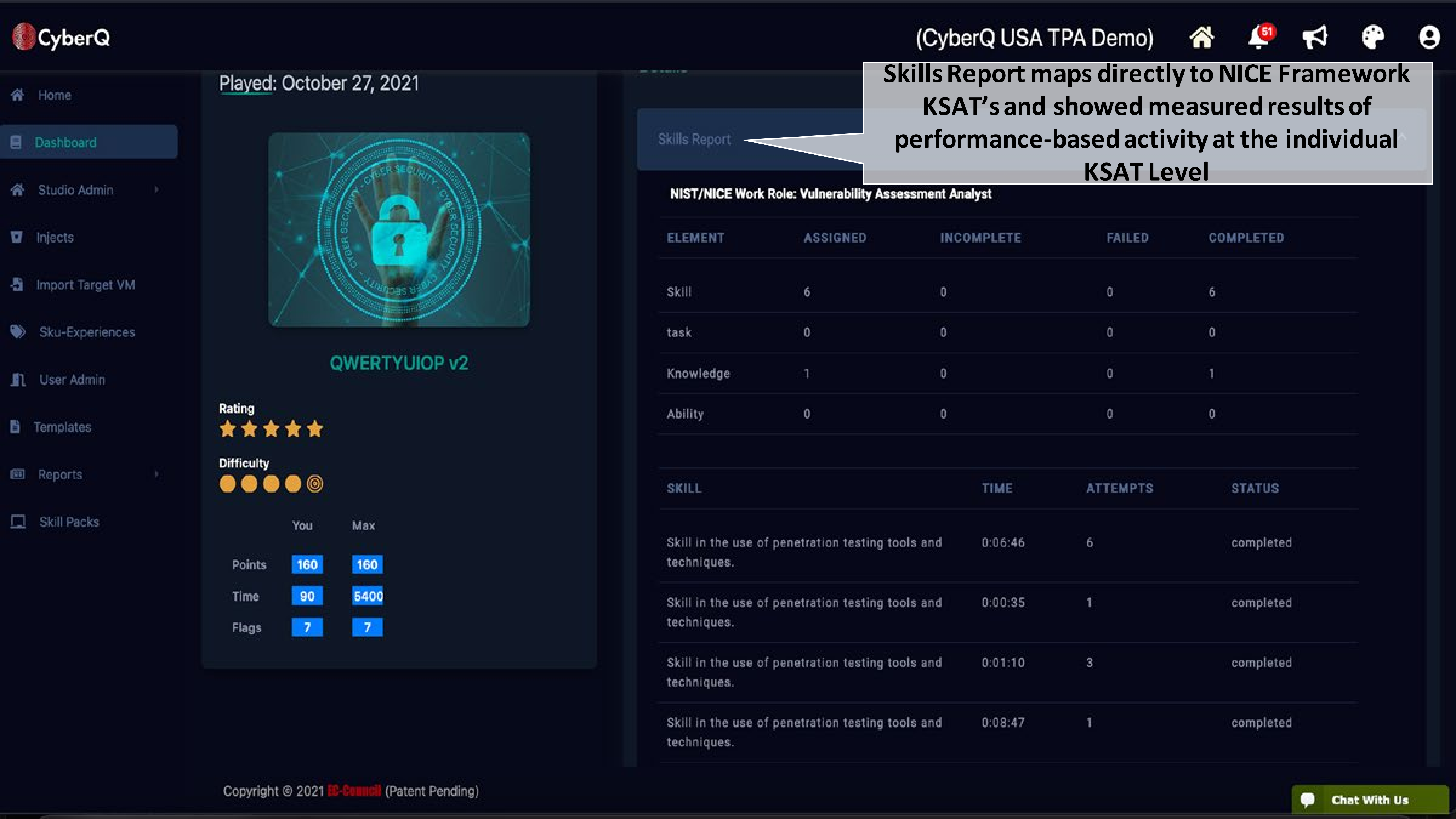
Skip Hint Submit

FLAGS

Blue Flags

Finish

Flags presented to students with simple Q&A Format (all complexities and data mapping is done by the platform)



Skills Report maps directly to NICE Framework KSAT's and showed measured results of performance-based activity at the individual KSAT Level

Played: October 27, 2021

QWERTYUIOP v2

Rating ★★★★★

Difficulty ●●●●◎

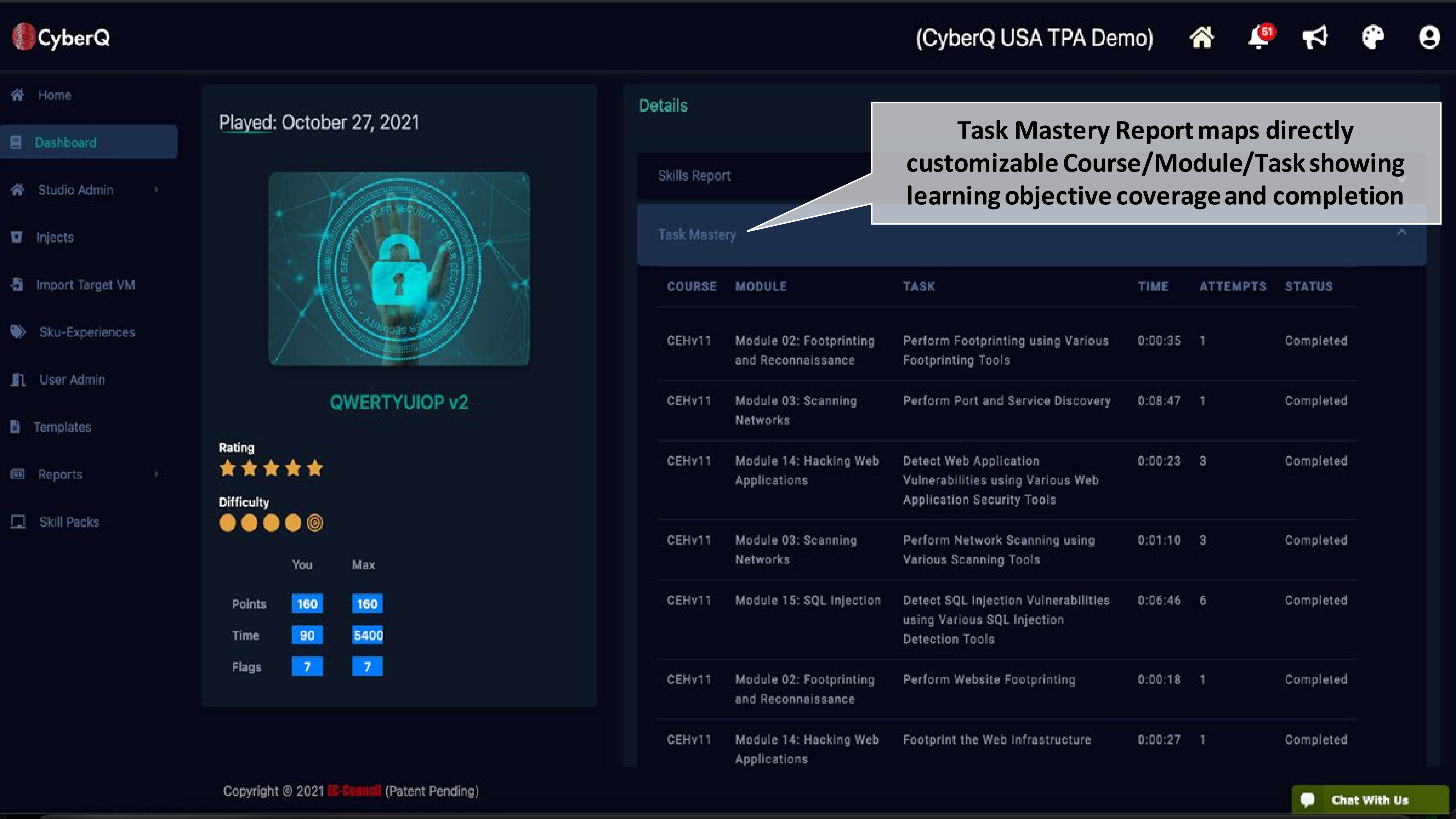
	You	Max
Points	160	160
Time	90	5400
Flags	7	7

NIST/NICE Work Role: Vulnerability Assessment Analyst

ELEMENT	ASSIGNED	INCOMPLETE	FAILED	COMPLETED
Skill	6	0	0	6
task	0	0	0	0
Knowledge	1	0	0	1
Ability	0	0	0	0

SKILL	TIME	ATTEMPTS	STATUS
Skill in the use of penetration testing tools and techniques.	0:06:46	6	completed
Skill in the use of penetration testing tools and techniques.	0:00:35	1	completed
Skill in the use of penetration testing tools and techniques.	0:01:10	3	completed
Skill in the use of penetration testing tools and techniques.	0:08:47	1	completed

Copyright © 2021 EC-Council (Patent Pending)



Task Mastery Report maps directly customizable Course/Module/Task showing learning objective coverage and completion

Played: October 27, 2021

QWERTYUIOP v2

Rating ★★★★★

Difficulty ●●●●◎

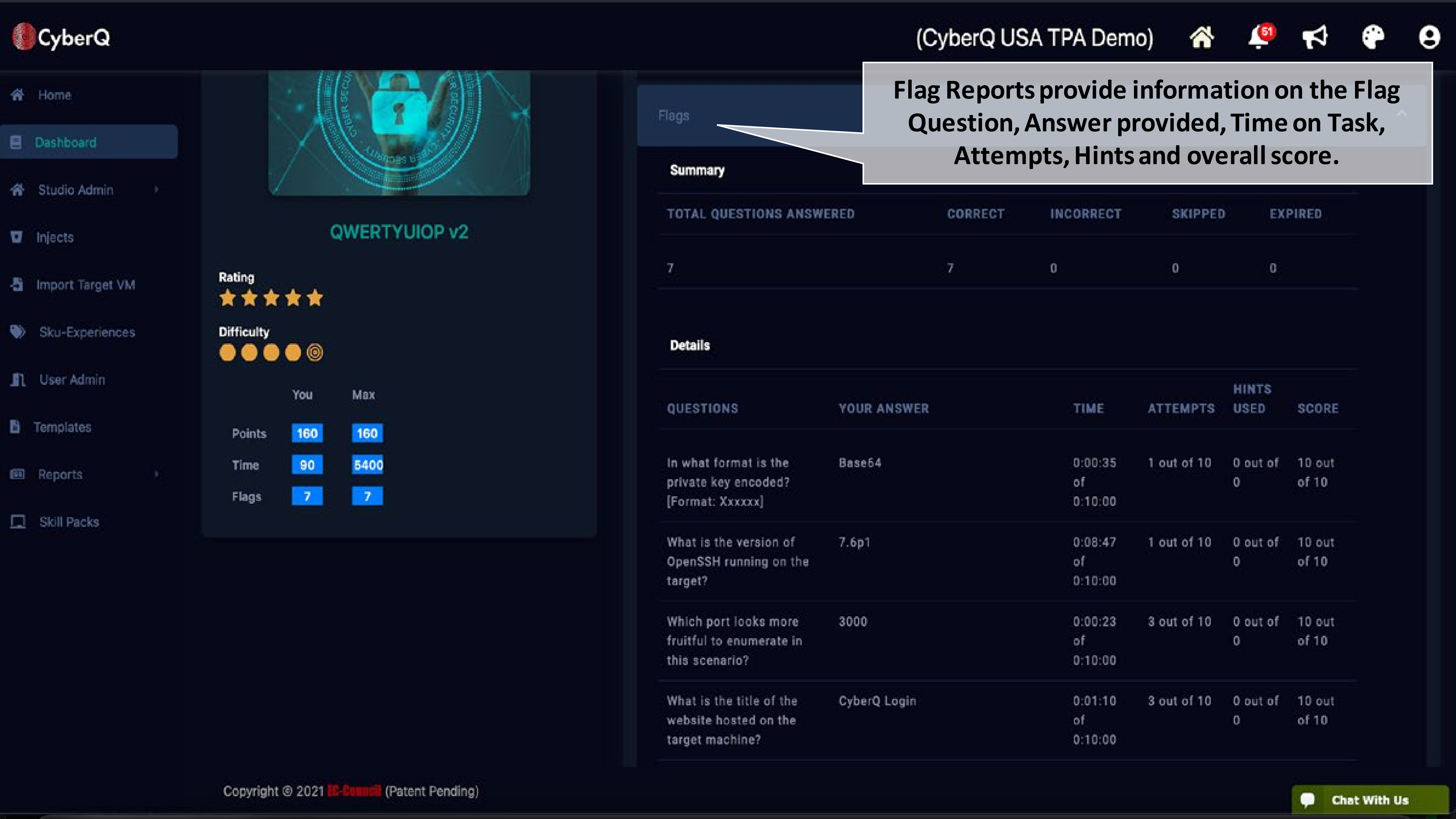
	You	Max
Points	160	160
Time	90	5400
Flags	7	7

Details

Skills Report

Task Mastery

COURSE	MODULE	TASK	TIME	ATTEMPTS	STATUS
CEHv11	Module 02: Footprinting and Reconnaissance	Perform Footprinting using Various Footprinting Tools	0:00:35	1	Completed
CEHv11	Module 03: Scanning Networks	Perform Port and Service Discovery	0:08:47	1	Completed
CEHv11	Module 14: Hacking Web Applications	Detect Web Application Vulnerabilities using Various Web Application Security Tools	0:00:23	3	Completed
CEHv11	Module 03: Scanning Networks	Perform Network Scanning using Various Scanning Tools	0:01:10	3	Completed
CEHv11	Module 15: SQL Injection	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	0:06:46	6	Completed
CEHv11	Module 02: Footprinting and Reconnaissance	Perform Website Footprinting	0:00:18	1	Completed
CEHv11	Module 14: Hacking Web Applications	Footprint the Web Infrastructure	0:00:27	1	Completed



Flag Reports provide information on the Flag Question, Answer provided, Time on Task, Attempts, Hints and overall score.

QWERTYUIOP v2

Rating ★★★★★

Difficulty ●●●●◎

	You	Max
Points	160	160
Time	90	5400
Flags	7	7

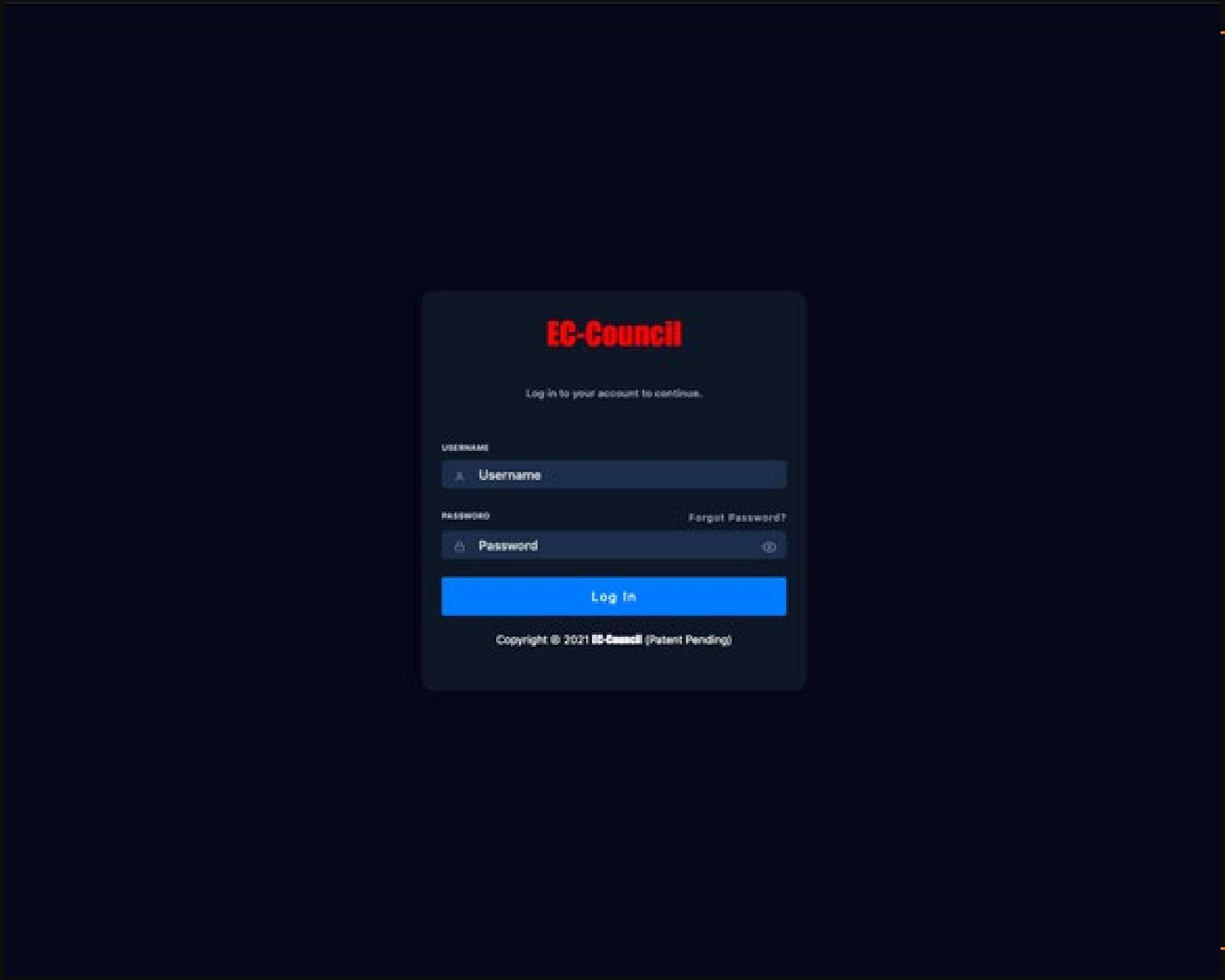
Flags

Summary

TOTAL QUESTIONS ANSWERED	CORRECT	INCORRECT	SKIPPED	EXPIRED
7	7	0	0	0

Details

QUESTIONS	YOUR ANSWER	TIME	ATTEMPTS	HINTS USED	SCORE
In what format is the private key encoded? [Format: Xxxxxx]	Base64	0:00:35 of 0:10:00	1 out of 10	0 out of 0	10 out of 10
What is the version of OpenSSH running on the target?	7.6p1	0:08:47 of 0:10:00	1 out of 10	0 out of 0	10 out of 10
Which port looks more fruitful to enumerate in this scenario?	3000	0:00:23 of 0:10:00	3 out of 10	0 out of 0	10 out of 10
What is the title of the website hosted on the target machine?	CyberQ Login	0:01:10 of 0:10:00	3 out of 10	0 out of 0	10 out of 10



Log in to your account to continue.

Copyright © 2021 EC-Council (Patent Pending)

Building Custom Range Activities

Internet –based Cloud Access

Instantly Launch any of hundreds of exercises

Solve Puzzles

Capture flags

Conduct Forensic Investigations

Hack Web Servers

Root Machines

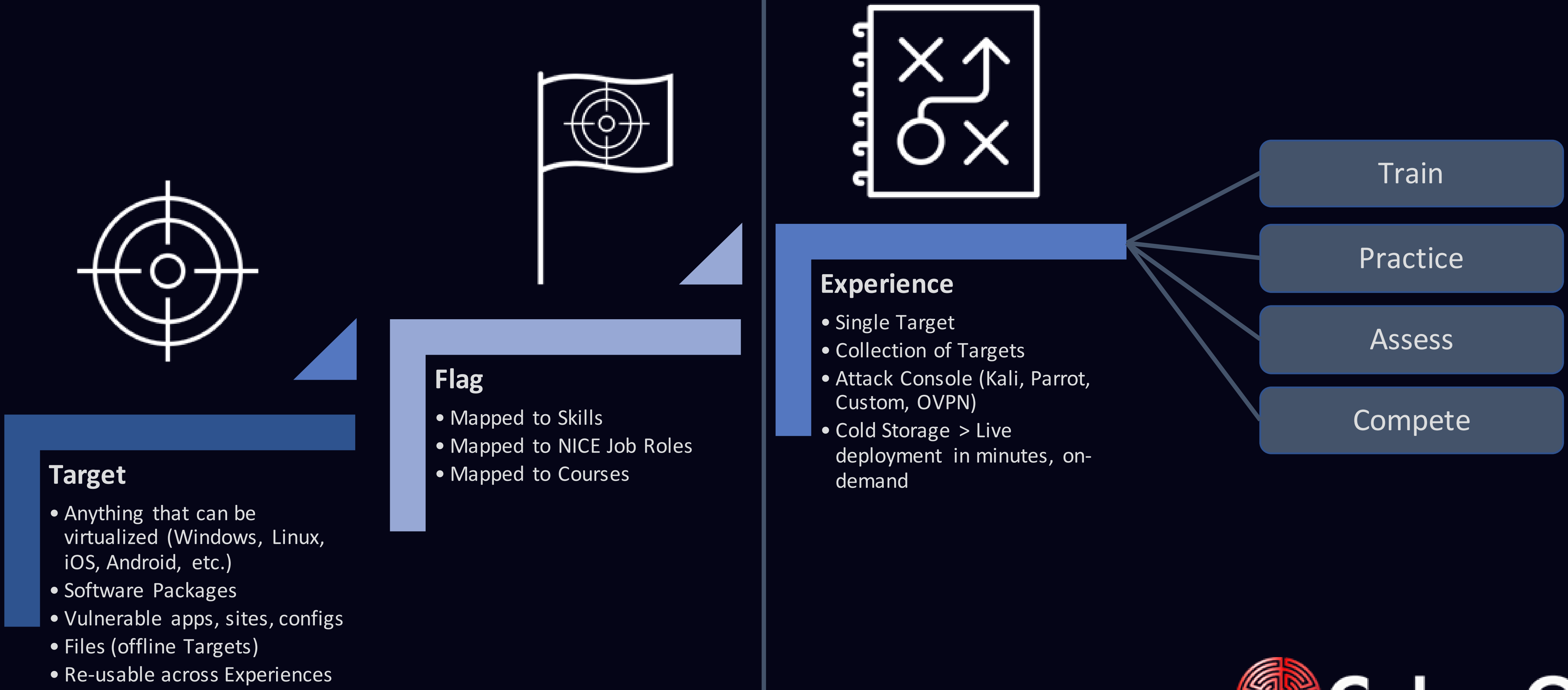
Crack Passwords

Investigate breaches

And much, much more!

CyberQ SKILLS-FIRST Approach

Skill mapped targets and flags are the building blocks of CyberQ – Not the Range



Target

- Anything that can be virtualized (Windows, Linux, iOS, Android, etc.)
- Software Packages
- Vulnerable apps, sites, configs
- Files (offline Targets)
- Re-usable across Experiences

Flag

- Mapped to Skills
- Mapped to NICE Job Roles
- Mapped to Courses

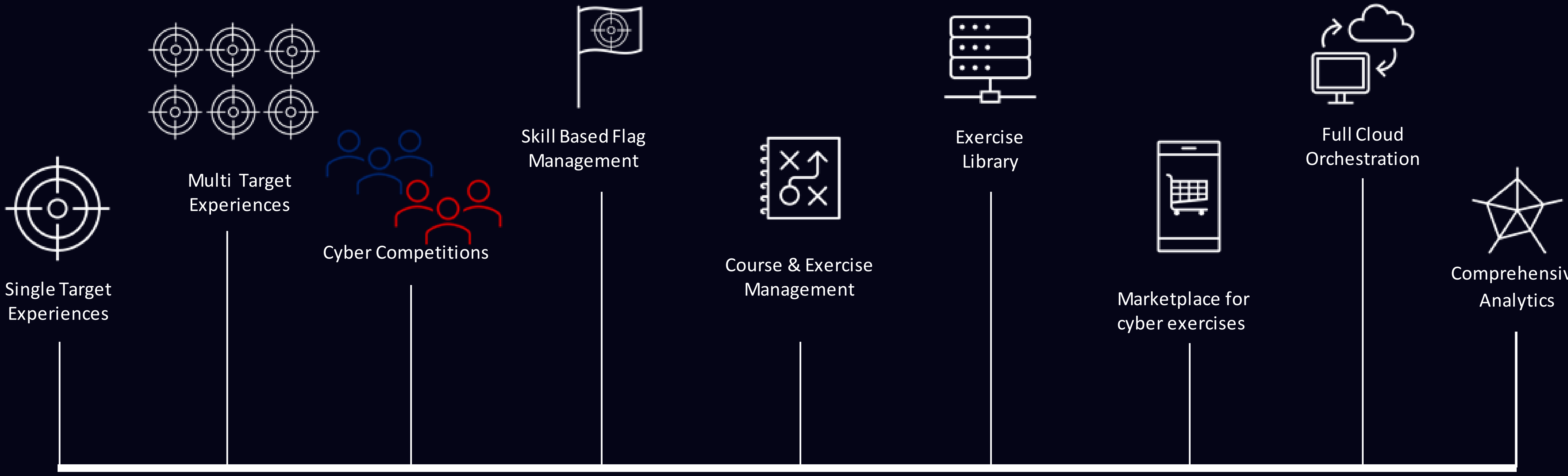
Experience

- Single Target
- Collection of Targets
- Attack Console (Kali, Parrot, Custom, OVPN)
- Cold Storage > Live deployment in minutes, on-demand

TRAIN | PRACTICE | ASSESS | COMPETE | EXECUTE

CyberQ

One Platform | Many Solutions



Single Target Experiences

Multi Target Experiences

Cyber Competitions

Skill Based Flag Management

Course & Exercise Management

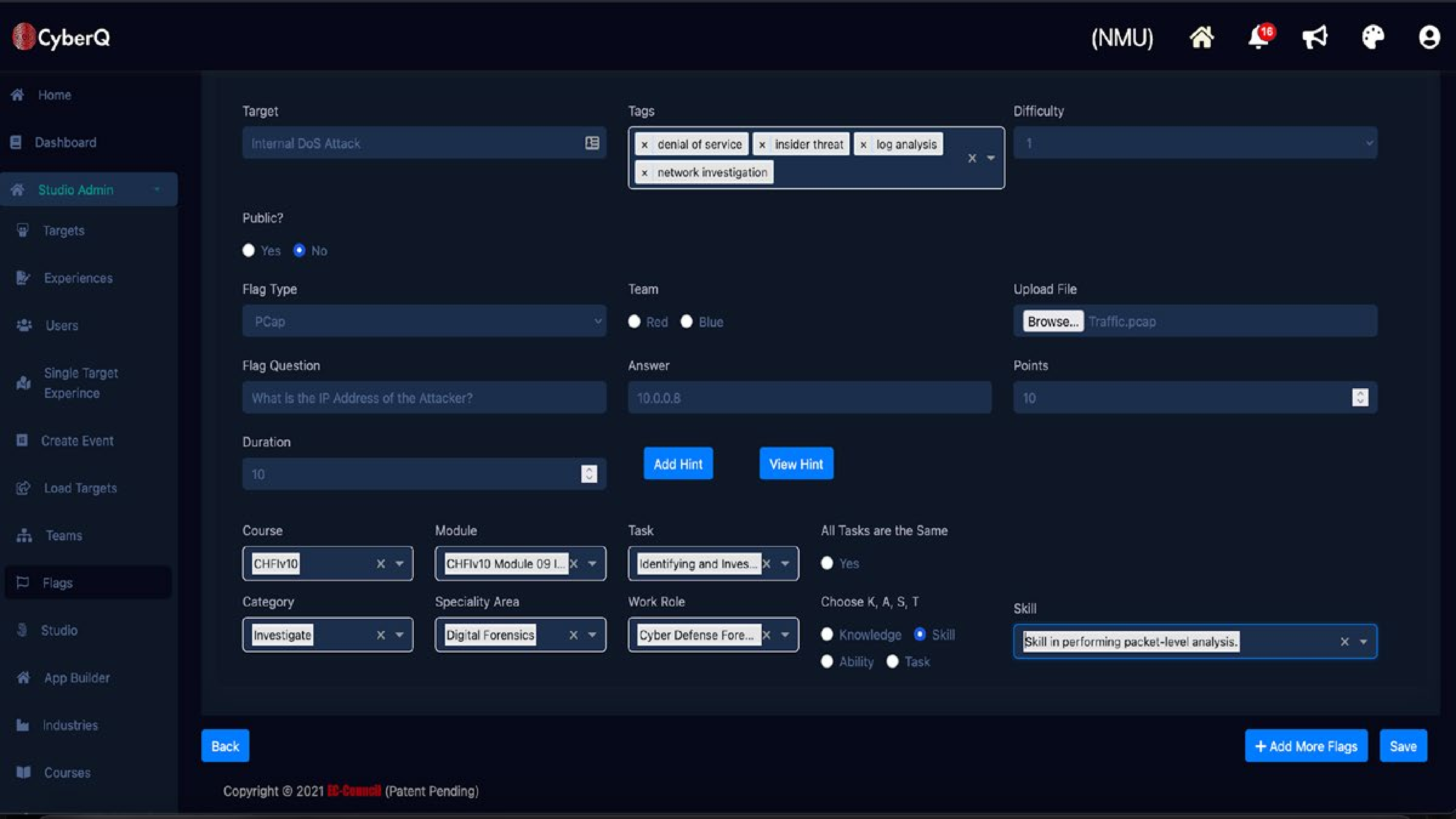
Exercise Library

Marketplace for cyber exercises

Full Cloud Orchestration

Comprehensive Analytics

CyberQ



Target: Internal DoS Attack

Tags: × denial of service × insider threat × log analysis × network investigation

Difficulty: 1

Public? ○ Yes ● No

Flag Type: PCap

Team ○ Red ○ Blue

Upload File: Traffic.pcap

Flag Question: What is the IP Address of the Attacker?

Answer: 10.0.0.8

Points: 10

Duration: 10

Course: CHFIv10

Module: CHFIv10 Module 09 I...

Task: Identifying and Inves...

All Tasks are the Same ○ Yes

Category: Investigate

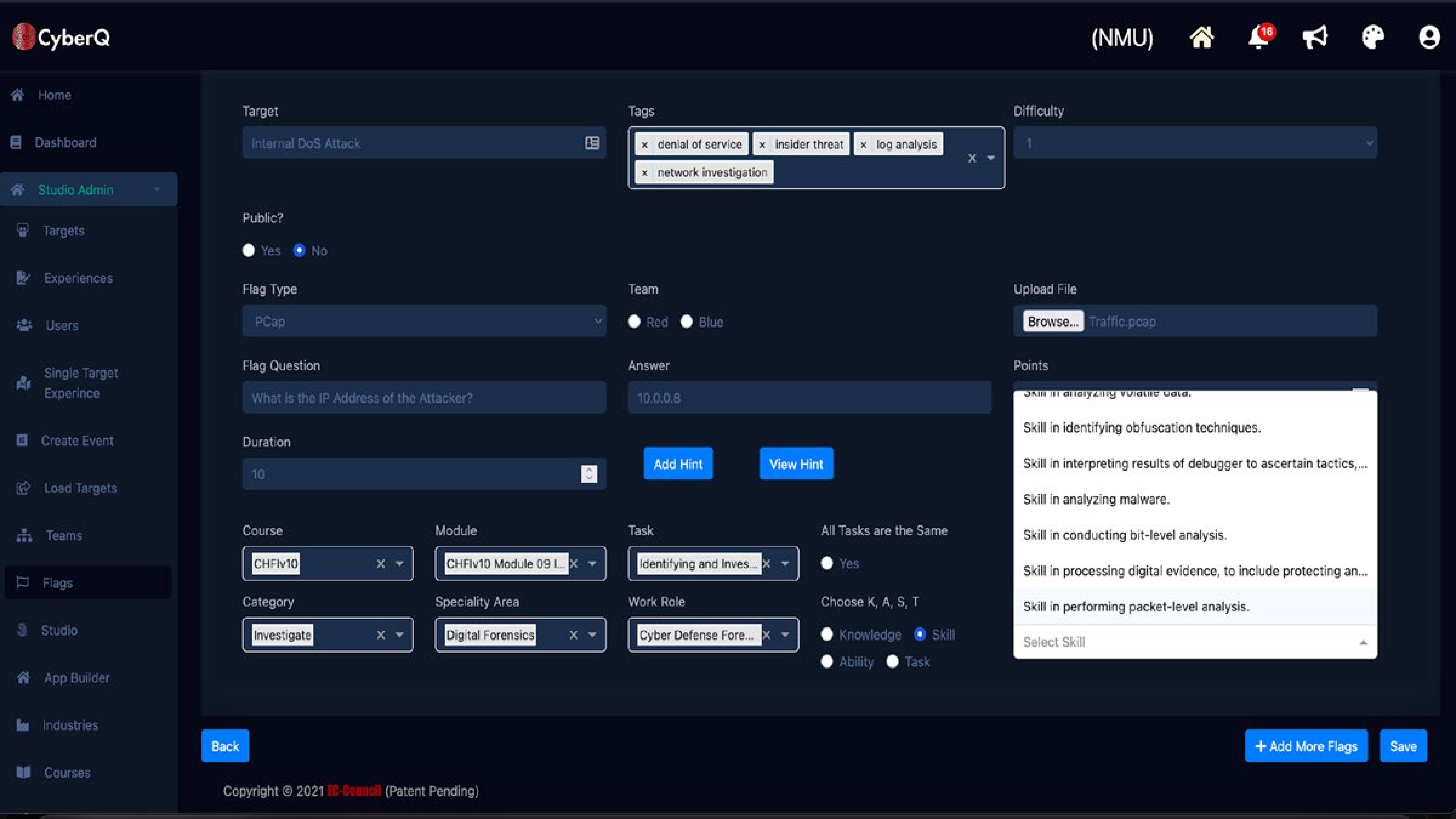
Speciality Area: Digital Forensics

Work Role: Cyber Defense Fore...

Choose K, A, S, T ○ Knowledge ● Skill ○ Ability ○ Task

Skill: Skill in performing packet-level analysis.

Copyright © 2021 EC-Council (Patent Pending)



Target: Internal DoS Attack

Tags: denial of service, insider threat, log analysis, network investigation

Difficulty: 1

Public?

○ Yes ● No

Flag Type: PCap

Team

○ Red ○ Blue

Upload File: Traffic.pcap

Flag Question: What is the IP Address of the Attacker?

Answer: 10.0.0.8

Points

Skill in analyzing volatile data.

Skill in identifying obfuscation techniques.

Skill in interpreting results of debugger to ascertain tactics,...

Skill in analyzing malware.

Skill in conducting bit-level analysis.

Skill in processing digital evidence, to include protecting an...

Skill in performing packet-level analysis.

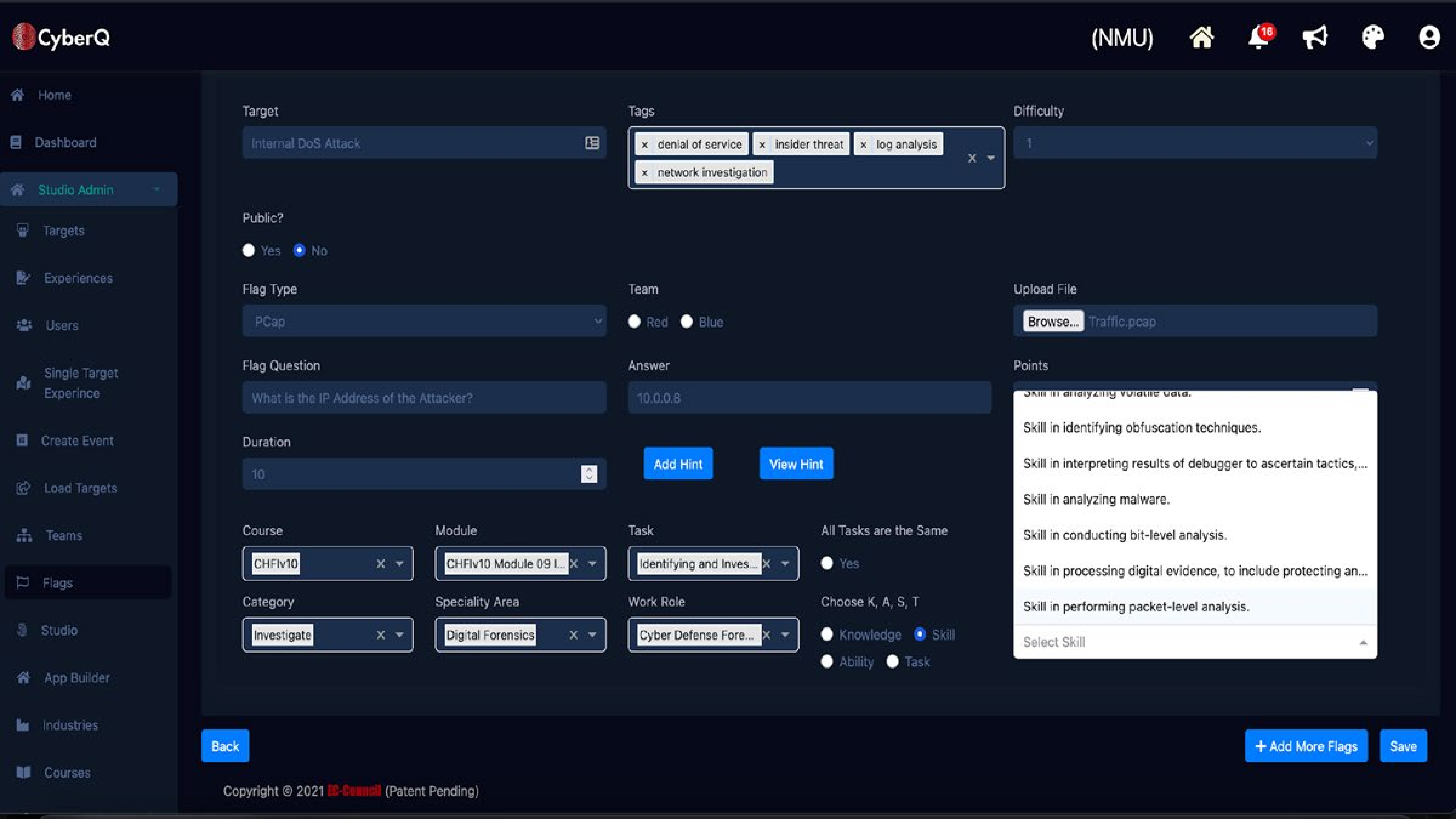
Select Skill

Duration: 10

Course	Module	Task	All Tasks are the Same
CHFIv10	CHFIv10 Module 09 I...	Identifying and Inves...	○ Yes

Category	Speciality Area	Work Role	Choose K, A, S, T
Investigate	Digital Forensics	Cyber Defense Fore...	○ Knowledge ● Skill ○ Ability ○ Task

Copyright © 2021 EC-Council (Patent Pending)



Target: Internal DoS Attack

Tags: × denial of service × insider threat × log analysis × network investigation

Difficulty: 1

Public?
○ Yes ● No

Flag Type: PCap

Team
○ Red ○ Blue

Upload File: Browse... Traffic.pcap

Flag Question: What is the IP Address of the Attacker?

Answer: 10.0.0.8

Points

Duration: 10

Course: CHFIv10

Module: CHFIv10 Module 09 I...

Task: Identifying and Inves...

All Tasks are the Same
○ Yes

Category: Investigate

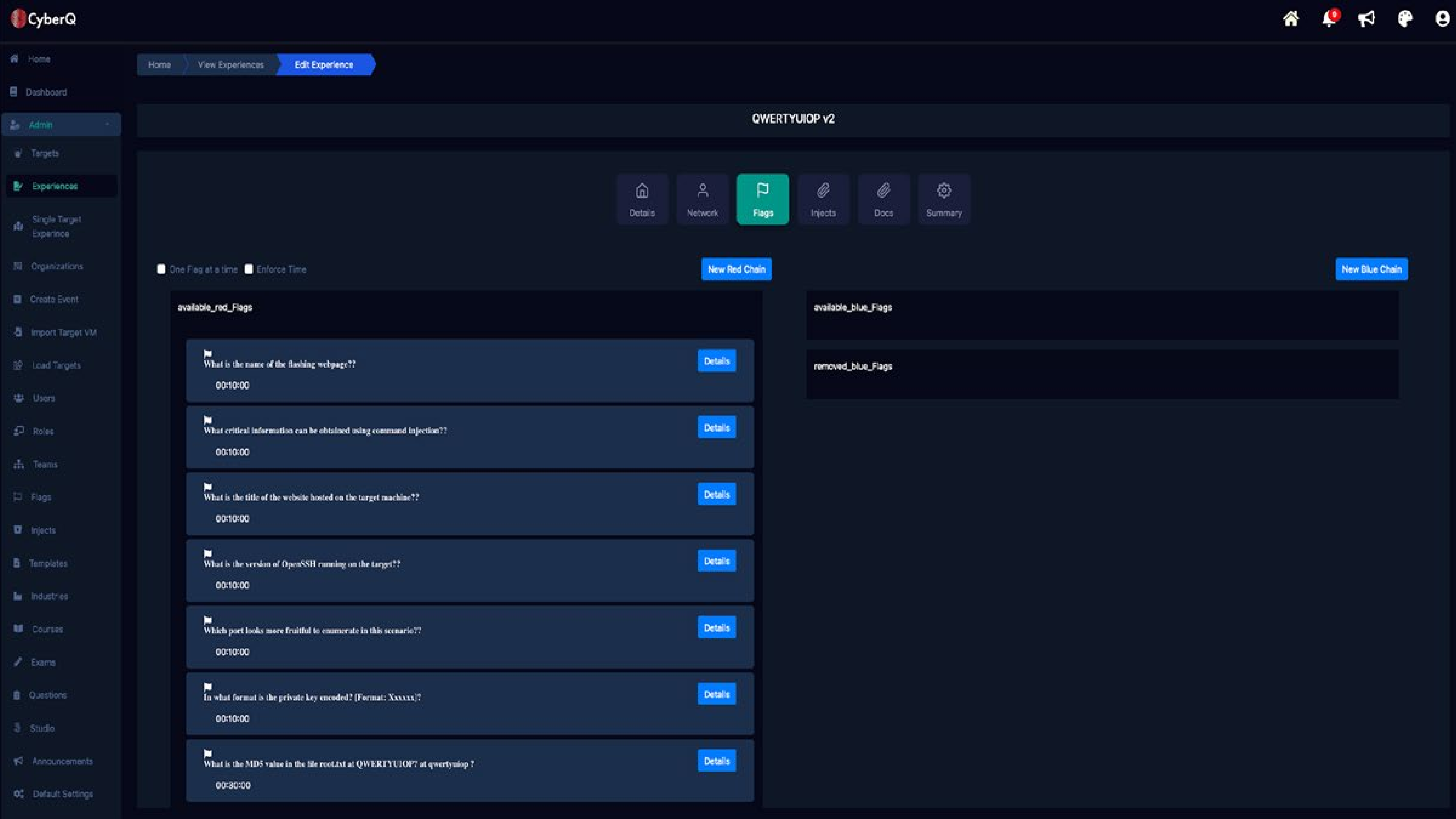
Speciality Area: Digital Forensics

Work Role: Cyber Defense Fore...

Choose K, A, S, T
○ Knowledge ● Skill
○ Ability ○ Task

Skill in analyzing volatile data.
Skill in identifying obfuscation techniques.
Skill in interpreting results of debugger to ascertain tactics,...
Skill in analyzing malware.
Skill in conducting bit-level analysis.
Skill in processing digital evidence, to include protecting an...
Skill in performing packet-level analysis.
Select Skill

Copyright © 2021 EC-Council (Patent Pending)



QWERTYUIOP v2

☐ One Flag at a time ☐ Enforce Time

available_red_Flags

What is the name of the flashing webpage??

00:10:00

What critical information can be obtained using command injection??

00:10:00

What is the title of the website hosted on the target machine??

00:10:00

What is the version of OpenSSH running on the target??

00:10:00

Which port looks more fruitful to enumerate in this scenario??

00:10:00

In what format is the private key encoded? [Format: Xxxxxx]?

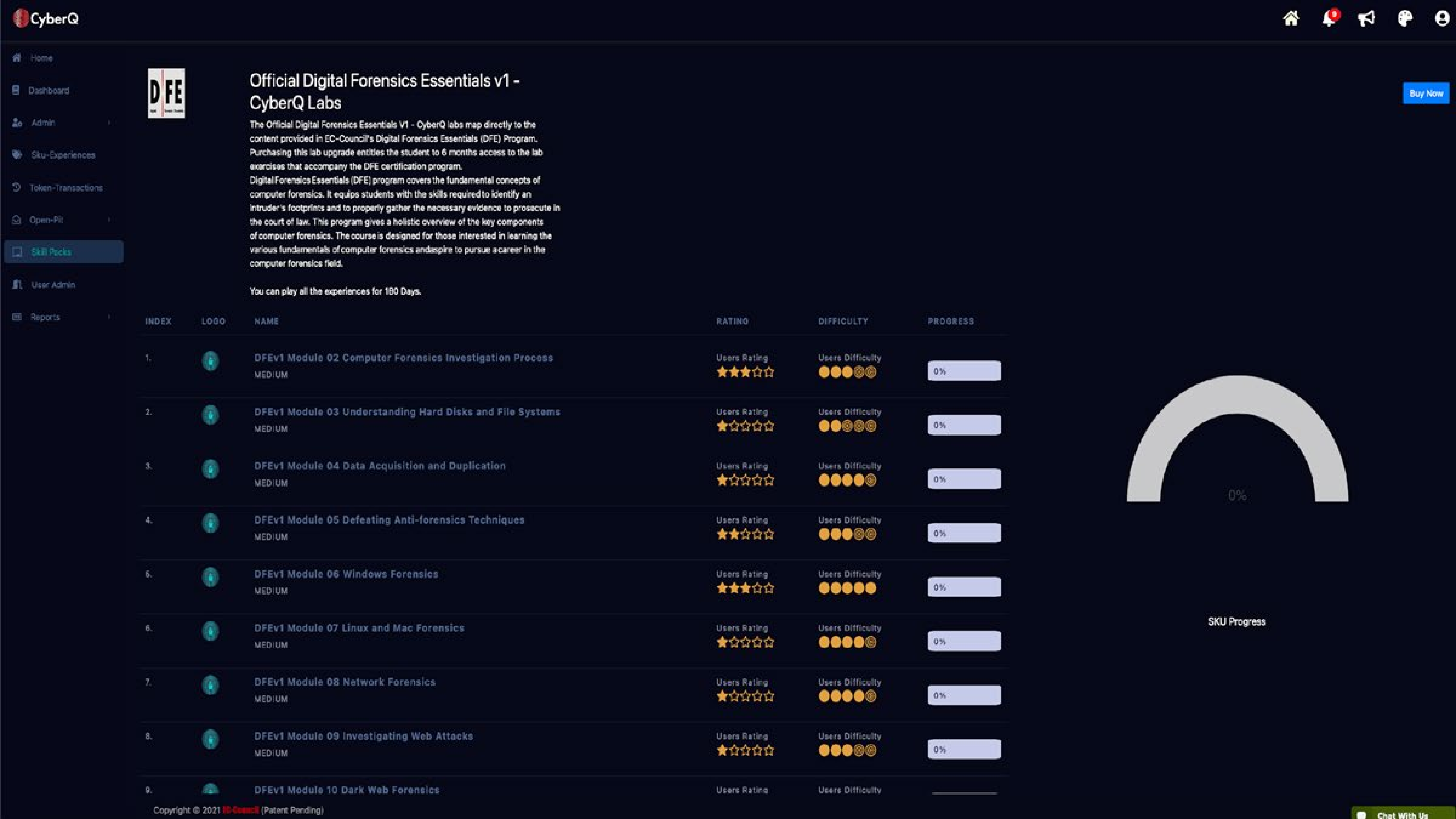
00:10:00

What is the MD5 value in the file root.txt at QWERTYUIOP? at qwertyuiop ?

00:30:00

available_blue_Flags

removed_blue_Flags



Official Digital Forensics Essentials v1 - CyberQ Labs

The Official Digital Forensics Essentials V1 - CyberQ labs map directly to the content provided in EC-Council's Digital Forensics Essentials (DFE) Program. Purchasing this lab upgrade entitles the student to 6 months access to the lab exercises that accompany the DFE certification program.

Digital Forensics Essentials (DFE) program covers the fundamental concepts of computer forensics. It equips students with the skills requiredto identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law. This program gives a holistic overview of the key components of computer forensics. The course is designed for those interested in learning the various fundamentals of computer forensics andaspire to pursue acareer in the computer forensics field.

You can play all the experiences for 180 Days.

INDEX	LOGO	NAME	RATING	DIFFICULTY	PROGRESS
1.		DFEv1 Module 02 Computer Forensics Investigation Process MEDIUM	Users Rating ★★★☆☆	Users Difficulty ●●●○○	0%
2.		DFEv1 Module 03 Understanding Hard Disks and File Systems MEDIUM	Users Rating ★☆☆☆☆	Users Difficulty ●●○○○	0%
3.		DFEv1 Module 04 Data Acquisition and Duplication MEDIUM	Users Rating ★☆☆☆☆	Users Difficulty ●●●●○	0%
4.		DFEv1 Module 05 Defeating Anti-forensics Techniques MEDIUM	Users Rating ★★☆☆☆	Users Difficulty ●●●○○	0%
5.		DFEv1 Module 06 Windows Forensics MEDIUM	Users Rating ★★★☆☆	Users Difficulty ●●●●●	0%
6.		DFEv1 Module 07 Linux and Mac Forensics MEDIUM	Users Rating ★☆☆☆☆	Users Difficulty ●●●●○	0%
7.		DFEv1 Module 08 Network Forensics MEDIUM	Users Rating ★☆☆☆☆	Users Difficulty ●●●●○	0%
8.		DFEv1 Module 09 Investigating Web Attacks MEDIUM	Users Rating ★☆☆☆☆	Users Difficulty ●●●○○	0%
9.		DFEv1 Module 10 Dark Web Forensics	Users Rating	Users Difficulty	

CyberQ

Thank you!

TRAIN | PRACTICE | ASSESS | COMPETE | EXECUTE

Q & A

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Complete Survey

https://www.surveymonkey.com/r/decnicewebinar

Thank You for Joining Us!

Upcoming Webinar: Mentorship Models to Enhance Diversity and Increase Persistence in Cybersecurity Careers

When: January 19, 2022, at 2-3pm ET

Register: https://nist-secure.webex.com/nist-secure/onstage/g.php?MTID=e5b026381618d86baa3431c0ca400ef0e

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION