



REWORK AMERICA
ALLIANCE
— A MARKLE INITIATIVE

Hiring Toolkit

Cybersecurity Analyst



Customizable, Ready-To-Use Resources

Included in this toolkit:

- **An inclusive, skills-based job posting**
- **Sourcing channels to reach a more diverse set of candidates**
- **Resume screening guide**
- **Skills-based interview guide and evaluation rubric**
- **Interviewee selection tool**
- **Onboarding plan**

CYBERSECURITY ANALYST TOOLKIT

Introduction	3
Skills-Based Approach in Action	4
Job Posting Template	5-7
Skill Comparison Guide	8
Resume Screening Guide	9-10
Interview Guide & Evaluation Rubric	11
Interview Guide Template	12-15
Assessment Template	16
Interviewee Selection Tool	17-18
Onboarding Plan	19
Blank New Hire Onboarding Plan	20
Example: New Hire Onboarding Plans	21-23
Sourcing Channels (In Development)	24-25

**The Rework America Alliance would like to thank the following partners
for their support in creating this resource.**



Introduction

The Rework America Alliance



Helping millions of workers from low-wage roles move into better jobs.

The Rework America Alliance is a unique partnership of civil rights organizations, nonprofits, private sector employers, labor unions, educators, and others helping workers from low-wage roles move into better jobs. The Alliance is opening opportunities for workers who have built capabilities through experience but do not have a bachelor's degree, particularly for people of color who have been disproportionately impacted by the current economic crisis.

As part of that work, the Alliance is developing a series of resources to help employers adopt more inclusive, skills-based talent management practices. This includes enabling employers to remove bias from the hiring process, better recognize the capabilities of candidates, increase diversity, and support their local communities.

What's included in the toolkit

This toolkit has customizable, ready-to-use resources to help you take a skills-based approach to sourcing and hiring talent for: **Cybersecurity Analyst**, a job that is projected to experience significant growth over the next 6-12 months and is accessible to many displaced workers based on their existing skills and / or minimal additional training.

- **Skills-based job posting:** Customizable job posting that highlights role-specific required and preferred skills and uses inclusive language. Designed to help you engage candidates and attract a diverse pool.
- **Resume screening guide:** Rubric outlining the role-specific required skills to help remove bias and keep resume reviews focused on the critical skills new hires need for the role.
- **Interview guide and evaluation rubric:** Questions specifically designed to assess skill against required skills and an accompanying rubric for evaluating responses. Asking all candidates the same skills-based questions reduces bias and makes it easier to compare candidate responses.
- **Interviewee selection tool:** Tool that aggregates candidate scores on interview questions and assessments to inform candidate selection.
- **Onboarding plan:** Sample plan to get new hires up to speed and ready to contribute
- **Sourcing channels (in development):** Starter lists of job boards, career fairs, and other channels to diversify and improve your candidate pool.

What are inclusive, skills-based practices?

Rather than relying on education, credentials, past experience, and other proxies for ability, a skills-based strategy recognizes that there are many ways to acquire knowledge and ability. Skills-based practices help employers identify and articulate the skills needed in a role and build processes for assessing and validating those skills.

Implementing inclusive skills-based hiring practices can help employers reduce bias and increase diversity, identify and articulate the skills needed in a role, fill skill gaps, support career development, reduce turnover rates, and open the door to more skilled employees from various backgrounds and industries.

[Research](#) has shown that hiring based on skills is 5x more predictive of future performance than hiring for education and 2.5x more predictive than hiring for work experience.

Want to learn more about skills-based practices?

Check out the Rework America Alliance's [Sourcing & Hiring Playbook](#) to get step-by-step advice, case studies, resources, and tips from leading employers on how to implement key skills-based talent practices.

Focusing on Skills Helps Job Seekers and Employers

Where a pedigree-based approach tends to result in new hires with the same background and experiences as existing staff, a skills-based approach enables organizations to leverage a wider talent pool and build a more diverse and high-quality workforce.

This approach also enables workers to see how their experiences and skills could help them succeed as a Cybersecurity Analyst.

For the Cybersecurity Analyst Role:



New sourcing channels enable companies to engage a broader set of candidates.

Example: By partnering with relevant IT & Cybersecurity training programs, employers are able to find a displaced **Delivery Services Driver** who has the skills to succeed as a Cybersecurity Analyst.



Job posting helps candidates see themselves in the role and apply.

Example: A **Retail Worker** realizes that her lack of a 4-year degree does not disqualify her for a Cybersecurity Analyst job and instead recognizes how her organizational and communication skills make her a great fit for the role.



Skills-based resume screen recognizes the candidate's abilities.

Example: Resume reviewers are able to recognize how a **Customer Service Representative from the hospitality industry's** interpersonal (e.g., active listening) and technical skills (e.g., Office Management Tools) will translate to the role.



Skills-based interview enables the candidate to showcase skills.

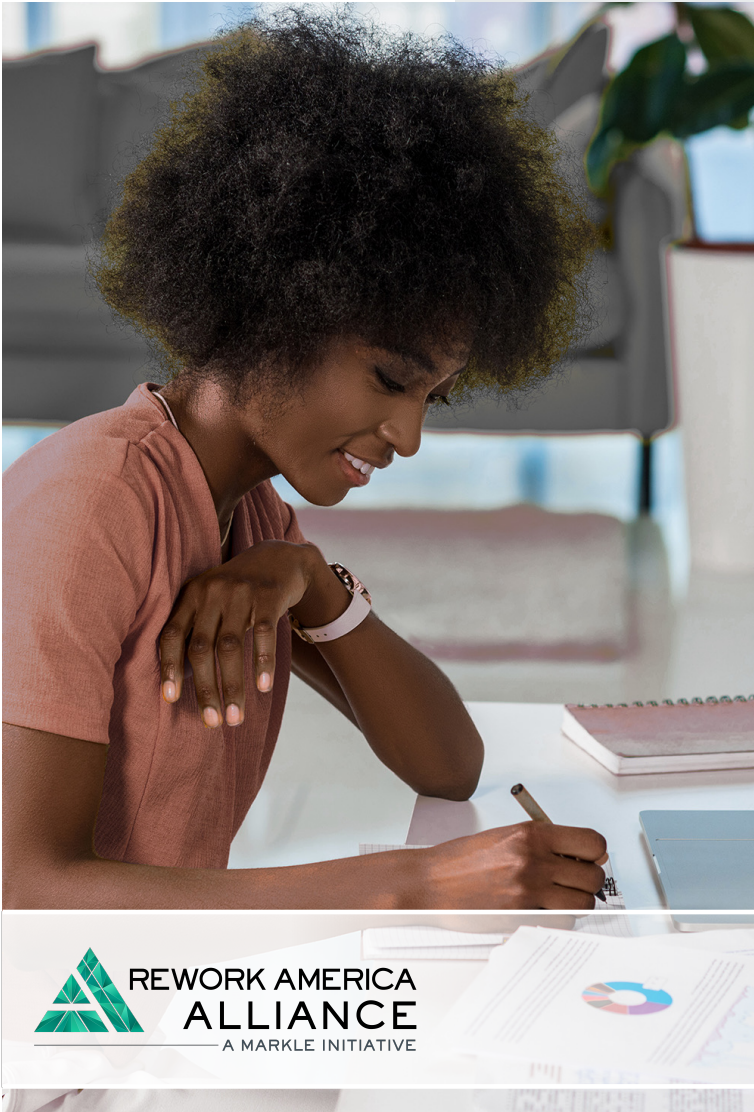
Example: In a skills-based interview, a **Waiter** demonstrates his service orientation, good judgement, and decision-making skills; interviewers recognize how these skills make him a good fit for the Cybersecurity Analyst role.



Enhanced onboarding sets the new hire up for success.

Example: A thoughtful onboarding plan helps a former **Receptionist** identify additional IT & Cyber-specific training courses to build out any gaps in skills needed for the Cybersecurity Analyst role.

Job Posting Template



Why Inclusive, Skills-Based Hiring Matters

Struggling to attract a diverse, job-ready candidate pool?

Your job posting could be turning top candidates away.

An inclusive, skills-based job posting removes bias-prone credential requirements that dissuade potential candidates – especially those from more marginalized communities – from applying.

It replaces them with descriptions of the responsibilities of the role and the skills needed to succeed, enabling candidates to visualize how their background and abilities might translate to the job. It also provides additional detail on the role, workplace culture, and compensation.

Want to learn more about how to write an inclusive, skills-based job description?

 Check out the [Job Description](#) section of our Sourcing & Hiring Playbook.

Instructions for use:

1. Add company-specific elements to the job posting, including a company overview and job details (e.g., salary, benefits, location).
2. Review list of required and preferred skills and their definitions. Adjust as needed.
3. Share final draft with a diverse set of employees to gather feedback and spot potential bias.
4. Begin sourcing candidates. Add to your company website, distribute to partners, and post with a diverse set of sourcing channels.



Download Customizable Job Posting Template [Here](#)

Job Posting Template

Cybersecurity Analyst

This toolkit model is an example of how to structure a skills-based job posting. Everything included in this toolkit can be tailored to each company's own needs.

Company Overview:

Job Summary and Responsibilities:

Cybersecurity analysts plan, implement, upgrade, and monitor security measures for the protection of an organization's systems, computer, networks and data. Security analysts are responsible for recognizing, communicating, and triaging security threats and working with internal and external clients, other technical positions, and members of the security team to resolve threats. Key responsibilities include maintaining the organization's firewall and other security systems, providing security risk analysis to management. Security analysts must be comfortable incorporating an active learning approach to stay up-to-date with latest security threats, trends in security control technology, and supporting technical skills needed to perform daily tasks.

Example Activities:

- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security
- Resolve security threats from every day, limited problems (e.g., desktop virus) and handle serious, system-wide threats (e.g., firewalls and intrusion prevention systems, virus propagating across the network and sending data externally).
- Develop plans, policies, and procedures to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs
- Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated
- Monitor use of data files and regulate access to safeguard information in computer files

Required Skills:

Required Technical Skills

- **Core Operating Systems (Security Monitoring & Event Analysis):** Ability to monitor multiple core operating systems (e.g., Windows, Linux, iOS, Android) for computer and mobile devices in local and enterprise-wide scenarios (e.g., understanding log analysis, malware analysis, threat hunting, etc.).
- **Infrastructure Design:** Capabilities related to the architecture and topology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.
- **Information Systems and Network Security:** Apply concepts related to the methods, tools, and procedures—including development of information security plans—to detect, respond, and protect information, information systems, and networks from risks and to provide or restore security of information systems and network services

Job Posting Template

Cybersecurity Analyst

Required Interpersonal Skills

- **Critical Thinking:** Use thorough critical analysis to identify risks and rewards of alternative solutions, conclusions, or approaches to problems related to security controls; use independent thought to think outside the box when looking for problems and resolutions.
- **Active Listening:** Give full attention to what superiors and clients are saying, taking care to fully understand by restating what's said, and asking questions to clarify as needed; provide enough feedback to make sure the other person thoroughly understood what has been said.
- **Strategic Planning:** Formulate effective tactics and metrics associated with the vision, mission, goals, and objectives of the organization or business unit.

Preferred Skills:

Preferred Technical Skills

- **Vulnerabilities Assessment:** Assess vulnerabilities and develop and recommend appropriate mitigation countermeasures for potential risks in systems network, operating systems, and protocols through the use of security principles, methods, and tools to improve security of all systems.

Preferred Interpersonal Skills

- **Complex Problem Solving:** Determining the accuracy and relevance of information; using sound judgment to generate and evaluate alternatives; and making well-informed, objective recommendations and decisions that take into account facts, goals, constraints, and risks while perceiving the impact and implications of the decisions.
- **Active Learning:** Take initiative on one's own learning to better improve understanding of new and existing threats, be aware of updates to network and operating systems, and learn new protocols for improving and maintaining security of relevant systems..

Required Certifications:

Job Details:

Location:

Department:

Salary or Hourly Pay Range:

Benefits:

Full / Part-Time Status:

Travel requirements and any night / weekend work:

Working conditions – remote vs. In-person, any physical requirements

Insert Additional details:

Inclusivity Statement:

The Rework America Alliance's Cybersecurity Analyst toolkit has been built in partnership with the National Initiative for Cybersecurity Education (NICE).

Download this guide for more detailed information about Cybersecurity Analyst skills, definitions and tasks: www.nist.gov/document/supplementnicespecialtyareasandworkrolesandtasksxlsx

Technical vs. Interpersonal Skills

Technical Skills

These skills are specific to an industry or job. These skills are the technical skills a person needs to perform narrowly defined tasks and duties.

Interpersonal Skills

These skills are professional knowledge and skills that are transferable from one job to another and across industries.

Required vs. Preferred

Limiting your requirements to what is truly required increases your chances of finding a candidate with the skills needed to get the job done.

		SKILL TRAINABILITY	
		Trainable	Non-Trainable
IMPORTANCE	Essential Job Duties	<p>Preferred: Skill is needed but can be trained after hiring.</p>	<p>Required: Skill is needed to perform job duties and cannot be trained.</p>
	Non-Essential	<p>Preferred: Skill can be learned over time to improve job performance.</p>	<p>Preferred: Skill is not necessary, but having it improves job performance.</p>

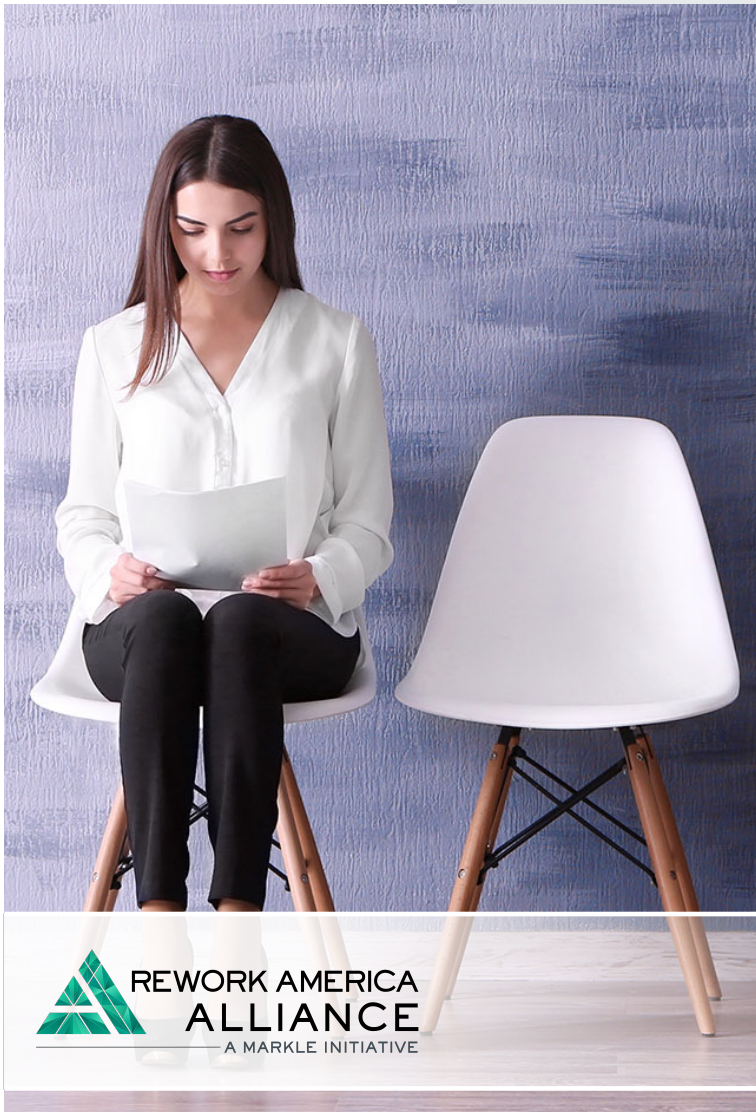
Required Skills

These skills are necessary to perform essential job duties at the specified level and there is no capacity to train; therefore, a candidate must have them on day one to complete job responsibilities.

Preferred Skills

These skills can be trained during onboarding and/or are used to perform non-essential job duties.

Resume Screening Guide



Why Inclusive, Skills-Based Screening Matters


Don't overlook the best candidates.

Traditional screening approaches are time-consuming and bias-prone.

Many of your top candidates, especially those from diverse backgrounds and those without a 4-year college degree, never make it to the interview stage.

Inclusive, skills-based screening focuses on whether candidates have the skills necessary to do the job regardless of where those skills were acquired.

Want to learn more about taking a skills-based approach to screening candidates?

 Check out the [Screening](#) section of our Sourcing & Hiring Playbook.

Instructions for use:

1. Ensure all required skills listed in your job posting are included in the left column of the guide.
2. Share the resume screening guide with the team involved in resume reviews. To help protect against bias, where possible have multiple team members from different backgrounds and departments review resumes.
3. Use the screening guide to inform which applicants advance to the next round of the hiring process. If using multiple reviewers, discuss any discrepancies between their evaluations.



Download Customizable Resume Screening Guide [Here](#)

Candidate Resume Screening Guide

Cybersecurity Analyst

Instructions for use:

- Use the table below to track whether a resume contains evidence of required skills.
- Scan through each resume to determine whether the candidate demonstrates the skill, is missing the skill, or if it is unclear.
- Appropriately mark resumes against each skill, and use the chart to compare resumes and help select candidates to interview.
- Some skills are easier to identify in a resume than others. Focus on required skills that you can reasonably expect to identify in a resume.

Identify whether this skill is:

Demonstrated	Missing	Might Have
Y (or) ✓	X	?

REQUIRED SKILL TO EVALUATE:	Resume / Candidate:									
	1	2	3	4	5	6	7	8	9	10
Core Operating Systems										
Infrastructure Design										
Info. Systems & Network Security										
Critical Thinking										
Active Learning										
Strategic Planning										

Preferred skills should not be evaluated at the resume screening stage.

REQUIRED SKILL TO EVALUATE:	11	12	13	14	15	16	17	18	19	20
Core Operating Systems										
Infrastructure Design										
Info. Systems & Network Security										
Critical Thinking										
Active Learning										
Strategic Planning										

Preferred skills should not be evaluated at the resume screening stage.

Interview Guide & Evaluation Rubric



The interview process is one of the points in the recruiting process in which the greatest number of qualified, diverse candidates and candidates without a 4-year college degree are unintentionally screened out as interviewers select candidates most like themselves or those already in the organization.

This process prevents employers from hiring the best talent and adding diversity to the organization.

An inclusive, skills-based interview works to combat “like-me” bias by providing a structured, consistent approach that focuses on the skills new hires need to possess for the role and ensures all candidates are asked the same questions.

Scoring candidates on a consistent 1-5 scale for each skill further ensures interviews are focused on evaluating critical skills.

Note: With many interviews shifting to remote environments during the COVID-19 pandemic, make sure to consider interview environment and offer phone interviews for people who may not have access to broadband or connected devices.

Want to learn more about taking a skills-based approach to interviewing candidates?

 Check out the [Interview & Selection](#) section of our Sourcing & Hiring Playbook.

Instructions for use:

1. Review the list of required and preferred skills in your job posting. Ensure there is at least one interview question to evaluate each skill.
2. Review the list of questions in the template. Adjust as necessary.
3. Review the evaluation rubric associated with each question. Adjust as necessary.
4. Share the interview guide with a diverse set of employees for feedback to help spot bias.
5. Equip interviewers with the final interview guide and evaluation rubric. Ensure all candidates are asked the same questions to reduce bias and make it easier for interviewers to compare candidates. Ask interviewers to complete the evaluation rubric during, or immediately following, the interview.



Download Interview Guide and Evaluation Rubric [Here](#)

Interview Guide Template

Cybersecurity Analyst

Instructions for use:

- Each question in this guide is designed to evaluate a specific required skill for the job.
- You can use the boxes beneath each question to take notes and record interview responses.
- Make sure to ask all candidates the same questions to make it easier to compare their abilities.
- Assign a numerical score for each question using the rubric as a guide.

Candidate Name:

Candidate #:

Interviewer:

Date:

Total Skills Score:

- Manually add together: [✓] Required and [★] Preferred skills scores from the following sections
-

[✓] Required Skills:

Foundation Setting

[✓] **Your Score:**

QUESTION: Tell us a little bit about yourself in relation to this specific position.

Rating	Description of Rating
1	Lowest Failed to explain previously related skill attainment & use of skills related to the position
2	Explained previously unrelated experience, did not demonstrate any skill attainment or skills correlated to required skills
3	Explained previously related experience but did not demonstrate skill attainment or correlate skills to required skills
4	Explained previous experience and skill attainment but did not correlate skills to required skills
5	Highest Fully explained previous skill attainment and directly aligned skills with required skills

Interview Guide Template

Cybersecurity Analyst

[✓] Required Skills:

Skill: Core Operating Systems (Security Monitoring & Event Analysis)

[✓] Your Score:

QUESTION: In this role you will be responsible for working closely with the IT department. How will you work with IT to ensure updates to the operating system do not create potential security risks?

1	Lowest Failed to provide response
2	Approaches failed to adequately address scope of the problem
3	Had thoughtful ideas that could be applied
4	Provided clear steps to maintain proper security
5	Highest Could provide broad strategy that included communication techniques in addition to technical resolution

Skill: Infrastructure Design

[✓] Your Score:

QUESTION: Tell us about a time in which you collaborated with a network administrator or department. How did you support security aspects of the network in collaboration with the administrator?

1	Lowest No examples of collaboration with network administrator
2	Brief collaboration with network administrators
3	Worked on or closely with network administrative teams
4	Ongoing collaboration with teams and clear approaches for supporting security
5	Highest Thoughtful approaches to collaboration and distinction of duties

Skill: Information Systems and Network Security

[✓] Your Score:

QUESTION: Tell us about a time in which you lead a resolution to a security threat. What ensured your success in resolving the threat?

1	Lowest Never resolved a security threat
2	Shared experience being involved with security resolution
3	Relied on expertise of others, but demonstrated learning from their example
4	Resolved threats, but lacked clear methods that they follow
5	Highest Resolved threats and had clear steps for future threat resolution

Interview Guide Template

Cybersecurity Analyst

[✓] Required Skills:

Skill: Critical Thinking

[✓] Your Score:

QUESTION: Tell us about a time in which you encountered a unique security threat. What steps did you take to respond to an unfamiliar threat?

1	Lowest Has not responded to security threats outside the scope of their training
2	Depended solely on the expertise of others to solve the problem
3	Evaluated key areas where improvements could be made
4	Used logical steps to evaluate the problem
5	Highest Applied logical steps to evaluate the problem and successfully triaged with other teams

Skill: Active Listening

[✓] Your Score:

QUESTION: In this role, you will have various teams and departments to provide security support for. What questions will you use to gather needed information on potential risk factors?

1	Lowest No clear methods for collaboration
2	Questions are basic and do not ask for proper depth for threat assessment
3	Key set of questions, but gaps in key areas for threat assessment
4	Structured and effective questions
5	Highest Understood nuances of different department needs and could provide examples unique to different teams

Skill: Strategic Planning

[✓] Your Score:

QUESTION: A security breach occurs on a system that you are monitoring. What steps do you communicate and triage relevant people and departments?

1	Lowest Demonstrates a lack of strategic planning capabilities
2	Provides 1-2 steps for a plan
3	Has a plan for triage and next steps
4	Plan is coherent and accounts for needed considerations
5	Highest Integrates a holistic view of the problem, including information gathering, communicating, and triage

Interview Guide Template

Cybersecurity Analyst

[★] Preferred Skills:

Skill: Vulnerabilities Assessment

[★] Your Score:

QUESTION: What are your steps to running a successful vulnerability assessment? What indicators of problems do you look for?

1	Lowest Lack of knowledge of running vulnerabilities assessment
2	Conceptual understanding, lack of practice
3	Run vulnerability assessments as a supportive member on the security team
4	Identify key steps
5	Highest Provide key steps and potential indicators

Skill: Complex Problem Solving

[★] Your Score:

QUESTION: Your security team identifies a security problem in a key design of the network. The network administrator tells you the network design is a critical function. How do you approach this problem?

1	Lowest Demonstrates a lack of creativity and collaboration
2	Prioritizes security over function and overrules network admin
3	Attempts to encourage a different approach, leaving it to network admin to find an alternative way
4	Has thoughtful approach to better understand the complexity of the problem and potential solutions
5	Highest Thoughtful approach to applying knowledge of network systems and security to provide alternative solutions to the problem

Skill: Active Learning

[★] Your Score:

QUESTION: Our systems are constantly evolving, and our teams are making upgrades to software and networks routinely. What steps do you take to ensure you are up-to-date with latest relevant knowledge on security?

1	Lowest Demonstrates no methods of active learning
2	Relies on instruction of supervisor
3	Has passive methods of learning important updates
4	Provides evidence that candidate has taken various opportunities for learning outside what is provided by previous employers
5	Highest Routinely takes initiative on finding learning opportunities, conferences, video instruction, books, or other learning materials

Assessment Template

Cybersecurity Analyst

Instructions for use:

- During the final round interview, provide 30 minutes for candidates to complete the following assessment to evaluate skills required for the Cybersecurity Analyst.
- This is an open ended assessment and allows for the evaluation of skills that may be hard to evaluate by answers to interview questions.

Summary of the problem:

- You are running a routine vulnerabilities assessment.
- During your assessment, you find a potential threat in the network system that leaves vulnerabilities for a data leak to occur.
- At this moment, you are uncertain to what caused the vulnerability and if a leak has occurred or not.
- As you consider the above situation, answer the following questions:

1. What steps will you take to better understand the scope of the problem?
(Evaluates INFRASTRUCTURE DESIGN skill)

2. Who in the organization will you conduct a deeper threat analysis with?
(Evaluates ACTIVE LISTENING skill)

3. What steps will you take to triage the threat? (Evaluates STRATEGIC PLANNING skill)

- Please include which departments may need to be involved;
- Who will make decisions to respond to the threat; and
- What technical steps need to be done to resolve the problem.

Interviewee Selection Tool



The Decision

You've completed your interviews and assessed each candidate's skills.

How do you determine whom to hire?

Selection conversations are often prone to bias as interviewers describe “gut-feelings” or ‘a level of comfort’ with candidates who are most similar to themselves.

The comparison tool introduces some structure and objectivity to the process, enabling hiring teams to compare interviewee scores across skill areas.

The tool helps keep selection conversations focused on candidate skills and abilities.

Want to learn more about taking a skills-based approach to interviewing candidates?

📍 Check out the [Interview & Selection](#) section of our Sourcing & Hiring Playbook.

Instructions for use:

1. Ensure the skills outlined in the selection tool match the ones outlined in the job posting and interview guide.
2. Add the minimum required score for each skill to the first column. This score should be determined in advance and should reflect the team's capacity to train a new hire in that skill area.
3. For each applicant, enter the score(s) they received from each interviewer for each skill.
4. Use the notes column to capture additional feedback from interviewers.
5. Reference the scores to evaluate and compare candidates and inform selection.



Download Interviewee Selection Tool [Here](#)

Interviewee Selection Tool

Cybersecurity Analyst

Instructions for use:

- Use the template below to compare applicants during the interview and selection process.
- Ensure the skills match the ones outlined in the job posting and interview guide.
- Add the minimum required score for each skill. This score should be determined in advance and should reflect the team's capacity to train a new hire in that skill area.
- For each candidate (Resumes 1-10), enter the score(s) the candidate received for each skill listed from each interviewer (A / B).
- Use the notes column to capture additional feedback from interviewers.
- Reference the scores to evaluate and compare candidates and inform selection.

Interviewer A: _____

Interviewer B: _____

	Resume #	1		2		3		4		5	
	Candidate Name										
Required Skills:	(#)*	A	B	A	B	A	B	A	B	A	B
Core Operating Systems											
Infrastructure Design											
Info. Systems & Network Security											
Critical Thinking											
Active Learning											
Strategic Planning											
Preferred Skills:											
Vulnerabilities Assessment											
Complex Problem Solving											
Active Learning											
Total Score											

(#)*minimum score required (determine prior to interviews)

	Resume #	6		7		8		9		10	
	Candidate Name										
Required Skills:	(#)*	A	B	A	B	A	B	A	B	A	B
Core Operating Systems											
Infrastructure Design											
Info. Systems & Network Security											
Critical Thinking											
Active Learning											
Strategic Planning											
Preferred Skills:											
Vulnerabilities Assessment											
Complex Problem Solving											
Active Learning											
Total Score											

Onboarding Plan



Skills-Based Strategies Enable Customization and Training

While traditional onboarding plans are often one-size-fits-all initiatives that focus on compliance and HR, a skills-based strategy enables much more customization and training.

An effective skills-based hiring strategy provides you with a lot of information on the abilities a new hire currently possesses and needs to learn to perform in their new role.

This information enables you to tailor their onboarding plan to get them up to speed in areas identified as potential gaps.

Want to learn more about taking an inclusive, skills-based approach to onboarding candidates?

📍 Check out the [Onboarding](#) section of our Sourcing & Hiring Playbook.

Instructions for use:

1. Ensure that all required and preferred skills from your job posting are included in the left-hand side of the onboarding plan. The goal should be to get all new hires up to a baseline level of skill as quickly as possible to ensure they can effectively contribute.
2. Review the onboarding plan with hiring managers. Adjust activities as needed based on training resources available and staff capacity. Make sure to build in training opportunities (informal on-the-job and/or structured training) for each skill.
3. Work with managers to customize the onboarding plan to each new hire, referencing their interview and assessment evaluation forms to identify areas of relative weakness.
4. Spread out training and onboarding activities to avoid overwhelming new hires with too many activities in the first day or week. Align training with job responsibilities to improve retention.



Download Customizable Onboarding Template [Here](#)

Blank New Hire Onboarding Plan Cybersecurity Analyst



Employee Name:

Manager:

Date:

Administrative
 Coaching/mentorship
 Interpersonal
 Training

	Day 1	Week 1	Week 2	30 Days	60 Days
Core Operating Systems Procedures					
Infrastructure Design					
Information Systems and Network Security					
Critical Thinking					
Active Listening					
Strategic Planning					
Vulnerabilities Assessment					
Complex Problem Solving					
Active Learning					

Example: New Hire Onboarding Plan Cybersecurity Analyst

Employee Name: **Example Onboarding Plan**

Manager: **Note: This is only an example**

Date:

■ Administrative
 ■ Coaching/mentorship
 ■ Interpersonal
 ■ Training

	Day 1	Week 1	Week 2	30 Days	60 Days
Core Operating Systems Procedures		Access to software details and operating manuals	Peer introduction to operating systems and related security measures	Meets with other teams to align on areas for monitoring security risks	Check in with supervisor to discuss areas of risk
Infrastructure Design		Access to network operating manuals	Introduction to network admin		Briefing on previous threats and current operations to maintain network security
Information Systems and Network Security	Access to security systems and manuals	Meets and gets to know the security team	Employee is given demonstration of security measures that currently exist		
Critical Thinking		Employee is connected to peer mentor	Example Only		Employee identifies example problem and resolutions and gets feedback on plan by peer mentor
Active Listening	Introductions to team and relevant departments		Develop a set of questions with experienced peer to use to evaluate security threats when they occur in other departments	Practice questions with one department	

Table background colors in PowerPoint can be changed by going to Table Design -> Shading

Split the table across two slides for more writing space, or copy and paste the table into an excel worksheet for more versatility. Use the program that works best for your team.

Instructions for splitting table across two pages:

- 1. Duplicate Slide:** In the slides panel to the left, right click on slide -> Duplicate Slide
- 2. Delete Bottom Rows:** Highlight the bottom rows of this table that you do not want on the first page. Then -> right click -> Delete -> Delete Rows
- 3. Delete Top Rows:** Go to the duplicated slide. Select the top rows of the table already included on the first page. Then -> right click -> Delete -> Delete Rows

Example: New Hire Onboarding Plan Cybersecurity Analyst

Employee Name: **Example Onboarding Plan**

Manager: **Note: This is only an example**

Date:

Administrative
 Coaching/mentorship
 Interpersonal
 Training

	Day 1	Week 1	Week 2	30 Days	60 Days
Strategic Planning		Employee is provided template structure for planning a triage response to active threat		Employee is coached by experienced peer on how to communicate and make decisions for active threats	
Vulnerabilities Assessment				Training on vulnerabilities assessments specific to networks/ operating systems	Conduct vulnerability assessment with supervision of experienced peer
Complex Problem Solving				Participate in cybersecurity threat simulation	Review outcomes of team's performance and brainstorm activities to improve problem solving unfamiliar threats
Active Learning		Determine areas for desired training		Check in with supervisor to discuss areas of desired learning	Access to relevant learning materials

Example
Only

Table background colors in PowerPoint can be changed by going to Table Design -> Shading

Split the table across two slides for more writing space, or copy and paste the table into an excel worksheet for more versatility. Use the program that works best for your team.

Instructions for splitting table across two pages:

1. **Duplicate Slide:** In the slides panel to the left, right click on slide -> Duplicate Slide
2. **Delete Bottom Rows:** Highlight the bottom rows of this table that you do not want on the first page. Then -> right click -> Delete -> Delete Rows
3. **Delete Top Rows:** Go to the duplicated slide. Select the top rows of the table already included on the first page. Then -> right click -> Delete -> Delete Rows

Example: New Hire Onboarding Plan Cybersecurity Analyst

Employee Name: **Example Onboarding Plan**

Manager: **Note: This is only an example**

Date:

	Administrative		Coaching/mentorship		Interpersonal		Training	
	Day 1	Week 1	Week 2	30 Days	60 Days			
Core Operating Systems Procedures		Access to software details and operating manuals	Peer introduction to operating systems and related security measures	Meets with other teams to align on areas for monitoring security risks	Check in with supervisor to discuss areas of risk			
Infrastructure Design		Access to network operating manuals	Introduction to network admin		Briefing on previous threats and current operations to maintain network security			
Information Systems and Network Security	Access to security systems and manuals	Meets and gets to know the security team	Employee is given demonstration of security measures that currently exist					
Critical Thinking		Employee is connected to peer mentor			Employee identifies example problem and resolutions and gets feedback on plan by peer mentor			
Active Listening	Introductions to team and relevant departments		Develop a set of questions with experienced peer to use to evaluate security threats when they occur in other departments	Practice questions with one department				
Strategic Planning		Employee is provided template structure for planning a triage response to active threat		Employee is coached by experienced peer on how to communicate and make decisions for active threats				
Vulnerabilities Assessment				Training on vulnerabilities assessments specific to networks/operating systems	Conduct vulnerability assessment with supervision of experienced peer			
Complex Problem Solving				Participate in cybersecurity threat simulation	Review outcomes of team's performance and brainstorm activities to improve problem solving unfamiliar threats			
Active Learning		Determine areas for desired training		Check in with supervisor to discuss areas of desired learning	Access to relevant learning materials			

Example Only

Sourcing Channels



Expanding Sourcing Channels Enables You to Reach Untapped Pools of Talent

Traditional sourcing strategies focus on a narrow set of colleges, job boards, and peer companies.


The result is a homogenous candidate pool, inflated recruiting budgets, and lower retention as companies compete over a small subset of the workforce.

Expanding your sourcing channels enables you to reach untapped pools of talent, leading to better and more diverse hiring.

The information below provides a starter list of job boards, community organizations, and other tools to help reach and engage a more diverse candidate pool.



Want to learn more about diversity related sourcing channels?

 Check out the [Sourcing](#) section of our Sourcing & Hiring Playbook

IN DEVELOPMENT – We are working on adding to this section to help employers identify good sources for reaching and engaging candidates, including those who have been displaced by the COVID-19 crisis.

IN DEVELOPMENT

The following are examples of organizations available for partnership to help you diversify your talent pipeline and tips and suggestions for working with them.

Establish relationships with external resources for a diverse talent pipeline

Job-readiness organizations that provide screening and training for employability and job-specific skills:

- [UnidosUS](#)
- [National Urban League](#)
- [Goodwill](#)
- [UnitedWay](#)

Virtual career fairs and job boards designed for specific populations:

- **Applicants with disabilities:**
[Gettinghired](#), [Recruit Disability](#), [Hire Autism](#), [Blind Institute of Technology](#)
- **Veteran applicants:**
[Veteran Recruiting](#), [Hire Purpose](#)
- **Applicants with criminal records:**
[70 Million Jobs](#)
- **LGBTQ applicants:**
[Out for Undergrad](#), [Pink Jobs](#), [Campus Pride](#), [Out & Equal](#)
- **Black and Hispanic applicants:**
[Jopwell](#), [Diversity.com](#), [PDN Recruits](#), [iHispano](#), [Black Career Network](#), [Black Jobs](#), [Hispanic/Latino Professionals Association \(HLPAA\)](#)
- **Female applicants:**
[Fairygodboss](#), [PowerToFly](#), [Career Contessa](#) (focus on millennials),
[Female Executive Search](#) (focus on C-level candidates), [The Mom Project](#)
- **Immigrant and refugee applicants:** [Upwardly Global](#), [Amplio Recruiting](#)

Support existing apprenticeship and pre-apprenticeship programs

- [The U.S. Department of Labor – Apprenticeship Site](#) is a good source to help you develop and launch an apprentice program.