CyberVi

HOW DO YOU MEASURE EXPERTISE?

A New Model for Cybersecurity Education

Simone Petrella
Chief Cyberstrategy Officer, CyberVista

cybervist

CyberVi

DAY'S BERSECURITY UCATION NDSCAPE

C|EH
Certified Ethical Hacker
CHFI
Microsoft
CERTIFIED
Professional
ARMY
WEST POINT
ENNSTATE
1855
CISA
CISM
CSX P
CompTIA
Security+
U.S. AIR FORCE
DSU
DAKOTA STATE
UMUC
CISSP
ITIL
GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org
GCFA
OFFENSIVE security
OSWP
EnCase Certified Examiner
EnCE
ACCESSDATA CERTIFIED EXAMINER
ACE

DAY'S
BERSECURITY
NDSCAPE

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.

VER 260

niversities teach cyber
efense skills

ABOUT 150

Universities teach offensive
cyber skills

85 DIFFERENT

Certifications, training courses, ar
classes were assessed by CyberVis

CyberVi

E 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

CyberVi

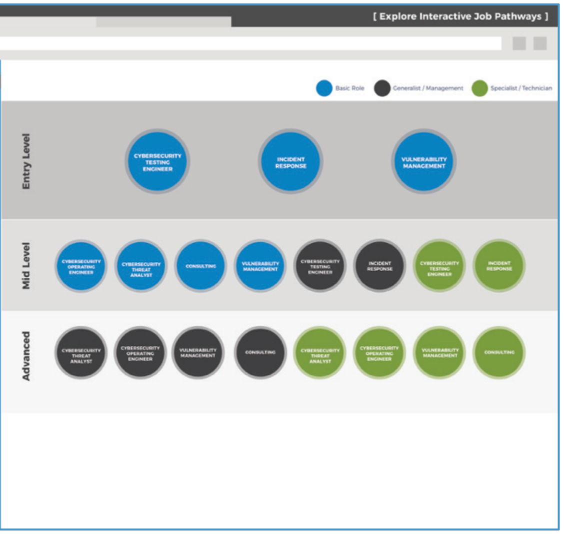
NEW
BER CAREER MODEL

The cybersecurity workforce, including employers an candidates, demands change and requires a new mo for developing careers while earning and maintaining skills. This new model must:

- Distinguish foundational skills from specialized skills
- Account for the multi-disciplined (and non-linear) nat of the profession
- Prioritize efficient and scalable career-pathing
- Assess aptitude and validate abilities
- Apply conceptual understanding to practical experier
- Focus on critical thinking and ability to learn new skil

CyberVi

OW TO GET THERE

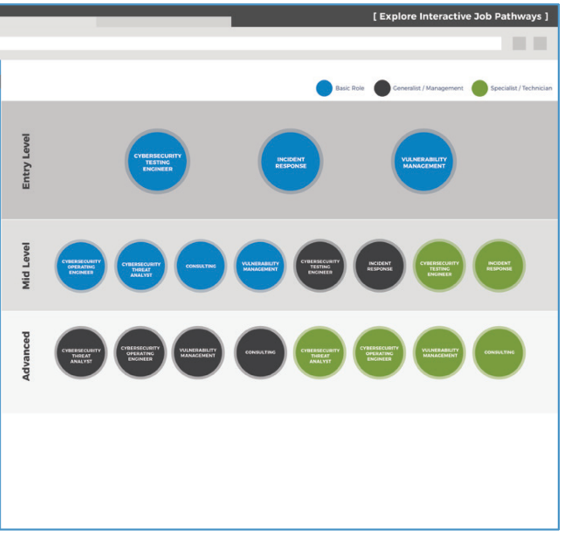

[Explore Interactive Job Pathways]
Basic Role
Generalist / Management
Specialist / Technician
Entry Level
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
VULNERABILITY MANAGEMENT
Mid Level
CYBERSECURITY OPERATING ENGINEER
CYBERSECURITY THREAT ANALYST
CONSULTING
VULNERABILITY MANAGEMENT
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
Advanced
CYBERSECURITY THREAT ANALYST
CYBERSECURITY OPERATING ENGINEER
VULNERABILITY MANAGEMENT
CONSULTING
CYBERSECURITY THREAT ANALYST
CYBERSECURITY OPERATING ENGINEER
VULNERABILITY MANAGEMENT
CONSULTING

Focus on a skills-based approach that addresses employer demand

- Start by understanding employer cyber roles and needs
- Develop a modular and flexible framework an model focused on skills as they align to specif job roles
- Standardize a more structured approach to assessing, learning, and reinforcing cyber skill
- Integrate and incorporate both knowledge-based as well as practical hands-on experienc

cybervist

W TO GET THERE


[Explore Interactive Job Pathways]
Basic Role
Generalist / Management
Specialist / Technician
Entry Level
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
VULNERABILITY MANAGEMENT
Mid Level
CYBERSECURITY OPERATING ENGINEER
CYBERSECURITY THREAT ANALYST
CONSULTING
VULNERABILITY MANAGEMENT
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
CYBERSECURITY TESTING ENGINEER
INCIDENT RESPONSE
Advanced
CYBERSECURITY THREAT ANALYST
CYBERSECURITY OPERATING ENGINEER
VULNERABILITY MANAGEMENT
CONSULTING
CYBERSECURITY THREAT ANALYST
CYBERSECURITY OPERATING ENGINEER
VULNERABILITY MANAGEMENT
CONSULTING

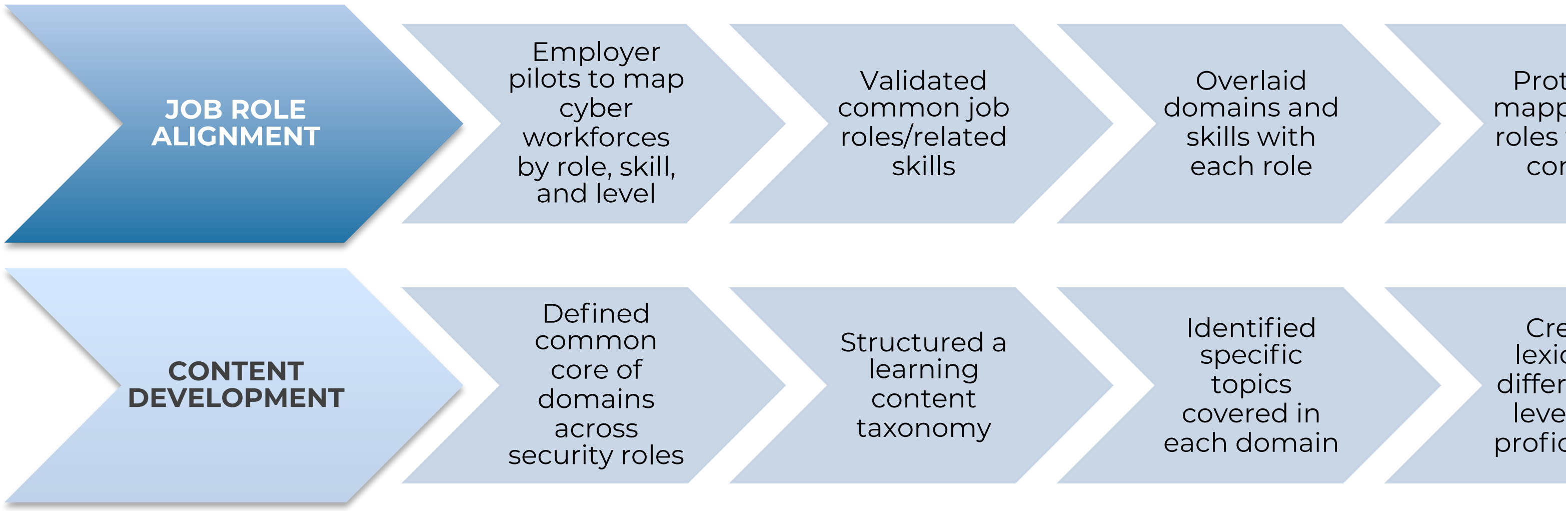
Start to move the cybersecurity industry towards professionalization

- 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

R RESEARCH
OCESS

CyberVi

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 employers** for job roles at multiple levels and **create a roadmap that ties role requirements and skills together.**



JOB ROLE ALIGNMENT

Employer pilots to map cyber workforces by role, skill, and level

Validated common job roles/related skills

Overlaid domains and skills with each role

Prot mapp roles cor

CONTENT DEVELOPMENT

Defined common core of domains across security roles

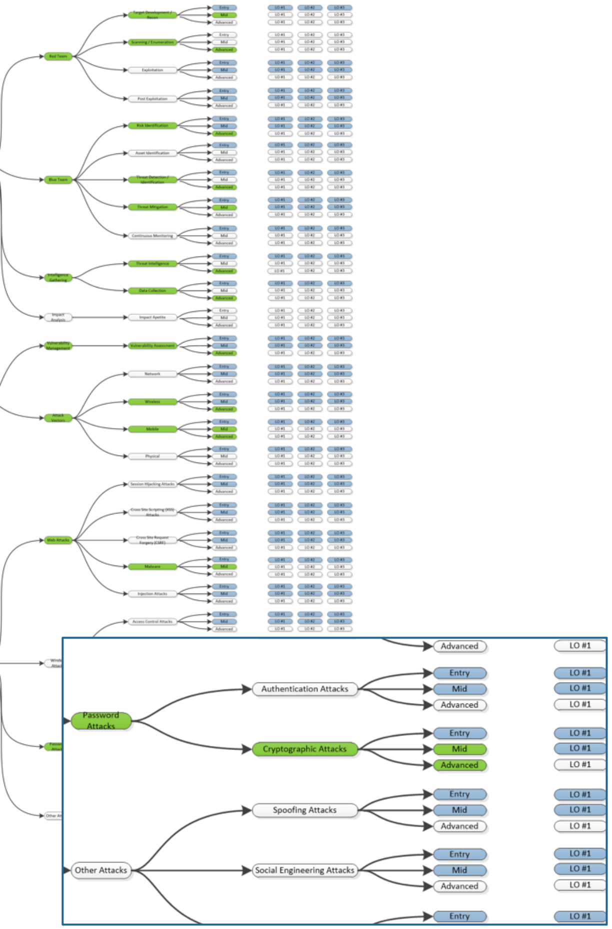
Structured a learning content taxonomy

Identified specific topics covered in each domain

Cre lexic differ leve profic

CyberVi

NTENT XONOMY



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

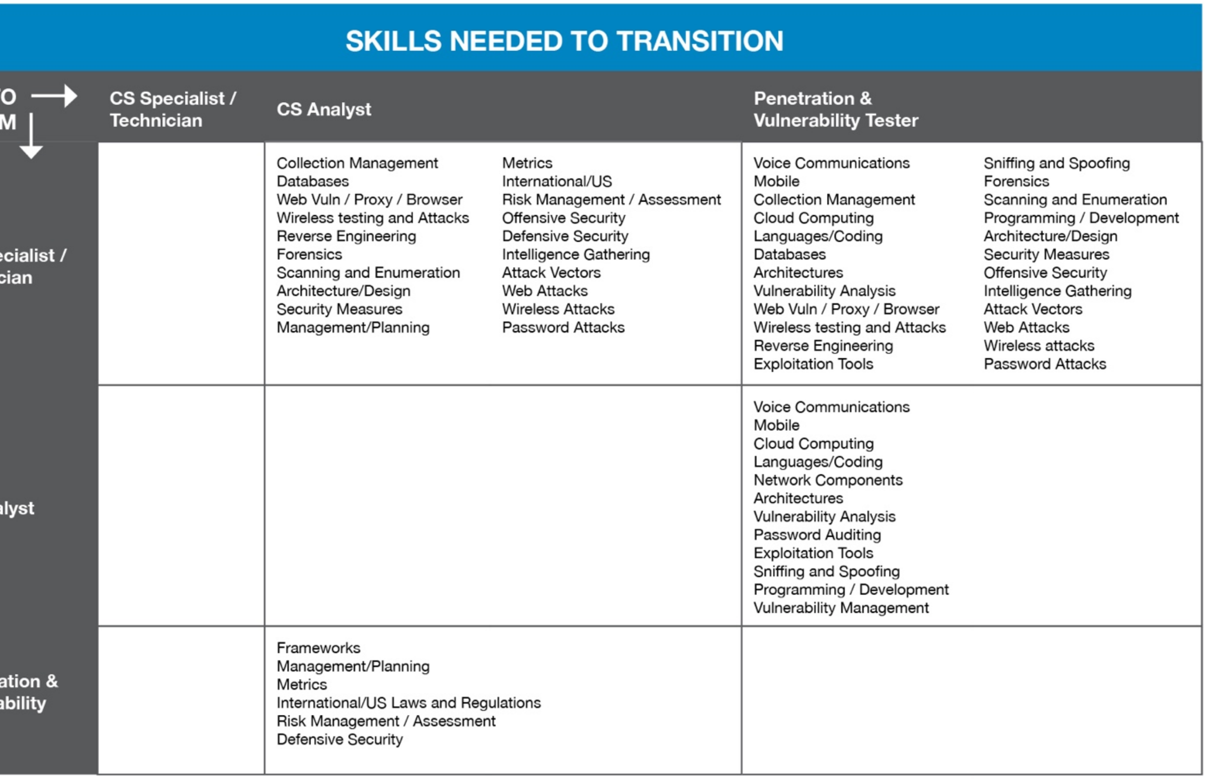
Domain Breakdown

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

Functional Overlay

- Tools and Techniques

ENTIFYING SKILLS
THWAYS

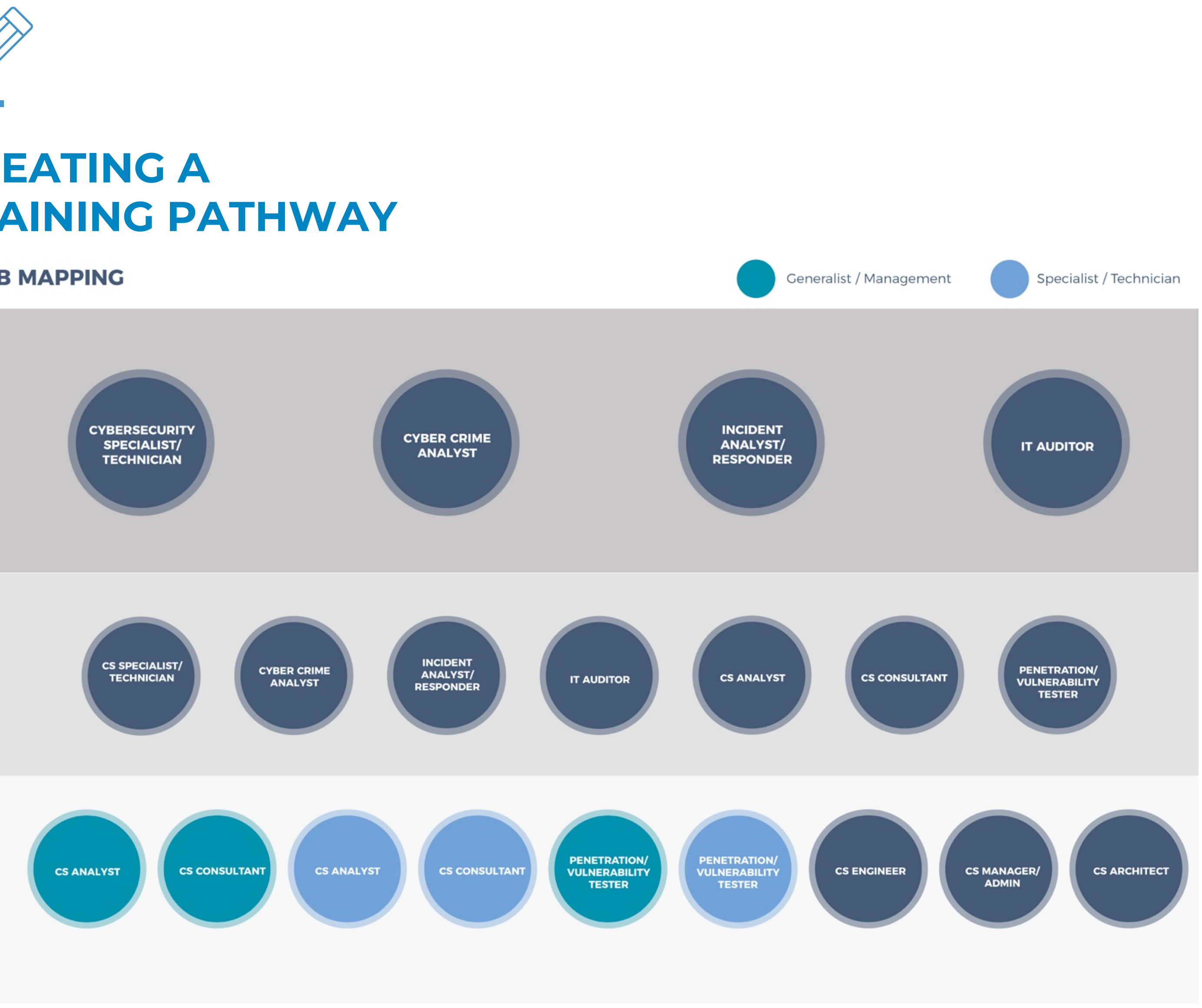


SKILLS NEEDED TO TRANSITION

O → M ↓	CS Specialist / Technician	CS Analyst	Penetration & Vulnerability Tester
ecialist / cian		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
lyst			Voice Communications Mobile Cloud Computing Languages/Coding Network Components Architectures Vulnerability Analysis Password Auditing Exploitation Tools Sniffing and Spoofing Programming / Development Vulnerability Management
ation & ability		Frameworks Management/Planning Metrics International/US Laws and Regulations Risk Management / Assessment Defensive Security	

Based on the NIST Cybersecurit Workforce Framework

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



EATING A AINING PATHWAY

B MAPPING

● Generalist / Management ● Specialist / Technician

CYBERSECURITY SPECIALIST/ TECHNICIAN

CYBER CRIME ANALYST

INCIDENT ANALYST/ RESPONDER

IT AUDITOR

CS SPECIALIST/ TECHNICIAN

CYBER CRIME ANALYST

INCIDENT ANALYST/ RESPONDER

IT AUDITOR

CS ANALYST

CS CONSULTANT

PENETRATION/ VULNERABILITY TESTER

CS ANALYST

CS CONSULTANT

CS ANALYST

CS CONSULTANT

PENETRATION/ VULNERABILITY TESTER

PENETRATION/ VULNERABILITY TESTER

CS ENGINEER

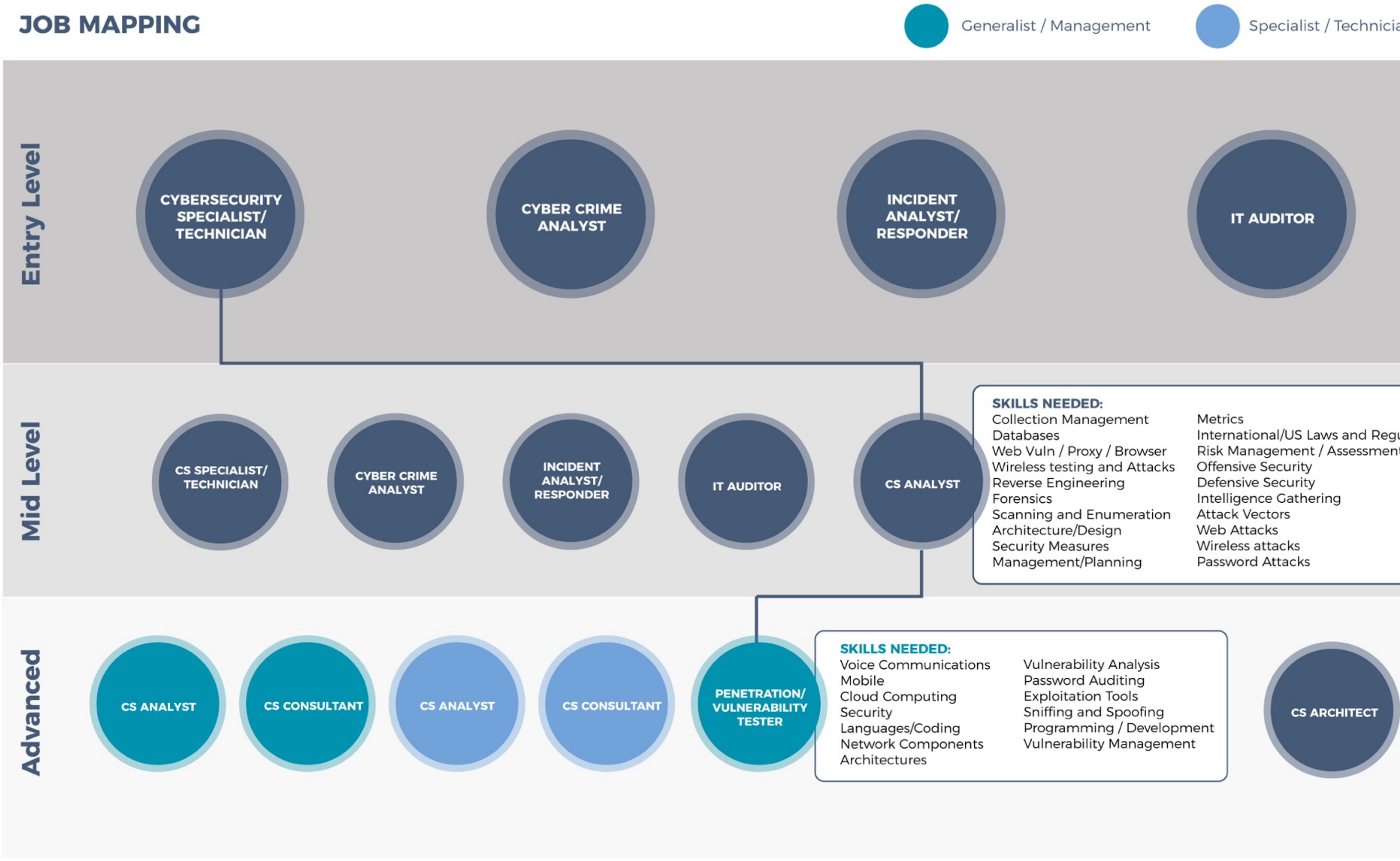
CS MANAGER/ ADMIN

CS ARCHITECT

Once we **defined a taxonomy,** we were able to apply it to a **realistic mapping of job roles** and **create career pathways** that **identify the skills gap** between different roles and their corresponding levels.

EATING A
AINING
THWAY

JOB MAPPING



● Generalist / Management ● Specialist / Technicia

Entry Level

- CYBERSECURITY SPECIALIST/ TECHNICIAN
- CYBER CRIME ANALYST
- INCIDENT ANALYST/ RESPONDER
- IT AUDITOR

Mid Level

- CS SPECIALIST/ TECHNICIAN
- CYBER CRIME ANALYST
- INCIDENT ANALYST/ RESPONDER
- IT AUDITOR
- CS ANALYST

SKILLS NEEDED:
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 Laws and Regu
Risk Management / Assessmen
Offensive Security
Defensive Security
Intelligence Gathering
Attack Vectors
Web Attacks
Wireless attacks
Password Attacks

Advanced

- CS ANALYST
- CS CONSULTANT
- CS ANALYST
- CS CONSULTANT
- PENETRATION/ VULNERABILITY TESTER
- CS ARCHITECT

SKILLS NEEDED:
Voice Communications
Mobile
Cloud Computing
Security
Languages/Coding
Network Components
Architectures
Vulnerability Analysis
Password Auditing
Exploitation Tools
Sniffing and Spoofing
Programming / Development
Vulnerability Management

LANCING
UALITATIVE AND
UANTITATIVE
EASURES

Help organizations better define their job roles assess and support the professional development of their 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-ski
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