Bridging the Skills Gap: An Examination of Competencies Needed for Cybersecurity Professionals

Gena Cox, Ph.D.
Executive Strategy Advisor
IBM Talent Management Solutions

Cyber attacks are ...

Increasing in volume

There were 918 data breaches which compromised 1.9 billion data records in the first six months of 2017, which was an increase of **164%** compared to 2016.

(CNBC, 2017)

Costly

The cost of cyber attacks is estimated to be somewhere between **$57 billion** and **$109 billion** in 2016.

(White House Council of Economic Advisers, 2018)

Creating a demand for Cyber professionals

With this unrelenting increase in cyber attacks, it is not surprising that worldwide spending on information security is forecasted to be **$93 billion** this year.

Gartner (2017)

There is a talent availability gap

49%

of Cyber professionals believe that qualified personnel is difficult to find

Global Information Security Workforce Study (2017)

1.8 million

Cyber positions will be unfulfilled by 2022

Global Information Security Workforce Study (2017)

41%

of Cyber professionals said that the skills shortage has increased time in high-priority issues which leads to increases workplace stress

Enterprise Strategy Group and the Information Systems Security Association (2018)

“…enterprises are having a difficult time hiring skilled people as it takes 53% of organizations between 3 and 6 months to fill a position and 10% cannot fill them at all…” (ISACA, RSA Conference)

The difficulties don’t end at raw numbers

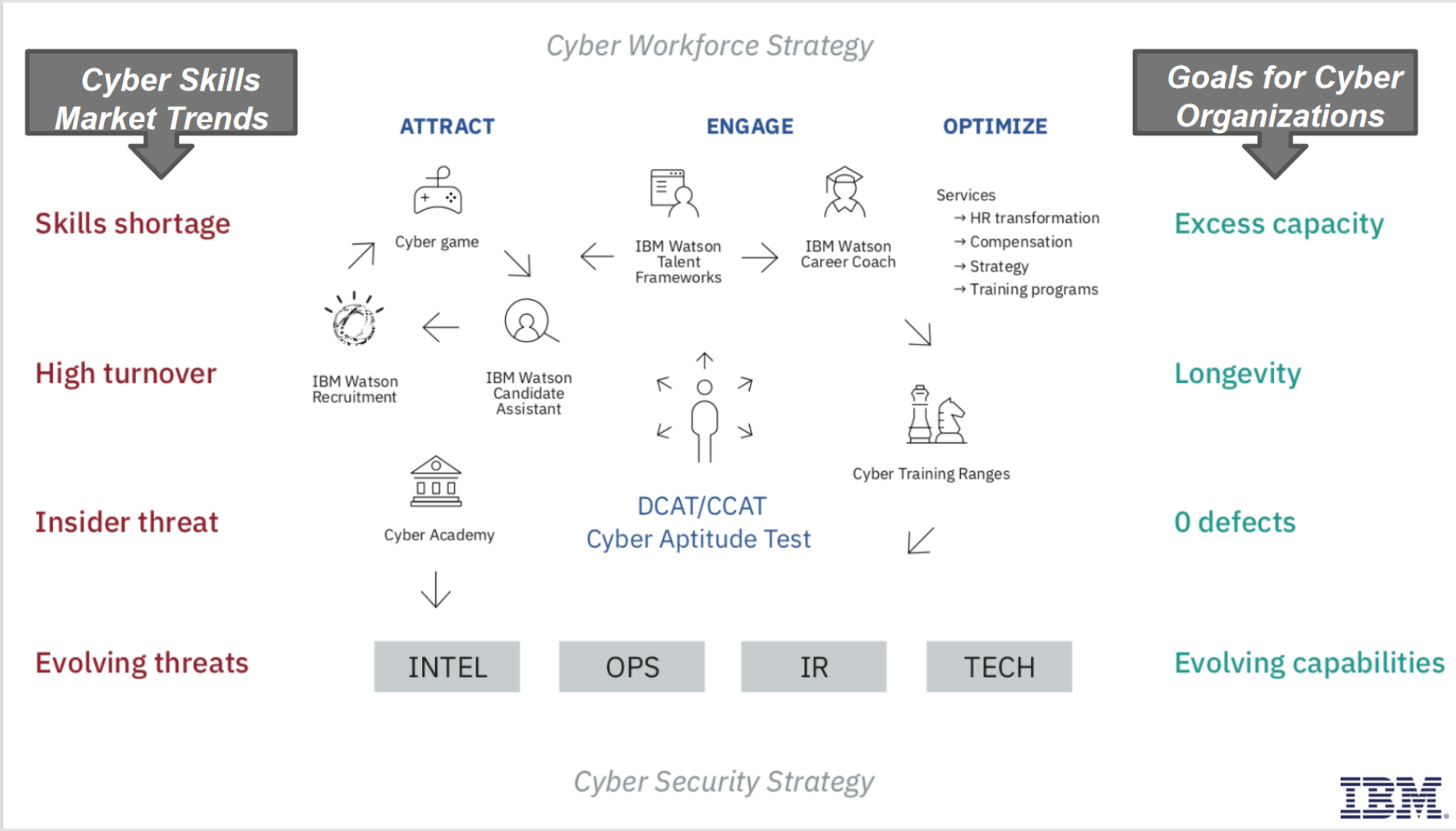
Everyone is challenged

Industry	Professionals	Academic institutions	Students
• Need security candidates with hands-on skills and product experience • Overall shortage of qualified candidates	• Cybersecurity professionals are under constant pressure – they don’t have the time to train new staff • Need for continuous training and professional development to keep up with the threat landscape	• There are shortage of qualified teachers and professors and competition with industry salaries • Struggling to keep pace with shifts in industry and technology	• Trouble defining a career path since there are myriad options • Many cybersecurity jobs require significant education and experience – students don’t know where to get started

Cross-profession challenges

- Underrepresentation of women and wage gaps in the field
- Competition between public and private sectors

A powerful cyber talent strategy is key



“Historically, there has been a lot of talent that is overlooked by many corporations due to formal degrees being the first requirement in many of their job postings.

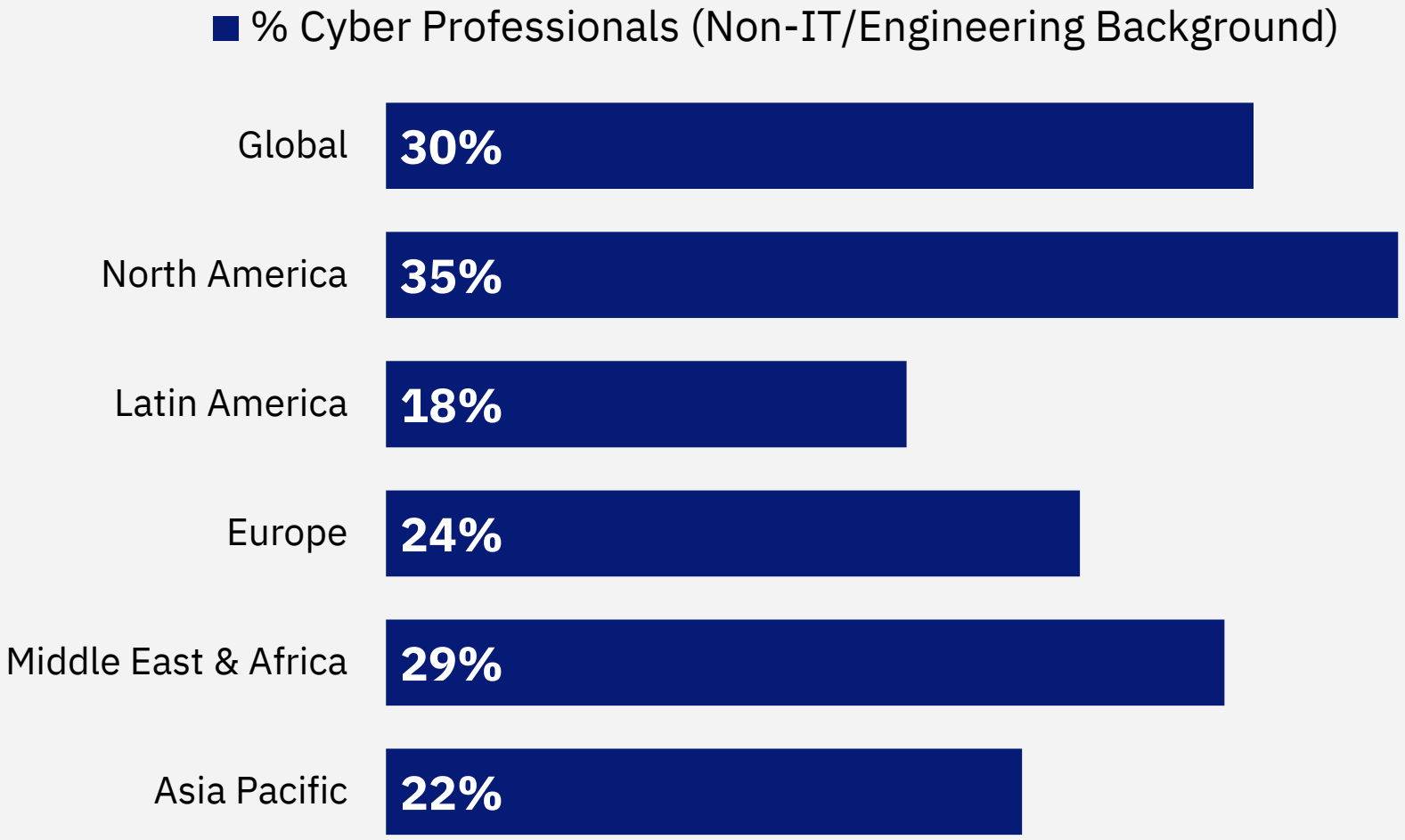
Everyone has a different path, and they may not have attended a four-year college due to cost or life challenges.

Sometimes a role may require ‘that degree,’ but there are other times I believe we may be filtering and scaring off talent without providing them the opportunity to represent their skills and value.”

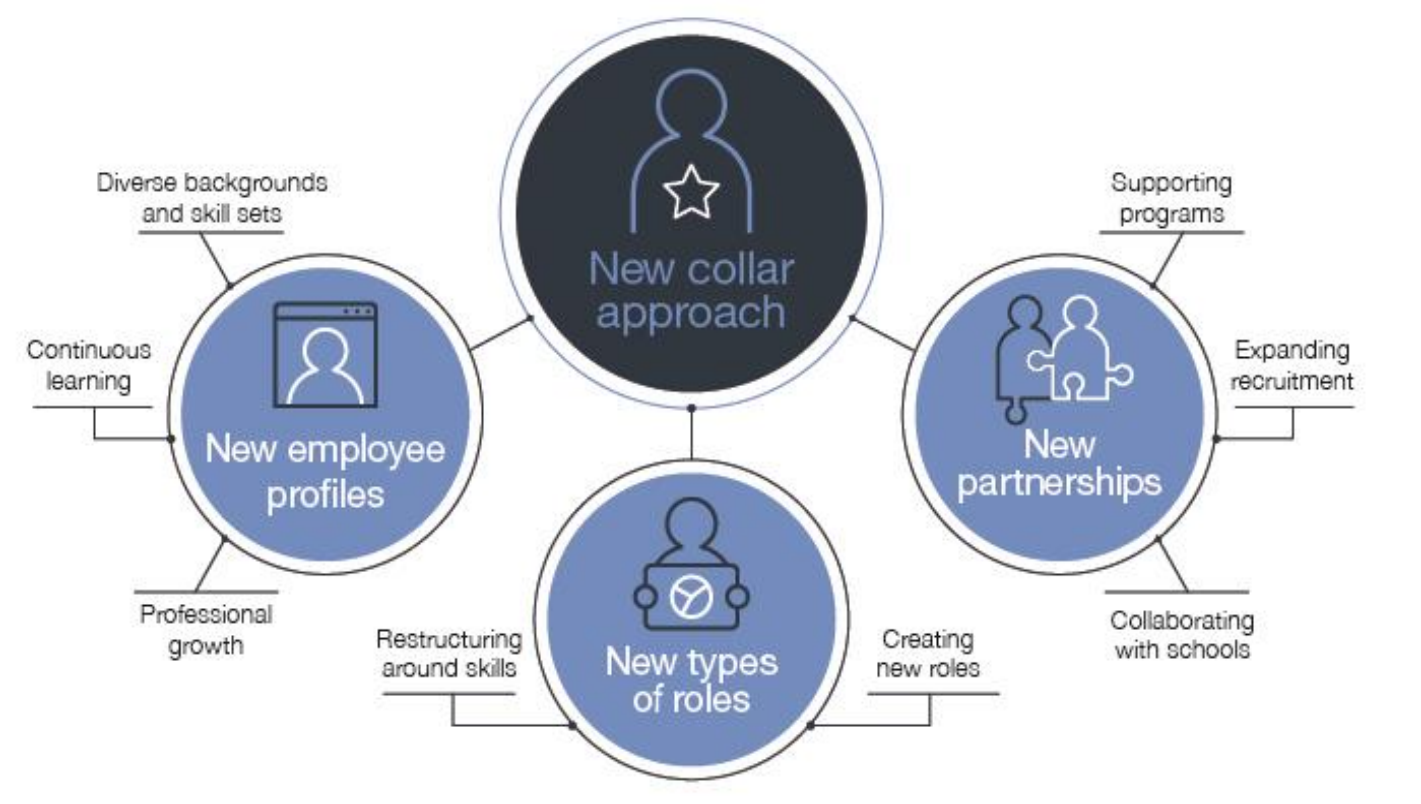
– Adam Griffin, Advisory Architect
Manager, Manager Security Services
Infrastructure & Endpoint Security, IBM Security

Wider Recruitment Pipeline

Although many of the Cybersecurity professionals started from a related field (e.g., IT), many of the started from a non-IT background.



The new collar model helps



Open the aperture on talent pipelines to take advantage of underutilized sources of talent for new types of work.

Skills and behaviors are at the center of a new collar approach – these are some that are essential for security professionals

	Explorer	Problem solver	Student	Guardian	Consultant
Core attributes	***Investigative and enjoys challenges***	***Analytic, methodical and detail oriented***	***Constantly learning***	***Protective, ethical and reliable***	***Works with others to understand and solve problems***
Skills	▪ An innate understanding of scenarios, risks and “what ifs”	▪ Verifiable hands-on experience with references, certifications and/or micro-credentials ▪ Familiarity with and some ability to code—to figure out how to build and take things apart	• Specific industry knowledge The ability to adapt to new and emerging security technologies	• Familiarity with applicable regulations, laws and policies—and the ability to interpret them	• The ability to work in dynamic and diverse teams • Effective communication skills—can articulate complex concepts and clearly explain technical issues • Experience educating others

How can behaviors help with the talent availability gap?

Identification

Provides insight into other areas that are often overlooked.

Clarity

Allows for insight into what the is needed for job success.

Simplification

Although each job have different knowledge and skill requirements, there are some behaviors that carry over from one job to the next.

Penetration Testing

Example Responsibilities

- Perform formal penetration tests
- Probe for vulnerabilities in applications
- Pinpoint methods that exploit weaknesses and logic flaws.
- Research, document and discuss security findings.
- Provide feedback and verification as an organization fixes security issues.

Key Behavioral Competencies

- Problem-solving
- Analytical thinking
- Integrity “Ethical high standards”
- Creativity
- Accuracy and Detail Orientation
- Oral and written communication skills
- Collaboration

Security Operations Center Analyst

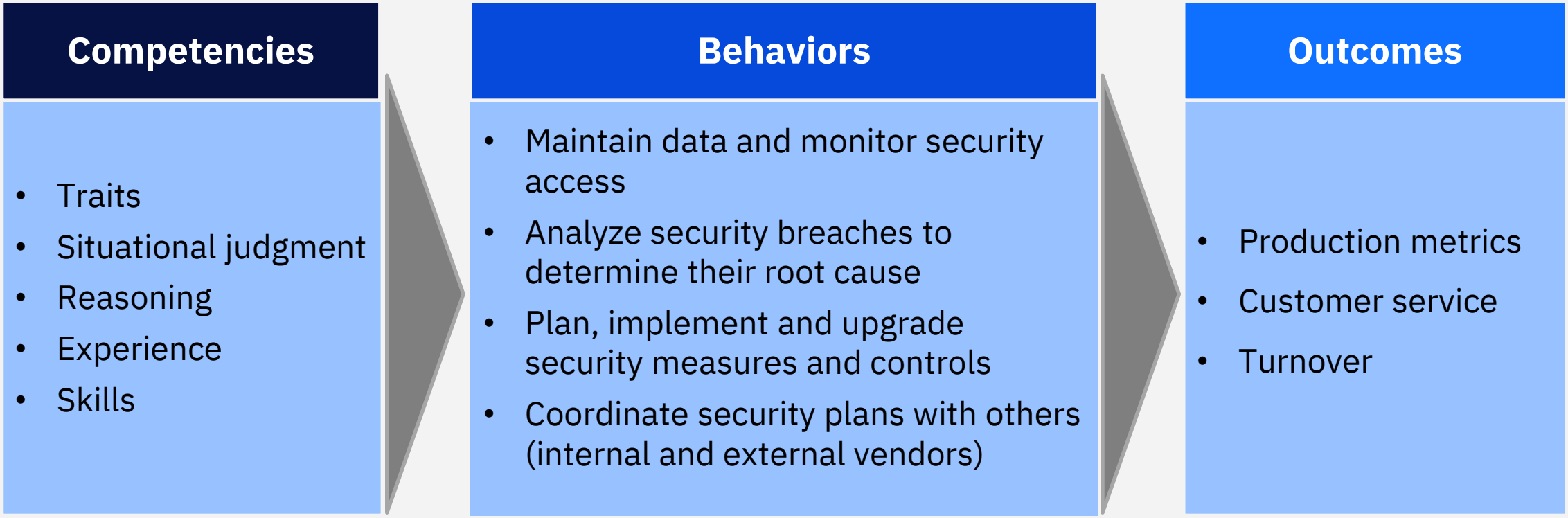
Example Responsibilities

- First responder to security event escalations
- Detect, escalate, and assist in remediation of critical information security incidents.
- Document and communicate findings, escalate critical incidents, and interact with customers.
- Keeps current on the current IT threat landscape and upcoming trends in security.

Key Behavioral Competencies

- Problem-solving
- Analytical thinking
- Accuracy and Detail Orientation
- Oral and written communication skills
- Flexibility and Adaptability

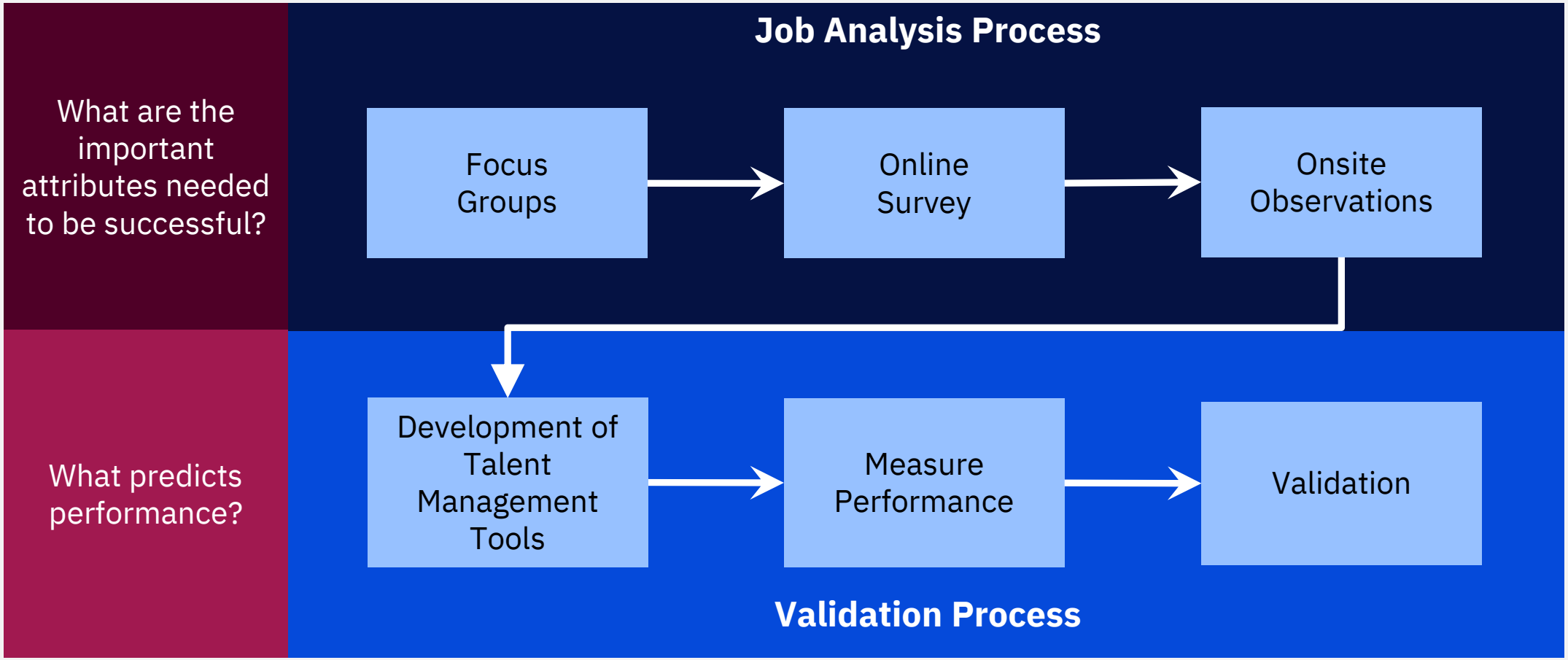
How to use behaviors to guide selection and development?



Identify and measure job requirements

Where does process start?

How do we evaluate effectiveness?



Examine competencies relevant for Cyber roles

Resilience

Ability to adjust to continuous change in work demands.

Maintains focus when facing unexpected challenges and work obstacles.

Adaptability

Adjusts to new or changing assignments, processes, and people.

Identifies and considers alternative approaches to situations or problems.

Accuracy and Detail Orientation

Utilizes a systematic approach for checking and cross-checking outputs.

Accurately gauges the impact and cost of errors, omissions, and oversights.

Problem Solving

Uses fact-finding techniques and diagnostic tools to identify problems.

Analyzes risks and benefits of alternative approaches and obtains decision on resolution.

How to measure these competencies?

Assessments

Traditional Assessments come in a variety of mediums and can a variety of constructs

Aspects of personality, reasoning skills, and problem solving are generally can be measured reliably with assessments

Simulations

Simulations provide a real-life experience of what the job entails

Incorporate the competencies into existing simulations that can be evaluated (adaptability, detail orientation)

Exercises and Interviews

Verbal communication skills are best evaluated using face-to-face or voice methods

Ask questions and/or have candidates complete exercises that allow to understand one’s competency on problem solving

Guidance for finding Cyber talent

Avoid over-emphasizing areas that might be trainable.

Examine the soft skills and aptitudes that are important for Cyber roles.

Identify methods and tools that measure soft skills and aptitudes reliably.

Explore outside “typical” Cyber profile and recruitment sources.

Re-examine your workforce strategy

Think about **what skills are essential today and in the future** for your organization; document them. Use that to help identify candidates who can be successful with the behavioral demands of the job and then trained for the technical skills.

Design clear career paths for these people and …watch them bloom!

IBM Talent Management Solutions Team

Website:
https://www.ibm.com/talent-management

Sales:
James Alvilhiera
Cybersecurity Assessments
j.alvilhiera@us.ibm.com

Global Content and Psychometrics Leader:
Jeff Labrador, PhD
jeff.labrador@us.ibm.com

Watson Talent Consulting:
Gena Cox, PhD
genacox@us.ibm.com