RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-F01

A New Employer-Driven Model of Cyber Workforce Development For Dell

John Scimone
Chief Security Officer
Dell Technologies

Simone Petrella
Chief Cyberstrategy Officer
Cybervista

TODAY'S CYBERSECURITY LANDSCAPE

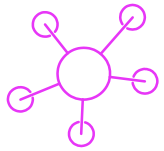
Current cybersecurity training and education solutions are fragmented, often geared towards building a pipeline of candidates, and yet rarely relate skills or competencies to actual job roles.

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

DELL/CYBERVISTA PARTNERSHIP

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
- Researching more effective and efficient training and upskilling solutions

CyberVista sought to create employer-driven training and curriculum that addresses actual skills needed on the job by:

- Fully understanding the skills needed to successfully perform cybersecurity job functions
- Identifying career, skill, and training pathways for cyber professionals
- Creating a detailed taxonomy roadmap that identified skill gaps between roles and levels
- Developing and investing in more effective and efficient training and upskilling solutions

RSAConference2019

Dell Workforce Analysis

Challenges

What challenges did we face?

- All leaders believe their job is distinctly different
- Tight job family structure within Dell
- Hiring ramp running concurrently with job family changes
- Alignment to approved salary survey vendors
- Lack of existing market trends

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 understand the market taxonomy and discrete skills needed by Dell for job roles at multiple levels and create a roadmap that ties role requirements and skills together.

This allowed us to gain a comprehensive understanding of our roles prior to market alignment.

The NCWF was also provided to our internal stakeholders and external consultant to ensure we were speaking the same language.

Approach

1. Job Inventory

- Reviewed 400 + existing team members' roles
- Identified what jobs we were planning for in our 150 + open requisitions

2. Job Analysis

- Conducted a thorough job analysis of all existing roles and open reqs through internal stakeholder interviews (50 + hours) with an external Radford consultant present
- Identified role responsibilities and skills required of the team member

3. Future State Needs

- Discussed future state of the organization and skills needed with leadership team
- Evaluated market landscape and trends, created internal job hierarchy with future in mind

4. Internal & External Alignment

- Hosted multiple alignment sessions with external partners and consultant
- Connected with internal Market Intelligence group and stakeholders

Job Family Analysis

Our job family analysis resulted in 5 net new job families to Dell and led to the adoption of several existing internal job families (ex: Compliance).

Identified job roles

- Digital Forensics
- Incident Response
- Cybersecurity Consulting
- Penetration Testing
- Cybersecurity Engineering & Operations
- Threat Hunter & Intelligence
- Business Continuity
- Vulnerability Assessment
- Governance, Risk and Compliance

Net new job families

Objectives

OBJECTIVES

1. Develop detailed job descriptions that recognize different areas of Security and Resiliency expertise and are validated by the market
2. Align jobs to market with increased precision that differentiates skills & expertise within Security and Resiliency

PROCESS

- Interviewed internal stakeholders
- Engaged an external Radford consultant
- Joined the inaugural Aon Cybersecurity Steering Committee

OUTCOME

Created an internal job hierarchy considering roles that are most difficult to fill in the market and the Dell risk landscape

IMPACT

- **5** new job families:
  - Business Continuity
  - Vulnerability Assessment
  - Incident Response
  - Cybersecurity Eng & Ops
  - Cybersecurity Consulting
- **460 +** Impacted team members; 4 statement templates and multiple languages
- Market Intelligence Team priced **44** new jobs
- Updated **hundreds of** reqs and trained global TA team on new job families and approach

What Next?

Continue to move our Dell security organization towards professionalization

- Monitor the market for emerging trends and continue to refine our job family structure
- Establish a training plan and identify skills gaps
- Create a diverse pipeline of security professionals

RSAConference2019

CyberVista Training Development

Research Process

Through working with Dell to map the skills required in current and future cybersecurity roles, 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.

We distilled and mapped the knowledge, skills, and abilities (KSA's) outlined for each specialty area in the NCWF to define domains of skill knowledge that would be useable and consumable as training in a corporate environment.

Approach to Address Training

1. Job Skill Analysis

- Created cyber workforce skill overview for each job family, divided by role, level, and track
- Validated common job families and roles again known skill requirements

2. Skill Gap Analysis

- Identified critical areas of skill gaps between level and various roles
- Created visual roadmap to show career/job role pathway options and associated skills

3. Training Paths

- Used this knowledge to define a common/generic core of domains across security
- Developed a detailed learning taxonomy that maps skills to roles, ensuring mapped to NCWF

4. Training Content

- Created lexicon to differentiate levels and proficiencies
- Identified specific topics covered in each domain to target curriculum development

Job Skill Analysis

Cybersecurity Threat			
Job summary	Acts proactively to hunt for and visualize potential future threats to the organization. Applies Dell specific knowledge of products and business processes to eliminate those potential risks.		
Fundamental Skills (prerequisites)	Defense in Depth Networking Operating Systems Research / Analytics Threat Analysis Proprietary Tools	Cryptography Defense in Depth Techniques IDS / IPS Networking Packet Capturing and Tools Research / Analytics Threat actor TTP's Threat Analysis Log Analysis	Defense in Depth Techniques IDS / IPS Packet Capturing and Tools Project Management Reporting Threat actor TTP's Threat Analysis Business Processes
Other Skills than can be learned on the job	Business Processes, Computer Network Operations, Cryptography, IDS / IPS, Log Analysis, Low Level Programming Languages, Project Management, Proprietary Networks, Scanners, Scripting Languages, Security Operations, Threat actor TTP's, Threat Modeling, Trend Analysis, Web Servers and Applications, Packet Capturing and Tools, Reporting	Cyber Forensics, Documentation, Low Level Programming Languages, Malware Analysis, Mobile Networks, Reverse Engineering, Sandboxing, Scanners, Targeting, Threat Modeling, Trend Analysis, Virtualization	Communications, Computer Network Operations, Data Collection Handling and Analysis, Governance, Information Assurance, Risk Assessment, Risk Management, SOP, Development, Threat Modeling, Trend Analysis
Trainings/Certifications to facilitate advancement w/in the job family	CEH Sec+ GIAC	OSCP CCSP CISSP CSIH Linux Certs	CISA CISM GSNA

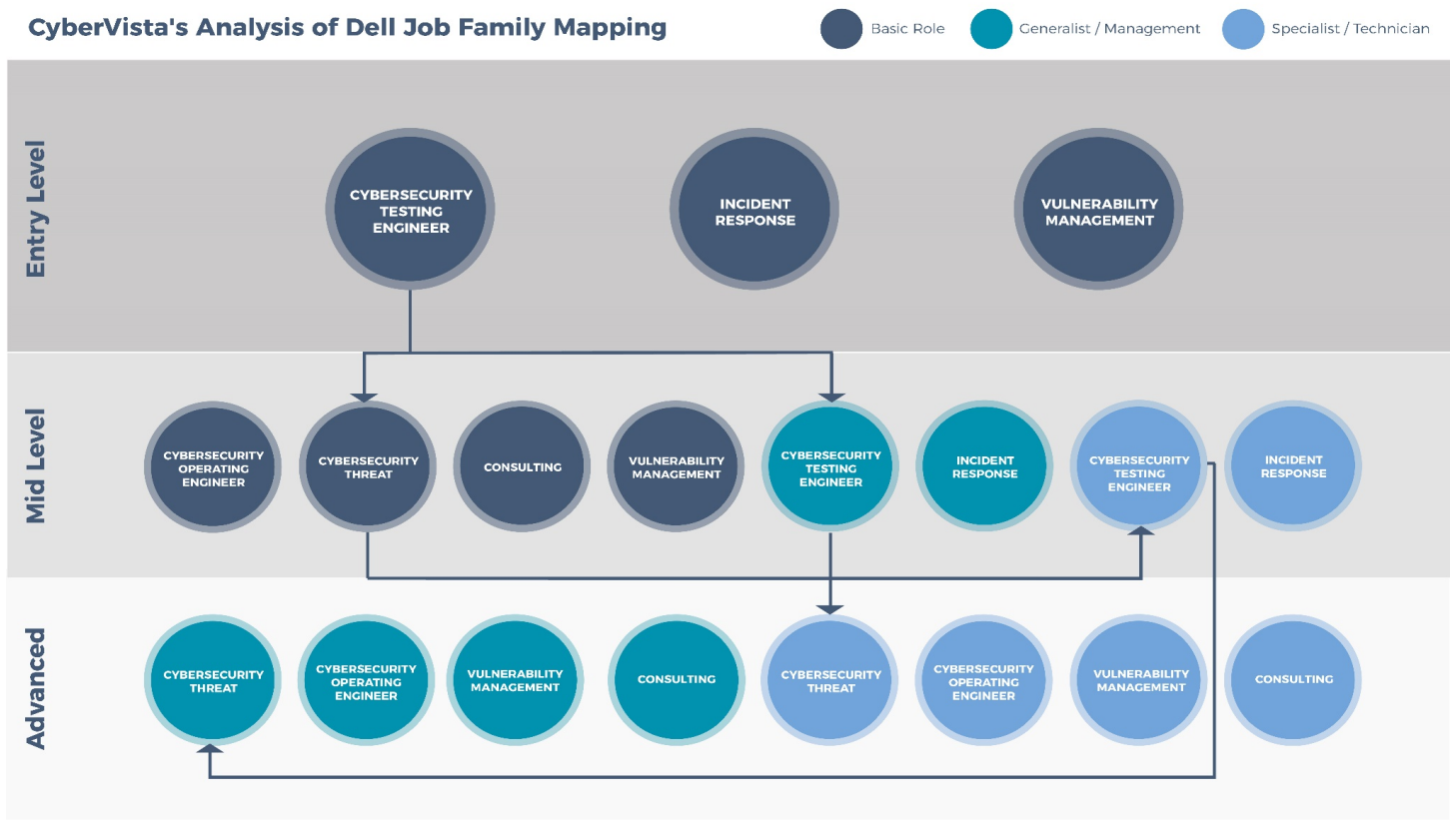
Skill Gap Analysis

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

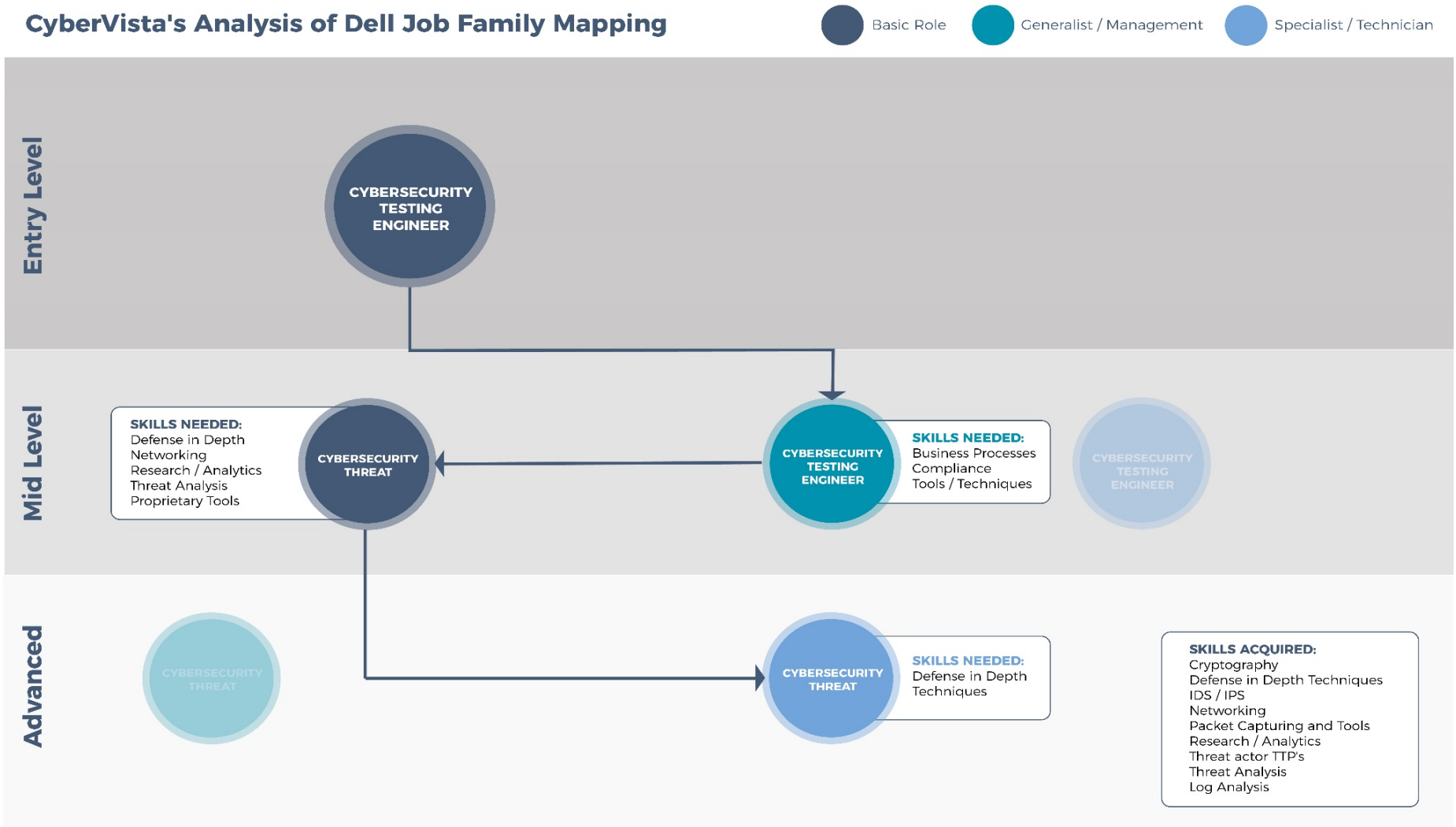
By analyzing the frequency of the requested skills we were able to group them into subsets and identify skills gap between roles

Creating Career Pathways

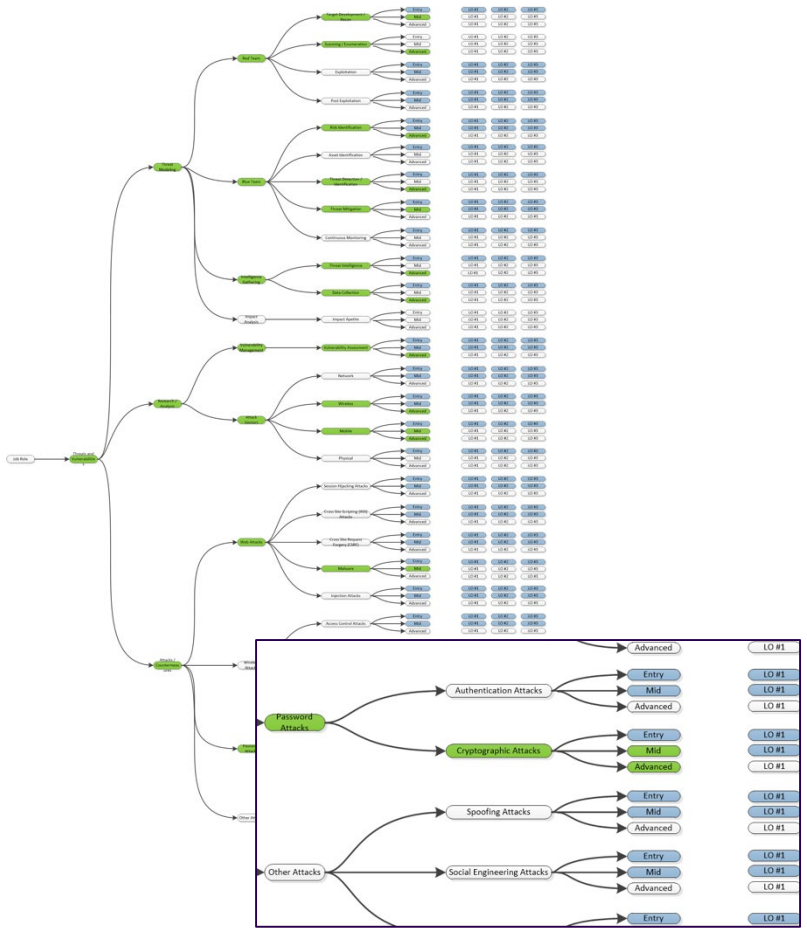


Combining the **defined skills** with a detailed understanding of **Dell's job roles**, we were able to **create and visualize career pathways** that **identify the skill gaps** between different roles and their corresponding levels.

Training Pathways



Training Content



As a result of this effort, we defined a common core of cyber domains, which allowed us to then develop a structured learning taxonomy.

Domain Breakdown

- Governance
- Networking
- Risk
- Threats & Vulnerabilities
- Security Engineering
- Software/Hardware
- Secure Coding
- Soft Skills

Functional Overlay

- Tools and Techniques

Training Content

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

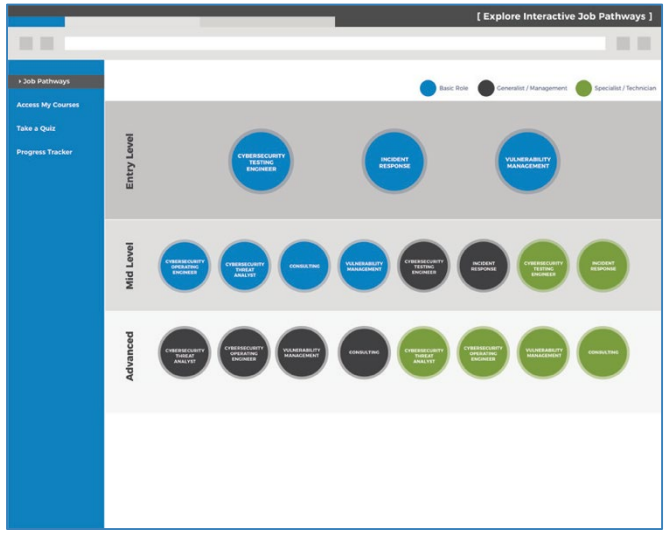
LEARNING/TRAINING

Online and modular for re-skilling or up-skilling

PRACTICE SKILLS

Online and modular for re-skilling or up-skilling

What Next?



Start to move the cybersecurity industry towards professionalization

- Distinguish baseline skills of a “cyber professional” versus those indicative of specialization as core training development
- Combine role-based training needs with the flexibility of a platform based training solution
- Focus on robust training that includes the ability to run diagnostics, provide knowledge-based and experiential learning, and measure results

Apply what you learned today

- Immediately
  - Request from HR your current job families, org comp, framework and guidelines – understand what are your constraints.
  - Determine what market data is being used to decide compensation
  - Formally assign workforce strategy to a leader in your organization

- Within 3 months
  - Inventory person by person the functional roles and responsibilities in your current organization
  - Assess what roles and functions are missing or misaligned