UNDERSTANDING WORKFORCE ATTRIBUTES BY EXPLORING EMPIRICAL CAREER PATHWAYS OF CYBERSECURITY PROFESSIONALS

Information Technology and Decision Sciences

November 8, 2018

Dan J. Kim, Ph.D.

University of North Texas

Need for Cybersecurity Workforce

- The 2018 Global Risk Report by the World Economic Forum has listed cybersecurity attacks as the second most likely cause of global instability behind environmental disaster.

- Cybersecurity workforce participation will grow at 10% annually from 2015 to 2020, and that annual spending on cybersecurity will reach $170 billion (Morgan, 2015).

Table 6: Top-Ten Most Difficult to Find and Most Important Technical Skills, 2017

Technical Skill or Capability	Percentage Selecting	
	Most Difficult to Find *(% Selecting)*	Most Important to Organization *(% Selecting)*
Security / Cybersecurity	**1** *(52.2%)*	**1** *(50.6%)*
Analytics / Business Intelligence / Big Data / Data Scientist	**2** *(41.7%)*	**2** *(36.0%)*
Analyst --- Business (a)	**3** *(23.3%)*	**3** *(31.0%)*
Functional Area Knowledge	**4** *(20.9%)*	**4** *(21.6%)*
Architecture / Architect --- Application / Solution (b)	**5** *(18.0%)*	**5** *(19.9%)*
Cloud	**6** *(17.4%)*	**8** *(19.1%)*
ERP (Enterprise resource planning)	**7** *(16.9%)*	**5** *(19.9%)*
Architecture / Architect --- Data / Information (c)	**8** *(15.9%)*	**10** *(15.3%)*
Architecture / Architect --- Enterprise (d)	**9** *(15.3%)*	**13** *(11.7%)*
Software Packages / COTS (e.g., ERP, CRM, DBMS, etc.) (e)	**10** *(13.8%)*	**11** *(14.0%)*
Agile Software Development	**11** *(12.6%)*	**9** *(15.6%)*
IT Project Manager	**12** *(12.2%)*	**5** *(19.9%)*

(a) New item added in 2017. However, "Business Analysis" appeared on the list of soft skills in 2015 and was 4th on most difficult to find and 3rd on most important.

(b) In 2015, "Architecture / Architect --- Application /Solution" was "Application / Solution Architecture."

(c) In 2015, "Architecture / Architect --- Data / Information" was "Data / Information Architecture."

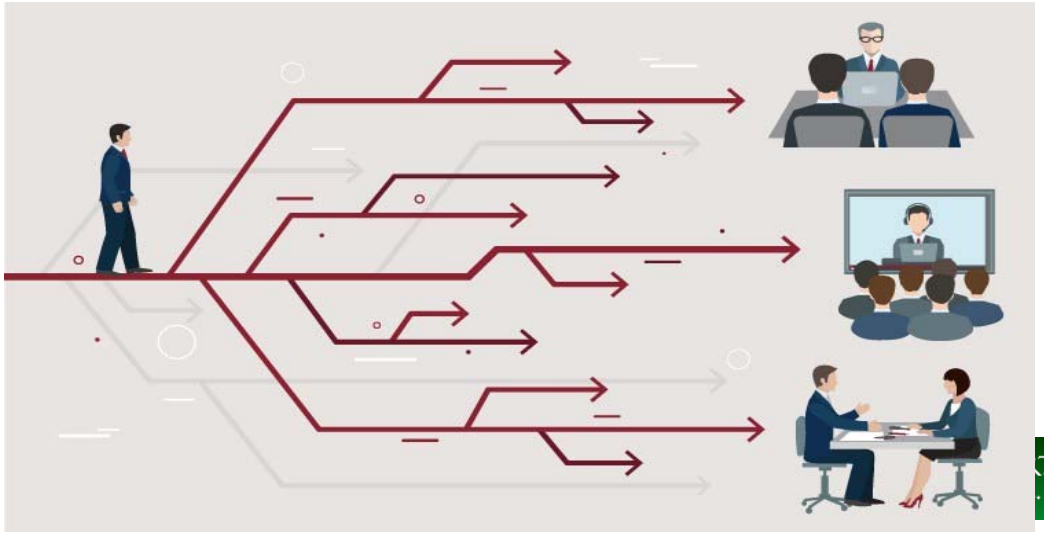
(d) In 2015, "Architecture / Architect --- Enterprise" was "Enterprise Architect."

(e) New item added in 2017.

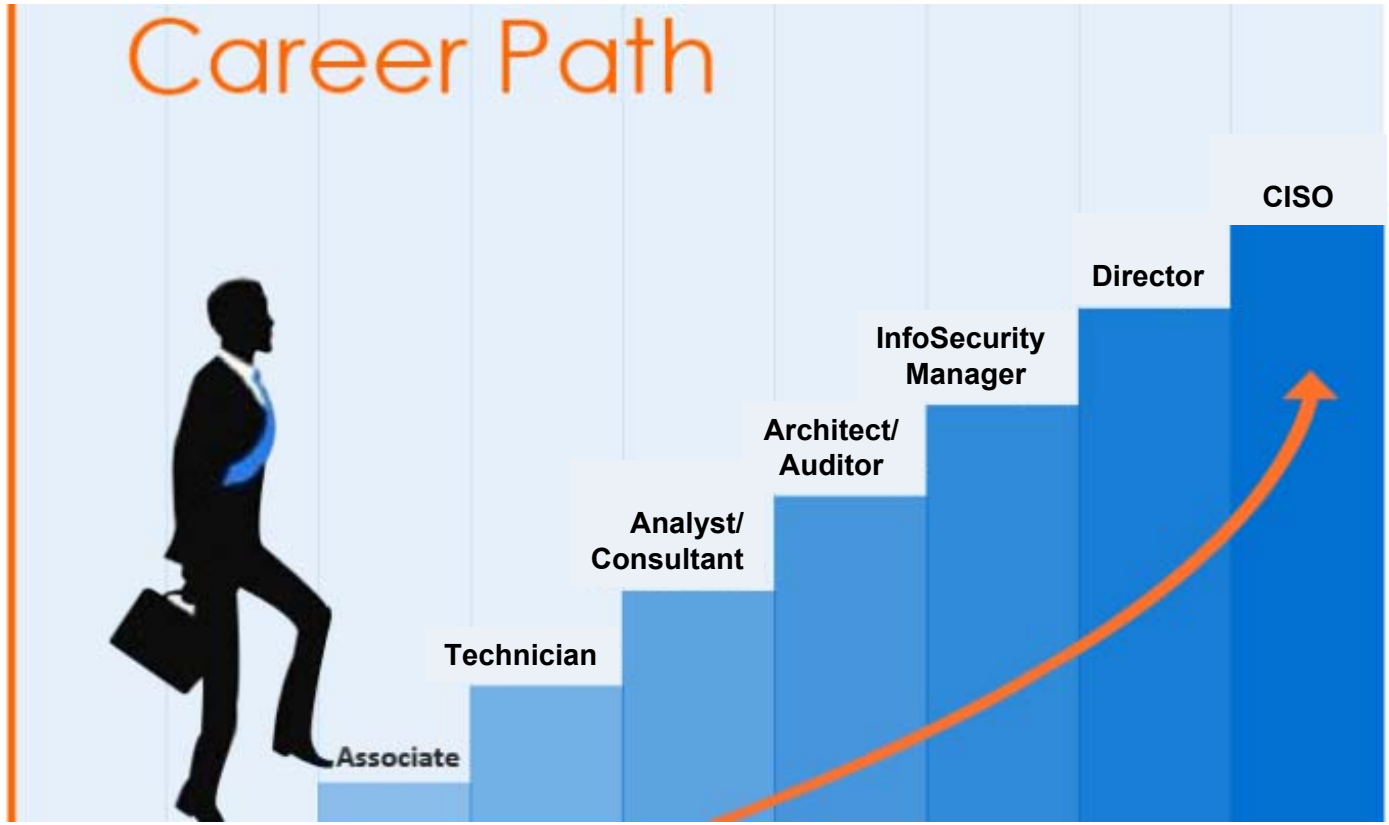
n = most senior IT leader in 769 unique organizations

Career Paths of Cybersecurity Professionals

- There are many opportunities for cybersecurity workforce
- There are many career paths with different workforce attributes (factors)



Factors Affecting Career Path



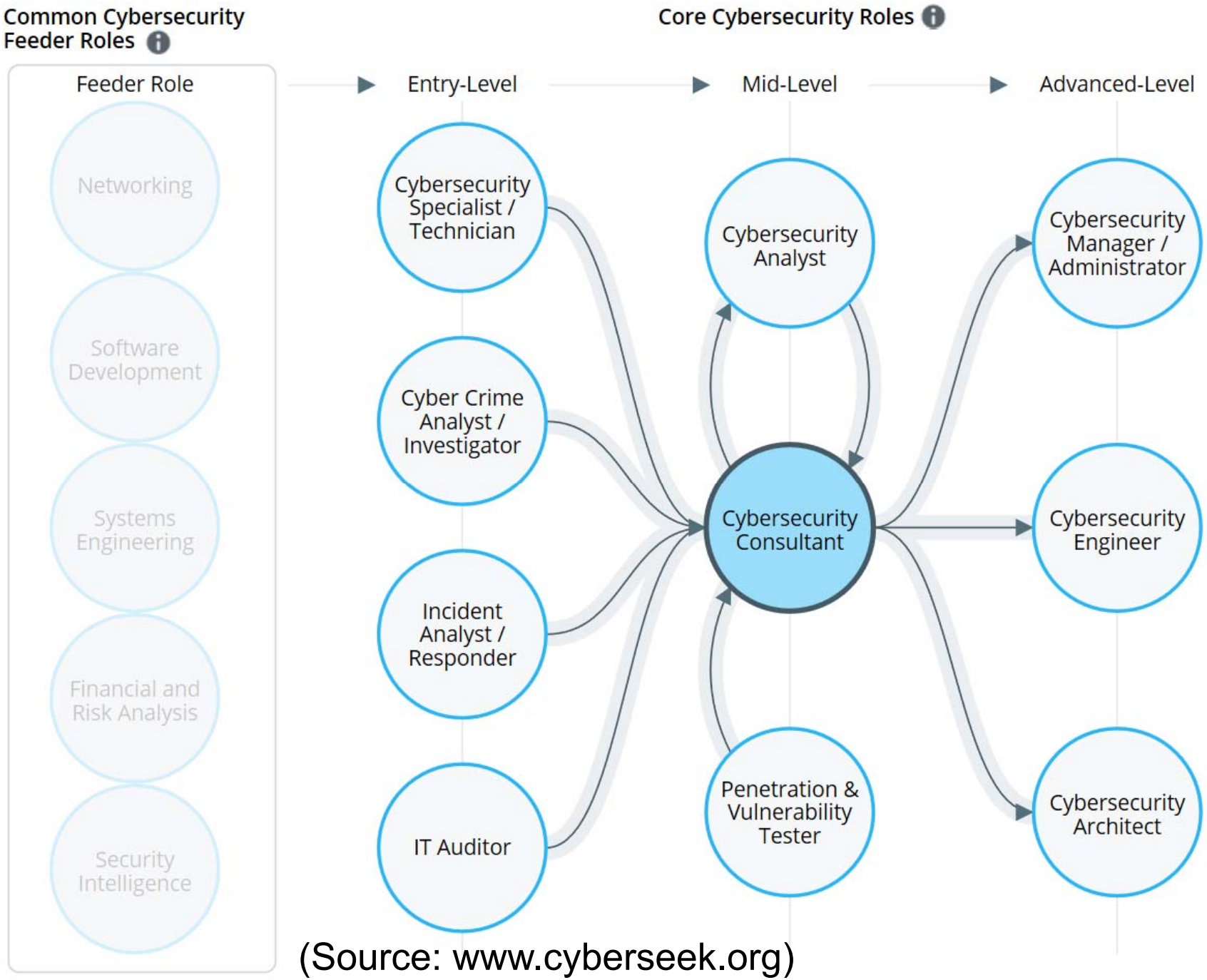
Leadership,
Knowledge
Skills, Ability
Credentials,
Experience,
Citizenship,
Security
Clearance, etc.

Not easy to see a big picture

Review on Previous Relevant Work

Existing Industry Frameworks

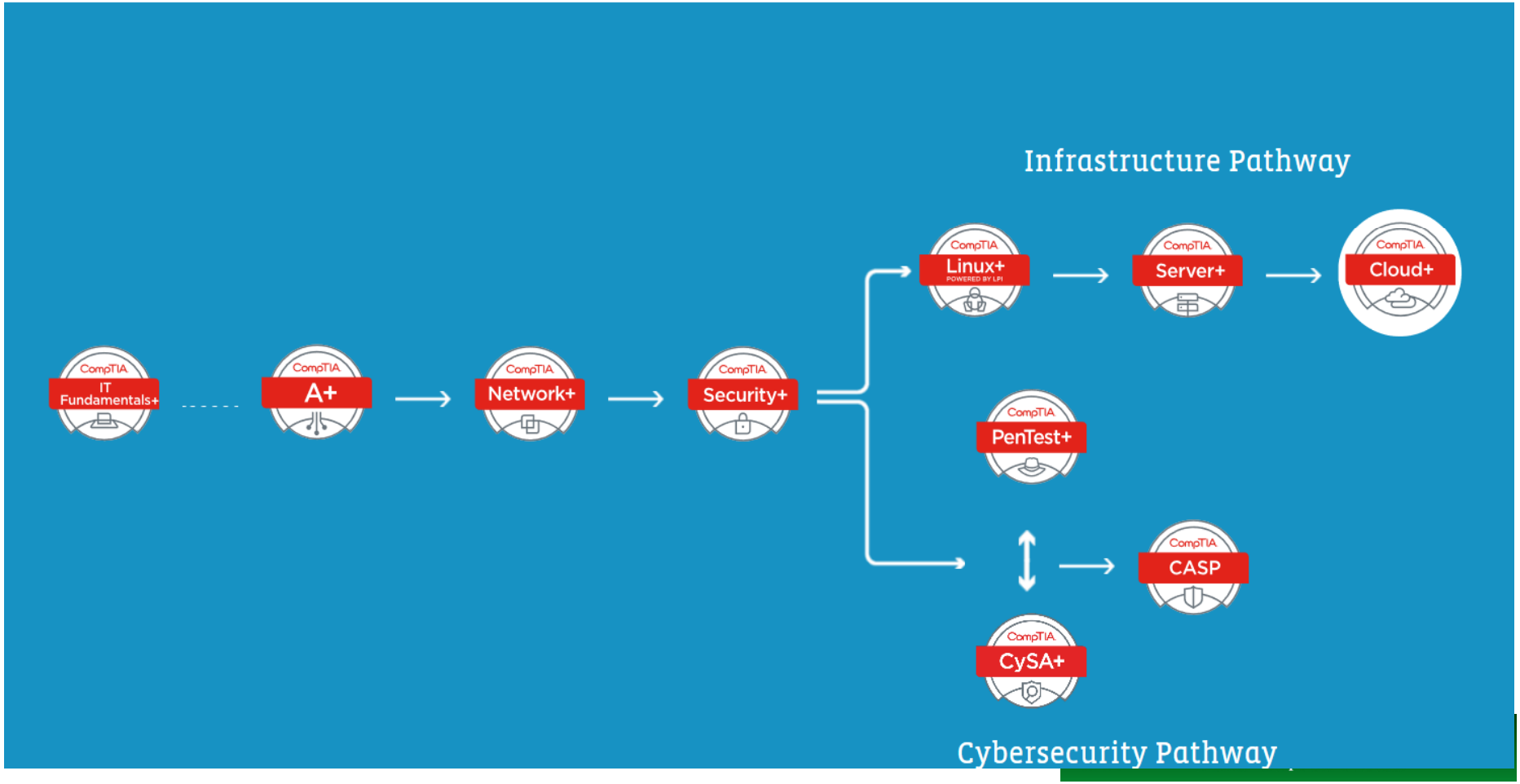
- Cybersecurity Career Pathway by CyberSeek (www.cyberseek.org)
- CompTIA Cybersecurity Career Pathway (certification.comptia.org/certifications)
- EC-Council Career Path by CAST (Center for Advanced Security Training)
- SANS training/certification roadmap (www.giac.org/certifications/get-certified/roadmap)



(Source: www.cyberseek.org)

CompTIA Career Pathway

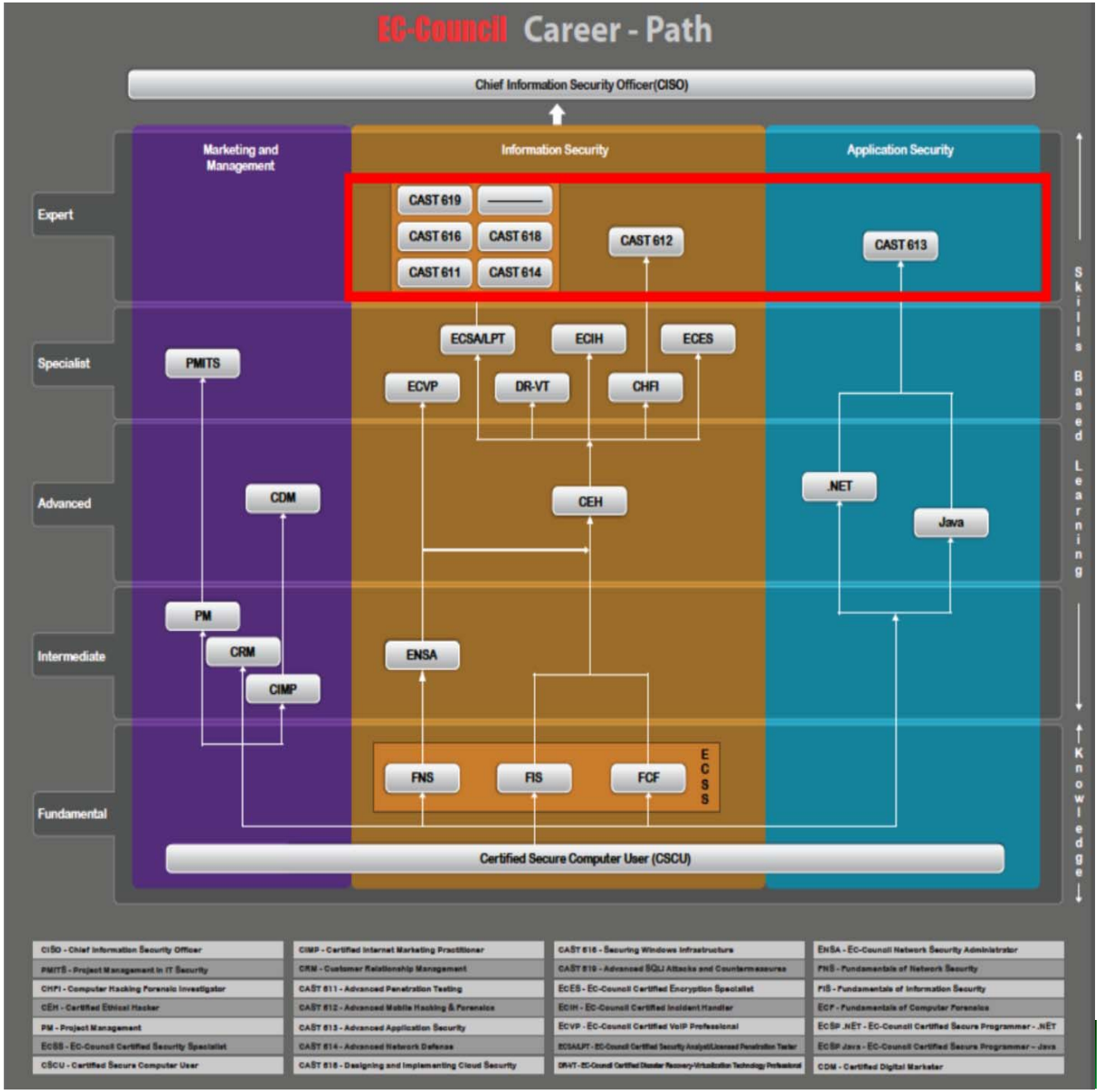
CompTIA certifications align with IT infrastructure and cybersecurity career paths, with each added certification representing a deepening of your expertise. Core certifications, like CompTIA A+, lay the groundwork for the specialized pathway certifications, and additional professional certifications cover necessary IT skills like project management.



EC-Council Career Path

EC-Council *offers a range of Information Security courses, starting from the bare essentials for fundamental preparation till they reach the most advanced and highly technical training.*

CAST *courses lie within the top layer of InfoSec training where professionals challenge their own knowledge and become subject matter experts.*



Training Roadmap | Development Paths

Key: Topic | Course Code | GIAC Certification
Advanced Generalist | SEC501 Advanced Security Essentials – Enterprise Defender | GCED
Course Title

Baseline Skills

Focus Job Roles

Crucial Skills, Advanced, or Specialized Roles

SANS comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

1 You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques | Prevent, Defend, Maintain

Every Security Professional Should Know	
Security Essentials	SEC401 Security Essentials Bootcamp Style | GSEC
Hacker Techniques	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

New to Cybersecurity	SEC301 Introduction to Cyber Security | GISF

1b You will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management | Managing Technical Security Operations

Every Security Manager Should Know	
Leadership Essentials	MGT512 Security Leadership Essentials for Managers | GSLC
Critical Controls	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

CISSP® Training	MGT414 SANS Training Program for CISSP® Certification | GISP

2 You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection | Intrusion Detection, Monitoring Over Time

Scan Packets & Networks	
Intrusion Detection	SEC503 Intrusion Detection In-Depth | GCIA
Monitoring & Operations	SEC511 Continuous Monitoring and Security Operations | GMON

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing | Vulnerability Analysis, Ethical Hacking

Every Pen Tester Should Know	
Networks	SEC560 Network Penetration Testing and Ethical Hacking | GPEN
Web Apps	SEC542 Web App Penetration Testing and Ethical Hacking | GWAPT

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but is essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting | Host & Network Forensics

Every Forensics and IR Professional Should Know		
Endpoint Forensics	FOR500 Windows Forensic Analysis | GCFE	FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting | GCFA
Network Forensics	FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GNFA	

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations | Harden Specific Defenses

Specialized Defensive Area	
Advanced Generalist	SEC501 Advanced Security Essentials – Enterprise Defender | GCED
Cloud Security	SEC545 Cloud Security Architecture and Operations
Windows/ Powershell	SEC505 Securing Windows and PowerShell Automation | GCWN
Linux/ Unix Defense	SEC506 Securing Linux/Unix | GCUX
Virtualized Data Centers	SEC579 Virtualization and Software-Defined Security
SIEM	SEC555 SIEM with Tactical Analytics | GCDA
Other Advanced Defense Courses	
Critical Controls	SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | GCCC
Security Architecture	SEC530 Defensible Security Architecture
Threat Defense	SEC599 Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses | GDAT

Specialized Penetration Testing | Focused Techniques & Areas

In-Depth Coverage	
Vulnerability Assessment	SEC460 Enterprise Threat and Vulnerability Assessment
Networks	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GXPN
	SEC760 Advanced Exploit Development for Penetration Testers
Web Apps	SEC642 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques
Mobile	SEC575 Mobile Device Security and Ethical Hacking | GMOB
Wireless	SEC617 Wireless Penetration Testing and Ethical Hacking | GAWN
Hands-On Ranges	SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise
Python Coding	SEC573 Automating Information Security with Python | GPYC

Digital Forensics, Malware Analysis, & Threat Intel | Specialized Investigative Skills

Malware Analysis	
Malware Analysis	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GREM
Threat Intelligence	
Cyber Threat Intelligence	FOR578 Cyber Threat Intelligence | GCTI
Digital Forensics & Media Exploitation	
Smartphones	FOR585 Advanced Smartphone Forensics | GASF
Memory Forensics	FOR526 Memory Forensics In-Depth
Mac Forensics	FOR518 Mac Forensic Analysis

Advanced Management | Advanced Leadership, Audit, Legal

Management Skills	
Planning, Policy, Leadership	MGT514 Security Strategic Planning, Policy, and Leadership | GSTRT
Project Management	MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep | GCPM
Audit & Legal	
Audit & Monitor	AUD507 Auditing and Monitoring Networks, Perimeters & Systems | GSNA
Law & Investigations	LEG523 Law of Data Security and Investigations | GLEG

Industrial Control Systems

ICS Security Professionals Need	
Essentials	ICS410 ICS/SCADA Security Essentials | GICSP
ICS Defense & Response	ICS515 ICS Active Defense and Incident Response | GRID
NERC Protection	
NERC Security Essentials	ICS456 Essentials for NERC Critical Infrastructure Protection | GCIP

Development & Secure Coding

Every Developer Should Know	
Secure Web Apps	DEV522 Defending Web Applications Security Essentials | GWEB
Secure DevOps	DEV540 Secure DevOps and Cloud Application Security
Language-Specific Courses	
JAVA/JEE	DEV541 Secure Coding in Java/JEE: Developing Defensible Applications | GSSP-JAVA
.NET	DEV544 Secure Coding in .NET: Developing Defensible Applications | GSSP-.NET

Issues and Our Approach

Drawbacks of existing industry frameworks

- Categorized by own products/types (e.g., certifications, training courses, job demands, etc.)
- A *Priori* (i.e., top-down) approach

Our approach,

- Take a *posteriori* (i.e., bottom-up) approach
- Map career progressions through job transitions

Research Purpose

- Develop a cybersecurity career path map
  - To show career progressions through work role transitions with detailed required elements (e.g., credentials, skillsets, knowledge, experience) associated with each role
  - To find key jobs within cybersecurity and common transition opportunities
  - Identify current empirical trends in experience and education preferences

Methodology

- Dataset: Over 1,000 CVs of cybersecurity professionals from “indeed.com” containing cybersecurity work roles
- Capturing:

  work role transitions and key elements
- Data Coding:

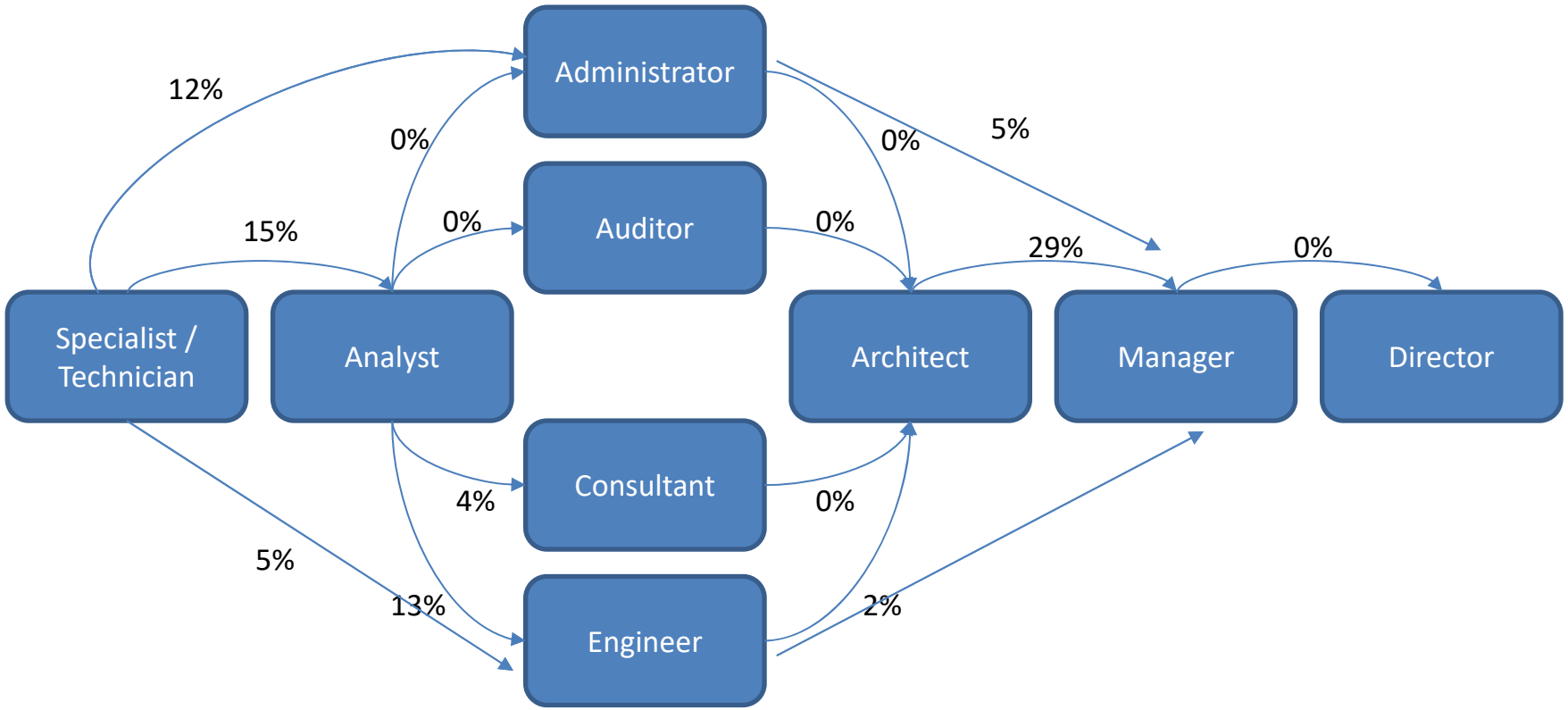
  Work role level/type, education time/type, location, certification type/#, skillsets, experience, military service, security clearance, etc.

CYBERSECURITY PROFESSIONAL JOB TRANSITIONS

		Previous Job Title (Pn-1)											
		Administrator	Analyst	Architect	Auditor	Consultant	Director	Engineer	Manager	Other	Other (Security)	Specialist	Technician
Current Job Title (Pn)	Administrator									1%			
	Analyst		**39%**			**26%**		22%	13%	17%	21%	30%	33%
	Architect							2%		1%	**5%**		
	Auditor				**17%**			4%		1%			
	Consultant		4%			**16%**		4%		2%	2%	4%	
	Director		2%	**43%**		16%	**33%**			1%	5%		
	Engineer		13%			5%	8%	**30%**	8%	8%	7%		
	Manager		5%	29%	**33%**	11%		7%	21%	1%	7%		
	Other		26%	29%	17%	16%	33%	9%	**38%**	**58%**	**40%**	**33%**	33%
	Other (Security)	50%	6%		**33%**		25%	7%	21%	6%	14%	7%	
	Specialist	50%	5%			11%		15%		4%		26%	33%
	Technician		1%							0%			

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

CYBERSECURITY PROFESSIONAL JOB TRANSITION MAP



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Expected Contributions

We can possibly answer following questions.

- What are the most common entry-level jobs in cybersecurity?
- What types of knowledge, skills, and educational credentials are needed to start a cybersecurity career?
- What types of knowledge, skills, and certifications are needed for a specific cybersecurity role?
- What cybersecurity certifications are most in demand in mid-level and advanced-level roles?
- What critical elements (e.g., education levels, certifications, experiences, etc.) do require to be executive-level cybersecurity professionals?

Relevant Literature

- Radziwill, N. & Benton, M. (2017). Cost of quality: Managing the costs of cybersecurity risk management. *Administrative Science Quarterly.* Vol. 19(4).
- Carnevale, A., Smith, N., & Strohl, J. (2010). Help wanted: Projections of jobs and education requirements through 2018. Washington, DC : Georgetown University Center on Education and the Workforce.
- Harris, M., Patten, K. (2015). Using Bloom and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. *Journal of Information Systems Education.* Vol 26 (3).
- Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education, 28*(2), 101-113.
- Schwartz, R. (2016). The career pathways movement: Strategy for increasing opportunity and mobility. *Journal of Social Issues.* Vol. 72(4).
- Wilbanks, L. (2011) Other duties as assigned?. *IT Pro.* IEEE Computer Society.
- National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, https://www.nist.gov/file/359261
- U.S. Department of Homeland Security, Cybersecurity Workforce Development Toolkit (CWDT), https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit