HOW DO YOU MEASURE EXPERTISE?

An Employer Driven Model for Cyber Workforce Development: How Dell Applied a Useable Workforce and Training Model to Cyber Job Roles and Skills

Simone Petrella
Chief Cyberstrategy Officer, CyberVista

cybervista.net

TODAY'S CYBERSECURITY EDUCATION LANDSCAPE

TODAY'S CYBERSECURITY LANDSCAPE

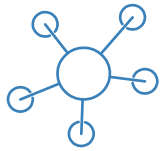
Current cybersecurity training and education solutions are fragmented, often geared towards building a pipeline of candidates, and yet rarely relate skills or competencies to actual job roles.

OVER 260

Universities teach cyber defense skills

ABOUT 150

Universities teach offensive cyber skills



85 DIFFERENT

Certifications, training courses, and classes were assessed by CyberVista

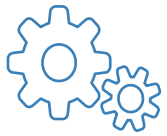
THE PROBLEM

The Employer's Perspective

- Struggle to identify/hire the right talent
- Difficulties training staff to have their cyber job roles
- Struggle to retain qualified talent

The Candidate's Perspective

- Struggle to find jobs despite their credentials
- Difficulty focusing their efforts on a professional career path

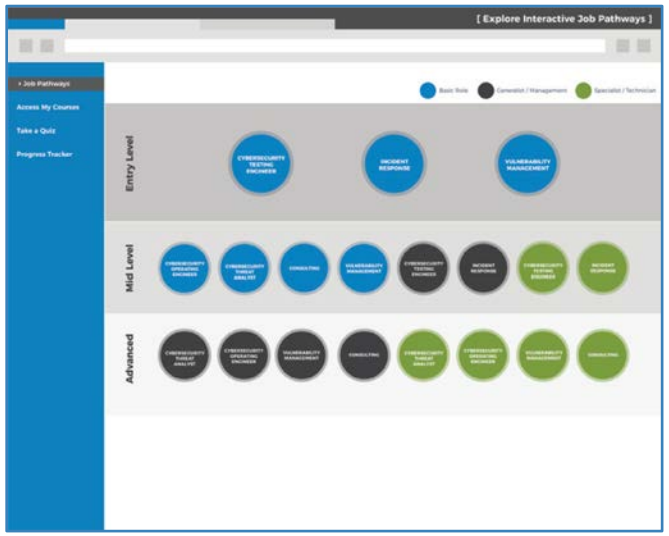


THE CHALLENGE

Dell sought to develop a human capital management plan for the company's current and anticipated cybersecurity staff by:

- Fully understanding the cybersecurity job roles within its enterprise
- Obtaining an underlying and comprehensive list of associated foundational and specialized skills mapped to each role
- Creating more accurately represented job families from a Human Capital perspective
- Developing and investing in more effective and efficient training and upskilling solutions

THE APPROACH

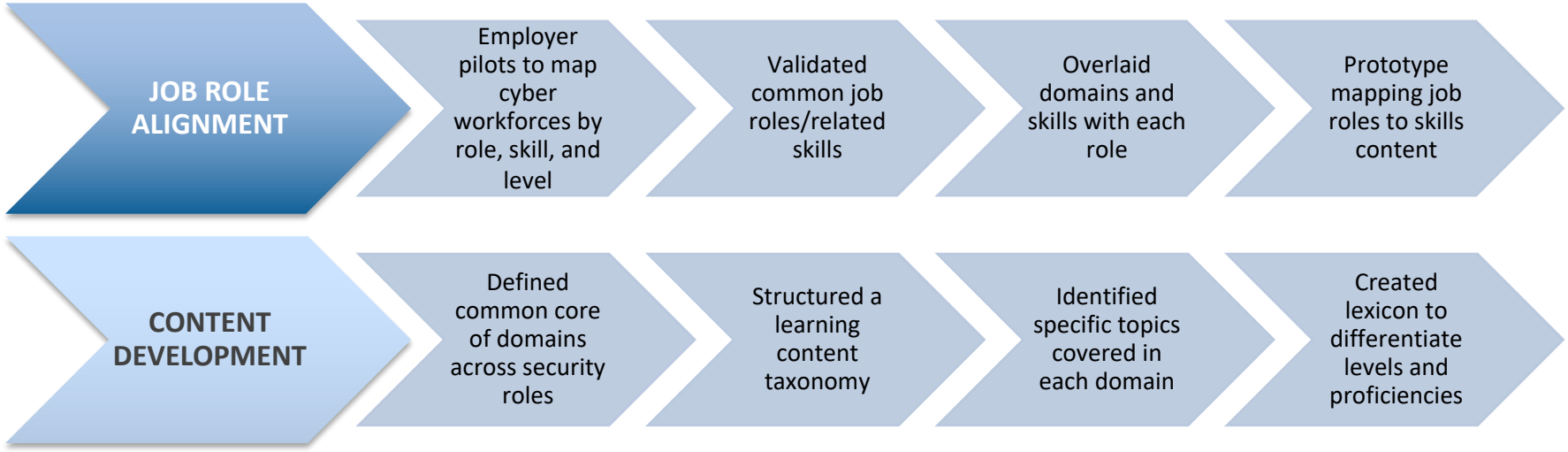


Focus on a skills-based approach that addresses Dell's cybersecurity workforce demand:

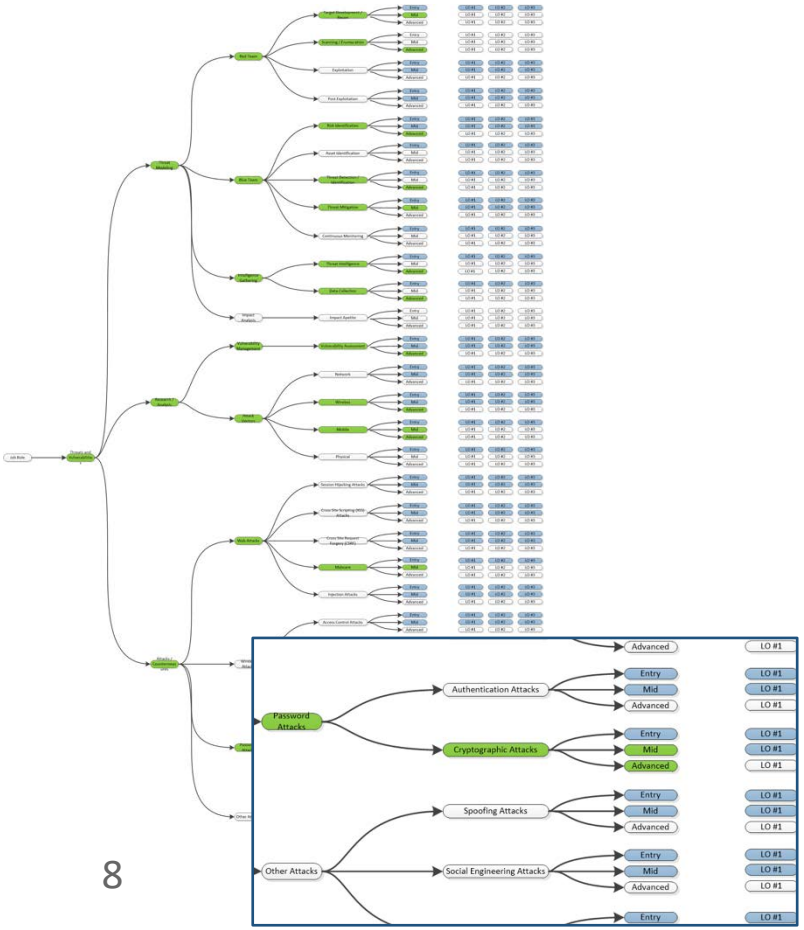
- Conduct an inventory of Dell's current cybersecurity job roles, including its desired and open job positions
- Perform a thorough job task analysis of current cybersecurity functions performed by Dell employees
- Develop a list of requested skills for each job role across various career levels
- Develop a job transition pathway that identifies both lateral and vertical progressions as well as a proposed modular skills-based path to transition between them

OUR RESEARCH PROCESS

Building upon research done by the **National Initiative for Cybersecurity Education (NICE)** and leveraging the **National Cybersecurity Workforce Framework (NCWF)**, we were able to **identify discrete skills needed by Dell** for job roles at multiple levels and **create a roadmap that ties role requirements and skills together.**



CONTENT TAXONOMY



The first step was to define a common core of cyber domains, which allowed us to then develop a structured learning taxonomy.

Domain Breakdown

- Governance
- Networking
- Risk
- Security Engineering
- Software/Hardware
- Threats & Vulnerabilities

Functional Overlay

- Tools and Techniques

A STARTING POINT

Dell Job Role (Entry/Mid/Advanced)			
Job summary	Internal job description		
Fundamental Skills (prerequisites)	Entry level foundational skills	Mid level foundational skills	Advanced level foundational skills
Other Skills than can be learned on the job	Entry level on the job skills that should be acquired	Mid level on the job skills that should be acquired	Advanced level on the job skills that should be acquired
Trainings/Certifications to facilitate advancement w/in the job family	CEH Sec+ CCNA Network+	OSCP CCIE GIAC GPEN	CISSP CISM CISA CCNP

IDENTIFYING SKILLS PATHWAYS

SKILLS NEEDED TO TRANSITION

TO → / FROM ↓	CS Specialist / Technician	CS Analyst	Penetration & Vulnerability Tester
CS Specialist / Technician		Collection Management Databases Web Vuln / Proxy / Browser Wireless testing and Attacks Reverse Engineering Forensics Scanning and Enumeration Architecture/Design Security Measures Management/Planning Metrics International/US Risk Management / Assessment Offensive Security Defensive Security Intelligence Gathering Attack Vectors Web Attacks Wireless Attacks Password Attacks	Voice Communications Mobile Collection Management Cloud Computing Languages/Coding Databases Architectures Vulnerability Analysis Web Vuln / Proxy / Browser Wireless testing and Attacks Reverse Engineering Exploitation Tools Sniffing and Spoofing Forensics Scanning and Enumeration Programming / Development Architecture/Design Security Measures Offensive Security Intelligence Gathering Attack Vectors Web Attacks Wireless attacks Password Attacks
CS Analyst			Voice Communications Mobile Cloud Computing Languages/Coding Network Components Architectures Vulnerability Analysis Password Auditing Exploitation Tools Sniffing and Spoofing Programming / Development Vulnerability Management
Penetration & Vulnerability Tester		Frameworks Management/Planning Metrics International/US Laws and Regulations Risk Management / Assessment Defensive Security	

Based on the NIST Cybersecurity Workforce Framework

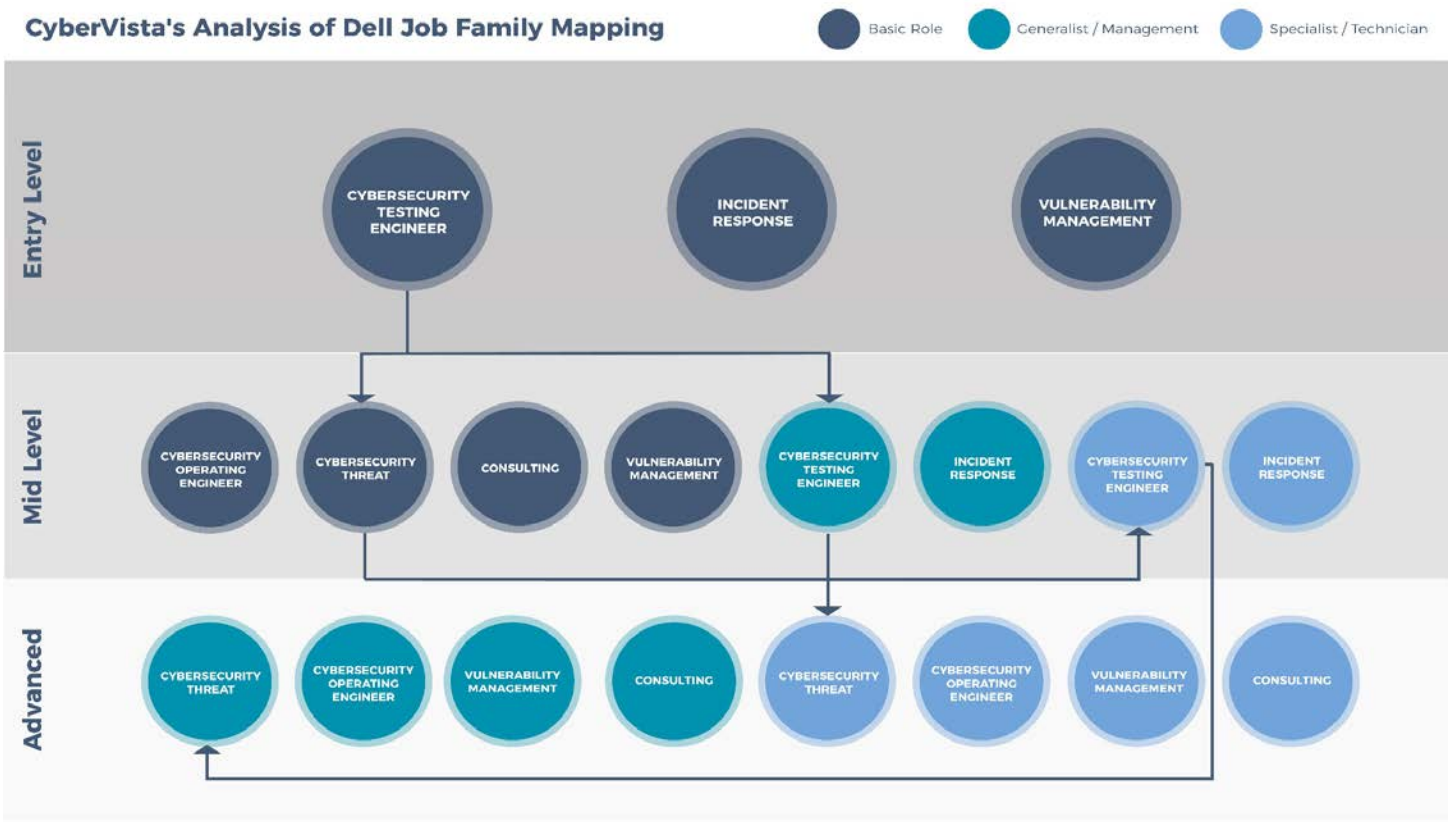
By analyzing the frequency of the requested skills we were able to group them into subsets and identify skills gap between roles

THE ANALYSIS

For all 6 Job families we analyzed there were 19 different types of roles

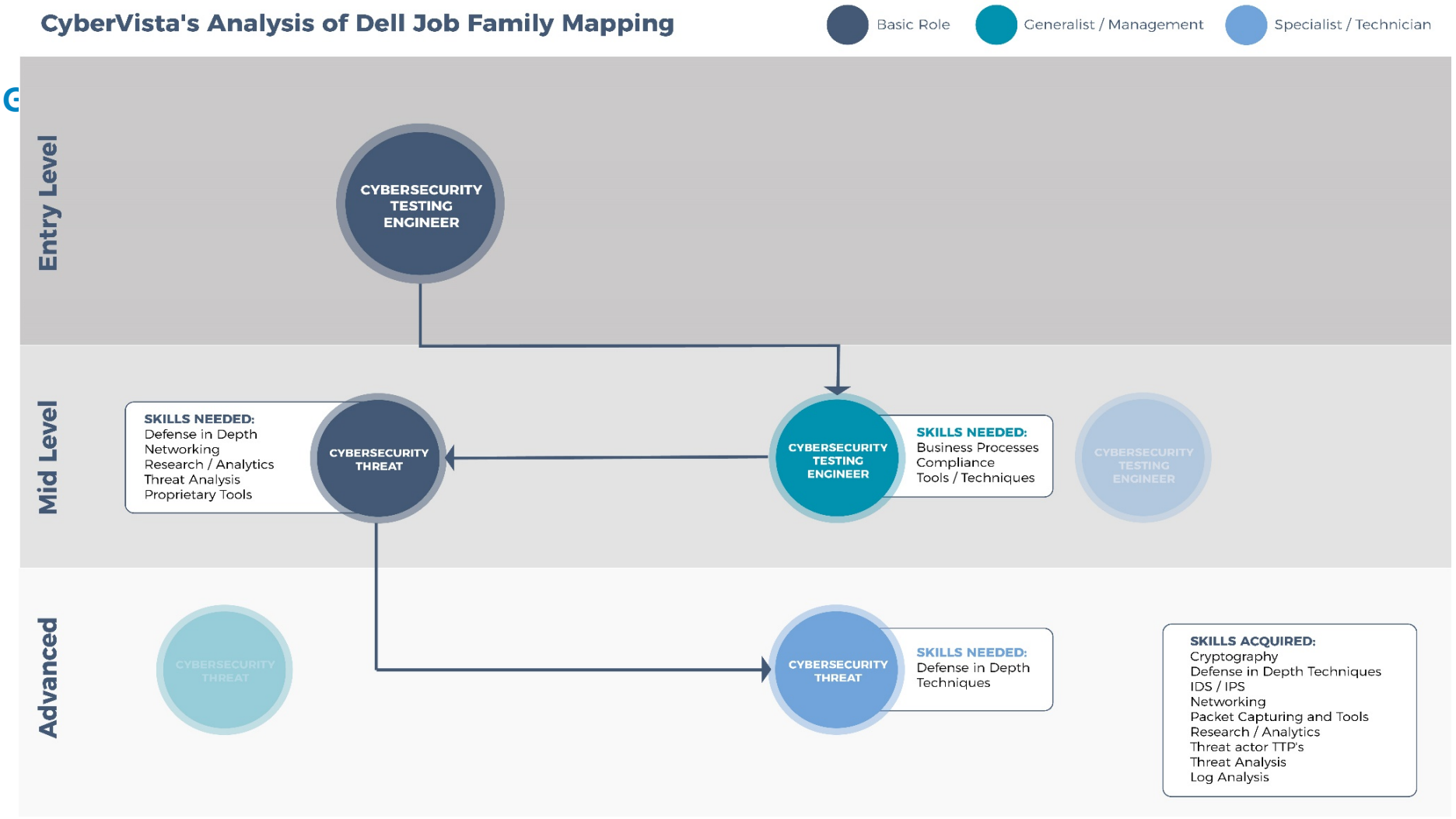
- For each role there was a career path to move both diagonally and vertically
- We assumed transitioning from one role to another would likely require additional skills, that are learned on the job or through external or internal training
- We laid out each of the 19 roles and grouped them based on career level (entry, mid, advanced) as well as type, (Specialist, Management)
- There werehundreds of possible transitions

CREATING A TRAINING PATHWAY

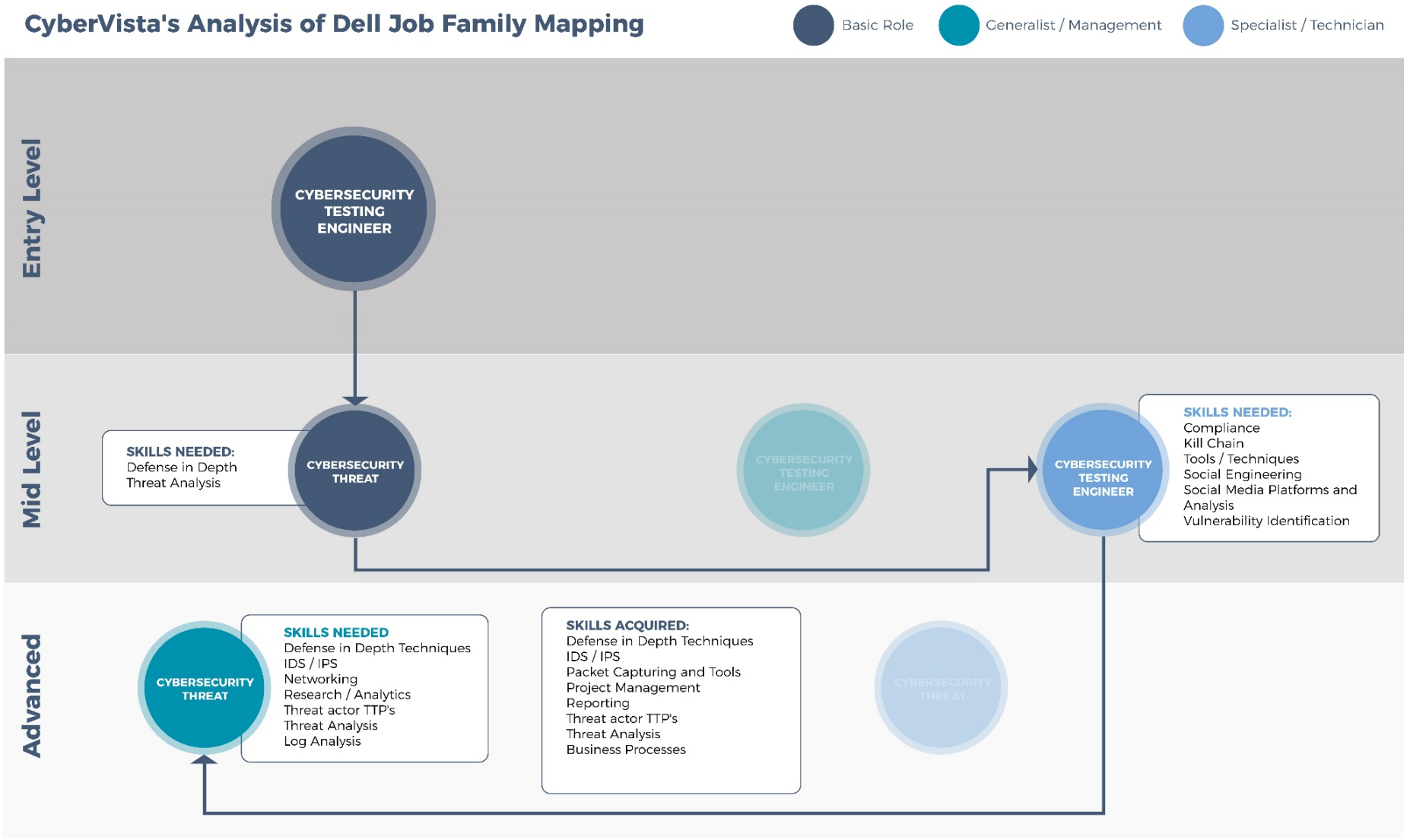


Combining the **defined taxonomy** with a detailed understanding of **Dell's job roles**, we were able to **create and visualize career pathways** that **identify the skills gap** between different roles and their corresponding levels.

CREATING A TRAINING PATHWAY



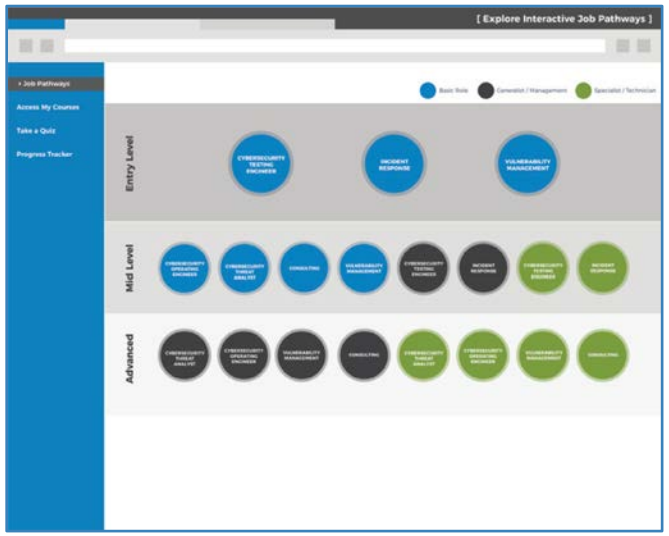
CREATING A TRAINING PATHWAY



OUTCOMES FOR DELL

DELL TO INSERT ANY ACTIONS TAKEN AS A RESULT OF THE PROJECT

WHAT NEXT



Start to move the cybersecurity industry towards professionalization

- Distinguish baseline skills of a “cyber professional” versus those indicative of specialization
- Create a usable lexicon and framework to identify cyber workforce needs and training requirements

IMPACT ON TRAINING

Align training to company-specific job roles to assess and support the professional development of staff.

ASSESSMENTS

Evaluate new or current employees on specific skills

LEARNING/TRAINING

Online and modular for re-skilling or up-skilling

PRACTICE SKILLS

Online and modular for re-skilling or up-skilling

Contact:

SIMONE PETRELLA
CyberVista
Chief Cyberstrategy Officer

T: 703.345.6418
M: 201.981.8895
simone.petrella@cybervista.net

1300 17th Street North
17th Floor
Arlington, VA 22209