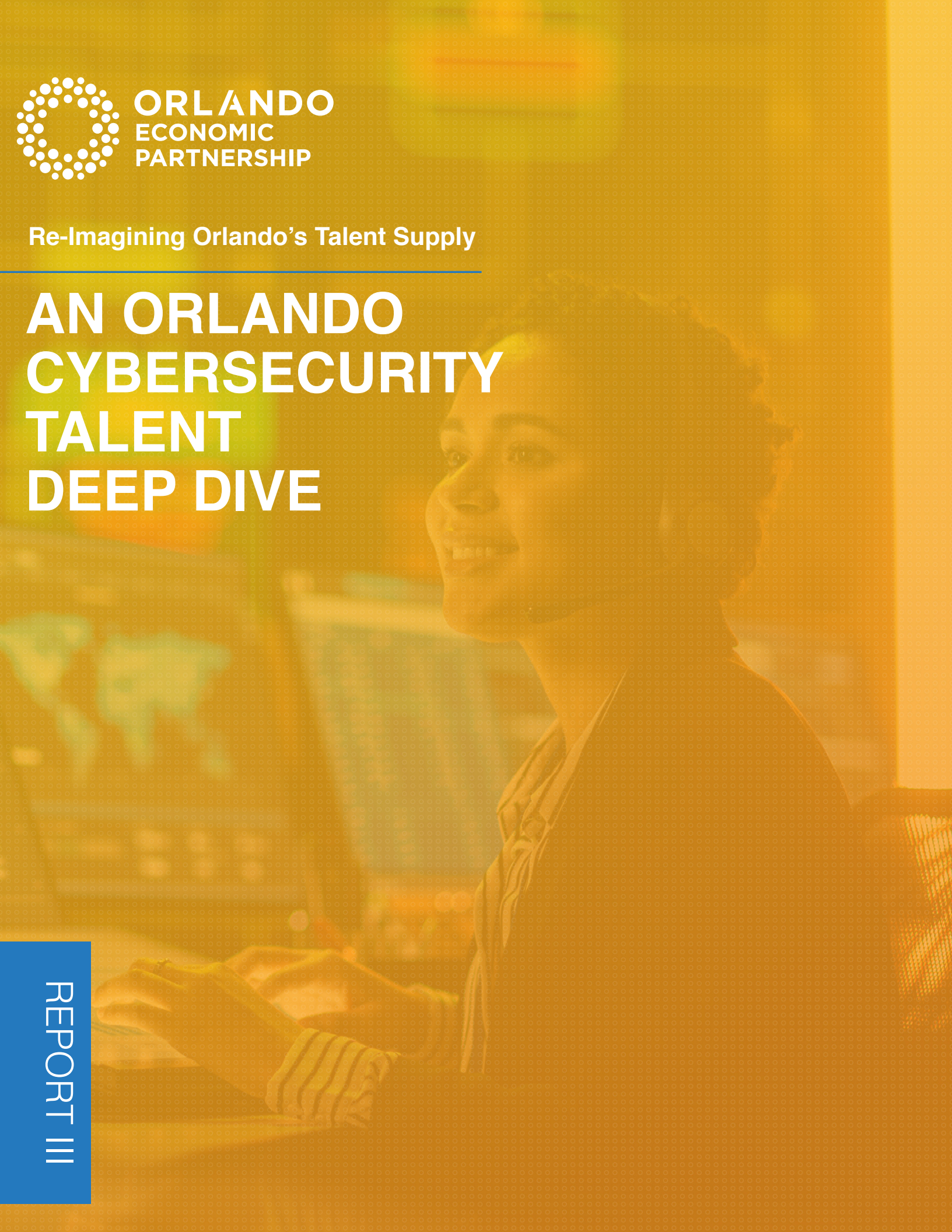
ORLANDO ECONOMIC PARTNERSHIP

Re-Imagining Orlando's Talent Supply

AN ORLANDO CYBERSECURITY TALENT DEEP DIVE



REPORT III

Contents

ORLANDO ECONOMIC PARTNERSHIP

RE-IMAGINING ORLANDO'S TALENT SUPPLY

An Orlando Cybersecurity Talent Deep Dive

REPORT III

Introduction

It should come as no surprise that demand for cybersecurity talent has increased drastically in recent years. Already on the rise before the COVID-19 pandemic, the need for cybersecurity talent is greater now than ever due to the widespread adoption of remote learning and work, skyrocketing demand for online shopping and an abundance of digital platforms collecting data on our personal health, movements, preferences, etc. Since 2020, cyber-attacks ranged from malware delivering emails using "COVID-19 as a social engineering lure"[1] to the ransom of the largest fuel pipeline in the United States.[2]

In 2021, roughly two-thirds (60 percent) of participants in an international survey of the cybersecurity workforce reported that "a cybersecurity staffing shortage is placing their organizations at risk."[3] Despite growth over the last year in the size of the cybersecurity talent pool, gaps between supply and demand are widening in North America; the global workforce needs to grow 65 percent to "effectively defend organizations' critical assets."[4]

Zooming in on the Orlando Metropolitan Statistical Area (MSA), there are roughly 4,300 cybersecurity job openings at any given time,[5] an amount larger than total headcounts for many of Central Florida's top employers.[6] According to Cyber Seek, the Orlando MSA has a supply to demand ratio of 71, meaning there are only enough cybersecurity workers to fill 71 percent of demand. This puts Orlando just above the U.S. average of 68.

Despite high demand, most employers have not managed to expand their talent pool as a means of closing the gap. "The largest feeder occupation for cybersecurity is…cybersecurity,"[7] meaning when companies need a job filled, they typically hire someone from an existing cybersecurity role. This leads to poaching between organizations effectively making talent more expensive and does nothing to solve the greater talent issue. Strictly recruiting talent with an existing cybersecurity background also does little to diversify the workforce. According to the professional membership organization known as the International Information System Security Certification Consortium, known as (ISC)^2, "the field continues to be predominantly male (76 percent) and Caucasian (72 percent) in North America."

However, there are solutions to these issues. They involve using a common language, based on skills and knowledge, for all educators, employers and workers. Solutions involve increased communication so that educators understand the rapidly changing needs of employers. Increased communication also helps workers understand their career options in the field. Closing the cybersecurity talent gap will mean challenging traditional hiring practices and re-thinking how candidates are currently evaluated.

The following report addresses each of these topics. The first two sections offer background on the industry. Section one dives into the NICE Framework, offering the building blocks for a common cybersecurity language. Section two defines Orlando's specific industry needs. This background information is combined in sections three and four to present a toolkit with tactics employers, educators, and individuals can use to help solve the current cybersecurity talent shortage. Presented as case studies, this toolkit uses examples of real job postings and worker profiles from the Orlando region to examine possible upward mobility pathways into the cybersecurity field.

1 Threat Intel, Cyber Attacks Leveraging the COVID-19/Coronavirus Pandemic, Sentinel Labs, September 2020

2 Hackers Breached Colonial Pipeline Using Compromised Password, Bloomberg, June 2021

3 (ISC)^2 Cybersecurity Workforce Study, 2021

4 (ISC)^2 Cybersecurity Workforce Study, 2021

5 Cyber Seek, accessed February 2022

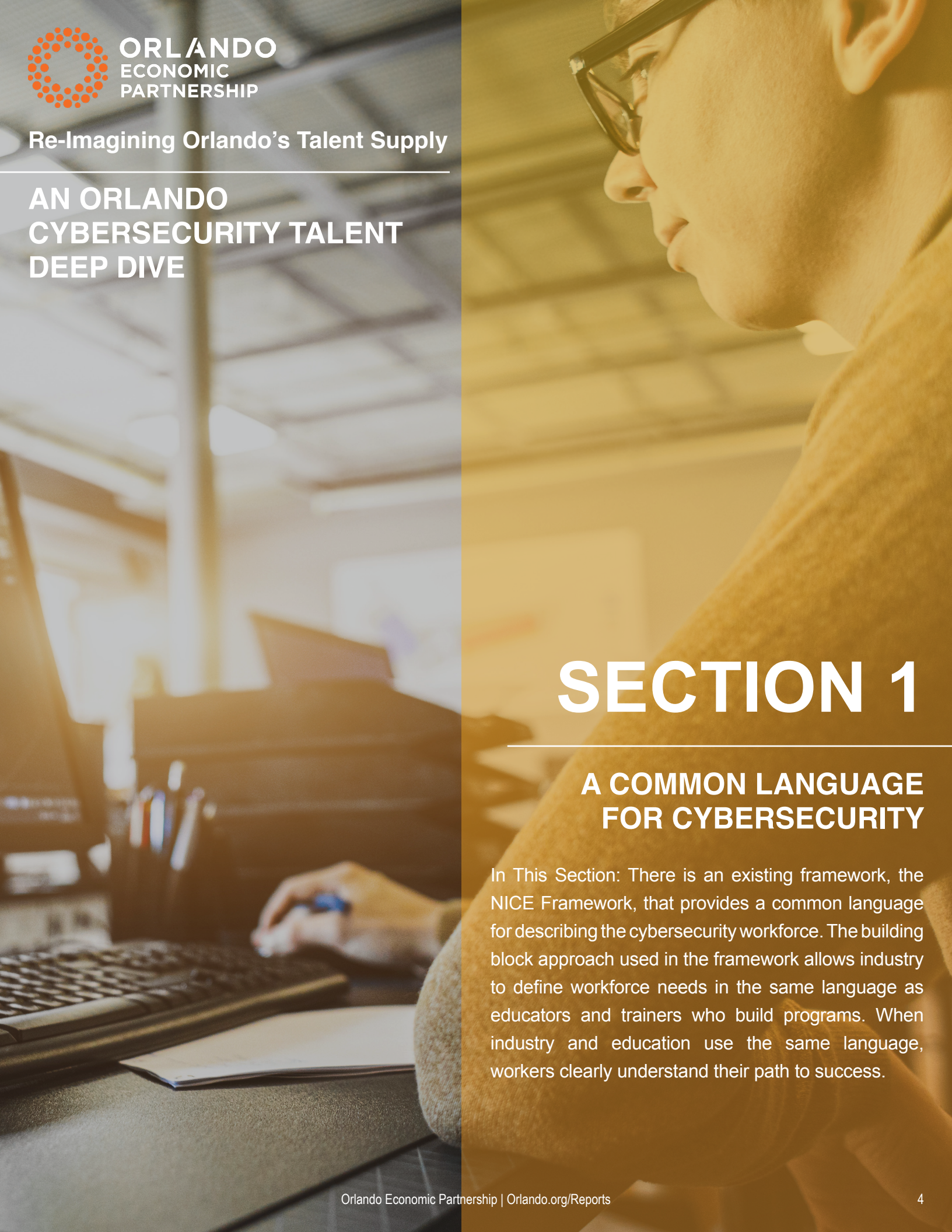
6 Orlando Economic Partnership, Top 75 Employers

7 EMSI, Build (Don't Buy) A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage, July 2020

ORLANDO ECONOMIC PARTNERSHIP

Re-Imagining Orlando's Talent Supply

AN ORLANDO CYBERSECURITY TALENT DEEP DIVE



SECTION 1

A COMMON LANGUAGE FOR CYBERSECURITY

In This Section: There is an existing framework, the NICE Framework, that provides a common language for describing the cybersecurity workforce. The building block approach used in the framework allows industry to define workforce needs in the same language as educators and trainers who build programs. When industry and education use the same language, workers clearly understand their path to success.

The Need for a Common Language

Defining the work done every day by an employee or colleague is difficult. The day-to-day tasks a person performs in their role may differ from their job description. Despite federal-level frameworks and taxonomies to categorize jobs into specific definitions, one could say there are as many unique jobs as there are people given that everyone uses their own experiences and methods differently to complete a task.

Even more difficult is the process of describing the actual skills, knowledge and abilities required to perform a job. What skills differentiate an Information Security Engineer from a Computer Systems Engineer? What abilities make a Network Architect unique from a Network Administrator? Throw in these confusions along with the fact that there is no consistency between companies when it comes to job titles and descriptions (see Box 1 below), and, suddenly, it feels like a daunting task to create a common language for cybersecurity workforce development.

BOX 1

A Common Title with No Common Skills

The list below shows the required skills, extracted using text analysis, from the responsibilities section of two different job postings. Both postings were from the Orlando area, had the same job title, Director of Cybersecurity, and both were posted in January 2022. The only difference is that these postings came from different companies.

Required Skills

- Jobs Posting A – Artificial Intelligence, Automation, Business Process, Cybersecurity, Incident Management, IT Security Architecture, Machine Learning, Planning, Security Information and Event Management (SIEM), Threat Detection, Threat Management
- Job Posting B – Authorization, Certified Information Systems Security Professional, Classified Information, CompTIA Security+, Configuration Management, Continuous Monitoring, Corporate Security, Information Systems Security, Information Technology, Linux, Operating Systems, Security Controls, Standard Operating Procedure, Unix, Variability.

These job descriptions have perfectly matching titles yet the text analysis software[8] did not return a single overlapping skill. Job posting A is much more hands on; the new hire is meant to design and develop solutions using artificial intelligence. Job posting B is more focused on government liaising and program management.

8 EMSI, Job Posting Optimizer

The NICE Framework - An Existing Solution

Unlike many other sectors and industries, cybersecurity has a preexisting framework for organizations and educators to tap into. The Workforce Framework for Cybersecurity (NICE Framework) is a special publication of the National Institute of Standards and Technology (NIST) from the U.S. Department of Commerce that was first created in 2012. Over the last decade, the NICE Framework has evolved to keep pace with industry changes via a system of revisions, public comment, stakeholder feedback, etc. The most recent version was released in November 2020.

"The NICE Framework helps organizations overcome the barrier of describing their workforce to multiple stakeholders by presenting a building block approach. Through the use of conceptual building blocks, the NICE Framework presents a common language for organizations to use internally and with others."[9]

This has many implications. A common language lowers barriers to entry for organizations that wish to work with others and collaborate on workforce development. The building blocks can be used to create common names for competencies and work roles. The framework identifies career pathways that inform learners how to prepare for advancement.

This report will not reiterate the NICE framework in its entirety and encourages anyone interested in using the NICE Framework to download the report and reference spreadsheets, which can be found here.[10] Instead, the following section introduces the basic concepts included in the framework.

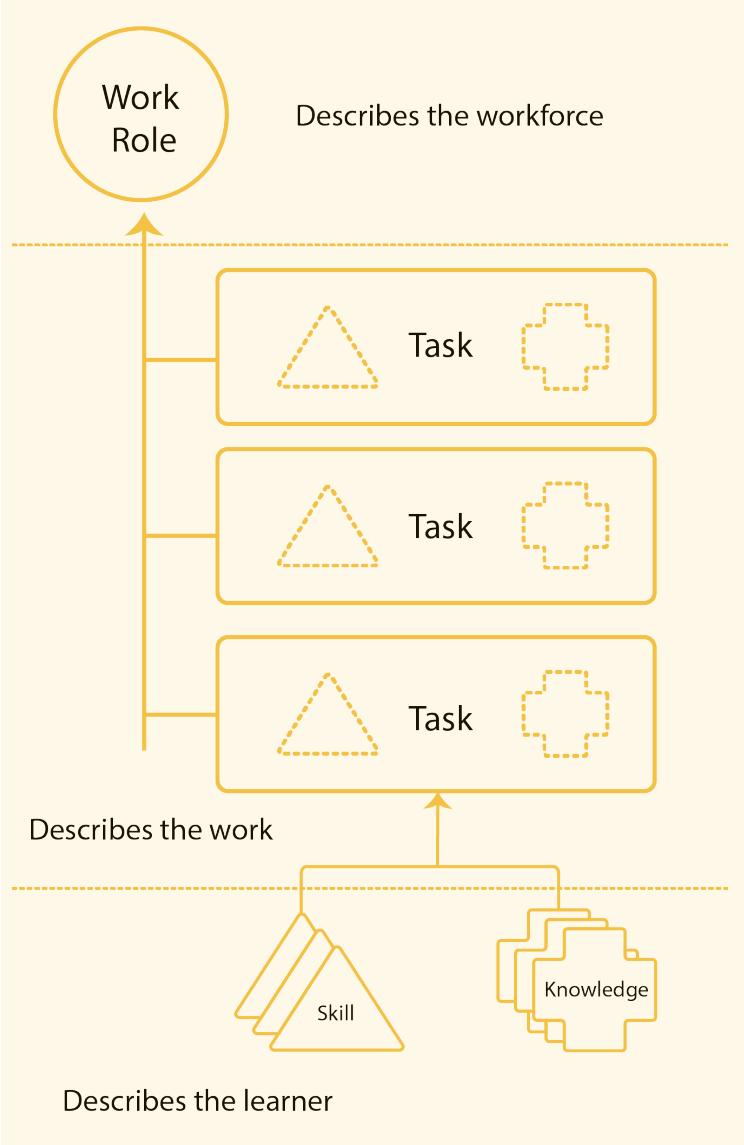
9 Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1

10 For those reading the report in print version, full links have been provided in the Links and References section at the end of this report.

NICE Framework Building Blocks

FIGURE 1

NICE Framework Building Blocks



Task, knowledge and skill statements are the basic foundations of the framework. In NICE terminology, knowledge and skills describe the learner. The NICE Framework refers to all users as learners. This could mean students, job seekers, employees, etc. and captures the idea that everyone is constantly learning in the cybersecurity industry. Combinations of knowledge and skills lead to the creation of task statements. In an organizational context, learners execute tasks. In an educational context, learners acquire new skills and knowledge.

Knowledge

- Knowledge is defined as a retrievable set of concepts within memory. Knowledge can be foundational of specific and like skill statements, multiple types of knowledge may be required to form a task. Ex: Knowledge statement 0036 for a System Security Analyst is "knowledge of human-computer interaction principles."

Skill

- Skills are the capacity to perform an observable action. Multiple skill statements can be used to describe a single task. Ex: Skill statement 0167 for a System Security Analyst is "skill in recognizing the vulnerabilities in security systems (e.g., vulnerability and compliance scanning)."

Task

- Task statements describe the work to be done for the organization. They are presented in an organizational context, easy to read and begin with the activity. They do not include the organization's overall goal or objective resulting from the task. Ex: Task 0085 for a System Security Analyst is "ensure all systems security operations and maintenance activities are properly documented and updated as necessary."

Task statements may be used in a variety of ways. For example, task statements can be grouped together to form specific work roles. A work role is "a way to describe a grouping of work for which someone is responsible or accountable." Rather than directly clustering knowledge, skills and abilities to define types of work, as some frameworks do, the NICE Framework methodology of inserting tasks simplifies communication and "represents learners' potential to perform those tasks."[11] See Figure 1 above.

While still grounded in an understanding of skills, this approach provides a more realistic description than simply listing the knowledge a worker should have. The concept of task statements is applied to a real cybersecurity job description in section three.

11 Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1

Key Idea: The NICE Framework breaks down cybersecurity activities to clearly define skills and abilities workers should have and learners should pursue. This creates a common language that, when utilized, reduces barriers employers and educators may have working together.

These are the building blocks that define the NICE Framework. The framework is constantly evolving from industry feedback and recognizes that organizations may need to create and design their own competencies and skills. The framework provides guidance on how to create custom task statements and work roles. Users are encouraged to download all of the NICE Framework resources here.[10]

The NICE Framework catalog of success stories outlines how organizations across the world have utilized the framework. JP Morgan Chase & Co. was an early adopter and used the framework for internal workforce development and to improve worker mobility.

Florida – and Orlando specifically – is a place of vibrant and growing opportunities, especially in cybersecurity. But potential hires are not always sure about what employers are looking for. As cybersecurity continues to take on priority for businesses, using similar language in job postings and clearly defining the skills workers need will help build the pool of qualified candidates, ease recruiting pains and reduce barriers to entry for job seekers."

TRACY Rebar
Head of HR for Consumer Branch Banking
JPMorgan Chase & Co

Cybersecurity Verticals

These building blocks come together in various ways to form specialty areas and categories in the cybersecurity industry. There are seven workforce categories in the NICE framework, each with their own specialty areas. Figure 2 to the right outlines how they connect to work roles, tasks and skills.

Think of these categories as verticals in the industry. They represent different lines of work or niches occupied by people with cybersecurity skills. This is an important distinction given that job descriptions often list key phrases such as "risk management" and "systems administration" as skills when they are broader topics.

Figure 3 below highlights the various categories and included specialty areas.

Understanding the different cybersecurity verticals is important for encouraging and growing the workforce. In (ISC)²'s 2019 workforce report, two of the top three pain points hindering career progression for individuals in the cybersecurity space were unclear career path opportunities and lack of knowledge about cybersecurity skills within organizations.

FIGURE 2

Defining Cybersecurity Verticals

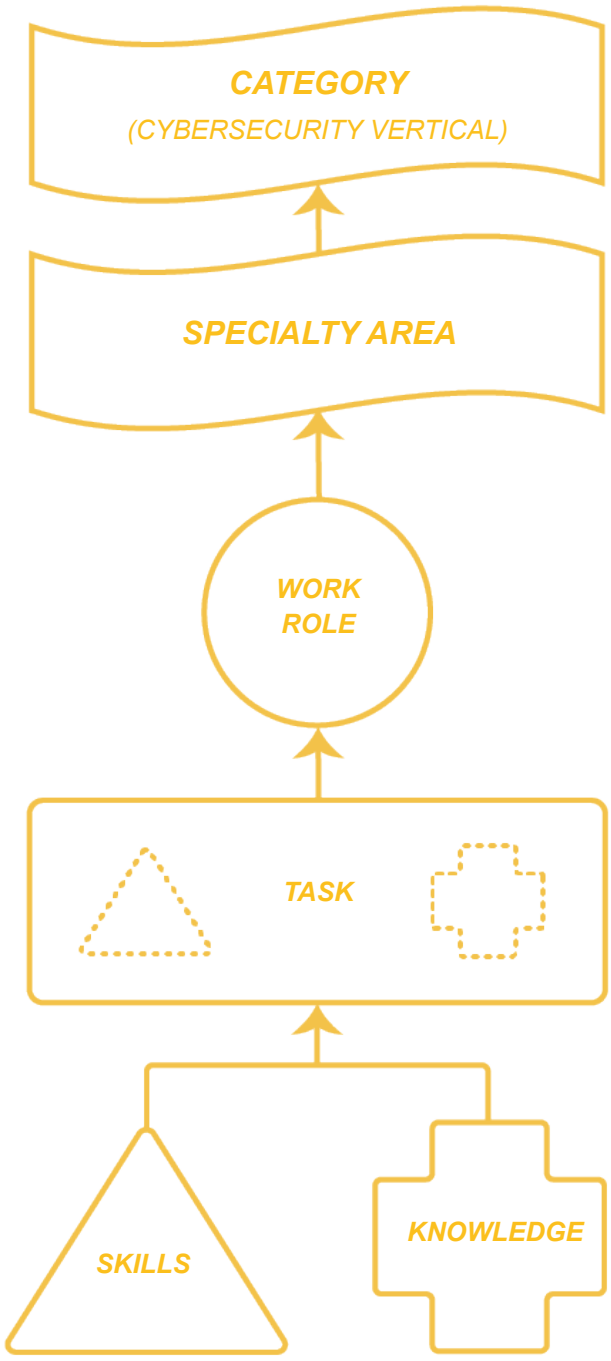


FIGURE 3

NICE Framework Cybersecurity Verticals

Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

Specialty Areas Include: *risk management, software development, systems architecture, technology R&D, test and evaluation and systems development*

Work Role Example: Security Architect

Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Specialty Areas Include: *data adminstration, knowledge management, customer service and technical support, network services, systems administration and analysis*

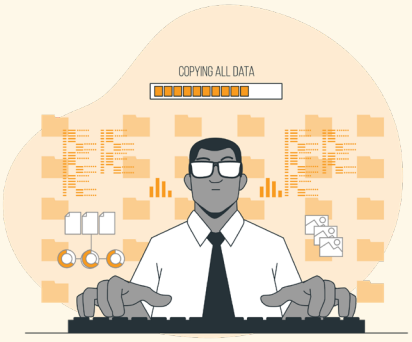
Work Role Example: *Data Analyst*

Oversee and Govern

Provides leadership, management, direction or development and advocacy, so the organization may effectively conduct cybersecurity work.

Specialty Areas Include: *legal advice and advocacy, cybersecurity management, strategic planning and policy program management and acquisition*

Work Role Example: *IT Project Manager*



Protect and Defend

Identifies, analyzes and mitigates threats to internal IT systems and/or networks.

Specialty Areas Include: *cybersecurity defense infrastructure support (INF), incident response, and vulnerability assessment and management*

Work Role Example: *Vulnerability Assesment Analyst*

Analyze

Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Specialty Areas Include: *threat and exploitation analysis, all-source analysis, targets and language analysis*

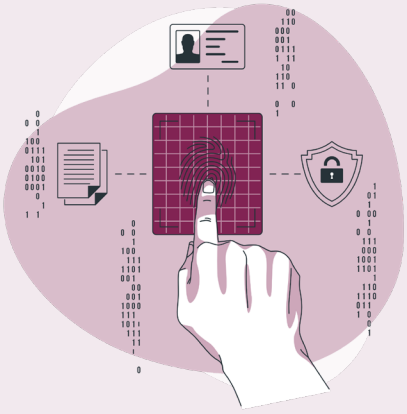
Work Role Example: *Threat/Warning Analyst*

Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Specialty Areas Include: *collection operations, cyber operational planning and cyber operations*

Work Role Example: *Cyber Intel Planner*



Investigate

Investigates cybersecurity events or crimes related to IT systems, networks and digital evidence.

Specialty Areas Include: *Cyber investigation and digital forensics.*

Work Role Example: *Cyber Crime Investigator*

Illustrations attributed to storyset.com

The Importance of Soft Skills

Before moving on to a deep dive on Orlando's cybersecurity industry specifically, a section about common language would not be complete without a note about the power of soft skills.

Previous UpSkill Orlando reports made the distinction that skills are either specific and honed on the job or foundational and needed across industries. From UpSkill Orlando's 2021 In-Demand Skills report, "specialized skills include professional and occupation-specific skills, which run the gamut from accounting and sales to database administration and welding. Baseline skills include cross-cutting or foundational skills that are found across industries and occupations [such as] organization, communication and project management."(12)

Other taxonomies hinting at this distinction include the common terms "hard and soft skills" or "technical vs. non-technical" skills. Whatever terminology or definition you choose to use, it is becoming increasingly clear that interpersonal skills (leadership, teamwork, communication, etc.) are the most important skills of all, even in the cybersecurity field where it might be assumed that technical skills reign supreme.

Udemy's 2022 Workplace Learning Trends Report noted that soft skills should be reframed as power skills given that in an increasingly automated world, "skills related to leadership, teamwork, communication, productivity and wellness are critical to every employee's performance."(13)

(ISC)²'s 2021 workplace study asked what the most important qualifications for cybersecurity professionals are. Many non-technical skills outranked or equaled technical experience, such as having a cybersecurity certification or background. See Figure 4.

The growing importance of a broader mix of skills, both technical and non-technical, underscores the reality that today's cybersecurity roles are multi-dimensional and increasingly varied across specializations, organizations and industries."(14)

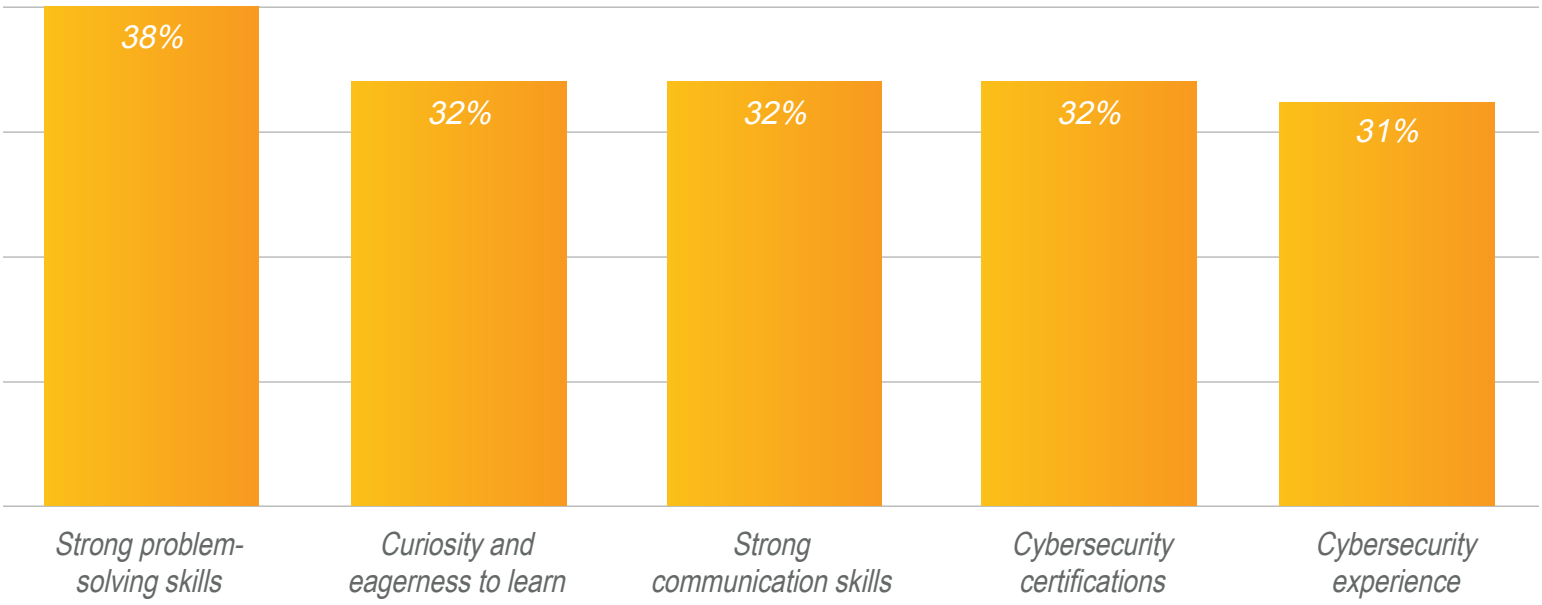
12 Foundation for Orlando's Future. Re-Imagining Orlando's Talent Supply, A Business Perspective on In-Demand Skills. 2021

13 Udemy, 2022 Workplace Learning Trends Report

14 (ISC)² Cybersecurity Workforce Study, 2021

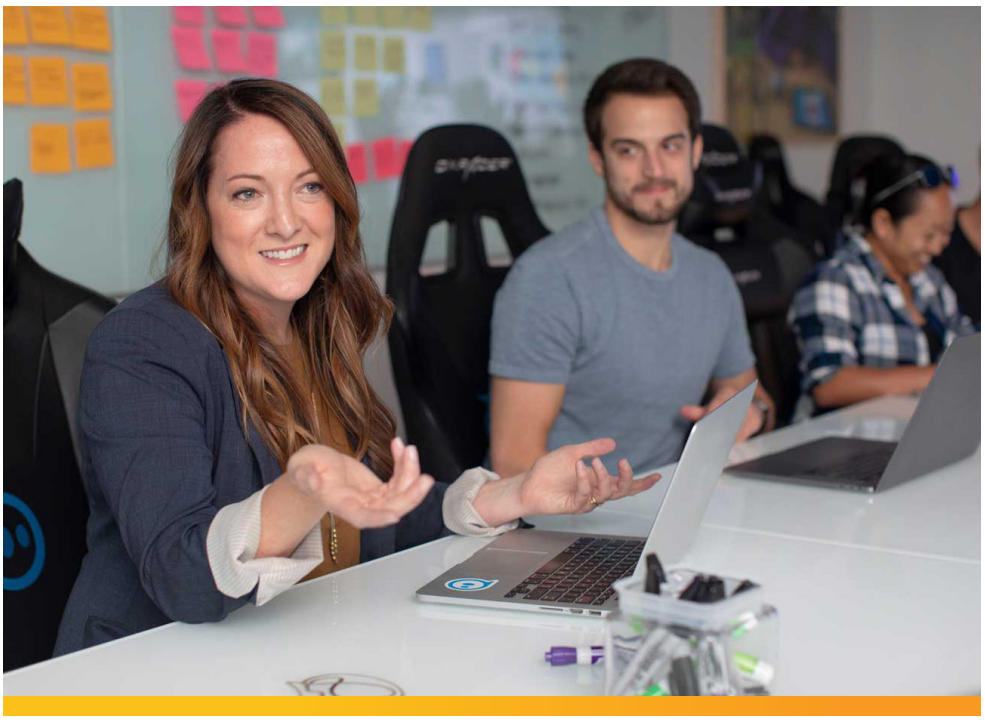
FIGURE 4

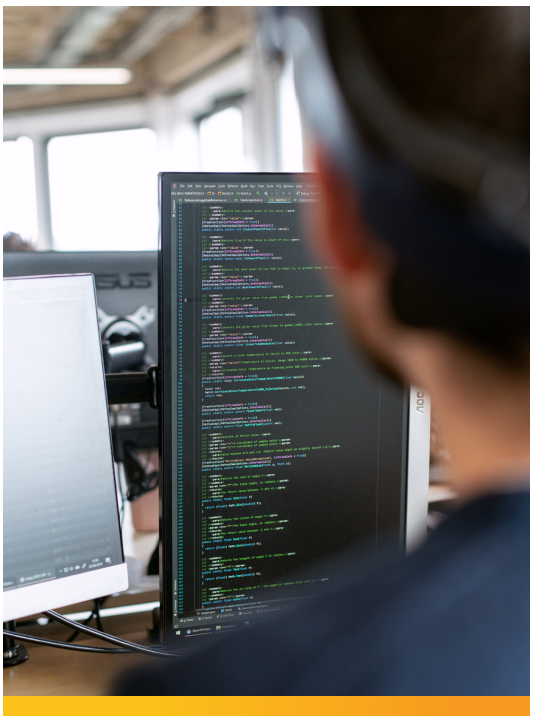
Most Important Qualifications for Cybersecurity Professionals
(respondents could choose more than one answer)



**Source: (ISC)² Cybersecurity Workforce Study, 2021*

Key Idea: In a role where technology is constantly changing, interpersonal and critical thinking skills are what set candidates apart from the crowd. According to some hiring managers, the most important attribute for a cybersecurity candidate is a sense of curiosity.





AN ORLANDO CYBERSECURITY TALENT DEEP DIVE

SECTION 2

ORLANDO'S CYBERSECURITY NEEDS

In This Section: Demand for cybersecurity talent in Orlando spans industries ranging from defense to tourism. It's clear there is not enough talent to fill the number of available job postings. This broad need stems from the fact that most local demand is concentrated in operating, managing and securing digital infrastructure, and not in areas such as counterintelligence or forensics. In their search for talent, Orlando organizations differ in their approach and desire for certified professionals.

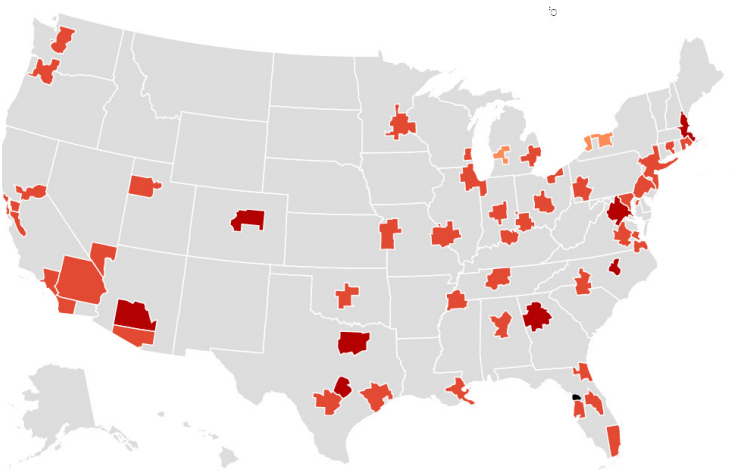
No Location is Meeting Demand

Orlando has a cybersecurity supply to demand ratio of 71. This means there are only enough cybersecurity workers in the four-county region to fill 71 percent of demand. The neighboring Space Coast has a score of 84 and Tampa, to the west, has a slightly lower value of 69. This range holds true for most large metropolitan areas across the United States where, on average, cybersecurity talent meets 68 percent of demand. No large metro has a surplus of talent, but Rochester, New York, comes close with supply filling 92 percent of demand. The metro areas with the greatest talent shortage are both in Texas; supply only meets 58 and 56 percent of demand in Dallas and Austin.[15]

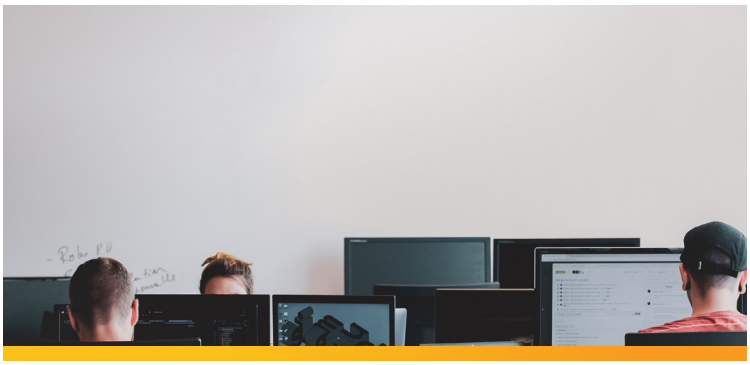
15 Cyber Seek, accessed February 2022, https://www.cyberseek.org/heatmap.html

FIGURE 5

Supply and Demand Ratio, Large Metropolitan Areas



Source: Cyberseek.org, February 2022



In-Demand Roles

Moving beyond high-level measures, the NICE Framework makes it possible to understand the specifics of Orlando's cybersecurity talent needs while using a common language backed by national standards. Section one of this report outlined the seven major categories (verticals) of work in the cybersecurity industry according to the NICE Framework: securely provision, operate & maintain, oversee & govern, protect & defend, analyze, collect & operate and investigate.

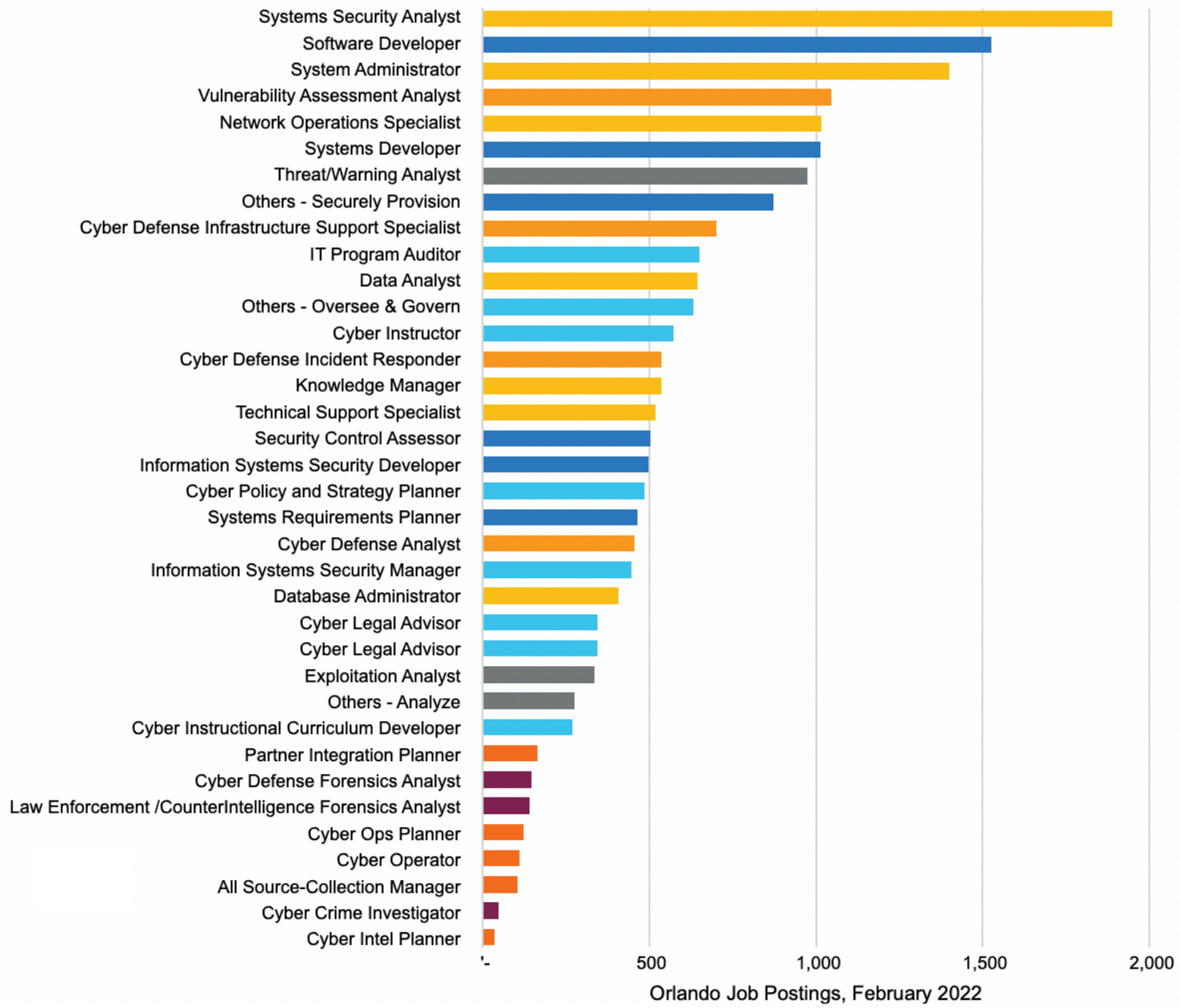
Most cybersecurity job postings in the country fit into one of two categories: operate & maintain and securely provision. This is true for Orlando as well. Work roles such as a Systems Security Analyst and Software Developer are some of the top jobs in these categories. There is one top job that does not fit into these two categories: Vulnerability Assessment Analyst. This role is part of the protect & defend vertical and works to "measure effectiveness of defense-in-depth architecture against known vulnerabilities."[16] It is not shocking that there is a large need for workers who can analyze a network to find chinks in digital armor, especially as companies transition to fully remote or hybrid work environments. The top Orlando companies posting for jobs using key phrases such as vulnerability scanning or vulnerability discovery include Lockheed Martin, Deloitte, the State of Florida, AdventHealth, Stax (previously Fattmerchant) and Disney. These companies represent members of the defense, consulting, government, healthcare, finance and tourism industries. It's clear the need to defend cyber assets spans all trades.

Roles with the smallest demand fall into the collect & operate and investigate categories. This distinction stems from the fact that most local demand is widespread and concentrated on operating, managing and securing digital infrastructure, and not in areas such as counterintelligence or forensics. See Figure 6.

16 Workforce Framework for Cybersecurity (NICE Framework), Reference Spreadsheet

FIGURE 6

Cybersecurity Jobs (Work Roles) In Demand* in Orlando



**This data is not meant to be aggregated. One job posting could match multiple work roles.*

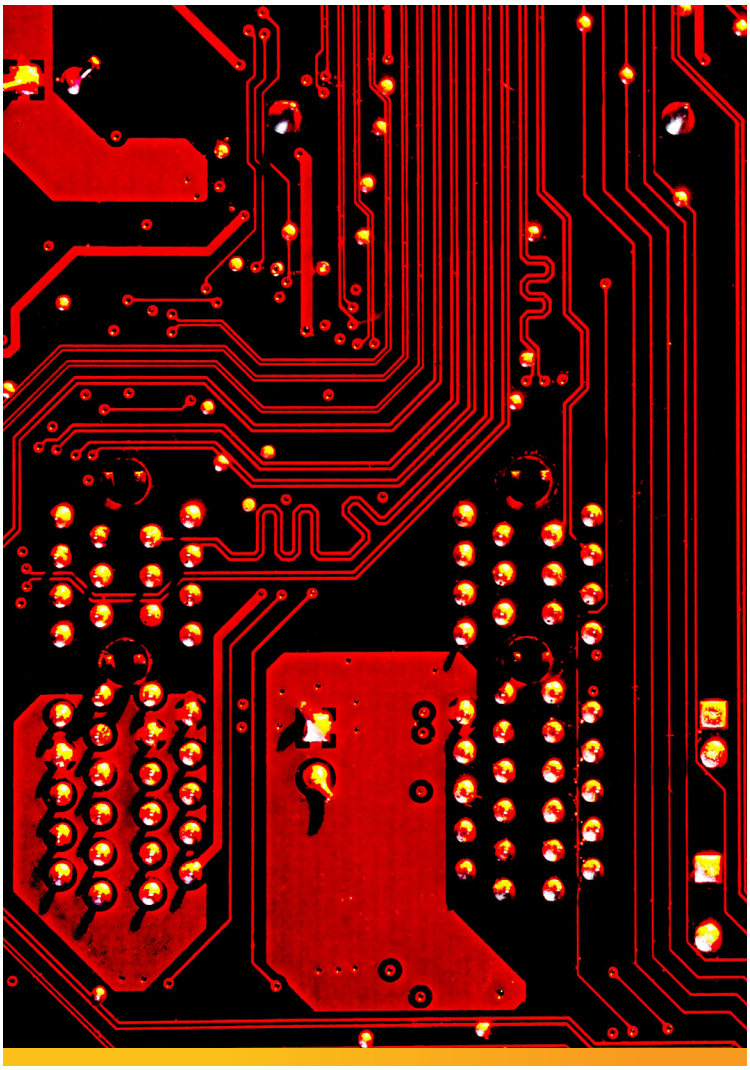
The table above dives deeper into the work roles in Orlando where there are currently more than 1,000 jobs postings. Note that, rather than listing the skills and knowledge associated with each work role, the table includes possible tasks those positions may be required to perform. This creates a better sense of the day-to-day operations of these positions, a concept that will come into play again in section three.

TABLE 1

Top Cybersecurity Jobs in Orlando

WORK ROLE	DESCRIPTION	POSSIBLE TASKS
Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations and maintenance of systems security.	• Perform cybersecurity testing of developed applications/or systems. • Analyze and report organizational security posture trends to leadership. • Ensure the execution of disaster recovery and continuity of operations.
Software Developer	Develops, creates, maintains and writes/codes new (or modifies existing) computer applications, software or specialized utility programs.	• Analyze user needs and software requirements to determine feasibility of design within time and cost constraints. • Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. • Consult with engineering staff to evaluate interface between hardware and software.
System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g. installing, configuring and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks).	• Develop and document systems administration standard operating procedures. • Manage accounts, network rights and access to systems and equipment. • Install, update and troubleshoot systems/servers.
Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	• Conduct and/or support authorized penetration testing on enterprise network assets. • Maintain knowledge of applicable cyber defense policies, regulations and compliance documents, specifically relate to cyber defense auditing. • Make recommendations regarding the selection of cost-effective security controls to mitigate risk.
Network Operations Specialist	Plans, implements and operates network services/systems to include hardware and virtual environments.	• Configure and optimize network hubs, routers and switches. • Install and maintain network infrastructure device operating system software. • Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
Systems Developer	Designs, develops, tests and evaluates information systems throughout the systems development life cycle.	• Design or integrate appropriate data backup capabilities into overall system designs and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data. • Utilize models and simulations to analyze or predict system performance under different operating conditions. • Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.

**This is not an exhaustive list of tasks associated with these roles. Readers are encouraged to view the NICE Framework reference spreadsheet here.*

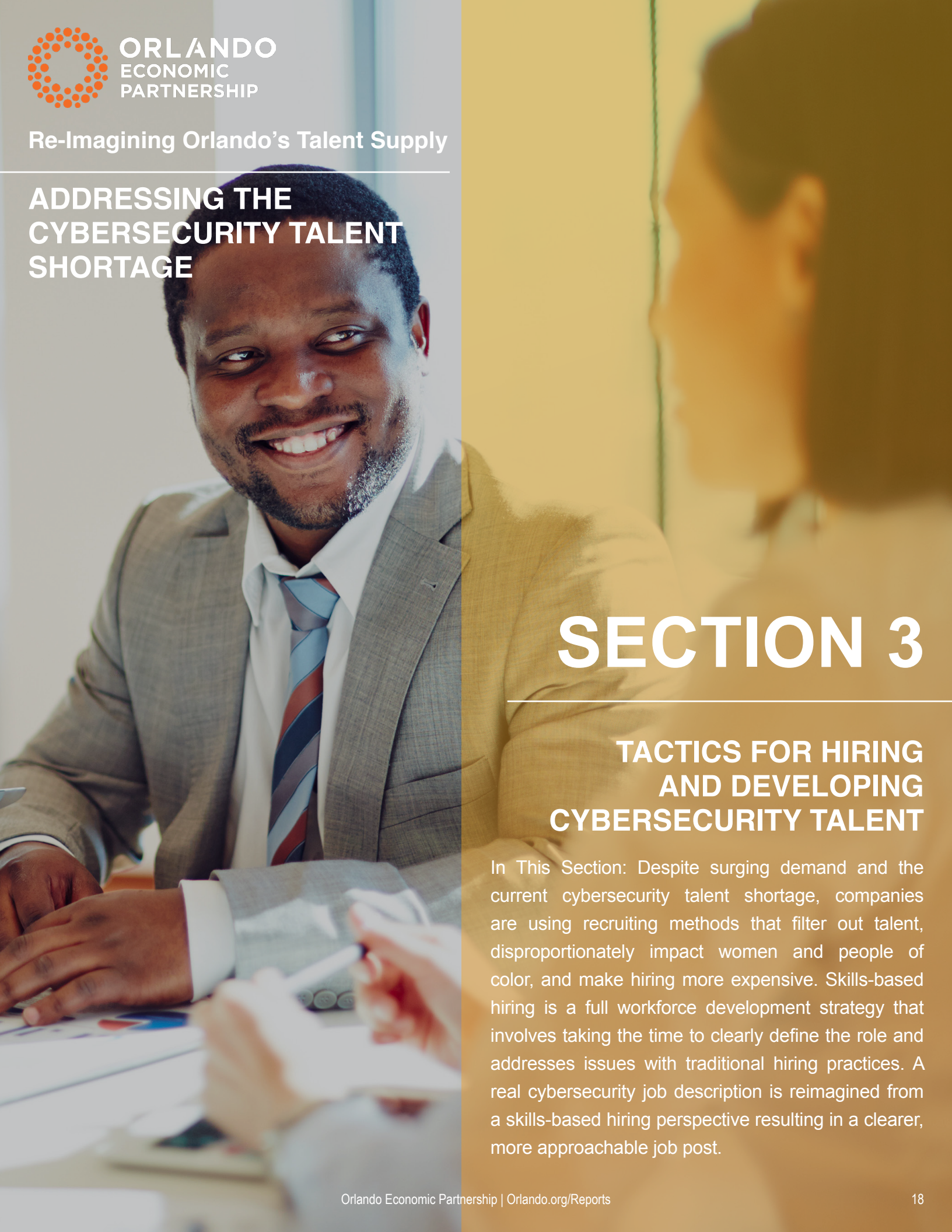


Cybersecurity is an in demand discipline, which is critical for fast growing companies in the financial technology space. The architecture and design of cybersecurity programs needs to take into account scalability which includes people, processes, and technology. We are actively looking to hire, retain and mentor talent in order to improve not just Stax but the lives of our team members."

DANIEL Poloche
Vice President of IT and Security
Stax

Key Idea: Using tasks to define jobs makes for a clearer job description. Individuals have an easier time imagining themselves performing the day-to-day tasks associated with the role. Hiring managers are not only able to highlight the need for skills such as communication and curiosity, but also how they will be used.

ADDRESSING THE CYBERSECURITY TALENT SHORTAGE



SECTION 3

TACTICS FOR HIRING AND DEVELOPING CYBERSECURITY TALENT

In This Section: Despite surging demand and the current cybersecurity talent shortage, companies are using recruiting methods that filter out talent, disproportionately impact women and people of color, and make hiring more expensive. Skills-based hiring is a full workforce development strategy that involves taking the time to clearly define the role and addresses issues with traditional hiring practices. A real cybersecurity job description is reimagined from a skills-based hiring perspective resulting in a clearer, more approachable job post.

The Industry Needs New Hiring Practices

Cybersecurity is a hybrid job that "requires a large amount of technical and domain knowledge, but it also requires an understanding of IT architectures, policies and human issues."[17] Given this definition plus surging demand and the constantly evolving aspect of the work, finding the ideal applicant with a flawless resume is far from likely.

Yet, organizations continue to post for the perfect candidate. In Orlando, 95 percent of cybersecurity job postings required a bachelor's degree or higher.[18] Consider that only 33 percent of the working age population in Orlando meets these credentials,[19] and it is clear the pool of candidates is rapidly shrinking. Similarly, 70 percent of Orlando cybersecurity job postings in a two-year period required four or more years of experience. This hints at one of the industry's main challenges with recruiting. "The largest feeder occupation for cybersecurity…is cybersecurity. When companies post for talent, they post for candidates who already have cybersecurity experience."[20] These practices only serve to shrink the talent pool, raise prices, and do little to diversify the industry. Roughly three-quarters of the cybersecurity workforce in North America identify as Caucasian men.[21]

Fortunately, pathways into the field are beginning to widen. While an IT background remains the single, largest path to a cybersecurity career, an international survey shows roughly half of professionals get their start outside IT – 17 percent transitioned from an unrelated field, 15 percent gained access through cybersecurity education, and 15 percent explored cybersecurity concepts on their own.[22]

The same survey shows that the younger Gen Z and Millennial cohorts are more likely to get their start outside of the IT sector than the Gen X and Baby Boomer age groups. Women are less likely to come from an IT background than men and women have higher rates of entry into the field from self-learning. For Orlando companies, removing barriers to employment such as bachelor's degree and industry experience requirements is one way to expand and diversify the workforce.

17 EMSI, Build Don't Buy Report

18 Analysis of EMSI Burning Glass Job Posting Data. Unique postings from Jan. 2020 to Jan. 2022.

19 US Census Bureau, American Community Survey, 2019

20 (ISC)² Cybersecurity Workforce Study, 2021

21 (ISC)² Cybersecurity Workforce Study, 2021

22 (ISC)² Cybersecurity Workforce Study, 2021

"There is an under-explored group of individuals available to fill cybersecurity positions if companies could advertise roles in such a way that more people could envision their pathway into the field."

Jacob Vigil
Senior Manager, Markle Foundation
Rework America Alliance

Skills-Based Hiring, A Win-Win Tactic for Employers

Skills-based hiring is a strategy that involves changing workforce management from top to bottom. It starts with a clear job description and ends with a professional development outline that improves retention and employee satisfaction. The most important piece of this process is the job description and related job post. It requires a different mindset – one that encourages employers to evaluate an individual's skills and abilities, instead of background, and rethink job description requirements. The benefits of skills-based hiring to employers are:

1. Fill jobs quickly Skills-based hiring encourages taking extra time to clearly define the role and associated competencies or tasks. When implemented correctly, this streamlines the hiring and onboarding process because candidates have a very clear idea of what the role entails.
2. Retain talent Employee turnover can be one of the biggest expenses in an organization. The Center for American Progress found that it can cost a business up to 21 percent of a person's salary to replace them. Again, skills-based hiring results in clearly defined expectations for the candidate upfront and encourages capability tests during hiring, equipping the employee for the job.
3. Diversify the talent pipeline There are racial disparities in the United States and Orlando when it comes to educational attainment. Only 24 percent of the Black population in Orlando has a bachelor's degree or higher compared to 35 percent of the White population.[23] Skills-based hiring addresses these disparities directly by using tactics that open the talent pool to individuals who may have the necessary skills to perform the job but lack a college degree.

Why do job posts typically require bachelor's degrees or years of experience in the first place? They act as filters. They come across as stand-ins on a resume for the skills and abilities employers hope to find in their new hires and automated candidate tracking systems use them as such. Rather than include filters that disproportionately weed out women and people of color from the candidate pool, employers should write clear job descriptions that use tasks and competencies as a means of judging talent. The skills-based hiring process offers a framework for writing clear job descriptions and removing bias from the hiring process, making it a win-win tactic for employers and employees.

A more in-depth explanation of these benefits can be found in the Upskill Orlando report, Re-Imagining Orlando's Talent Supply, Skills-Based Hiring for Upward Mobility.

Key Idea: This report is not suggesting that higher education is not necessary or that individuals should stop pursuing degrees. A bachelor's degree is simply one avenue to gaining the skills and knowledge required to perform a job. Skills-based hiring is a methodology for writing better job descriptions that attract the right talent. Removing bachelor's degree requirements opens the candidate pool to the 750,000 working adults without a four-year degree in Orlando.(24)

23 US Census Bureau, American Community Survey

24 Analysis of US Census Bureau, American Community Survey, 2019 data for the population 25-64, and labor force participation rate from February 2022.

Writing Better Cybersecurity Job Posts

The basic elements of skills-based hiring are:

1. Remove credential requirements when possible
2. Use competencies specific to the job
3. Reduce bias and increase diversity

To demonstrate these elements in action and combine components from the NICE Framework, the following case study reimagines a cybersecurity job post to meet the requirements of skills-based hiring.The following is an excerpt of a real job posting from January 2022. The position is a Cybersecurity Manager in the company's governance, risk management and compliance (GRC) department. The position could be filled from any one of the company's U.S. offices. See Box 2 below.

BOX 2

Original Job Posting – MANAGER, Cybersecurity – GRC SERVICENOW

Responsibilities

- *Experience in guiding clients and developing their Cyber GRC vision, strategy, and implementation roadmap*
- *Experience demonstrating out-of-the-box capabilities within ServiceNow IRM/GRC, ServiceNow SecOps, and/or OneTrust and aligning those capabilities against client's objectives*
- *Experience designing, architecting and implementing Cybersecurity, Cyber Risk, SecOps and GRC / IRM programs and technology platforms in one or more of the following areas: Policy and Compliance, Risk, Vendor Risk, Business Continuity, Data Privacy, Issues Management, Vulnerability Response and Security Incident Response*
- *Oversee implementation of one or more applications in ServiceNow IRM/GRC, ServiceNow SecOps, or OneTrust GRC supporting Cybersecurity and Cyber GRC programs*
- *Experience with agile and scrum methodology, creating process designs and technical designs, defining user stories, working with diverse development teams in multiple geographies, leading user acceptance testing (UAT), and providing the necessary end-user training to deliver the proposed solution to the highest caliber*
- *Facilitate requirements gathering, scrum, sprints, testing, and deployment by working directly with clients*
- *Actively participate in practice development such as innovative solutions to complex problems, knowledge management and work towards building a strong Cyber GRC community*

Qualifications

- *A minimum of five years' experience in the field of Cybersecurity, Cyber Risk and GRC with a strong working knowledge of ServiceNow and/or OneTrust GRC*
- *Bachelor's degree from an accredited college/university or equivalent professional experience*
- *Certifications in any of the following: ServiceNow Certified System Administrator (required for candidates with ServiceNow experience); ServiceNow CIS certification in IRM in either: Risk and Compliance, Vendor Risk Management OneTrust GRC Professional Certification ServiceNow CIS certification in SecOps in either; Security Incident Response or Vulnerability Response (a plus)*
- *Solid competencies in processes related to Cyber GRC domain including Security Policy Management, Security Compliance Management, Cyber Risk, Vendor Security Risk, Business Continuity, Data Privacy Vulnerability Management, Security Incident Response Management and / or Issues Management*
- *Competency in security frameworks including NIST CSF, NIST 800-53, ISO 27001, HIPAA, PCI, SOX*
- *Competency in Unified Controls Framework (UCF) and mapping to common controls*
- *Experience with security tools such as Nessus, Rapid 7, Tanium, Qualys, Splunk, QRadar, LogRhythm, etc. is a plus*
- *Demonstrable interpersonal, facilitation and presentation skills to help clients navigate through complex cybersecurity and GRC challenges*
- *Ability and Willingness to Travel*

Why this is a poor job posting

- *Few responsibilities outline the day-to-day activities of the position. Most of the bullets read as qualifications, asking for "experience in" or "with" certain methodologies.*
- *Immediately uses industry jargon by not clarifying the acronyms such as GRC, SecOps and IRM.*
- *Requires a minimum number of years in cybersecurity field.*
- *Requires a bachelor's degree. Does not clarify what it means to have equivalent professional experience and conflicts with the minimum years of cybersecurity experience requirement above.*
- *Long list of certifications with no mention of which are preferred or if any will be included as part of a professional development plan for the position.*
- *Lists necessary competencies and experiences without outlining how they will be applied.*
- *Multiple skills, competencies or tasks are included in single statements.*

In Box 3, the same job posting has been reimagined using the elements of skills-based hiring and the NICE Framework. Industry-specific jargon has been removed along with unnecessary qualifications. Responsibilities are clearly defined using pre-existing task statements from the NICE Framework.

BOX 3

Skills-based Hiring Job Posting - Manager, Cybersecurity - Governance, Risk, and Compliance (GRC)

Responsibilities

- *Establish and maintain communication channels with clients*
- *Coordinate and manage the overall service provided to a customer end-to-end*
- *Provide policy guidance to cyber management, staff and clients*
- *Provide enterprise cybersecurity and supply chain risk management guidance*
- *Analyze organizational cyber policy*
- *Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities*
- *Interpret and apply applicable laws, statutes and regulatory documents and integrate into policy*
- *Develop methods to monitor and measure risk, compliance and assurance efforts*
- *Resolve conflicts in laws, regulations, policies, standards or procedures*
- *Draft and publish supply chain security and risk management documents*

Required Skills

- *Facilitation and presentation skills to help clients navigate complex cybersecurity challenges*
- *Interpersonal skills to work with a diverse team across multiple geographies*
- *Experience with agile and scrum methodology to manage multiple projects and timelines simultaneously*
- *Knowledge of cyber governance, risk and compliance domains such as security policy management, cyber risk, vendor security risk, business continuity and data privacy vulnerability to propose and deliver solutions to clients*

Prefferred Skills

- *Knowledge of security frameworks including NIST CSF, NIST 800-53, ISO 27001, HIPAA, PCI, and SOX*
- *Knowledge of Unified Controls Framework (UCF) and ability to map to common controls*
- *Experience with security tools such as Nessus, Rapid 7, Tanium, Qualys, Splunk, QRadar and LogRhythm*
- *Certifications in any of the following are a plus*
  - *ServiceNow Certified System Administrator*
  - *ServiceNow Certified Implementation Specialist (CIS) certification in Integrated Risk Management (IRM) in either: Risk and Compliance or Vendor Risk Management*
  - *OneTrust GRC professional certification*
  - *ServiceNow CIS certification in Security Operations (SecOps) in ether; Security Incident Response or Vulnerability Response*

Travel is required for this role.

Opportunities for professional development, including the preferred certifications, are available.

Why this is a good job posting

- *No industry jargon. Where acronyms are used, they have been defined.*
- *Responsibilities clearly reflect day-to-day tasks of the job. Using pre-existing NICE Framework statements that include only one task per statement helps to define the role and ensures the use of a common language.*
- *No vague experience or bachelor's degree requirements.*
- *The qualifications section is split into required and preferred skills. Skills-based hiring requires determining where there is capacity to train on the job vs. what a new hire needs to know on day one. Interpersonal skills and background knowledge may be required skills while specific certifications or tools can be taught on the job making them preferred skills.*
- *Qualifications include a nod to how the skill or knowledge will be used. Doing so increases the candidate's understanding of the role and helps them envision how they will apply their own transferable skills.*
- *Opportunities for professional development are clearly labeled. Clearly offering opportunities for professional development directly in the job post opens the role to more individuals and helps those already in the cybersecurity space understand how they will continue to learn and grow..*

Overall, this case study demonstrates how the tenants of skills-based hiring help clarify job posts so that a wider set of individuals might envision themselves growing into the role. Taking the time up front to clearly define roles and responsibilities makes job posts more approachable. This process also results in an exact list of competencies that need to be tested for during hiring vs. those that can become part of a new hires professional development plan.

ORLANDO ECONOMIC PARTNERSHIP

Re-Imagining Orlando's Talent Supply

AN ORLANDO CYBERSECURITY TALENT DEEP DIVE

SECTION 4

UPSKILLING TALENT

In This Section: Skills-based hiring is a general tactic that expands the talent pool and diversifies hiring in any industry. However, Cybersecurity faces a severe talent shortage and individuals must be actively upskilled to completely meet demand. Existing programs at regional higher education institutions help fill some of this need. Another tactic for upskilling potential employees includes paying certification costs.

Identifying Potential Talent Using Skills-Based Strategies

Skills-based hiring and actively upskilling talent are not the same thing, even though they may overlap. Skills-based hiring is the process of writing clear, non-biased job descriptions and using those descriptions to recruit, onboard and develop talent. Upskilling involves identifying an individual's existing skills and finding or creating training programs that will take him/her to the next level in their career. When implemented correctly, skills-based hiring can lead to internal career pathway growth and upskilling.

Higher education institutions may upskill a region's talent with programs designed for adult learners. Organizations may upskill their existing employees into new roles. Individuals often upskill themselves in search of new opportunities. The following case study highlights this distinction by showcasing existing cybersecurity talent from a skills-based hiring search and the talent that could be available to cybersecurity employers with some upskilling.

CASE STUDY

Using an online language processing tool, EMSI's online skills extractor, skills were identified from the required section of the job posting in Box 3 and used as search criteria to find work profiles. Search criteria are highlighted in Box 4. Box 5 shows a profile of a real Orlando worker that returned as a skills match using EMSI's complimentary profile analytics tool.

BOX 4

Required Skills, Skills-Based Job Post

- *Facilitation and presentation skills to help clients navigate complex cybersecurity challenges*
- *Interpersonal skills to work with a diverse team across multiple geographies.*
- *Experience with agile and scrum methodology to manage multiple projects and timelines simultaneously*
- *Knowledge of cyber governance, risk, and compliance domains such as security policy management, cyber risk, vendor security risk, business continuity and data privacy vulnerability to propose and deliver solutions to clients*

BOX 5

Candiate A Overview

Latest Employer: *Verizon*
Latest Job Title: *International Information Security Officer*
Selected Skills: *Cyber Governance, Cybersecurity, Cyber Risk, IT Infrastructure, Systems Development Life Cycle, Corporate Security, Finance, Cost Control.*
Licenses and Certifications: *Project Management Professional, Certified Information Systems Auditor, Certified Information Systems Security Professional (CISSP).*
Notes: *Previous employers include Lockheed Martin as a Supply Chain Cybersecurity Practice Lead*

Candidate A was one of only a few profiles returned by the system when cybersecurity, cyber governance and cyber risk were included as required skills. This is common when using this type of tool to find talent. EMSI is searching through online LinkedIn profiles to standardize and aggregate skills. This means the individual must be on LinkedIn and have listed somewhere in his/her profile a skill matching the search criteria. However, Candidate A does appear to be a good match for the Manager, Cybersecurity Governance, Risk and Compliance role studied in section three.

In this case, the skills-based job posting returned a candidate who has previous cybersecurity experience and a bachelor's degree, even though those qualifications were excluded from the search criteria. This goes to show the multifaceted challenge facing those looking for cybersecurity talent. Writing better, more approachable job posts alone will not solve the cybersecurity talent shortage. Talent needs to be actively recruited and upskilled into empty roles for organizations to meet demand and effectively protect their networks.

Boxes 6 and 7 showcase the potential for existing talent not currently working in the cybersecurity space to upskill into the area; either through employer-sponsored avenues or self-pursued education. In this case, the only required skills are presentations, interpersonal communication and experience with agile development and scrum methodology.

BOX 6

Required Skills – Skills-Based Job Post

- *Facilitation and presentation skills to help clients navigate complex cybersecurity challenges.*
- *Interpersonal skills to work with a diverse team across multiple geographies.*
- *Experience with agile and scrum methodology to manage multiple projects and timelines simultaneously.*

BOX 7

Candidates B-D Overview

Candidate B

Latest Employer: Disney Parks, Experiences and Products

Latest Job Title: Telecom Services Manager

Licenses and Certifications: Revenue Management: Cornerstone of Revenue Strategy

Selected Skills: Customer service, interpersonal communications, ServiceNow, presentations, financial analysis, agile methodology, scrum, revenue management

Notes: Bachelor's Degree in Accounting

Candidate C

Latest Employer: Harrah's Hoosier Park Racing & Casino

Latest Job Title: Floor Manager

Licenses and Certifications: None listed

Selected Skills: Video game development, security clearance, agile methodology, mechanics, presentations, scrum (software development), team leadership, interpersonal communications.

Notes: Previously US Air Force aircraft systems specialist, M.S. in game design from Full Sail University

Candidate D

Latest Employer: Siemens Energy

Latest Job Title: Project Management Specialist

Licenses and Certifications: Siemens Project Manager certified (S-level)

Selected Skills: Agile methodology, resource management, data analysis, AutoCAD, Presentations, scrum (software development), interpersonal communications, stakeholder engagement.

Notes: Bachelor's in Materials Engineering.

The candidates shown above range wildly in previous experience. Candidate C alone has experience designing video games and training teams to troubleshoot U.S. aircraft. However, they all share interpersonal communication, presentation, agile development and scrum methodology skills. That makes

them all potential candidates for the Cybersecurity Governance, Risk and Compliance role. Removing the need entirely for familiarity with cybersecurity domains and focusing on essential power skills widens the potential talent pool.

Of course, the next step in the upskilling journey would be for these candidates to gain that necessary background in the cybersecurity field, either through certifications or career training programs.

> *Key Idea: Skills-based hiring and upskilling are not the same thing. However, both tactics will be required to solve the cybersecurity talent shortage.*

Existing Training Programs

Individuals may choose to upskill themselves in search of a new career or employers may sponsor their continued education. Thankfully, there are a multitude of possible training programs available in Orlando ranging from online classes to full bootcamps.

University of Central Florida Cyber Defense Professional Certificate

For individuals looking to make a strong pivot into the cybersecurity field and gain a thorough background in a wide range of topics, the University of Central Florida (UCF) offers a Cyber Defense Professional Certificate. With 400 hours of class time, the UCF Certificate is one of the more extensive programs available in the region. However, the program does include elements that make it more accessible to adult learners looking for a career change.

- No previous technical experience required to enroll.
- A 30-hour introductory course helps individuals decide if cybersecurity is the career path for them before committing to the full program.
- The nights and weekend course schedule is designed for working adults.

The course catalog, available online, breaks down each class and the specific topics covered. The catalog also notes which professional certifications the course prepares students for. While not a test preparation course specifically, the certificate helps students gain the background knowledge necessary to pass certifications required by the Department of Defense including: CompTIA Network+, CompTIA Security+, CompTIA CySA+, Cisco Certified CyberOps Associate, and (ISC^2) SSCP††. More information about commonly required certifications is included in the section below.

Valencia College Cybersecurity Technical Certificate

Other programs exist in the region as well. Valencia College offers a cybersecurity technical certificate. This 30-credit hour program includes outcomes such as “audit organizational preparedness capabilities in responding to cyber-attacks” and “identify causes of networking problems, using diagnostic testing software and equipment.”

Seminole State College Cybersecurity Technical Certificate

Seminole State also offers a cybersecurity technical certificate. This 20-credit hour program requires courses titled Network Concepts and Operating Systems, Fundamentals of Cloud Networking and Security and Advances in Cybersecurity, to name a few.

Other Resources

Overall, multiple options for learning about cybersecurity are available across Orlando ranging from Lake Sumter State College to Osceola Technical College. This report will not attempt to duplicate efforts and catalog them all here. Resources such as Cyber Seek's education and training providers map visualize this information for the entire country. The Florida Consortium of Metropolitan Research Universities has also undergone a cataloging process to capture the existing cybersecurity programs in Orlando, Tampa and Miami.

Key Idea: Tactics for higher education providers that seek to speak the same language as employers and educate the workforce of the future can be found in the UpSkill Orlando Report Re-Imagining Orlando's Talent Supply: A Business Perspective on In-demand skills, available here. This report goes into the benefits of working directly with industry to build programs and communicating the value of those programs by "skillifying" syllabi.

When to Require Certifications?

Each employer in the Orlando MSA approaches credential requirements differently. At a meeting of top cybersecurity employers at the Orlando Economic Partnership's office, a representative of the Naval Air Warfare Center Training Systems Division (NAWCTSD) noted that they do require certification and security clearances to qualify for specific positions. Northrop Grumman must maintain a general percentage of credentialed employees to meet an overall requirement.

TABLE 2

Top Certifications Demanded in Orlando

CERTIFICATION	LISTED IN JOB POSTS
Certified Information Systems Security Professional (CISSP)	656
Security Clearance	627
CompTIA Security+	300
SANS/GIAC Certification	269
Cisco Certified Network Associate (CCNA)	268
Certified Information Systems Auditor (CISA)	209
Certified Information Security Manager (CISM)	209
Cisco Certified Network Professional (CCNP)	200
Information Systems Certification	163
IT Infrastructure Library (ITIL) Certification	130
GIAC Security Essentials Certification	129
Systems Security Certified Practitioner (SSCP)	107

**Source: Florida Consortium of Metropolitan Research Universities*

According to the Florida Consortium of Metropolitan Research Universities "the cybersecurity positions in the Orlando MSA include a large demand for national certified candidates."[25] Table 2 shows the certifications with the largest demand in the Orlando MSA. The original job posting in section three required many of these certifications as well, including the top certification, the Certified Information Systems Security Professional (CISSP).

Note that because CISSP is "based on time (5 years' experience) in addition to passing the certification test, many employers recognize that requiring this may hinder hiring talented-but-younger workers or hiring straight out of college. It is a goal and aspiration, less a requirement, for many firms."[26]

For this reason, it is recommended to clearly label these certifications as "preferred" on job posts; and, if possible, note that the company is willing to pay for the costs of becoming certified.

This change would address the No. 1 hurdle hindering career progression for the cybersecurity workforce: the cost of certifications. In a 2019 cybersecurity workforce study, 28 percent of participants selected the cost of cybersecurity certifications as their number one barrier. "More than half of respondents reported having to pay out of pocket for at least some of the costs of cybersecurity certifications."[27] See Figures 7 and 8 below.

25 Florida Consortium of Metropolitan Research Universities, Cybersecurity Orlando MSA Occupation Review, December 2021

26 Florida Consortium of Metropolitan Research Universities, Building Cybersecurity Talent Pipelines, CAEL Project Report December 2021

27 (ISC)2 2019 Cybersecurity Workforce Study

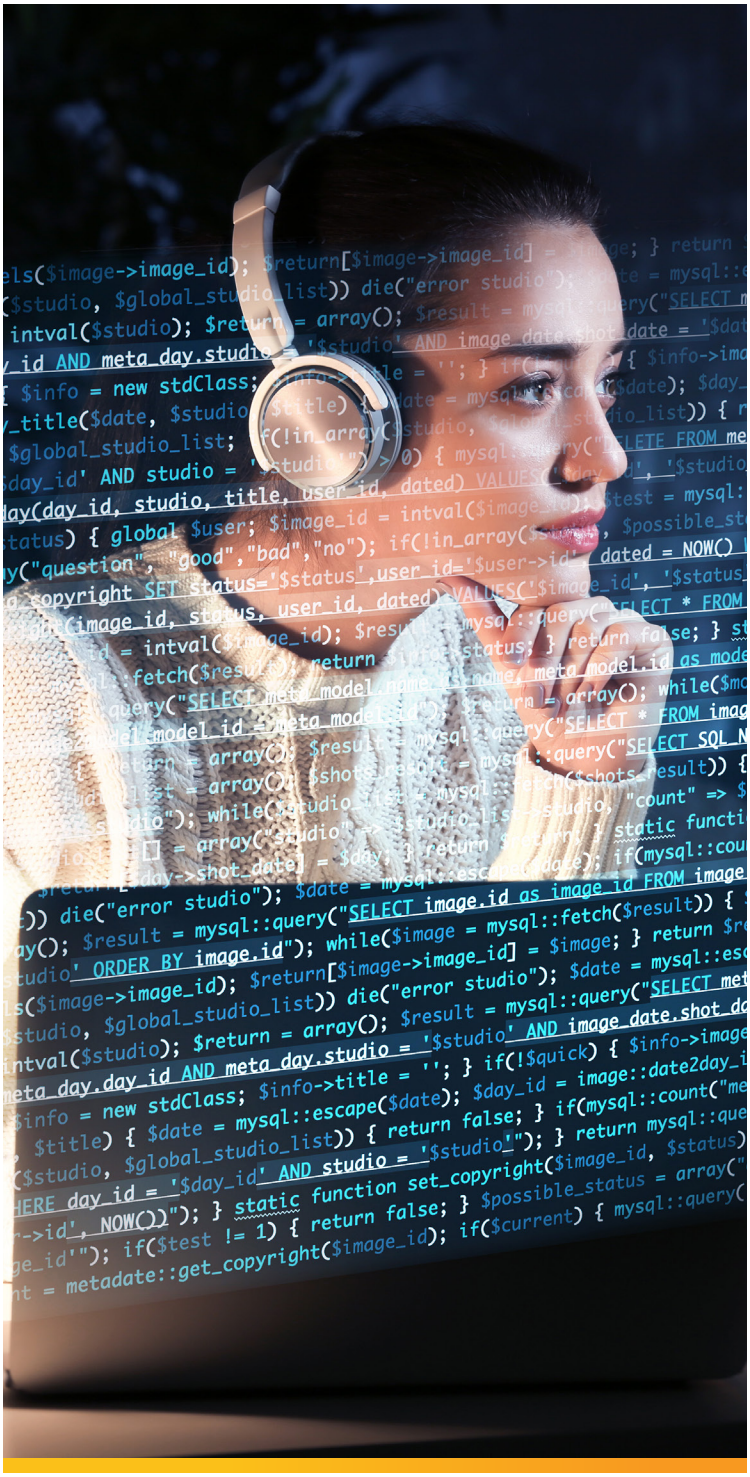
FIGURE 7

Key Items Hindering Career Progression

FIGURE 8

Who Pays for Cybersecurity Certificates?

This tactic is a win for the company in the long run as well. Individuals who work for companies that pay for certifications reported higher rates of satisfaction with their job than their peers. Roughly 72 percent of respondents whose employers pay their training bills said they are either very or somewhat satisfied with their job. While only 63 percent of respondents whose organizations pay for part or none of their training said the same.[28]



28 (ISC)2 2019 Cybersecurity Workforce Study

Key Idea: True skills-based hiring practices would have companies remove certification requirements from job posts entirely. However, this report recognizes this is not possible for every organization bound by higher governing orders. Instead, organizations should consider offering to pay for the cost of a new hire's certification, as it is a major barrier to career progression, and continue to clearly list the required and preferred skills associated with these certifications in job descriptions.

Conclusion

Accelerated by the COVID-19 pandemic, the demand for cybersecurity jobs is only growing as more and more of our daily interactions and work take place online. Ranging from protecting personal data to matters of national security, the new frontier of work will take place in the digital realm.

In Orlando specifically, the need for cybersecurity talent is not concentrated in one industry or location. Major employers such as Lockheed Martin, Deloitte and NAWCTSD demand much of the cybersecurity talent. Nevertheless, cybersecurity jobs in healthcare, local government, finance, education, etc., are also available. While some metropolitan areas have a huge demand for cyber forensics or investigative skills (take Washington D.C. for example), cybersecurity talent demand in Orlando is focused on managing, operating and securing each organization's own digital networks and assets.

This increases the need for mid-career managers, as opposed to entry-level hires, who have honed their collaboration, communication and problem-solving skills over time. Soft skills, or power skills, outrank raw technical ability in terms of importance for cybersecurity workers.

However, with only enough supply to meet 71 percent of demand (just slightly better than the national average), Orlando employers need new tactics for hiring and developing talent. There are multiple strategies for employers to pursue as a means of widening candidate pools.

The tactics sprinkled throughout this report are listed together below. While some reflect cybersecurity talent trends and needs, the tactics represent general strategies that could be applied to any industry facing workforce development challenges.

1. **Use a common language for job descriptions.** This makes it easier to compare roles from one company to another, develop in-demand training programs, and helps potential hires understand the job requirements. The NICE Framework offers a pre-existing, national standard to use as a common language.
2. **Elevate soft skills in job postings.** Orlando employers have repeatedly touted the importance of skills such as collaboration and creativity when describing their talent needs. Job postings that elevate these skills as required and demonstrate a willingness to train on more technical skill sets open the talent pool to a wider audience.
3. **Use clear task descriptions to define roles** Skills-based hiring does not mean simply adding a long list of skills to job postings. When clear task descriptions are used in conjunction with the skills they require, candidates can clearly imagine themselves in the role and imagine how their own skills may transfer into the field.
4. **Remove unnecessary requirements from job descriptions.** Bachelor's degrees are only one avenue to gaining the skill necessary for a cybersecurity job. Removing degree requirements and clearly listing the skills required for a job opens the talent pool to individuals who may have gained their skills from experience in a different industry or through self-learning. This also serves to diversify the talent pool.
5. **Pay for certifications when possible.** The cost of certifications is the No. 1 barrier to an individual's career progress in cybersecurity. Listing certifications as preferred, when possible, and clearly offering to pick up the tab as a professional development perk, also widens the pool of potential talent.

ORLANDO ECONOMIC PARTNERSHIP

Re-Imagining Orlando's Talent Supply

AN ORLANDO CYBERSECURITY TALENT DEEP DIVE

Download this report and all other reports from the Foundation for Orlando's Future at **Orlando.org/reports**

OFFERING THE PARTNERSHIP'S ASSISTANCE:

Danielle Permenter
Vice President
Talent & Community Development
danielle.permenter@orlando.org

Conclusion Cont...

Complementary strategies for Orlando's higher education institutions include:

1. **"Skillify" syllabi using the same common language.** The benefits of the NICE Framework include its use of common language, not only for employers but also educators. Using this language to define syllabi directly links learning outcomes to opportunities for employment, un-muddying the path for new entrants to the field.

2. **Collaborate with industry to build rapid credentialing programs.** Many programs currently exist in the region to teach cybersecurity skills. Working directly with employers to build on these options and develop rapid credentialing programs that are designed for adult learners and minimize costs would continue to remove barriers.

Thankfully, the region is not starting from scratch. Orlando's collaborative spirit and problem-solving culture means that top industry and education leaders have already begun the process of coming together to discuss their mutual needs and common language. Consider the lists above as starting points that could be implemented all together or one-by-one.

Events of the last few years prove a great need exists to develop cybersecurity talent. But, it is also imperative to do it equitably and with the needs of the worker in mind. By approaching these challenges with the mindset of removing barriers to development, the Orlando region continues to work toward the goal of reaching Broad-based Prosperity® in a technologically advanced region.

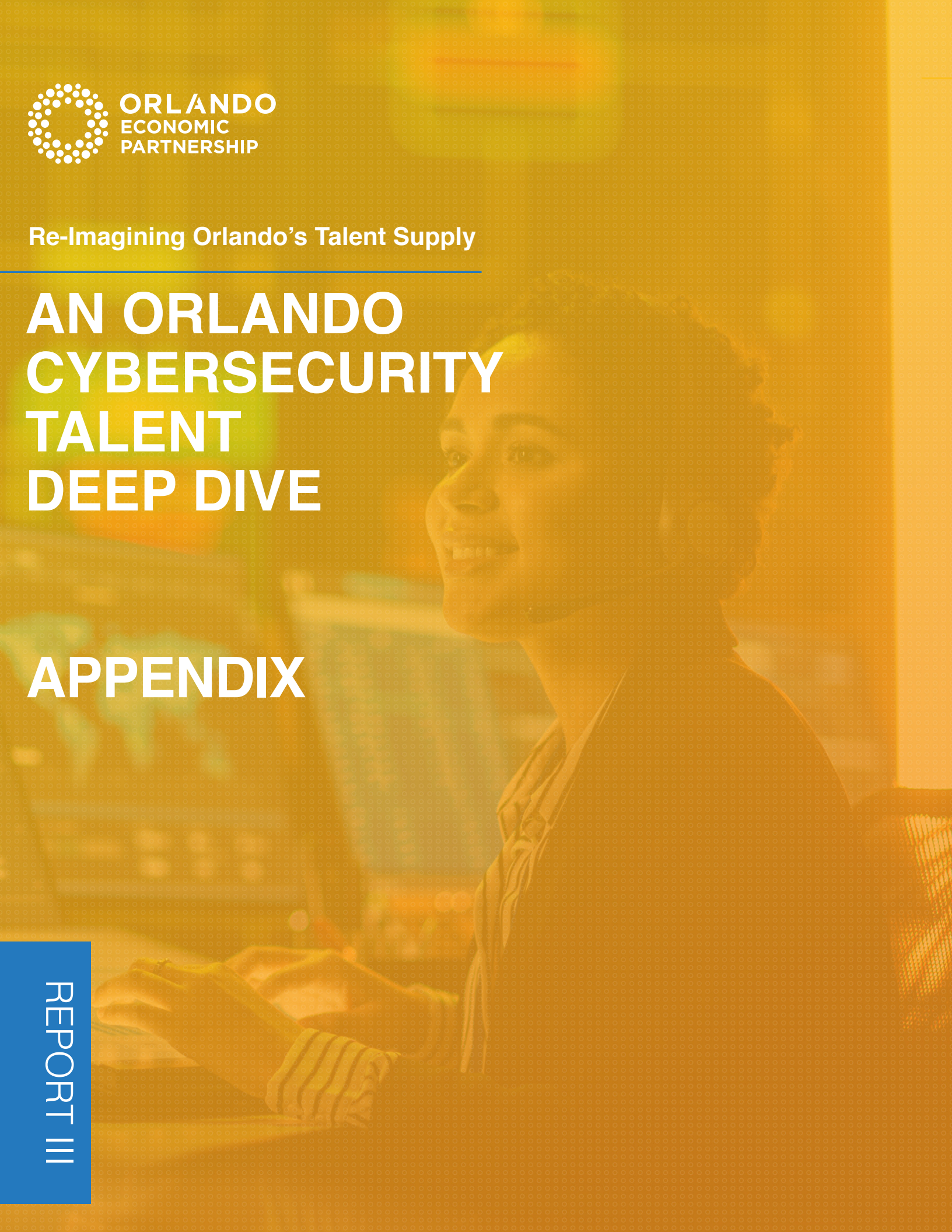
ORLANDO ECONOMIC PARTNERSHIP

Re-Imagining Orlando's Talent Supply

AN ORLANDO CYBERSECURITY TALENT DEEP DIVE

APPENDIX

REPORT III



Appendix A

In Order of Reference

Introduction

- Cyber Seek Heatmap - https://www.cyberseek.org/heatmap.html
- Orlando's Top 75 Employers - https://business.orlando.org/l/data-downloads/

Section One

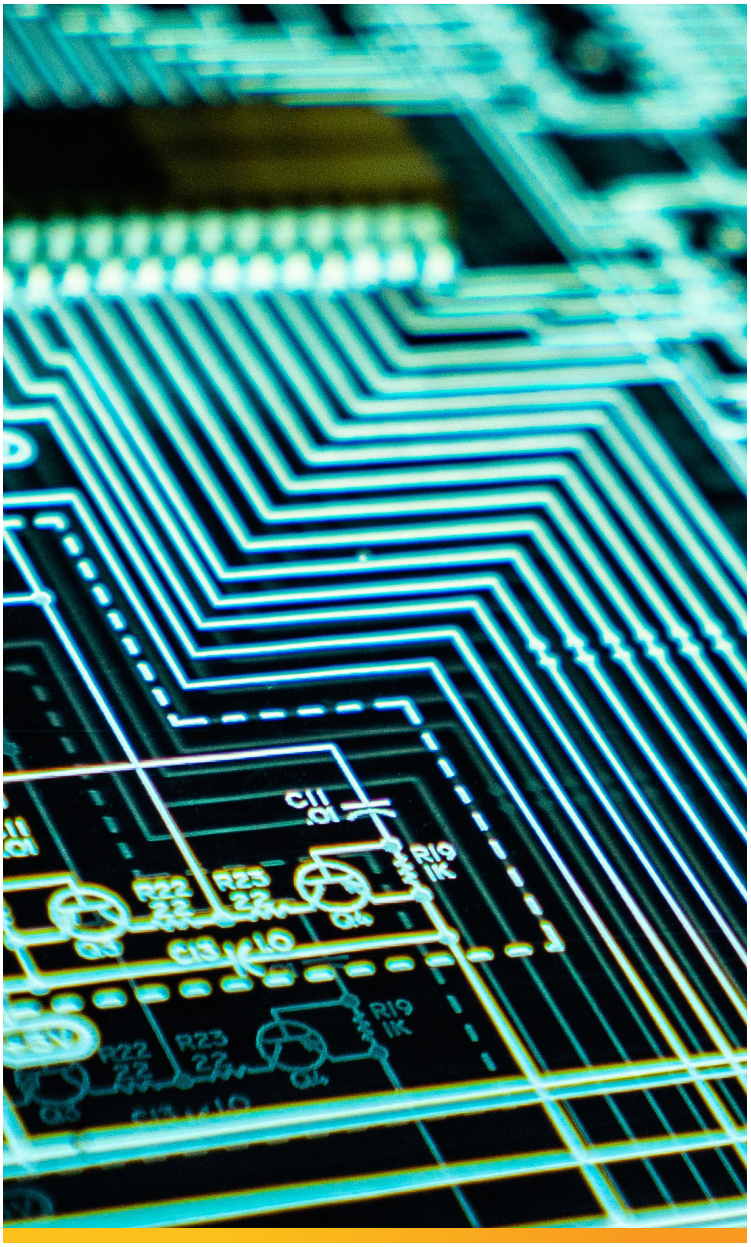
- EMSI Job Posting Optimizer - https://skills.emsidata.com/posting-optimizer
- The Nice Framework Resource Center - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice

Section Three

- Upskill Orlando Skills-Based Hiring Report - https://orlando.org/l/skills-based-hiring-report/

Section Four

- Cyber Seek's Education and Training Providers Map - https://www.cyberseek.org/training.html
- Florida Consortium of Metropolitan Research Universities - https://floridaconsortium.com/
- UpSkill Orlando Report, A Business Perspective on In-demand Skills - https://orlando.org/l/in-demand-skills-from-a-post-covid-19-economy/



ORLANDO ECONOMIC PARTNERSHIP

About the Orlando Economic Partnership

The Orlando Economic Partnership (the Partnership) is the Orlando region's economic and community development organization that is seizing the moment to advance Broad-based Prosperity® by growing the diversity of the economy and driving investment into the region. The Partnership catalyzes the collaborative ethos of the region to fuel regional leadership and improve the region's competitiveness. For more information, visit Orlando.org.

This report was made possible through the generous contributions of

JPMorgan Chase & Co.

200 S. Orange Avenue, Suite 200, Orlando, FL 32801 | 407.422.7159