



HAYSTACK
SOLUTIONS

2024 WiCyS Mentor/Mentee Overview

Important Dates



November 6 - Initial emails to access CyberGEN.IQ will be sent out from "CyberGEN.IQ" <cata@haystacksolutions.com>



December 3rd - CyberGEN.IQ access closes



December 10 at 12 pm CT - Understanding Your CyberGEN.IQ Results Webinar

THE STORY

The Need:

DoD had an immediate need to identify and retain talent in cybersecurity, specifically Cyber Warfare Operators. Not enough cybersecurity professionals to keep up with ever-intensifying demand to protect and defend critical infrastructure and commercial enterprises.

The Solution:

In 2016, the Haystack Solutions Team, along with the University of Maryland, developed the only cyber aptitude and talent assessment known as CyberGEN.IQ.

Case Study:

Selecting US Air Force
Cyber Warfare Operators

97%

predicting elite
Cyber Warfare
Operators

84%

predicting
Cyber Warfare
Operators vs
IT professionals



HOW IT WORKS

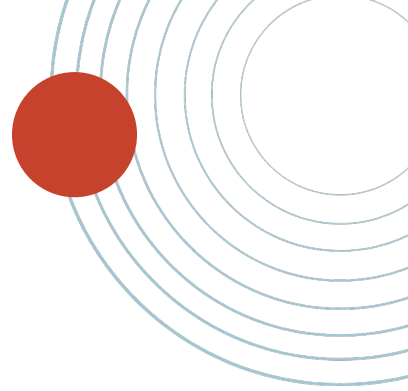
Assessment focuses on five key cerebral areas:

- Critical thinking
- Deliberate action
- Real-time action
- Proactive thinking
- Reactive thinking

Maps to four domains of cybersecurity:

- Offensive operations
- Defensive operations
- Analytics and forensics
- Design and development

Domains mapped to NICE Framework Work Roles



Cognitive Analysis

Cognitive Capabilities Analyzed by CATA			
Critical Thinking spans all the dimensions, exploring visuospatial working memory, rule induction, complex problem-solving, spatial visualization, and attentional capacity.			
Initiating creatively solving problems, with the ability to model program execution	Responding detects anomalies and monitors a continuously running information stream, when doing so is mentally taxing	Real-time scans and interprets information, to respond quickly to events during online processing, and to inhibit the intrusion of distracting or irrelevant information	Exhaustive thinking can delay closure in resolving a task or problem, considering other inputs, while balancing risk and reward

Cognitive Assessment	Short Name	Dimension
Need for Cognition	NFC	Critical Thinking
Dynamic Systems Control	DSC	Critical Thinking
Matrix Reasoning	MRC	Critical Thinking
Paper Folding	PFB	Critical Thinking
Remember and Count	RAC	Critical Thinking
Remote Associates	RAT	Initiating
Spatial Integration	SRIA	Initiating
Coding Speed	CSB	Responding
Pattern Vigilance	PVA	Responding
Anomaly Detection Rule Based	ADRA	Responding
Statistical Learning	SLB	Responding
Recent Probes - 1 item	RP1A	Real-Time
Need for Cognitive Closure	NFCC	Exhaustive
Number Picker	NPA	Exhaustive

Cognitive Disposition: **offensive operations**

Example Jobs in this quadrant:

- Cyber Warfare
- Penetration Testing
- Ethical Hacking

Cognitive Disposition: **design and development**

Example Jobs in this quadrant:

- Enterprise security management
- Application Security
- Enterprise Management

Cognitive disposition: **defensive operations**

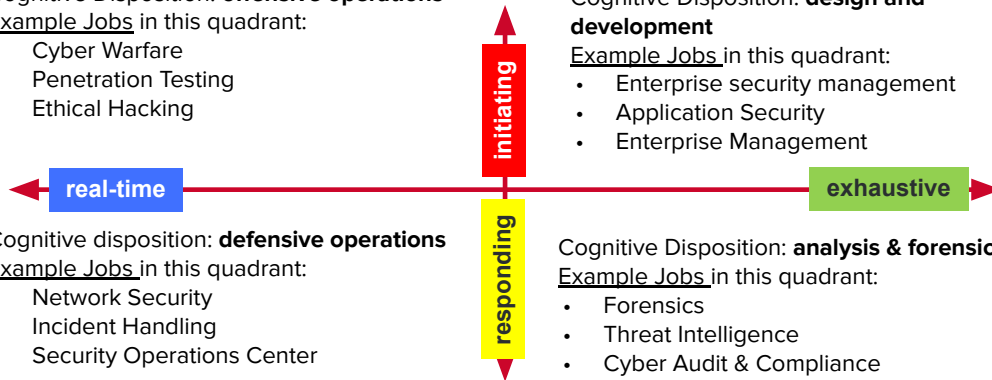
Example Jobs in this quadrant:

- Network Security
- Incident Handling
- Security Operations Center

Cognitive Disposition: **analysis & forensics**

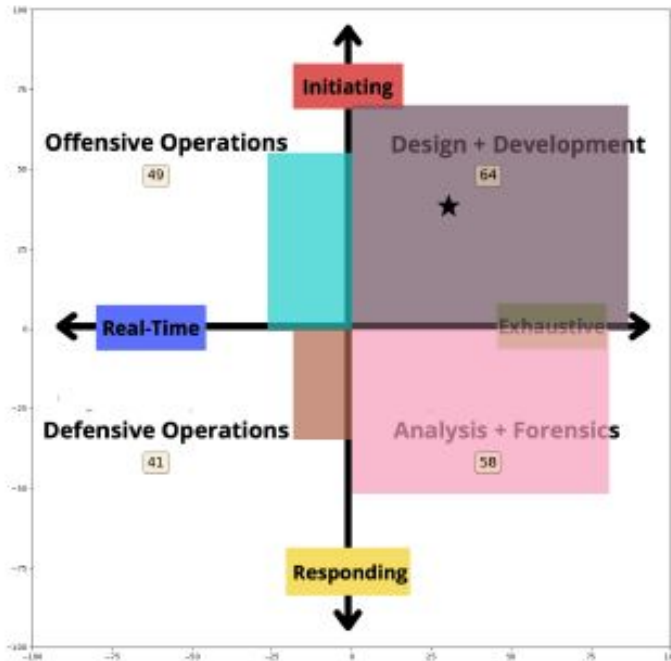
Example Jobs in this quadrant:

- Forensics
- Threat Intelligence
- Cyber Audit & Compliance



UNDERSTANDING RESULTS

Cognitive Capabilities Analyzed by CyberGEN.IQ			
Critical Thinking spans all the dimensions, exploring visuospatial working memory, rule induction, complex problem-solving, spatial visualization, and attentional capacity.			
Initiating creatively solving problems, with the ability to model program execution	Responding detects anomalies and monitors a continuously running information stream, when doing so is mentally taxing	Real-time scans and interprets information, to respond quickly to events during online processing, and to inhibit the intrusion of distracting or irrelevant information	Exhaustive thinking can delay closure in resolving a task or problem, considering other inputs, while balancing risk and reward



Cognitive Disposition: **offensive operations**

Example Jobs in this quadrant:

- Cyber Warfare
- Penetration Testing
- Ethical Hacking

Cognitive Disposition: **design and development**

Example Jobs in this quadrant:

- Enterprise security management
- Application Security
- Enterprise Management

Cognitive disposition: **defensive operations**

Example Jobs in this quadrant:

- Network Security
- Incident Handling
- Security Operations Center

Cognitive Disposition: **analysis & forensics**

Example Jobs in this quadrant:

- Forensics
- Threat Intelligence
- Cyber Audit & Compliance

RESULTS EXAMPLE

COLORS = COGNITIVE CONSTRUCTS

GRAY = CRITICAL THINKING

RED = INITIATING

YELLOW = RESPONDING

BLUE = REAL-TIME

GREEN = EXHAUSTIVE

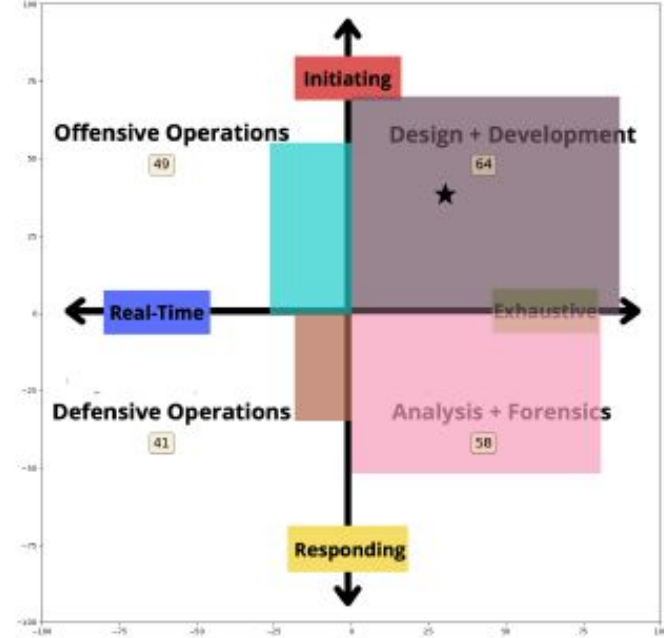
Task	Percentile	Construct	Measures	Insights	Relation to Cyber
Dynamic Systems Control	58	Critical Thinking	Complex problem solving	You are self reflective and use this to analyze problems and your solutions. You often can think outside the box to develop clever solutions.	You can analyze and debug complex functions. You understand how entangled systems work and looking for areas of weakness are tasks they would likely enjoy.
Matrix Reasoning	26	Critical Thinking	Rule induction	You work well in situations where the rules are clearly laid out ahead of time and can find optimal solutions.	You work best with systems that are well documented.
Remember and Count	98	Critical Thinking	Visuospatial working memory	You're able to focus in the midst of distractions. You did well in school and generally have strong reading skills. You might also have a future as a plate spinner!	Your strong working memory gives you an ability to juggle a large number of factors in your head at once. This could take the form of juggling multiple 16-digit hex addresses, debugging symbols, or forensic artifacts.
Need for Cognitive Closure	31	Exhaustive	The need to arrive at a solution during problem solving.	You don't like to commit to answers too soon. You thrive in ambiguity and love the freedom it provides. You hate predictability.	Exhaustive search problems and open ended monitoring are strong suits of these individuals.
Number Picker	90	Exhaustive	Tolerance for risk	You're open to risk and love the thrill and excitement that come along with it. Maybe you are interested in the stock market, playing cards, or gambling.	Your ability to make risk-based decisions helps juggle many competing factors in determining the most successful course of action.
Pattern Vigilance	71	Responding	Vigilance	You are vigilant and can maintain concentration for long periods of time. You don't mind long hours of work that requires focus.	You can monitor information or data for long periods of time while remaining vigilant. This would be required for monitoring large volumes of security alerts, understanding which matter, without being lulled to boredom by those that don't.
Remote Associates	42	Initiating	Creative thinking	You like linear problems that have a clear path. Seeing a goal and the steps needed to achieve that goal help you succeed.	It may take more effort to see relationships between loosely affiliated data points. This might require more time for testing connections between indicators of attack.

Insights	Relation to Cyber
...ing a bunch of values might use reference to help you build new facts.	There are many tools that can help translate binary data, debugging data, or network trace data into other formats. Employing those tools may speed your response times to unusually encoded data or artifacts.
...distracted and may if scrolling through between tests!	In responding to the real-time issues that come up during a penetration test, you may need extra time and space for concentration.
...gnizing patterns and ou may enjoy sudoku llar puzzles.	You can detect anomalies buried within data. Cyber security and other fields where strong patterns emerge suit these individuals.
...ats or memorize ideas tentation and you may ng for a few sessions.	Cyber response circumstances that don't allow you to review results, data, or inputs may be very stressful. For example, it might be hard to decide on shutting off a network connection now, even though the data to support the decision won't be available for another 30 minutes.
...on your environment. hinker and enjoy e big picture.	Success in cybersecurity requires extreme persistence. Increasing your willingness to keep at those thorny challenges will increase your ability to tackle the hardest problems.
	To increase this capability, try to learn and master games like Go that require complex, multi-move visualization.

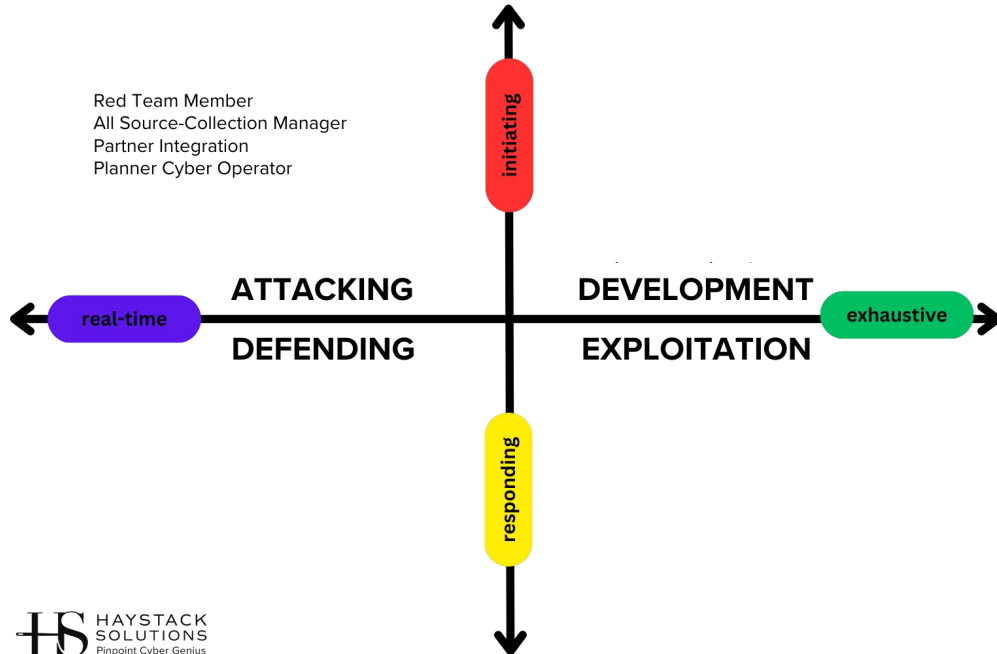
Paper Folding	10	Critical Thinking	Spatial visualization	You work well with problems where the entire task is right in front of you.	
---------------	----	-------------------	-----------------------	---	--



MAPPING TO NICE FRAMEWORK WORK ROLES



Red Team Member
All Source-Collection Manager
Partner Integration
Planner Cyber Operator



Click on any of the below links to visit the
NICE Framework Work Role Page:

[All-Source Collection Management](#)

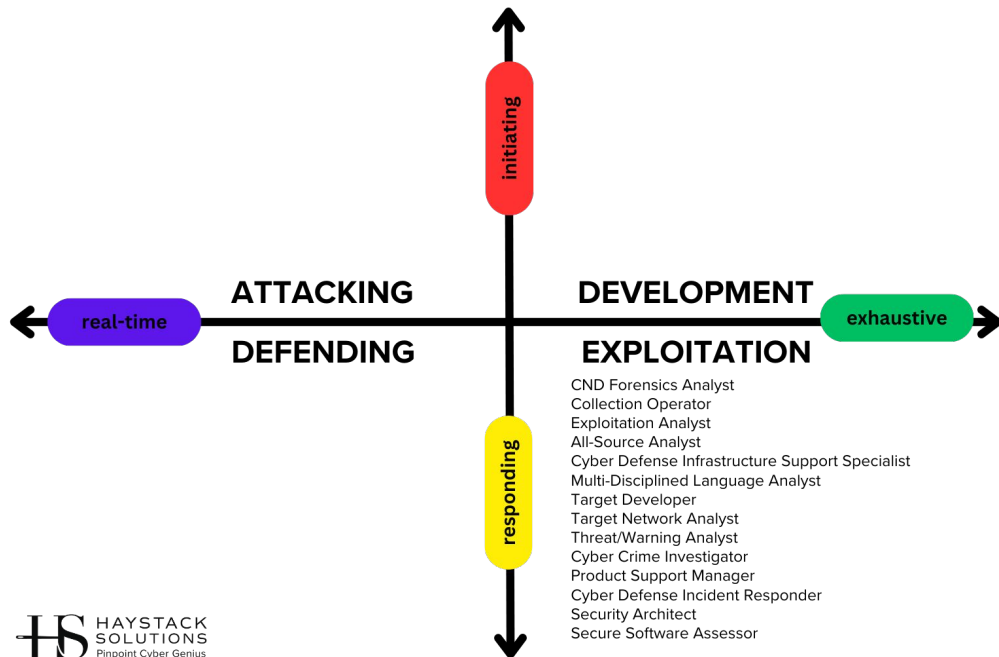
[All-Source Collection Requirements Management](#)

[Partner Integration Planning](#)

[Cyberspace Operations](#)

[Cyber Operations Planning](#)

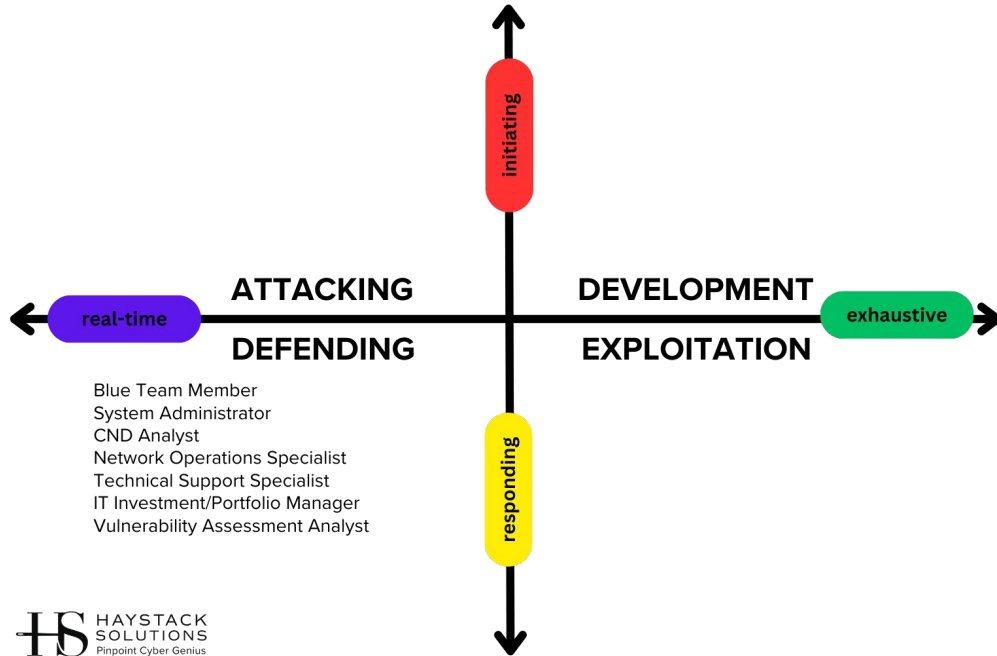
FORENSICS & ANALYSIS



Click on any of the below links to visit the NICE Framework Work Role Page:

- [All-Source Analysis](#)
- [Program Manager](#)
- [Infrastructure Support](#)
- [Exploitation Analyst](#)
- [Multi-Disciplined Language Analyst](#)
- [Vulnerability Analysis](#)
- [Target Network Analyst](#)
- [Threat Analyst](#)
- [Data Analysis](#)
- [Systems Security Analysis](#)
- [Insider Threat Analysis](#)
- [Product Support Manager](#)
- [Cybercrime Investigation](#)
- [Cyber Intelligence Planning](#)

DEFENSIVE OPERATIONS



Click on any of the below links to visit the NICE Framework Work Role Page:

[Network Operations](#)

[Technical Support](#)

[Digital Forensics](#)

[Vulnerability Assessment Analyst](#)

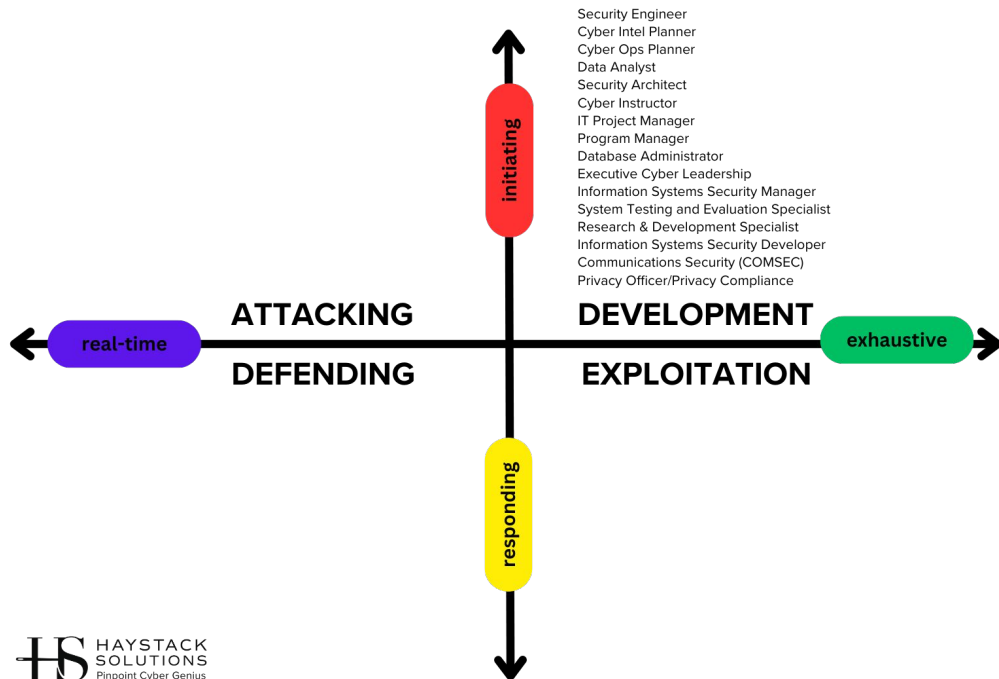
[Defensive Cybersecurity](#)

[Incident Response](#)

[Infrastructure Support](#)

[Digital Evidence Analysis](#)

DESIGN & DEVELOPMENT



Click on any of the below links to visit the NICE Framework Work Role Page:

[Technology Portfolio Management](#)

[Security Control Assessment](#)

[Cybersecurity Workforce Management](#)

[Cybersecurity Policy and Planning](#)

[System Authorization](#)

[Secure Project Management](#)

[Systems Security Management](#)

[Technology Program Auditing](#)

[Cybersecurity Architecture](#)

[Executive Cyber Leadership](#)

[Cyber Legal Advisor](#)

[Enterprise Architecture](#)

[Secure Software Development](#)

[Communications Security \(COMSEC\) Manager](#)

[Secure Systems Development](#)

[Software Security Assessment](#)

[Cybersecurity Curriculum Developer](#)

[Cyber Instructor](#)

[Systems Requirements Planning](#)

[Systems Testing and Evaluation](#)

[Technology Research and Development](#)

[Systems Administration](#)

[Knowledge Management](#)

[Database Administration](#)

Resources Discussed



NICE Workforce Framework WiCyS Video Album

<https://www.wicys.org/resources/nice-workforce-framework-wicys-video-album/>

Link to the work roles

<https://niccs.cisa.gov/workforce-development/nice-framework>

Compare your resume with job descriptions for keywords: [jobscan.com](https://www.jobscan.com)

Find the keywords in a job description: [wordclouds.com](https://www.wordclouds.com)

Helps strengthen your resume bullets: cultivatedculture.com/resume-bullet-analyzer

Resume templates: cultivatedculture.com/resume-templates

Additional Resources

The [DoD Cyber Workforce Framework](#) establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator. The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).

[Cybersecurity Career Profiles](#) - career profile cards mapped to the NICE Framework, designed to inspire and bring the cybersecurity career field to life for students (Grades 6-12).

[CyberSeek](#) – an interactive jobs heat map and career pathway tool that shows cybersecurity jobs across the U.S. by state and metropolitan area. Jobs are organized by categories of the NICE Framework to which they align to.

[National Cyber League](#) - challenges that are based on nine critical cybersecurity workforce categories mapped to the NICE Framework.

[NICE Framework Work Role Videos](#) - a video album from Women in Cybersecurity (WiCyS) that illustrates Work Roles with women who are already actively working in these roles.

[NICE Framework in Focus Interviews](#) - profiles of cybersecurity practitioners that illustrate application of the NICE Framework Categories, Specialty Areas, and Work Roles.

CHAT GPT Example

Brief Description

The CyberGEN.IQ assessment evaluates innate cognitive abilities across key dimensions relevant to cybersecurity. It highlights an individual's natural fit within four cybersecurity domains—Offensive Operations, Defensive Operations, Design and Development, and Analysis and Forensics—based on five cognitive constructs: Exhaustive, Responding, Real-Time, Initiating, and Critical Thinking. This enables individuals to better understand their strengths and align them with career paths.

Examples of Resume Applications

1. Highlighting Aptitude for Cyber Roles

- *Example:* "Achieved high percentile in 'Responding,' demonstrating exceptional vigilance and ability to maintain focus on security alerts for prolonged periods—ideal for SOC Analyst roles."

2. Showcasing Analytical and Problem-Solving Skills

- *Example:* "Strong performance in 'Exhaustive' dimension indicates a natural ability for thorough research and decision-making under uncertainty, excelling in roles like Threat Intelligence Analyst or Cyber Forensics Specialist."

3. Demonstrating Critical Thinking Across Domains

- *Example:* "Scored consistently across 'Critical Thinking' tasks, showcasing strengths in rule induction, complex problem-solving, and adaptability—skills applicable to roles such as Penetration Tester or Security Engineer."

By linking their assessment scores to specific cybersecurity competencies, individuals can craft resumes that stand out to employers looking for targeted skills.

CHAT GPT Recommendation

When highlighting your **CyberGEN.IQ assessment results** on a resume, focus on the most relevant results that align with the role you're pursuing. Tailor these highlights to showcase your innate cognitive strengths and their direct applicability to cybersecurity domains. Here are the key points to emphasize:

1. Cognitive Strengths with Specific Relevance

- Highlight the top-scoring cognitive constructs, and link them to job responsibilities.
- Example:
 - **"Excellence in 'Responding' (77th percentile):** Proven ability to maintain vigilance and focus over extended periods, ideal for roles requiring continuous monitoring of security alerts (SOC Analyst, Threat Analyst)."

2. Alignment with Cybersecurity Domains

- Indicate how your strengths fit into specific domains like Offensive Operations, Defensive Operations, Analysis and Forensics, or Design and Development.
- Example:
 - **"High aptitude in 'Exhaustive' reasoning indicates strong fit for Analysis and Forensics roles, with skills in detailed research and ambiguity management for effective decision-making in threat intelligence and compliance."**

3. Critical Thinking as a Foundational Skill

- Emphasize critical thinking as it applies across cybersecurity domains, showing adaptability and problem-solving.
- Example:
 - **"Strong critical thinking abilities demonstrated through high scores in rule induction and complex problem-solving, essential for penetration testing and security engineering roles."**

CHAT GPT Recommendation Continued

4. Real-World Applications of Skills

- Frame the results in a practical, relatable manner.
- Example:
 - **"Quick decision-making under pressure (Real-Time scoring) supports rapid incident response in high-stakes environments."**

Resume Example

CyberGEN.IQ Assessment Results:

- **Responding (77th percentile):** Demonstrated ability to maintain focus and vigilance in high-pressure environments, ideal for monitoring large data sets and detecting anomalies.
- **Exhaustive Thinking (68th percentile):** Exceptional capacity for in-depth research and solving ambiguous problems, aligning with roles in threat intelligence and cyber forensics.
- **Critical Thinking (top performance):** Adaptability and advanced problem-solving across domains, supporting roles in penetration testing, compliance, and security architecture.

How to Incorporate: Include this in a "Skills" section or under a "Professional Certifications and Assessments" heading to enhance credibility and stand out in the candidate pool.