

A complex network diagram with numerous nodes and connecting lines, primarily in blue and red, set against a white background with light blue wavy lines.

Building New Age Cybersecurity workforce for future cyber resilience

Conceptualized and Developed: May– 2021

The objective of this document is to provide an overview of the most imminent cyber threats that are expected to emerge across industries, and how HR leaders can play a crucial role in building a Cybersecurity workforce with New Age skills with Location Intelligence for targeted hiring as well as more notably using Reskilling strategies to overcome the challenge Cybersecurity talent shortage

Copyright @2021 Draup. All rights reserved.

CONTENTS

Pages

3-5

- **How companies are mitigating Cybersecurity threats by partnering with Cybersecurity solution providers**

7-9

- Overview of Cybersecurity team structure with New Age skills

11-13

- Location Intelligence for Cybersecurity roles

15-19

- Reskilling strategies to meet the unmet hiring demands of Cybersecurity roles

This section covers:

- Top cyber breaches & reasons for cyber breach
- Cyber attacks: common & New Age methods
- Top Cyber Security companies & startups

Different loopholes in a company's security Infrastructure are creating new opportunities for threat actors

Poor risk assessment

Inability of organizations to estimate cyberattack risk, exposes the organizations to even greater risks

Social engineering

It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

State Sponsored cyber attacks

With growing geopolitical tensions, Cyber attacks are being funded by rival countries to attack on organizations & stifle business growth

System vulnerabilities

Cybercriminals keep hunting for weakness in system to take advantage. Weakness can be in software or network

Insider Attack

The threat that originates within the targeted organization, this can be current employee or any other former employee, consultant etc.

draup. All Rights Reserved.

Recent major data breaches in companies have caused irreparable damage to company's credibility to safeguard its user data

Exposure: 885 Million Users

Year-2019



Data contained bank account numbers, bank statements, mortgage records, tax documents, Social Security numbers etc., and was available without any protection

Exposure: 130 Users

Year-2020



Social engineering attack on twitter resulted in a selection of high-profile accounts publishing a bitcoin scam. 130 accounts were targeted including those of Barack Obama & Elon Musk

Exposure: 18,000 Users

Year-2020



The attack that was likely orchestrated by Russia, which gave access to thousands of companies and government offices information that used SolarWinds products

Exposure: 1.5 million records

Year-2020



A former employee stole sensitive data of about 1.5 million customers, including names, addresses, phone numbers and account balances.

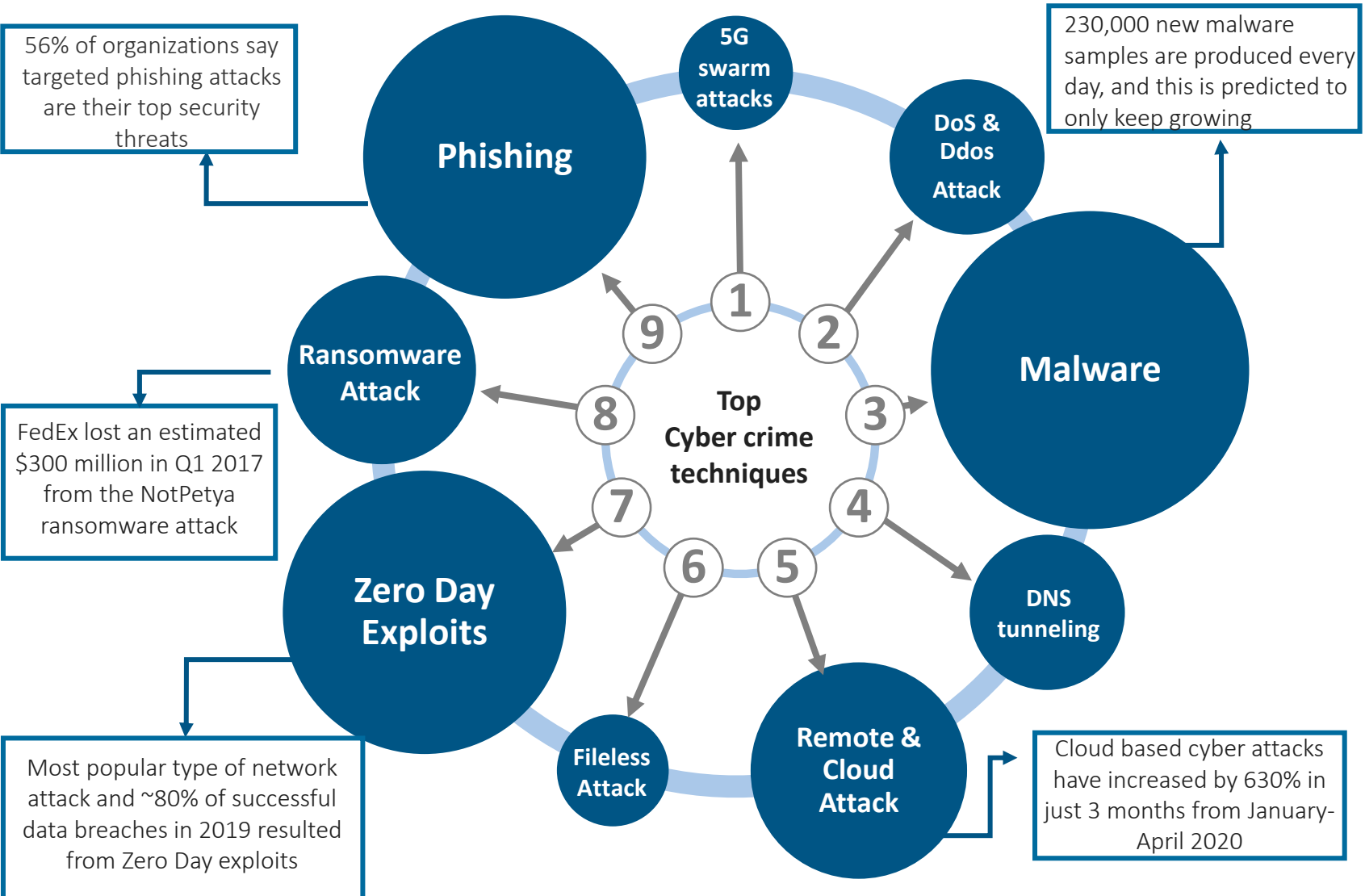
Exposure: 533 million users

Year:2021



Facebook has been part of few biggest data breaches, the most recent data exposed included phone numbers, DOB, locations, past locations, full name, & email addresses.

New techniques like 5G swarm attack, Fileless attacks are also increasingly used by cyber criminals now



Cyber criminals and hackers are getting smarter by using following techniques

Man-in-the-Middle (MiM) attacks to eavesdrop on entire data conversations

Spying software and Google Glass to track fingerprint movements on touch screens

Memory-scraping malware on point-of-sale systems

Bespoke attacks that steal specific data (instead of compromising an entire system)

Copyright © 2021 Draup. All Rights Reserved.

Source: The analysis is based on internal research, insights from customer engagement, and industry blogs, and whitepapers

Top enterprise cybersecurity companies



Broadcom's product Symantec is one of key leader in Endpoint Security, Web Security, Information Security, Email Security, and Privileged Access Management



Infoblox is a leader in secure cloud-managed network services. Helps in securing DNS, DHCP & IPAM, collectively known as DDI. It serves 60% of the Fortune 2000 Companies



Palo Alto Networks' advanced firewalls and cloud-based security products are used by more than 85 of the Fortune 100 companies and 63% of the Global 2000



McAfee's Global Threat Intelligence tools helps to keep businesses, governments, and consumers one step ahead of hackers & protect them from hackers











first cloud-native endpoint security platform, providing services to 10 of 20 largest financial institutions & 5 of 10 largest healthcare providers



Part of Dell tech, SecureWorks offers network, IT, and managed security solutions utilizing automation and AI, actionable insights, analysts, and visibility to predict & combat cyber attacks

Major Start-ups in Cybersecurity space

Start-up	Area of work
	Incident response Investigation
	Cloud native forensics & response platform
	Endpoint Protection
	Threat Detection
	Regulatory Compliance
	Security Segmentation
	Networking, monitoring & security
	Privacy, security & Data Governance

CONTENTS

Pages

3-5

- How companies are mitigating Cybersecurity threats by partnering with Cybersecurity solution providers

7-9

- **Overview of cybersecurity team structure with New Age skills**

This section covers:

- Job role analysis & Technology associated with these roles
- Emerging Skills analysis for job roles

11-13

- Location Intelligence for Cybersecurity roles

15-19

- Reskilling strategies to meet the unmet hiring demands of Cybersecurity roles

Companies are focusing on upgrading their cybersecurity workforce and seeking specific job roles across their Cybersecurity sub domains



Draup has analysed Cybersecurity teams of 100+ leading organizations to provide sample Cybersecurity job taxonomy

Job Family	Cybersecurity							
Sub-family	Security Software Development	Security Architecture	Incident Response	Vulnerability Assessment	Governance & Compliance	Research	Cryptography	Data Loss Prevention & Forensics
Job Roles Across Sub-Categories	Security Software Analyst/ Engineer/ Developer	Network & Information Security Analyst/ Engineer	Security Engineer (Incident Response)	Penetration Tester/ Test Engineer	Analyst Compliance Audit	R&D Specialist	Cryptographer	Digital Forensics expert
	Cyber Security Software Engineer	Cloud Security DevOps Engineer	Incident Response Analyst	Threat Monitoring Analyst	Security Risk & Compliance Analyst	Security Applied Research	Crypt-Analyst	Data loss prevention Engineer
	Application Security Engineer	Cyber Security Architect	Cyber Threat Intelligence Analyst	Vulnerability (Assessment) Analyst	Engineer – Risk, Audit and Compliance	Vulnerability Researcher	Encryption/ Decryption Engineer	Data Loss prevention expert
	Cloud Security Software Engineer	Information Security Consultant	Incident Responder	Web Application Penetration Tester	GRC Consultant	Security Researcher	Crypt Specialist	Fraud prevention manager
	Security Software Infrastructure Developer	Cyber security specialist	Intrusion Detection Specialist	Network Penetration Tester	Privacy and Compliance Officer	Security Research Engineer	Identification Access Management Engineer	Digital Forensics Analyst
	Security Solutions Engineer	Information Security Architect, Cloud	Senior Incident Handler	Threat/ Vulnerability Reporter	IT Risk and Compliance Officer	Threat Research Analyst		Intrusion detection specialist
	Cyber Security Implementation Engineer	Network/Firmware Security Architect	Incident Risk Manager	Vulnerability assessor	GDPR Program Manager	Security Research Specialist		Counterintelligence Forensics Analyst
	Blockchain developer	IoT security specialist		Threat Hunter	GRC manager	Forensics and Malware Research Manager		

Note: Job roles listed in the taxonomy are indicative and not exhaustive. Allied and corporate roles related to areas such as Curriculum Design & Development, Business Continuity, Training have not been included to focus only on core Cyber Security roles



High-demand roles



Emerging roles

Source: Draup

These New Age Cybersecurity roles are using New Age technologies against the highly advanced threat actors to safeguard their company's security

New Age technologies are being leveraged by companies to protect data from tech savvy hackers



Deep Learning

AI/ML is used to analyze mass volume of data sources to predict certain outcomes or optimize processes

AI along with ML is helping enterprises create a real-time, dynamic and global authenticated framework and system that adjusts the access rights based on location or network

Microsoft is using deep learning capabilities to detect & prevent cyber attacks



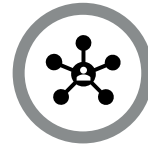
Behavioural & Big Data Analytics

UBA uses big data analytics to identify anomalous behavior by a user

Peer analysis to identify how everyone else is behaving in same department to identify account breach

To identify & train people who are likely to breach company policies

~81% of **US federal agencies** are using big data analytics for cyber security

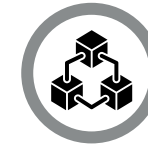


Virtual dispersive network

Dispersive Network splits a message into multiple parts, encrypts each component separately and routes them over servers, computers and even cell phones

Optimization of data flow, thereby increasing speed/performance with negligible network downtime

Clovity has deployed VDN in its critical IoT solutions to benefit retail, healthcare & finance Customers



Blockchain Cyber Security

Blockchain is specific type of database that is stored in blocks and chained together

Blockchain provides cutting-edge Privacy and Data Integrity along with Protected Private Messaging

Helps in improved Public Key Infrastructure (PKI) & Reduced distributed denial-of-service (DDoS) attack

NASA has introduced blockchain in security and is using to secure air traffic services and support

Other Future Technologies

Anti-Malware Detection Systems

Cloud Based security

Quantum Computing

5G based cyber security

Hypervisors

Advanced cybersecurity professionals with New Age skills are limited in the market, there is a huge demand spike of these talent across Industries...

A sample in-demand role '**Cybersecurity Specialist**' have been analyzed further in detail



Sub Function	Workload	Conventional/Existing skills	Emerging Skills	Growth rate (2018-20)
Security Software Development	Developing, implementing, maintaining & testing software security framework to mitigate security vulnerabilities	<ul style="list-style-type: none"> Programming skills & secure coding practices Ethical hacking skills Threat modeling Network architecture/Virtualization technologies 	<ul style="list-style-type: none"> AI knowledge including NLP, ASR & automation. Machine learning skills like predictive analysis Technology specific skills for blockchain & IoT 	↑ 33%
Security Architecture	Identifying weakness in system & build high tech system , solutions to protect against cyber attacks	<ul style="list-style-type: none"> Computer programming Security technology(SIEM, firewall, cloud security) Cloud security & authentication tools knowledge Clustering, Networking 	<ul style="list-style-type: none"> Cryptography fundamentals Security firmware design Threat hunting & trusted platform module knowledge 	↑ 26%
Incident Response	Curate and develop threat intelligence and provide critical support for the Threat Hunting, Cyber Security Operations and Incident Response services	<ul style="list-style-type: none"> Scripting language knowledge SIEM tools like ArcSight, Qradar Log Analysis, threat hunting & escalations Multilingual 	<ul style="list-style-type: none"> External threat assessment(political, economical, social) Threat modelling Automation tools(Phantom/XSOAR) 	↑ 25%
Vulnerability Assessment	perform simulated attacks on computer systems to understand the impact of attacks on business & advising on methods to fix them	<ul style="list-style-type: none"> High level programming skills Encryption algorithms knowledge Testing techniques(white-box, black-box) General networking knowledge 	<ul style="list-style-type: none"> Authentication and authorization protocols, cryptography, automation modern secure development frameworks (Microsoft SDL, OWASL SAMM 2, ASVS, and MASVS) 	↑ 22%
Governance & Compliance	Perform Periodic security testing & Updating risk Management framework including policy, procedures, due diligence questionnaires	<ul style="list-style-type: none"> Project Management Network firewall functionalities Security firmware design framework knowledge 	<ul style="list-style-type: none"> Cryptography fundamentals Advanced security audit skills International IT security risk management & compliance standard knowledge 	↑ 19%
Research	Design, implement, and test components of research prototypes and software systems aimed at solving cutting-edge cyber security research problems	<ul style="list-style-type: none"> Programming skills Reverse engineering skills Rapid prototyping for proof of concepts 	<ul style="list-style-type: none"> Complex Machine learning models Security automation 	↑ 18%
Cryptography	Developing security systems using algorithms and cyphers to encrypt sensitive data & testing cryptology theories according to organization needs	<ul style="list-style-type: none"> High level programming skills Diffie-Hellman key exchange Privacy mechanism Risk management framework, vulnerability management 	<ul style="list-style-type: none"> Machine learning knowledge Familiarity with other post-quantum cryptography families Elliptic curve cryptographic principles 	↑ 16%
Data Loss Prevention & Forensics	Detecting, harvesting and then analyzing all the potential evidence of cyber crime from computers, networks and other associated information	<ul style="list-style-type: none"> Coding knowledge Decompiler tools knowledge Forensics tools like Encase, FTK, X-Ways, SIFT, Splunk 	<ul style="list-style-type: none"> Live response tooling & log aggregation solution Big data experience (Hadoop, HDFS, Apache) Malware reverse engineering Cloud based enterprise systems knowledge 	↑ 22%

Note: Draup leveraged its corpus of 65M+ JDs and 650M+ professional profiles to extract relevant talent data such as workloads, skills, and Job responsibilities for the relevant job roles; Draup leveraged its database of 1M+ digital intentions for employers across multiple industries, extracted from sources such as news articles, job descriptions, video interviews, journals to analyse the digital strategies and use cases of peer companies.

CONTENTS

Pages

3-5

- How companies are mitigating Cybersecurity threats by partnering with Cybersecurity solution providers

7-9

- Overview of Cybersecurity team structure with New Age skills

11-13

- **Location Intelligence for Cybersecurity roles**

This section covers:

- Global & US hotspot for **Cybersecurity Engineer** role
- Top location overview for 'Cybersecurity engineer' role

15-19

- Reskilling strategies to meet the unmet hiring demands of Cybersecurity roles

Global hotspots for 'Cybersecurity Specialist' talent: US is the top location with highest talent availability; Non-US Locations like Sao Paulo, Bengaluru, Johannesburg are highly favorable for cost-effective hiring



Draup analysed 400+ global locations and identified top hotspots with availability of 'Cybersecurity Specialist' talent

'Cybersecurity Specialist' Talent Hotspots – Global

US is one of the key locations with high availability of 'Cybersecurity Specialist' Talent



Talent size globally across Industries

~42,000

Talent cost Globally

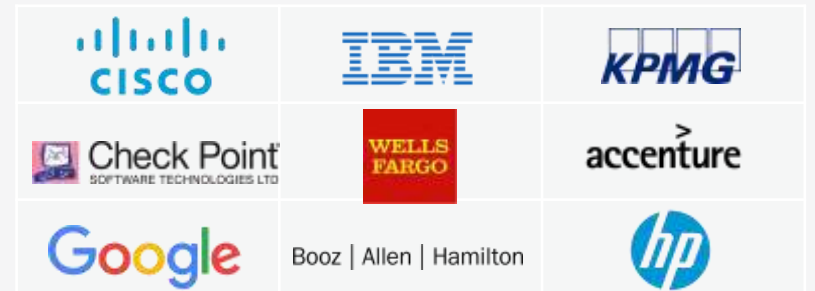
Median Wage/Salary

\$66K

Lowest Salary Globally:

\$9K

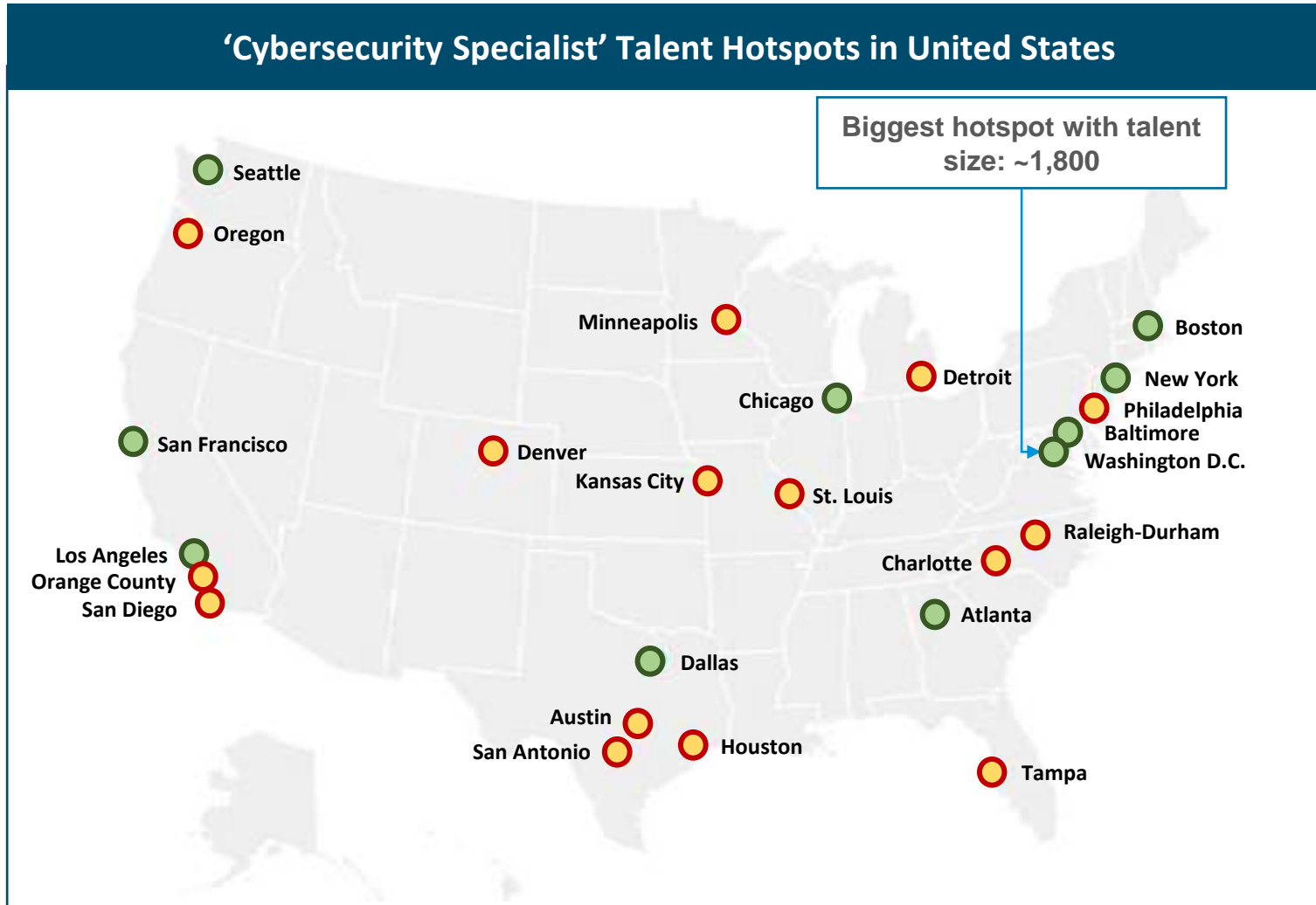
Top Employers with highest 'Cybersecurity Specialist' talent



Copyright © 2021 Draup. All Rights Reserved.

U.S hotspots for 'Cybersecurity Specialist' talent : Washington D.C., San Francisco, New York, Chicago have the largest talent base for 'Cybersecurity Specialist' role

Draup analysed 50+ US locations and narrowed down key talent hotspots of 'Cybersecurity Specialist' roles based on Talent availability



● Talent size > 300
 ● Talent size < 300

Talent size in US
~14,500

Talent cost in US

Median Wage/Salary **\$96K** Highest Salary in US **\$137K**

Top Employers with highest 'Cybersecurity Specialist' talent

Copyright © 2021 Draup. All Rights Reserved.

Source: The represented data has been derived using DRAUP Proprietary Talent Database, Similar analysis can be performed for any job role

Top US Locations Overview for 'Cybersecurity Specialist': Due to huge talent demand in companies across industries, Talent cost for 'Cybersecurity Specialist' role is on higher side across top US locations



Location	Talent Size	Talent Cost	Ethnic Diversity of the talent pool	Top Employers
Washington D.C. Area	1,800	\$93K — \$107K	63% White, 12% Asian, 8% Hispanic, 15% African American, 1% 2 or more races, 1% American Indian and Alaska Native	Booz Allen, Lockheed Martin, CACI
San Francisco Bay Area	1,300	\$125K — \$148K	55% White, 22% Asian, 8% Hispanic, 10% African American, 4% 2 or more races, 1% American Indian and Alaska Native	Check Point, Google, hp
Greater new York City Area	1,100	\$105K — \$123K	60% White, 13% Asian, 12% Hispanic, 11% African American, 4% 2 or more races, 0% American Indian and Alaska Native	IBM, verizon, CISCO
Greater Chicago Area	530	\$91K — \$109K	70% White, 11% Asian, 8% Hispanic, 9% African American, 1% 2 or more races, 1% American Indian and Alaska Native	BOEING, Protection1, Trustwave
Greater Atlanta Area	510	\$91K — \$102K	62% White, 7% Asian, 5% Hispanic, 21% African American, 4% 2 or more races, 0% American Indian and Alaska Native	DELTA, FirstData, IBM
Dallas City Area	500	\$93K — \$104K	65% White, 10% Asian, 10% Hispanic, 13% African American, 1% 2 or more races, 1% American Indian and Alaska Native	AT&T, mitre, CISCO
Greater Los Angeles Area	470	\$98K — \$117K	63% White, 11% Asian, 12% Hispanic, 11% African American, 2% 2 or more races, 1% American Indian and Alaska Native	EDISON, PARSONS, RIOT GAMES
Greater Boston Area	430	\$95K — \$111K	71% White, 10% Asian, 4% Hispanic, 12% African American, 3% 2 or more races, 0% American Indian and Alaska Native	Raytheon, CISCO, mitre

Entry level (0-2 Years) Median Salary Range Senior (8+ Years)
 ■ White ■ Asian ■ Hispanic ■ African American ■ 2 or more races ■ American Indian and Alaska Native

CONTENTS

Pages

3-5

- How companies are mitigating Cybersecurity threats by partnering with Cybersecurity solution providers

7-9

- Overview of Cybersecurity team structure with New Age skills

11-13

- Location Intelligence for Cybersecurity roles

15-19

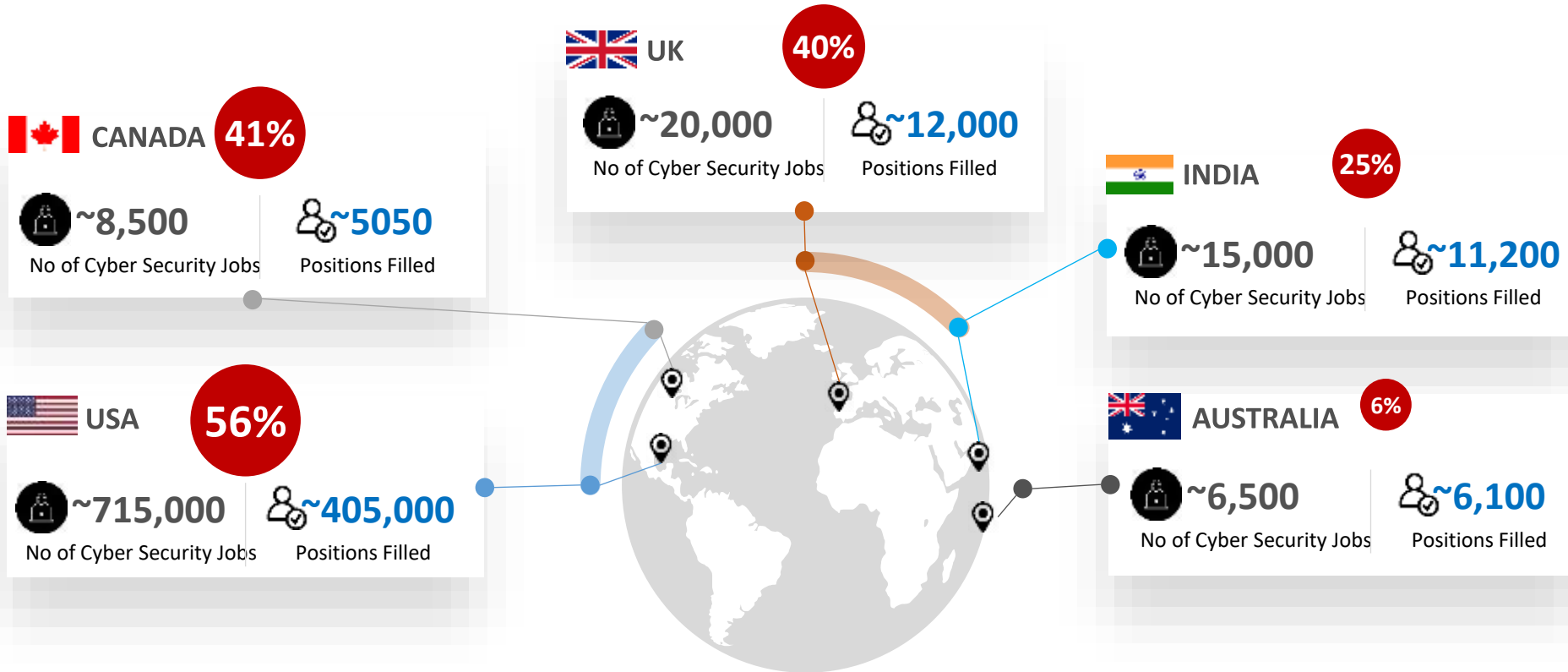
- **Reskilling strategies to meet the unmet hiring demands of Cybersecurity roles**

This section covers:

- Reskilling overview: why reskilling is important for organizations
- Reskilling framework for different types of roles in an organization
- Detailed reskilling analysis for Cyber Security Specialist role

Due to high demand of Cybersecurity professionals, Nearly 3 million Cybersecurity positions are expected to go unfulfilled globally in 2021

Top locations across the globe with unfulfilled Cybersecurity jobs (for year 2020)



~2,000

Jobs posted¹ for Cybersecurity roles in organisations

~46%

professionals² contacted by recruiters weekly, whether they are looking for job or not.

~42%

Organisations unable³ to convert security data into relevant info. due to lack of skilled workforce

~60%

Cybersecurity teams² in organisations are understaffed

0%

Unemployment rate¹ for Cyber security professionals(2011-21).

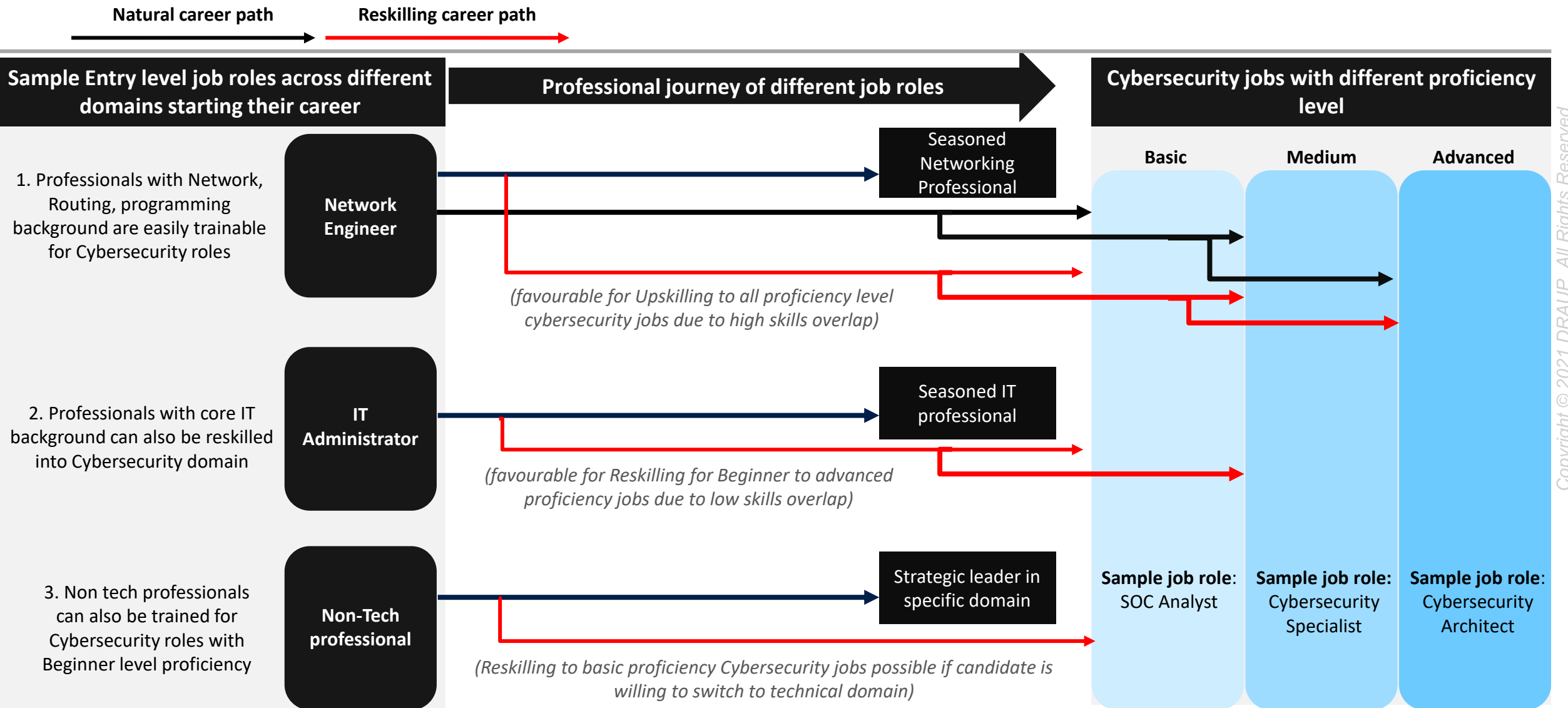
~68%

current Cybersecurity employees³ hold at least one security related certification

As the demand supply gap is expected to further widen, Reskilling has become a key alternative for firms to meet the unmet hiring demand



Sample illustration of how Reskilling can provide an alternate career path of Cybersecurity to both tech and non-tech professionals



Copyright © 2021 DRAUP. All Rights Reserved.

Reskilling/Upskilling can also provide a viable career path for traditional IT job roles as well as Non-tech professionals towards a highly rewarding Cybersecurity career



Sample Reskilling Propensity analysis(RPI¹) of traditional digital native talent existing in the firms who can transform into Cybersecurity roles

	Job roles that can be Upskilled/Reskilled (Experience required: 4+ years)	RPI ²	Sample Parameters ¹ to analyse different skill gaps and career transition trends				Desired role
			Technical Proficiency	Functional Proficiency	Specific Soft Skills Overlap	Observed Career Transitions	
IT professional	Network Engineer	8.2	High	Medium	Low	Low	Cybersecurity Specialist
	System Administrator	6.2	High	Medium	Medium	High	
	Web Developer	5.4	Medium	Medium	Medium	Low	
	IT Administrator	5.2	Medium	Medium	Medium	High	
Uninitiated Non-tech professional	Risk Analyst	4.7	Low	Medium	High	Medium	
	Sales & Marketing Manager	4.4	Low	Medium	High	High	

RPI Range >6.5 - Upskilling

>5 - Reskilling

Score in Individual Parameter

High

Medium

Low

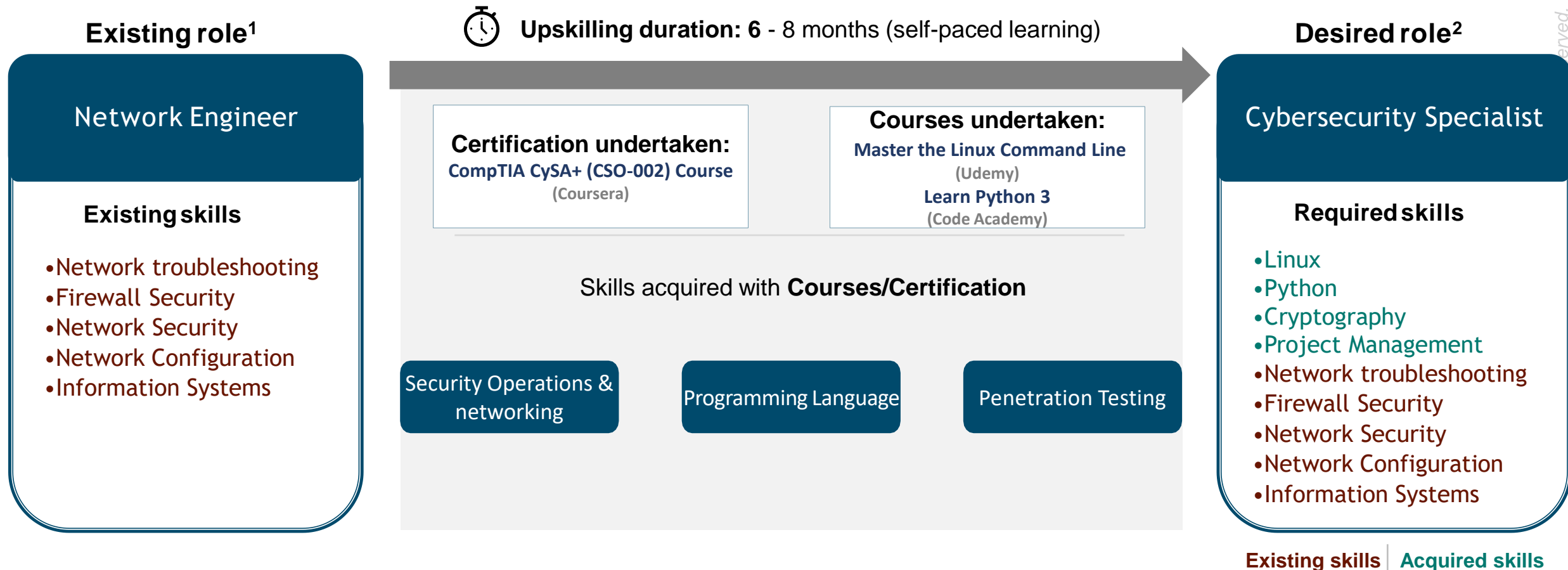
Note: Several other Upskilling parameters are considered in detailed analysis

1. RPI or Upskilling Propensity Index is the Draup's Proprietary scoring index methodology for Reskilling which is based on detailed analysis of relevant parameters

Upskilling case study: Conventional job role such as Network Engineer can be easily upskilled into 'Cybersecurity Specialist' job role by providing programming, Operating systems and cloud security skillsets



Sample Reskilling case study: Based on skill gap analysis, a relevant learning module/course was selected to showcase how A traditional 'Network Engineer' can be reskilled to evolve into high demand 'Cybersecurity Specialist' role



erved.

1. Network Engineer considered here should have 4+ years experience with high overlapping skill sets of Cyber Security Specialist
2. During transition time (6-8 months), Upskilled Network Engineer can be utilised to cater basic level Cyber Security Specialist workloads and can be trained simultaneously inhouse to gain advanced expertise
Note: Draup performs complex assessment around various other critical Reskilling parameters between existing and desired roles to understand skill gap and match it with relevant learning modules

Reskilling case study: Core IT roles and Non- tech professionals can also transition into Cybersecurity roles with strategic Reskilling; Nearly 30% of global Cybersecurity professionals are from non-tech background



Reskilling journey of professionals with little or zero skills overlap with Cybersecurity roles

Starting role

Understanding computer programming & Linux systems will create solid foundation to learn advanced cybersecurity skills

Networking systems & cloud certification course will provide intermediary knowledge required to be job ready

Project management & Agile methodology for easier cross team collaboration & working

End role

Uninitiated professional

Computer Programming

- C Programming For Beginners Udemy
- Perl 5 Essential Training LinkedIn Learning
- Learn Python 3 Code Academy
- Java Fundamentals: The Java Language Pluralsight

Security operations & Networking

- CompTIA CySA+ (CSO-002) Course Udemy
- SIEM with Tactical Analytics SANS
- Fundamentals of Network Communication Coursera
- Cisco Networking Foundation LinkedIn Learning

Scripting – Linux & Unix Systems

- Linux Mastery Udemy
- Linux Security and Hardening Linux Academy
- The Unix Workbench Coursera
- PowerShell Essential Training LinkedIn Learning

Cloud Security

- Cloud Security Basics Coursera
- Splunk Fundamentals 1 Splunk
- CompTIA Cloud+ (CV0-002) Certification Course LinkedIn Learning

Agile Methodologies

- Agile Process, Project, and Program Controls edX
- Software Processes and Agile Practices Coursera

Cyber Security Specialist

Certification program and hands on sample project

Certified Cybersecurity Professional™ - A Flagship Certification of Global Tech Council

Developing surveillance software with ability to record every keystroke made on that system - Keylogger

Job Ready Proficiency (8 -12 Months)

Copyright © reserved.

Note: Draup performs complex assessment around various other critical Reskilling parameters between existing and desired roles to understand skill gap and match it with relevant learning modules

About Draup

About Draup: Draup uses Machine learning models to perform analysis provided in the report, Global HR leaders of leading firms are leveraging Draup for taking Data-driven Talent decisions



Draup Capabilities & Data Assets



EMPOWERS DECISION MAKING IN

- Recruitment**
- Strategic Workforce Planning**
- Peer Intelligence**
- Diversity & Inclusion**
- Learning & Development**
- Compensation & Benefits**
- University Relations**
- Mergers and Acquisitions**

and diverse other use cases...

Draup highlights: Draup tracks insights of 4,500+ job roles across 2,500+ locations and analyses 50 Million+ digital & digitally influenced professionals to help HR leaders in their Talent Acquisition, Workforce planning, and Reskilling initiatives



50M+

DIGITAL AND DIGITALLY
INFLUENCED
PROFESSIONALS

4.5K+

JOB ROLES

300K+

PEER GROUP
COMPANIES

33

INDUSTRIES

65M+

JOB
DESCRIPTIONS

100K+

COURSES

2.5K+

LOCATIONS

7K+

UNIVERSITIES

4M+

CAREER PATHS
ANALYZED

30K

SKILLS

7K+

DIGITAL TOOLS &
PLATFORMS

30K+

UNIVERSITY PROFESSORS

52

MACHINE LEARNING
MODELS DEVELOPED

10M+

DAILY DATA POINTS
ANALYZED

100+

LABOR STATISTICS
DATABASES

1000+

CUSTOM TALENT
REPORTS



 **draup**
www.draup.com

info@draup.com

SANTA CLARA | HOUSTON | BANGALORE | GURGAON | COIMBATORE | NEMILI

© 2021 Draup. All Rights Reserved.