

An Employer's Guide to Writing Effective Cybersecurity Job Descriptions

A Tool for Hiring
Managers and Human
Resource (HR)
Professionals:

Connect, Collaborate
and Hire with Success.

September 2023



A project of the public Modernize Talent Management (MTM) working group, led by NICE under the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce. NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

We offer our thanks to the following companies whose representatives participated in workshops to prepare this guide.



An Employer’s Guide to Writing Effective Cybersecurity Job Descriptions

A Tool for Hiring Managers and Human Resource (HR) Professionals: Connect, Collaborate and Hire with Success.

Table of Contents

Introduction	1
Planning Your Hire	3
Activity 1: Create Your Hiring Ecosystem	4
Identifying Tasks, Knowledge, and Skills for the Job	5
Activity 2: Define Your Job	8
Assessing Candidates	10
Activity 3: Create an Assessment Rubric.....	11
Summary	12
Stay in Touch.....	12
Contributors.....	13
Appendix 1: Worked Example	14
Appendix 2: Partner Use Case (Google)	18

Quick Start

- Use this guidance before, during, and after writing a job description
 - Use the checklist to discuss organizational needs, identify your hiring ecosystem and plan your hire (page 4)
 - Use the Workforce Framework for Cybersecurity (NICE Framework) to help draft (or re-draft) your job description (p7)
 - Create an assessment rubric tied to your job description (p9)
 - Look at the appendices for examples of this process (draft > refine > create a rubric) (p12, 17)
-

Introduction

This document was created in collaboration with industry professionals and is intended for use by those who hire or are seeking to hire for cybersecurity roles. It was developed by the public Modernize Talent Management (MTM) working group in support of the NICE Strategic Plan: to align hiring requirements according to proficiency levels to better reflect candidate competencies and capabilities (Goal 3.3). This guide offers tactics and strategic guidance on how to:



We will walk through the stages of developing an effective job description: from planning to drafting and revising, finally creating an assessment rubric aligned to your job description for use during hiring.

A diverse workforce is good for business – our focus on knowledge and skills will help you create job descriptions that attract candidates from as many walks of life as possible.² Be aware that the greater diversity of candidates you seek, the more flexible your hiring solutions will need to be. When assessing candidates for example, especially those who may learn, communicate, or process information differently, providing alternatives to traditional verbal interviews is recommended. Best practices to open up the candidate aperture are imperative for some candidates and usually helpful for all. These include:

- Technical assessments and showcase options (e.g., inviting portfolio submissions).
- Permitting accommodations for any candidate seeking them.
- Transparency on the interviewing agenda, interviewers, expected questions, and break opportunities.

1. If you are not sure what this is, we recommend [Getting Started with the NICE Framework](#).

2. For guidance on creating inclusive job descriptions (seek feedback, reduce jargon...), see [this article](#) from Forbes.

Today's Cybersecurity Workforce

There is a large—and growing—cybersecurity workforce in the United States, in both public and private sectors (Figure 1).³ According to CyberSeek.org, 76% of private sector companies had difficulty recruiting and hiring security professionals in 2021. Of those, 25% cited their own job postings as unrealistic, and 29% said their HR department did not understand the skills required.⁴

HR professionals are key to a well-functioning hiring process. They support efforts to broaden recruitment, review positions, benchmark salaries, and engage with recruiters.⁵ However, they are not cybersecurity experts, and it is essential that they work closely with cybersecurity hiring managers throughout the hiring process to effectively recruit and retain cybersecurity expertise. Together, along with other relevant internal teams and recruiters, they form a **hiring ecosystem**. Making sure that you are developing job descriptions within this ecosystem is a first, and crucial, step to success.

You will learn more about the hiring ecosystem, get some hints on how to establish it in your organization, and learn how to work with the players in your own ecosystem to identify the organizational needs that will inform job requirements and hiring goals.

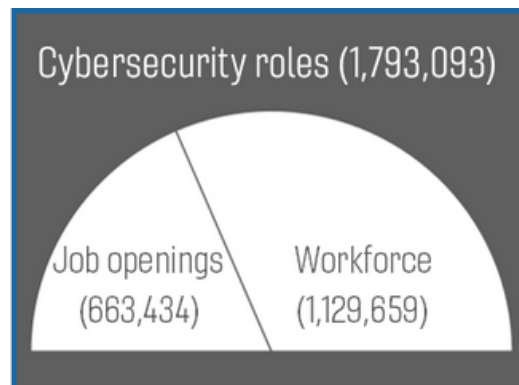



Figure 1: Cybersecurity jobs that have been filled (63%) versus available jobs (37%).

Diversity in Hiring

 This symbol highlights opportunities to demonstrate inclusive hiring practices. Use this to give your company more choice while clearly communicating diversity, equity, inclusion, belonging and accessibility objectives (DEIB, DEI or DEIA). This work also offers opportunities for collaboration across your organization which allows you to connect and educate internally.

Use this guidance to set realistic expectations, re-think qualification requirements, and understand the importance of hiring language.

3. Cybersecurity workforce data taken from CyberSeek, May 2023: <https://www.cyberseek.org/heatmap.html>
4. For more information, see [this 2021 report](#) from ESG & ISSA or [this webinar](#) from the SANS Institute about.
5. For more information, see [this report](#) from the UK Government (2022).

Planning Your Hire

Your organizational culture and hiring culture are intertwined. Every company has their own unique way of hiring, onboarding, developing and (eventually) saying goodbye to talent.

Quality hires come from seeking multiple perspectives, and job clarity,⁶ while breakdowns in communication can lower quality. To know your hiring ecosystem is to understand who the key players are, what their role is, and how they interact with one another during the recruitment process. You should also be aware of any external and internal forces that may impact your hiring efforts.

Figure 3 (next page) offers a template for identifying your hiring ecosystem: the community, environment, and interconnections within your organization. Consider your resources—will your hire involve one or two people? Does your organization have access to internal or external recruitment teams? Will you ask for employee input? own hiring ecosystem.

Understanding Organizational Context

The importance of understanding why your organization is hiring cannot be understated. Advances in technology, best practices, frameworks, threats, and regulation are dynamic workplace drivers that require a flexible, responsive approach to identifying talent requirements and hiring.

The 2020 COVID pandemic accelerated the transition towards Cloud technologies and services. This shift away from on-site data centers brought down operational costs and wiped millions of dollars in assets from balance sheets. Demand was created for skills and practices not readily available, and the scarcity of Cloud talent has been exacerbated by companies wanting to hire people with a lot of Cloud experience. This worsens the talent skills gap, as Cloud environments are difficult to navigate for even the most seasoned cybersecurity, infrastructure, and IT teams.

When hiring for current and future needs in the context of Cloud, legacy, or hybrid environments, a realistic viewpoint is recommended best practice:

1. Talent with the desired experience may not exist. If they do, they come at a higher price point.
2. Use questions to establish a candidate's appetite for skill development (i.e., becoming competent).
3. Be prepared to budget for upskilling or reskilling the new hire.

The hiring ecosystem

Community, environment, and the resulting interconnections needed to recruit employees into an organization.

This includes:

- Human components
- Institutional processes
- Different technologies.

Use Figure 3 to explore your own hiring ecosystem.

6. Brigitte Skeene, 2021, [Understanding the Hiring EcoSystem](#).

Activity 1: Create Your Hiring Ecosystem

Hold an all-hands kick-off meeting.

Consider the position you are hiring for. Collate information you have:

- What is your hiring budget?
- Do you have an existing job description, list of keywords, etc.?

Identify the information that you do not have:

- Draw out your hiring process.
- Who is in your hiring system? Map out who is (or should be) involved.
- Identify internal and external forces that may apply to your organization.

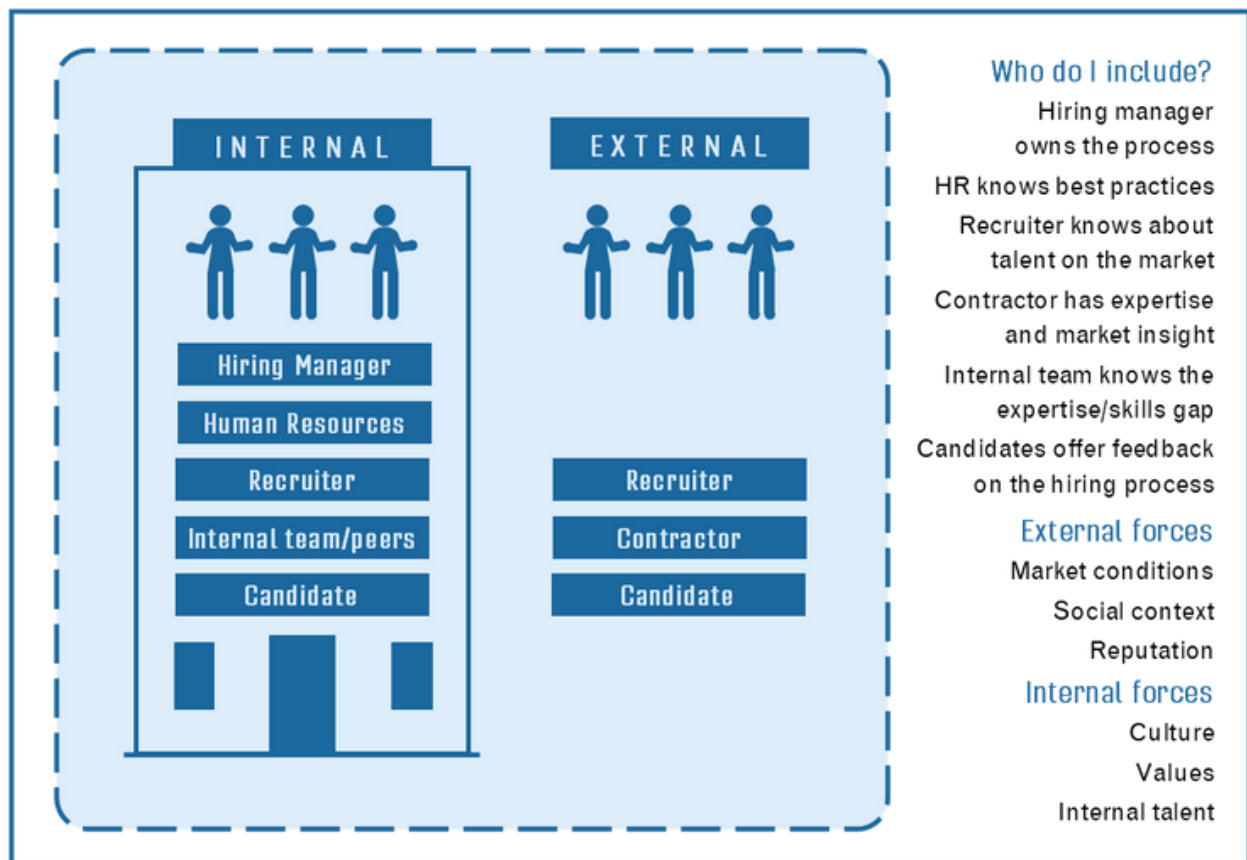


Figure 2: Template for mapping an organization's cybersecurity hiring ecosystem (find internal and external partners, forces & interconnections).

Identifying Tasks, Knowledge, and Skills for the Job

[ACTION] Create Task, Knowledge, and Skill Statements for your role.

[IMPACT] You will develop a job description with qualification requirements aligned to the NICE Framework and clarify the appropriateness of credentials for the role. This aligns with objectives 3.3.1 and 3.3.5 of the NICE Strategic Plan.

There is a gap in your organization that will be filled by this job. At this stage, you should have an understanding of the needs of your organization and have established a hiring ecosystem. The next step is to specify what the job will entail.

You will need to identify the responsibilities of the job so that they can be clearly defined in a job description. A clear job description helps to attract qualified candidates and can be used to establish candidate requirements. This helps with candidate assessment and later workforce management and development.

The NICE Framework serves as a starting point to help your team visualize what this new hire will be doing and learning on the job. You can signal to candidates the work that needs to be done, and what you expect them to be capable of.

The NICE Framework offers structure – once you have an idea of the work and the capabilities someone needs to complete that work, you can think about how competent you will require a candidate to be (i.e., their proficiencies). The NICE Framework provides a common language via Task, Knowledge, and Skill statements (see Table 1 for examples).

Statement types

Task: Define the work to be done. These activities achieve company objectives.

Knowledge: A set of concepts within memory. Candidates need to be able to discuss these ideas.

Skill: A candidate’s capacity to perform a certain action. Can be fundamentals, or more complex.

Task statements	Task: Determine appropriate level of test rigor for a given system.
	Task: Improve network security practices.
	Task: Integrate black-box security testing tools into quality assurance processes.
Knowledge statements	Knowledge of intrusion detection tools and techniques.
	Knowledge of network systems management principles and practices.
	Knowledge of virtual collaborative workspace tools and techniques.
Skill statements	Skill in scanning for vulnerabilities.
	Skill in identifying cybersecurity issues in partner interconnections.
	Skill in developing learning activities.

Table 1: Task, Knowledge and Skill (TKS) statements taken from the NICE Framework.

Identifying Tasks, Knowledge, and Skills for the Job (continued)

By starting with the NICE Framework, you are using language that is widely recognized and clearly signals job requirements to prospective employees. This also lays a foundation for the next stage of work—defining an assessment rubric to help you effectively and consistently compare candidates with different backgrounds, qualifications, and skillsets.

Within the NICE Framework, TKS Statements can be grouped into:

- **Work Roles:**⁷ Groupings of Tasks for which someone would be responsible.
- **Competency Areas:** Groupings of Skills and Knowledge that can be used to demonstrate capability in domains rather than a Work Role (e.g., foundational, or emerging areas of technology).⁸

Figure 3 illustrates how you might use either Work Roles or Competency Areas, depending on the focus of the job you are hiring for. Although they vary in scope, you may find that both perspectives can be helpful.

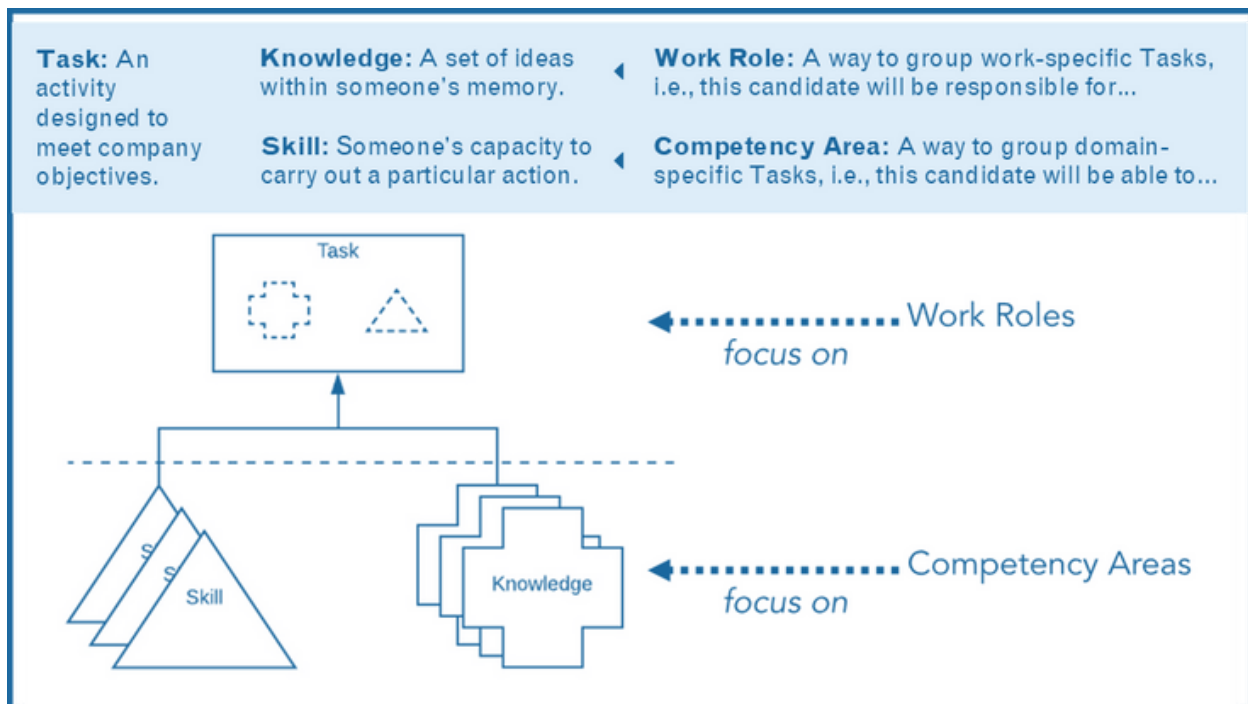


Figure 3: Separating Tasks, Knowledge and Skills into Work Roles and Competency Areas using the NICE Framework.

⁷ See [this resource page](#) from NIST for information on breaking Work Roles into Knowledge and Skill statements.

⁸ For a full list of NICE Framework TKS Statements, Work Roles, and Competency Areas visit www.nist.gov/nice/framework.

Identifying Tasks, Knowledge, and Skills for the Job (continued)

You can use Work Roles or Competency Areas to help you think about your organizational needs, what the candidate needs to be able to demonstrate, and where you may be willing to mentor an otherwise strong candidate. You can use the NICE Framework to develop a job description in different ways, including:

Start with Work Roles

- Use Work Roles to guide you to the roles closest to your job. These categories broadly describe the kind of work to be done (e.g., governance, design, defense, etc.). Choose a role that aligns with your job. You may need to draw from more than one Work Role.

Identify Tasks

- The Work Role/s you have selected list common tasks for each role. Use these as a starting point for the kind of work your position will be responsible for. Some tasks will not apply, and you may need to create some of your own. Pinpoint these context-specific tasks—include them in your job description.

Identify Knowledge and Skills

- Each Work Role includes Knowledge and Skill statements. Use these to identify the capabilities someone needs to complete the work. Review this list for any that should be included in your job description.

Identify Competency Areas

- You may want to include Competency Areas as part of your job description. If you have chosen a Work Roles, this will likely relate to work specific TKS statements. Competency Areas are more likely to represent Knowledge and Skills in foundational, emerging, or cross-cutting domains.

Activity 2: Define Your Job

Define the core responsibilities of the job and identify key knowledge and skills required for the position—i.e., the must-haves, and the nice-to-haves.

- What NICE Framework cybersecurity Work Roles and Competency Areas will the position be responsible for?⁹
- Will this position be responsible for all the Tasks under a Work Role? Are there any missing? Are any shared across a team? Do any NICE Framework Tasks need to be adjusted?
 - Are there any subject-specific knowledge or skills gaps in your description? This refers to networking, SIEM, data analysis, programming, customer service etc.
 - The NICE Framework offers a technical view. What professional knowledge and skills will you require? This refers to communication, problem solving, initiative etc.
- Which of the identified tasks will be needed on day one, and which can be learned on the job?
 - Are there areas your organization would be willing to offer mentorship in, for candidates that meet minimum qualifications but may need additional development?
- What academic degrees, industry-recognized certifications, work experience, or other credentials (if any) are required or preferred to show sufficient qualifications for the position?
 - Does your hiring process recognize those who are skilled through alternative routes? ¹⁰
 - Consider removing academic degrees as a non-negotiable requirement. In doing so, you remove a barrier to entry and show candidates that your focus is on meeting job requirements irrespective of the combination of experience and qualifications.
 - Encourage candidates to convey how their qualifications relate to the role!

Continues on next page.

⁹. You can search here: <https://niccs.cisa.gov/workforce-development/nice-framework/work-roles>

¹⁰. For more information on 'skilled through alternative routes' (STARs), see [this report](#) from the National Bureau of Economic Research.

Activity 2: Define Your Job (continued)

- Hiring is not just about defining the job, but also considering longer-term plans for the candidate.
 - Do you have a career pathway for this position?
 - Does your organization have internal training programs or professional development initiatives?
- Draft the job description.
 - Use the identified Work Roles, Competency Areas, and TKS statements to help you.
- Prioritize your non-negotiables and limit them to 3-5. Identify nice-to-haves.
- Be precise and concise.
 - What do you need?
 - How proficient do you need your candidates to be in each area that you will assess (entry, intermediate, advanced, other)?
 - Ensure that candidates with little to no experience can apply for entry-level positions.
- Consider where you will look for candidates:
 - Internal routes: Do you have internal candidates that you'd like to encourage to apply for the position? Can this role be filled by upskilling or reskilling an existing employee?
 - External routes: Are you posting in a variety of places where you may increase your candidate pool and reach a broadly diverse audience?

Assessing Candidates

Key question: Does this person have the skills and knowledge required to carry out the tasks needed for this position?

Key benefit: Knowing how to align your practices with the NICE Framework shows your organization is in line with evolving best practices around cybersecurity recruitment and talent development.

Use this guidance to open up your candidate aperture. A candidate's proficiency level is how capable they are of doing something, as defined on a scale.¹¹ Consider 'show vs. tell' as some skilled candidates can find it hard to perform under observation. You will create categories to describe the levels of skill and knowledge required for the position you want to hire for.

This group of categories (which we call a [rubric](#)) lets you:

- Measure how proficient candidates are.
- Identify whether candidates satisfy your job requirements. Some of your criteria will be rigid while others might be more flexible.

This lets your organization compare people with different backgrounds and qualifications for the role. A well-written job description speaks to a wide pool of potential candidates and defines specific duties and functions of the position to be filled. Considerable thought and effort are required to:

- Communicate the hiring process so that potential candidates know what to expect from the hiring organization.
- Provide criteria for assessment that allows a comparison of candidates.
- Describe necessary and preferred qualifications according to the job description.
- Define how candidates are screened (and assessed, if hired). Try to keep the job description short¹² and tell a story.
- Think in terms of skills. Skills-based hiring focuses on what a candidate can do rather than credentials alone.¹³
- Tell a story about organizational fit: what is the route into (and through) this job? Keep it simple, e.g., This job can lead to opportunities in... or 60% of people in this role go on to...
- Use language that is candidate focused. I.e., You are someone who is [X], rather than We are a company that does [Y].

¹¹. For a deeper dive into proficiency (those with a lower proficiency are led, those with higher proficiency are better equipped to lead), see this report from NIST.

¹². Shorter posts (300 words) receive more applications. See this article on talent acquisition.

¹³. For more information about skills-based hiring, see this article on talent strategy.

Activity 3: Create an Assessment Rubric

Be specific—vague language leaves room for interviewer bias.

- Consider the position you are hiring for and keep your expectations in line with what you need.
- Does your security analyst need to be excellent (a score of 4+ out of 5) at communicating? Why?
- Who will they need to communicate with?
- Could someone with low conversational skills (1 or 2 out of 5) be coached or mentored to succeed in this role?
- Consider how you will test candidates. You could use freeform or timed, written, or verbal tasks; you may choose to assess candidates on both professional and technical components.

An example of assessing 'Knowledge of...' on a scale of 1 [Lowest] - 5 [Highest]	
1-2	No/Some knowledge of a concept. Weak communication or demonstration. Candidate seems uninformed. No evidence of interest or further study. Seems uncomfortable with the topic of interest.
3	Intermediate level of knowledge. Candidate struggles to distinguish between different levels of abstraction or audience. Shows interest in the area. Seems comfortable with the topic of interest.
4-5	Subject matter expert. Describes examples of communicating complex ideas to multiple audiences or conveys importance of this and demonstrates. Clear interest in and knowledge of the area. Persuasive. Comfortable in discussion or demonstration, asks questions or signals for help, links ideas.
An example of assessing 'Skills in...' on a scale of 1 [Lowest] - 5 [Highest]	
1-2	Cannot convey examples of application or demonstrate skills. No portfolio or evidence of practice. Cannot discuss or demonstrate skills on resume. Candidate seems uncomfortable with practical application.
3	Can convey examples of practical application. Can demonstrate or discuss skills claimed on their resume. Shows interest in potential applications, may demonstrate confidence in conversation or demonstration
4-5	Confidently describes examples of practical application. Examples are specific and the candidate has a clear interest in and knowledge of the area. Comfortable in discussion and problem solving, asks questions, may link and apply new ideas.

Summary

- Know the proficiencies you will ask candidates to demonstrate, and which are the most important.
- Understand that you can hire from inside and outside of your organization. Upskilling allows your organization to increase knowledge and skills, whereas reskilling converts existing talent.
- Be mindful of the language you use to attract candidates: seek and be open to alternative and appropriate balances of qualification and experience (STARs); avoid language that emphasizes bias on the grounds of age, gender, race, disability, etc.; seek to accommodate neurodiverse candidates (i.e. show, don't tell).
- Know who is in your hiring ecosystem (internal & external) and keep communication channels clear.

Stay in Touch

This document is subject to ongoing edits and revisions.

Please send feedback via [this form](#), or submit comments to nice@nist.gov.

LinkedIn: <https://www.linkedin.com/company/nist-nice>

Twitter: [@NISTcyber](#)

The Modernize Talent Management (MTM) working group

The aim of this project of the Modernize Talent Management Working Group (MTM WG) is to help employers create effective and more attractive job descriptions, and more easily compare diverse candidates.

As a NICE public working group, MTM WG seeks to create actionable guidance based on the successful practices of exemplar organizations.

The Modernize Talent Management working group focuses on the NICE Strategic Plan goal to Modernize the Talent Management Process to Address Cybersecurity Skills Gaps. (Strategic Goal #3.)

The Workforce Framework for Cybersecurity (NICE Framework)

The NICE Framework establishes a standard approach and common language for describing cybersecurity work and learner capabilities. We hope to improve communication among stakeholders throughout the cybersecurity ecosystem, aligning employers, learners, and education and training providers.

NICE

The mission of NICE is to energize, promote, and coordinate a robust community to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

Contributors

Author: Arianna Schuler Scott, Senior Associate Director, Integrated Security Centre, Virginia Tech

NICE Modernize Talent Management working group contributors

Nelson Abbott, Senior Director, Advanced Program Operations, NPower

Liz Green, CEO, Occupational Therapist, Link OT

Cynthia H, Founder, Project Management Professional, Altor GRC, Inc.

Lynsey Caldwell, Cybersecurity Workforce Program Director, Leidos

Peter Meehan, SVP International & Partnerships, iQ4 Corporation/ Co-founder, Cybersecurity Workforce Alliance (CWA).

Terry L, Founder, Solutions Architect, Astrolytes

Dana Winner, President, (ISC)2 Kuwait

Megan Smith-Branch, Research Analyst, Lead Associate, Booz Allen Hamilton

Jo Justice, Business Information Security Office, Defense Group, Leidos (MTM WG Co-Chair)

Olesya Menon, Security Education Program Manager, Google (MTM WG Co-Chair)

Karen A. Wetzel, NICE Manager, NICE Framework, NIST

Marian Merritt, NICE Deputy Director and Lead for Industry Engagement, NIST

Expert Contributors

Donna M. Cusimano, Manager, Tech Apprenticeships, Workforce Solutions, CompTIA

Liz Fraumann*, Sr. Project Manager, synED – Cyber-Guild Program

Mike Prebil, IT Specialist (Security), NICE/NIST

Austin C, Leadership Program Manager, Cybersecurity and Infrastructure Security Agency (CISA)

Jorge Marquez, Senior Vice President, Apprenticeship Intermediary, Workforce Innovation and Diversity & Inclusion Leader, Robert Half

Miranda H, Director, Talent Acquisition, ForgeRock

*This project guide is dedicated to the memory of our beloved colleague **Elizabeth Ann “Liz” Fraumann** who passed away shortly after the completion of this project. She will be missed by all of us.*

Appendix 1: Worked Example

This appendix offers an example of rubric development for a Security Analyst position ([available online](#)). We will walk through a meeting between a hiring manager and HR representative.

Activity 1: Create Your Hiring Ecosystem

A conversation that we revisited over a period of time with: Hiring Manager + HR rep + External recruiter (cannot attend) + Team lead (for team we are hiring into).

Job description: initial edits ([Security Analyst](#))

We are seeking a self-starting and experienced security professional to join our team. Your passion for finding creative approaches to solve security problems will shine as you troubleshoot existing and create new security capabilities that close information gaps, strengthen our defenses, and defend some of the largest companies in the world from emerging security threats. We are a fast-paced team that constantly provides new opportunities to learn and grow.

Clearer description (+ more concise)

We are seeking a security professional to join our team. You will show us that you can take initiative and be creative when you need to troubleshoot and solve security problems. We are a solutions-focused team that constantly provides new opportunities to learn and grow.

Primary Responsibilities

- Collaborate with broader response teams. [*Add: to create risk remediation plans, escalating with urgency as necessary – they won't know our operations, so we will mentor. Needs to understand what risk is and what a response team does/frameworks etc.*]
- ~~Gather customer requirements and work with the development team to provide solution enhancements.~~ [*We do not need someone customer facing, we need an internal facing analyst.*]
- ~~Exhibit strong team and thought leadership and integrity in monitoring day to day domain security and vulnerability.~~ [*Instead: Exhibit personal integrity, teamwork and communication skills, and be comfortable owning and asking for help with relevant projects.*]

Qualifications

- ~~3+ years of~~ [*Evidence of professional*] cyber security experience using IAM, AD and SQL.
- Ability to analyze, interpret and present large sets of data to present across client teams, at all levels of management. [*This will need a development plan, comms is hard*]
- Strong deductive reasoning, critical thinking, problem solving, prioritization skills.
- ~~Ability to effectively~~ [*Can*] manage multiple efforts simultaneously. [*seeking support as necessary*].

Activity 2: Define Your Job

- ✓ **What is your hiring budget?** *Unknown, need to circle back [To do]. CompTIA tool recommends \$89-153k.*
- ✓ **Do you have an existing description or list of keywords?** *From our existing job description: identity & access management; data analysis; initiative, teamwork. CompTIA's Job Posting Optimizer suggests^[14]: tech skills (cybersecurity + vulnerability) and professional skills (management + problem solving). Recommended certifications: CISSP, Sec+ (removed management & vulnerability – not relevant to job)*
- ✓ **What NICE Framework cybersecurity Work Roles and Competency Areas will the position be responsible for?** *Used the search feature to look up "Security Analyst". No direct match, so looked at "Systems Security Analyst" Work Role.*
- ✓ **What academic degrees etc. are required or preferred?** *Degree not required. Would like to review portfolio/project work, etc.*
- ✓ **Required technical competencies:** *data analytics, identity and access management, documentation, cybersecurity, tools.*
- ✓ **Required professional competencies:** *communication, problem solving, initiative, teamwork.*
- ✓ **Are there areas your organization would be willing to offer mentorship in?** *Yes—candidate likely needs guidance with business communication, creating and managing risk remediation plans using our processes, and knowing when to escalate a situation.*
- ✓ **Do you have a career pathway for this position?** *Start as Security Analyst > progression > Progression through roles in Incident Response Teams. Could be technical or governance.*
- ✓ **Does your organization have internal training programs or professional development initiatives?** *Unknown—to be confirmed. Offer funds/time off for classes. Mentoring? [To do]*
- ✓ *Need candidate to be proficient in: Advanced: data analytics; documentation; problem solving; teamwork; initiative. Intermediate: identity and access management; cybersecurity; tools. Entry: communication.*
- ✓ **Non-negotiables:** *Candidate needs to know about risk and mitigation in identity and access management; needs data analysis skills; needs to want to work as part of a team; needs to be good at problem solving and asking for help when required.*
- ✓ **Nice-to-have:** *experience with security tools; they have an interest in cybersecurity; they can set up or create documentation; shows initiative.*
- ✓ **Internal routes: Can this role be filled by upskilling or reskilling an existing employee?** *Share internally. Revisit next week. [To do]*
- ✓ **External routes: Are you posting in a variety of places?** *Can we go on a podcast/guest-write a blog post for the local cyber range (Get sign-off to liaise with PR/communications office)? They have a conference & career fair coming up. Links to community colleges too. [To do]*

14. Found at <https://optimize.comptia.org>.

Activity 3: Create an Assessment Rubric

Work Role used: [Systems Security Analyst \(OM-ANA-001\)](#)

Looked at the Tasks, Knowledge, and Skills linked to the Work Role. This provisional list will need to go to the Risk Team for review. But We're narrowing down key requirements. Going through the checklist beforehand and identifying key competencies helped keep us on task.

X1234 = high proficiency required, X1234 = medium/will develop, X1234 = aware but not proficient.

Task	T0016	Apply security policies to meet security objectives of the system.
	T0017	Apply security principles to meet organizational confidentiality, integrity, and availability needs.
	T0085	Ensure system security operations and maintenance activities are documented and up to date.
	T0088	Ensure security control technologies reduce identified risk to an acceptable level.
	T0123	Implement specific cybersecurity countermeasures for systems and/or applications.
Knowledge	K0024	Knowledge of database systems.
	K0044	Knowledge of cybersecurity and privacy principles and organizational requirements.
	K0056	Knowledge of network access, identity, and access management.
	K0284	Knowledge of developing and applying user credential management system.
	K0297	Knowledge of countermeasure design for identified security risks.
Skill	S0031	Skill in developing and applying security system access controls.
	S0036	Skill in evaluating the adequacy of security designs.
	S0141	Skill in assessing security systems designs.
	S0147	Skill in assessing security controls based on cybersecurity principles and tenets.
	S0367	Skill to apply cybersecurity and privacy principles to organizational requirements.

Rubric for cybersecurity expertise. To do: identify a technical pre-task (will need to engage with Risk Team).

Go back to HR—how are we already measuring professional competencies (initiative etc.)?

In this rubric, **red lines** mark the desired proficiency for the candidate, for this job.

	0—1 Does not/marginally meets criteria	2—3 Meets the criteria	4—5 Exceeds criteria/exceptional	Total
Tasks (role-focus): looking for evidence of candidate having done an activity that met org. objectives				
	Candidate has not done this before.	Candidate has done this before.	Candidate also reflects on impact.	
T0016				
T0017				
T0085				
T0088				
T0123				
Knowledge (candidate-focus): looking for evidence of candidate being able to convey these ideas.				
	Candidate does not know this.	Candidate is curious/knows this.	Candidate also applies in scenario.	
K0024				
K0044				
K0056				
K0284				
K0297				
	Candidate cannot demonstrate.	Candidate can demonstrate.	Candidate also applies in exercise.	
S0031				
S0036				
S0141				
S0147				

Appendix 2: Partner Use Case (Google)

NICE Framework for Job Descriptions Trial / Working Session @ Google

Input provided by Google Recruiting

[NICE Framework](#) - Working Session

Part 1/3

We looked at the [existing job description](#) that has been recently approved for an open role in Google Cloud (screenshot below, in case the job is no longer available).

The screenshot shows a job listing for a Security Engineer, Detection and Response, Insider Threat role at Google. The listing includes the company name, location (Reston, VA, USA), and a blue 'Apply' button. Below the button, there are sections for 'Minimum qualifications', 'Preferred qualifications', 'Responsibilities', and 'About the job'. The 'Minimum qualifications' section lists requirements such as a Bachelor's degree in Computer Science, 4 years of coding experience, and experience analyzing system security. The 'Preferred qualifications' section lists 6 years of relevant work experience, experience with large data sets, and Google Cloud Platform. The 'Responsibilities' section lists collaborating with teams across GCP, building new detection capabilities, hunting for security events, and participating in incident response. The 'About the job' section describes the role as part of the Google Detection and Response team, focusing on developing advanced detection mechanisms and performing threat hunting and network forensics.

Security Engineer, Detection and Response, Insider Threat

Google Reston, VA, USA Mid

Apply

Minimum qualifications:

- Bachelor's degree in Computer Science, a related technical field or equivalent practical experience.
- 4 years of experience in coding in one or more of the following programming languages: Python, Go, Java, C++.
- Experience analyzing the security of systems (e.g., penetration testing, web application security testing, vulnerability scanning, threat modeling, etc.).

Preferred qualifications:

- 6 years of relevant work experience, including responding to security problems in target-rich environments, examining security alerts, front-line analysis and response.
- Experience leading the analysis of large data sets and intrusion detection systems.
- Experience with Google Cloud Platform or other similar cloud technologies.
- Demonstrated expertise with signals development and threat hunting/modeling.

Responsibilities

- Collaborate with teams across GCP to model insider risks and cultivate new data sources.
- Build new detection capabilities to protect our GCP customers.
- Hunt for and respond to security events on Google networks as part of our 24/7 global operation.
- Investigate a wide variety of security events across various Alphabet systems to assess threats to Google or its customers.
- Participate in response to security incidents.

About the job

As a Part of Google Detection and Response team, the Insider Threat group develops, maintains, and constantly evolves the signals, tools, and infrastructure to detect sophisticated attackers. On our team, you will build advanced and novel detection mechanisms for attacker techniques, tactics and procedures, developing systems to automate remediation, conducting threat hunting, and performing network and systems forensics. We are responsible for detecting all malicious activity on Google's networks. You will perform deep analysis of threats across Google corporate, production, and acquisition environments.

Using the NICE Employer Guidance:

- ❖ Matching to [Work Roles](#) in the [NICE Framework](#)
 - Best match would be [Information Systems Security Engineer](#) or [Threat / Warning Analyst](#)
- ❖ Considering position competencies:
 - Technical skills are represented in Minimum and Preferred Qualifications
 - Soft skills: communication, problem solving, teamwork
 - Areas open for teaching / mentorship:
 - Cloud technologies (prefer Google Cloud knowledge but can teach easily if the candidate has knowledge of other Cloud platforms);
 - Detection and Response Security Engineers who may not have focused on Insider Threat but are interested in doing so
 - Career level of job: Mid-level industry experience; internal and external candidates
 - Competencies
 - Security Engineering detection & response techniques - advanced
 - Cloud technologies - intermediate
 - Coding - intermediate
 - Data analysis - advanced
 - Communication & org awareness - intermediate
 - Teamwork - intermediate
 - Non-negotiables -
 - Deep understanding of Detection and Response tactics and hands on experience monitoring or examining security threats and front-line response
 - Proficiency in and experience with operating & monitoring threats in a Cloud environment
 - Coding proficiency
 - Teamwork
 - Location - must be able to work onsite (hybrid) in Reston, VA
 - Nice-to-have -
 - College degree in Computer Science or related field
 - Experience detecting internal threat actors at a large corporation
 - Can this role be filled by upskilling a current employee?
 - Possibly software developer with deep interest in Security
 - Qualifications & alternative routes
 - Yes to alt routes - degree is not required; language in MQs lists "Bachelors ***or equivalent experience***"
 - Type of company background - big/small, private/public, nonprofit, gov't, etc.
 - Coding languages - open to a variety (C, C++, Python, Java)
 - Long term - multiple career growth opportunities, typical of a large company
 - Internal training programs or professional development initiatives:

- Contributor to other internal projects; access to internal learning resources
 - [Google Cybersecurity Certificate](#) (public)
- Hiring ecosystem: Recruiters & Sourcers, Hiring Managers, Interviewers, Hiring Committee members

Part 2 of 3

Tasks, Knowledge, Skills

NICE Framework:

- T0124: Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).
- K0086: Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.
- S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.

Part 3 of 3

Assessment Rubric for Cybersecurity Expertise

Candidate Assessment	0-1	2-3	4-5	Total
T0124 Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).			Required: 5	
K0086 Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.		Required: 3		
S0001 Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.		Required 3		