

An abstract background graphic consisting of numerous thin, wavy lines in shades of blue and red, some with small dots at their ends, creating a sense of movement and data flow. The lines are more densely packed on the left side and spread out towards the right.

Global Cybersecurity Talent shortage: Hiring and Reskilling strategies

Conceptualized and Developed: April – 2022

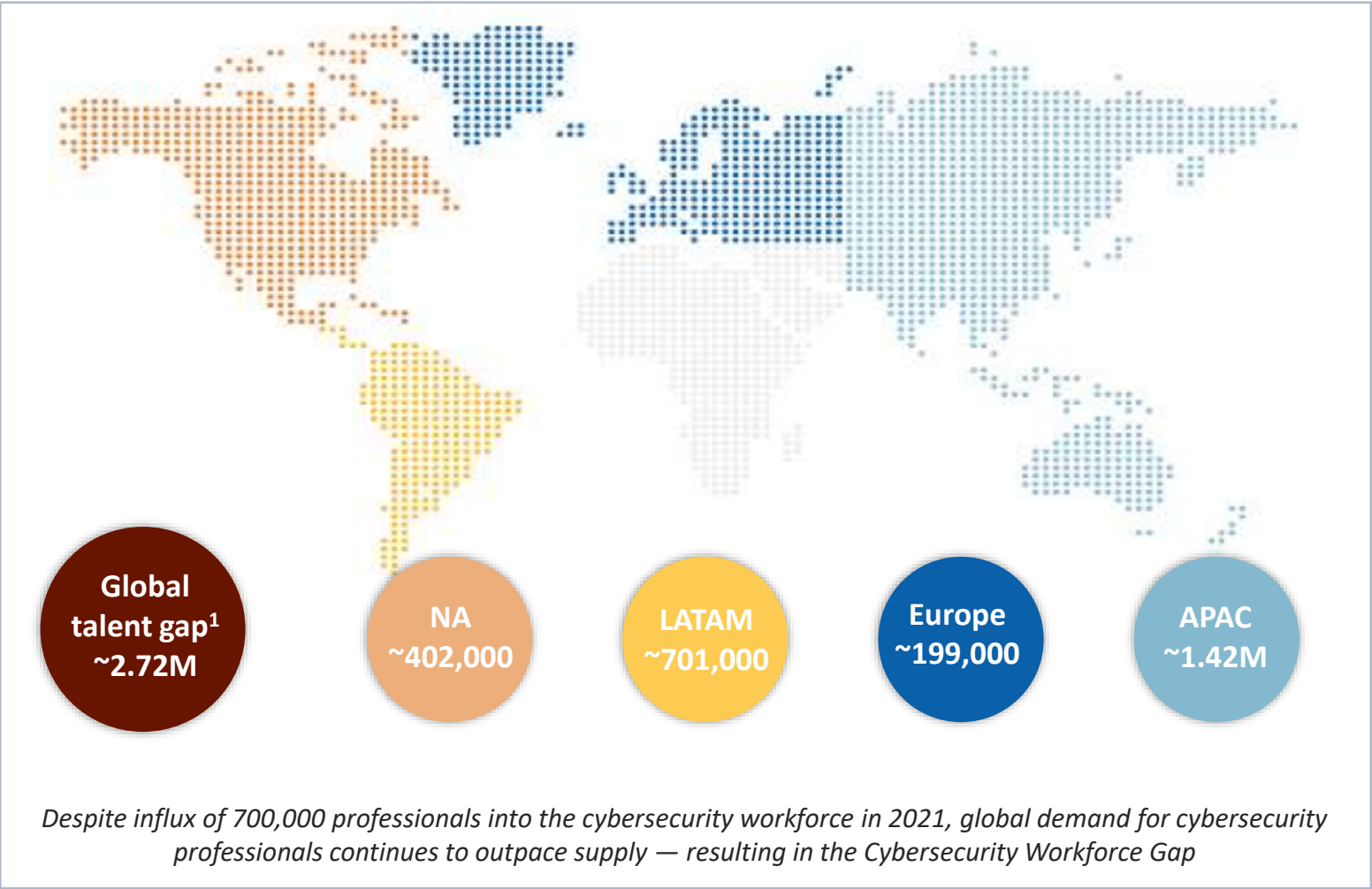
The objective of this document is to showcase how the demand-supply gap in Cybersecurity talent is widening due to limited talent availability but increasing demand and how a targeted Reskilling strategy can help navigate companies through extreme Cybersecurity talent shortages. This document also provides high-level Talent Intelligence for prominent global locations with the availability of Cybersecurity talent

Copyright @2022 Draup. All rights reserved

CONTENTS

Pages		
3-6	<ul style="list-style-type: none">• Widening demand-supply gap of Cybersecurity talent	This section covers: <ul style="list-style-type: none">• Cybersecurity talent gap and consequences of talent gap• Rising demand for talent to protect organization from Cyber risk and Challenges in finding Cyber Security talent• Classifying Cybersecurity job role through detailed taxonomy and identifying key focus area for HR
8-11	<ul style="list-style-type: none">• Hiring insights and Location Intelligence for 'Cybersecurity Engineer' role	
13-16	<ul style="list-style-type: none">• Reskilling/Upskilling strategies for Cybersecurity job roles	

Global demand-supply gap of Cybersecurity talent (2021)



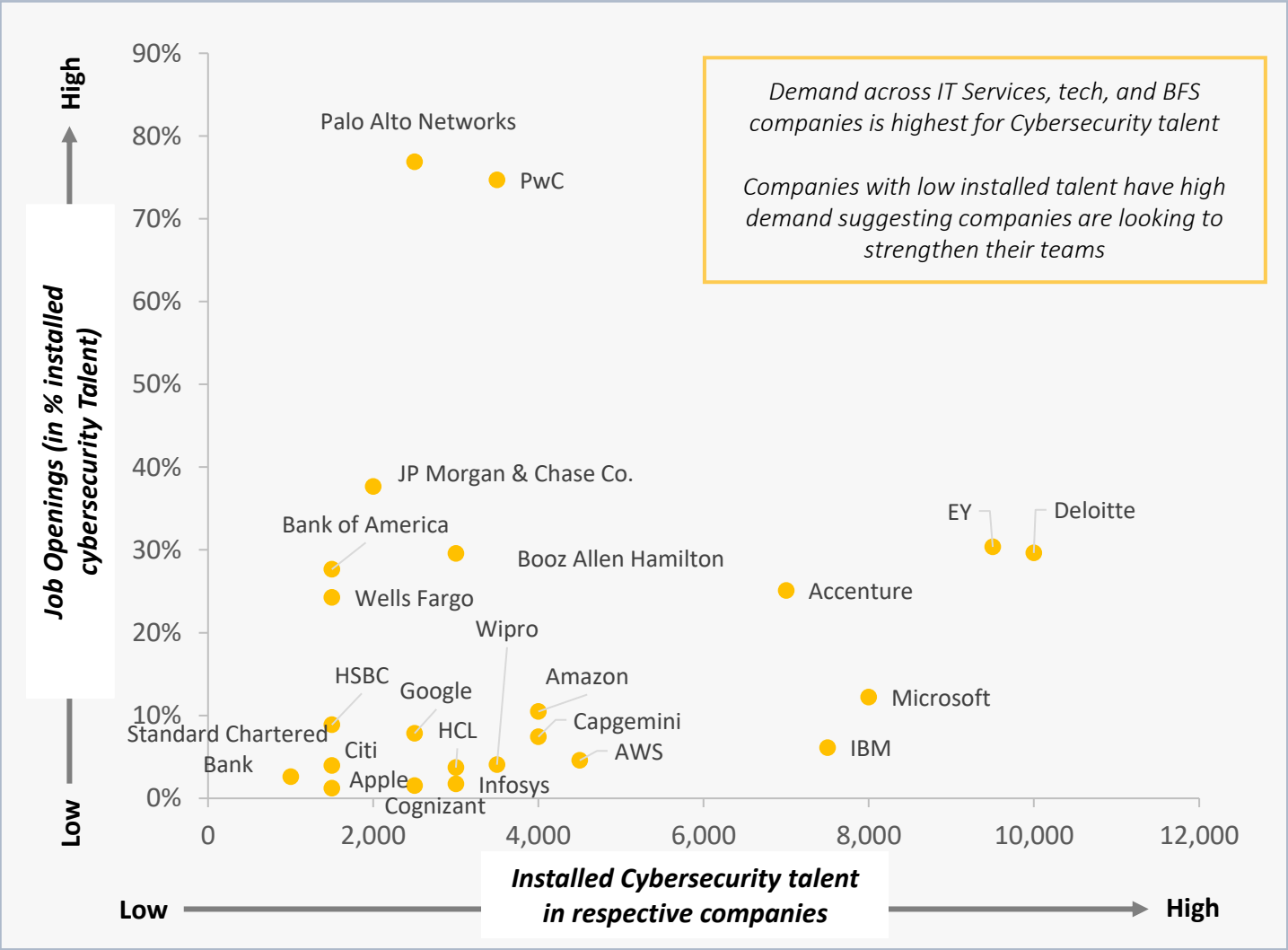
Consequences of Cybersecurity workforce gap²



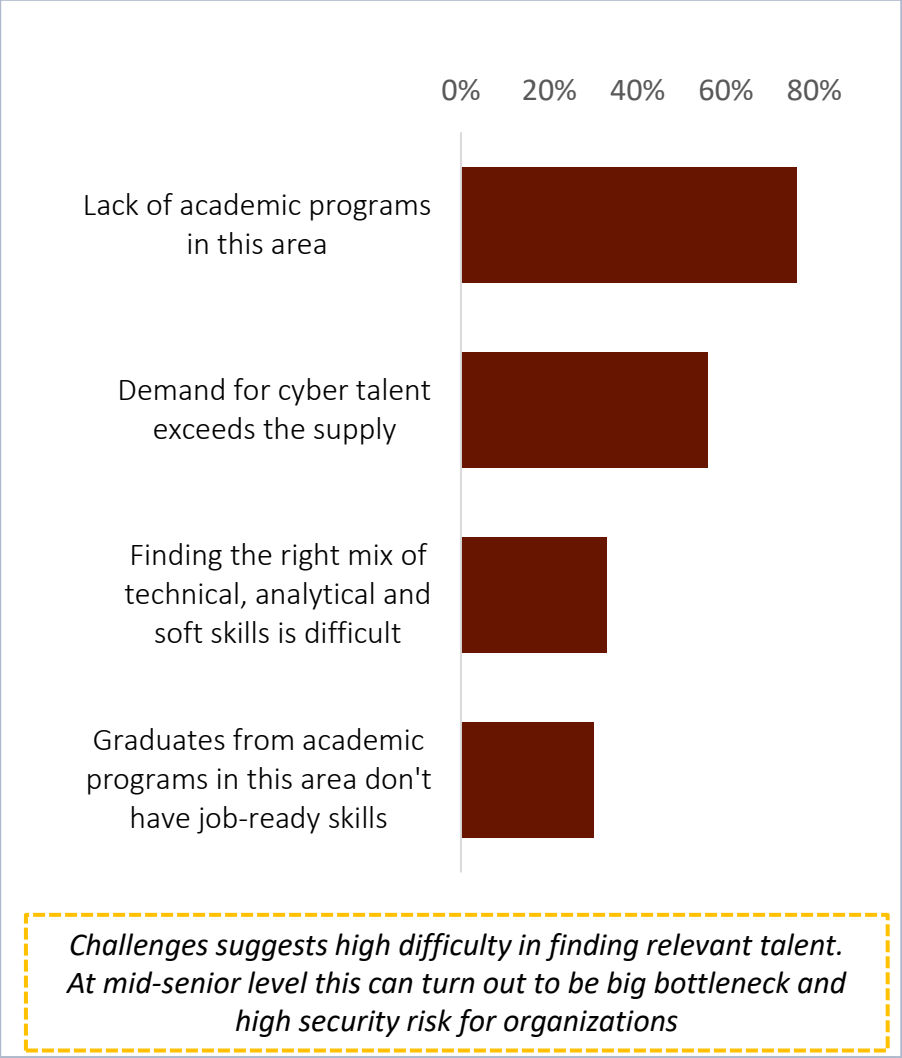
Companies across Industries are aggressively trying to scale their Cybersecurity teams but are faced with multiple hiring challenges due to talent shortage



Leading organizations are increasing their Cybersecurity budgets by ~80% which can be seen in the amount of job openings*



Challenges faced in scouting Cybersecurity talent by companies¹



Draup has analysed Cyber Security teams of 100+ leading organizations to provide sample job roles taxonomy

Critical in-house, Outsourced, and Emerging job roles

	Security Software Development	Security Architecture	Incident Response	Vulnerability Assessment	Governance & Compliance	Research	Cryptography	Data Loss Prevention & Forensics
Mid to senior level		Network/Firmware Security Architect	Incident Risk Manager		GRC Manager	Security Research Specialist	Identification Access Mang. Engineer	Digital Forensics Expert
	Cybersecurity Engineer	Cybersecurity Architect	Security Engineer (Incident Response)	Penetration Tester/ Test Engineer	GDPR Program Manager	Security Researcher	Crypt Specialist	Fraud Prevention Manager
	Blockchain Developer	Information Security Consultant	Cyber Threat Intelligence Analyst	Threat Hunter	GRC Consultant	R&D Specialist	Cryptographer	
	Cloud Security Software Engineer	IoT Security Specialist	Incident Response Analyst	Vulnerability (Assessment) Analyst		Vulnerability Researcher	IAM Consultant	Counterintelligence Forensics Analyst
Entry level	Security Software developer	Cloud Security DevOps Engineer	Cybersecurity Incident Response Analyst	Threat Monitoring Analyst	Security Risk & Compliance Analyst	Threat Research Analyst	Crypt-Analyst	Intrusion Detection Analyst
	Security Analyst	Network & Information Security Analyst	Incident Responder	Vulnerability Assessor	IT Risk and Compliance Officer			

In-house critical talent hiring difficulty faced by HR in an organisation insights:

80% of HR struggle to fill Mid and Senior level talent position as there is limited availability of talent and companies look for specific technical, analytical, and soft skills

Companies have started training program to improve the skillset of fresh graduates thereby making it easier to hire entry level talent
Ex: Microsoft pledging to train 250,000 talent in US by 2025

High in-demand Cyber Security Engineer role has been analysed further in detail to provide Hiring and Reskilling insights

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

High-demand in-house roles

Emerging roles

Outsourced roles

Copyright © 2022 DRAUP. All Rights Reserved.

Cyber Security Engineer

Cyber Security Engineer is responsible for planning, managing, monitoring, and upgrading security measures for the protection of the organization's data, systems, and networks.

Top Certifications for Cyber Security Engineer

CISSP: Certified Information Systems Security Professional	CompTIA Security+
Certified Ethical Hacker (CEH)	Security+
CompTIA Security+ Ce Certification	CCNA
CompTIA Network+	GIAC Certified Incident Handler (GCIH)

Key Workloads

Assess the quality of security controls using performance indicators.
Develop or implement software tools to assist in the detection, prevention, and analysis of security threats.
Identify security system weaknesses using penetration tests.
Develop response and recovery strategies for security breaches.
Develop information security standards and best practices.

Technical/Core Skillsets required

Risk, and Compliance frameworks	DoD CC SRG	NIST 800-53/171	RMF, FedRAMP
Cloud Deployment Tools	Kubernetes	Docker	
Programming Language	Python	C/C++	Java
Network/Web related protocols	TCP/IP HTTP/HTTPS	UDP SSL	Routing protocols
Other Technical skillsets	Risk Assessment, Risk Management Methodologies, Threat Modelling, Vulnerability Ranking		

CONTENTS

Pages	
3-6	<ul style="list-style-type: none">• Widening demand-supply gap of Cybersecurity talent
8-11	<ul style="list-style-type: none">• Hiring insights and Location Intelligence for 'Cybersecurity Engineer' role
13-16	<ul style="list-style-type: none">• Reskilling/Upskilling strategies for Cybersecurity job roles

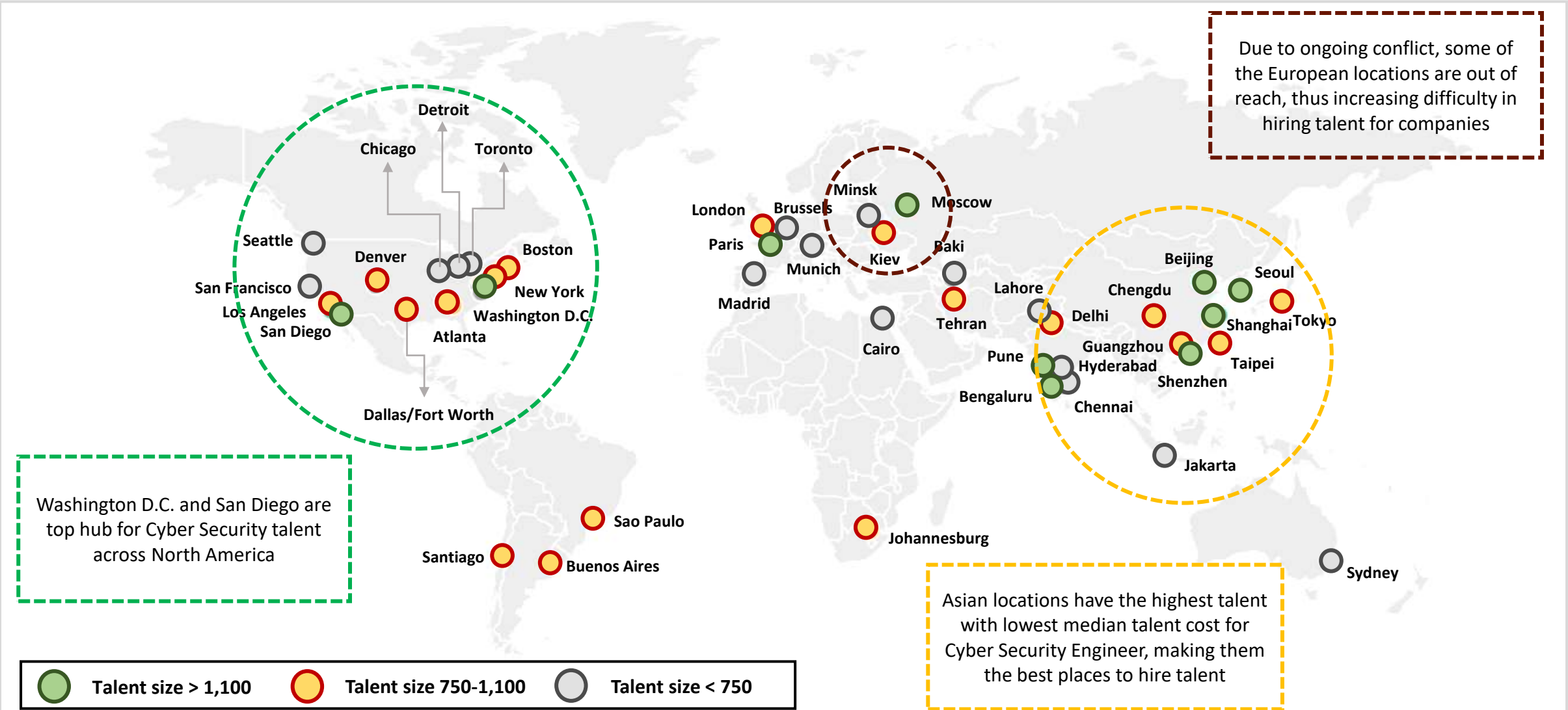
This section covers:

- Location hotspot analysis for Cybersecurity Engineer role
- Talent cost analysis for leading MSAs across globe
- 'Bengaluru' location overview and analysis
- Sample Cybersecurity Engineer profiles

Global hotspots for Cybersecurity Engineer talent: Washington D.C. and San Diego have the highest talent in the US, while Shanghai, Beijing, Seoul, and Bengaluru have the highest Cyber Security Engineer talent in Asia

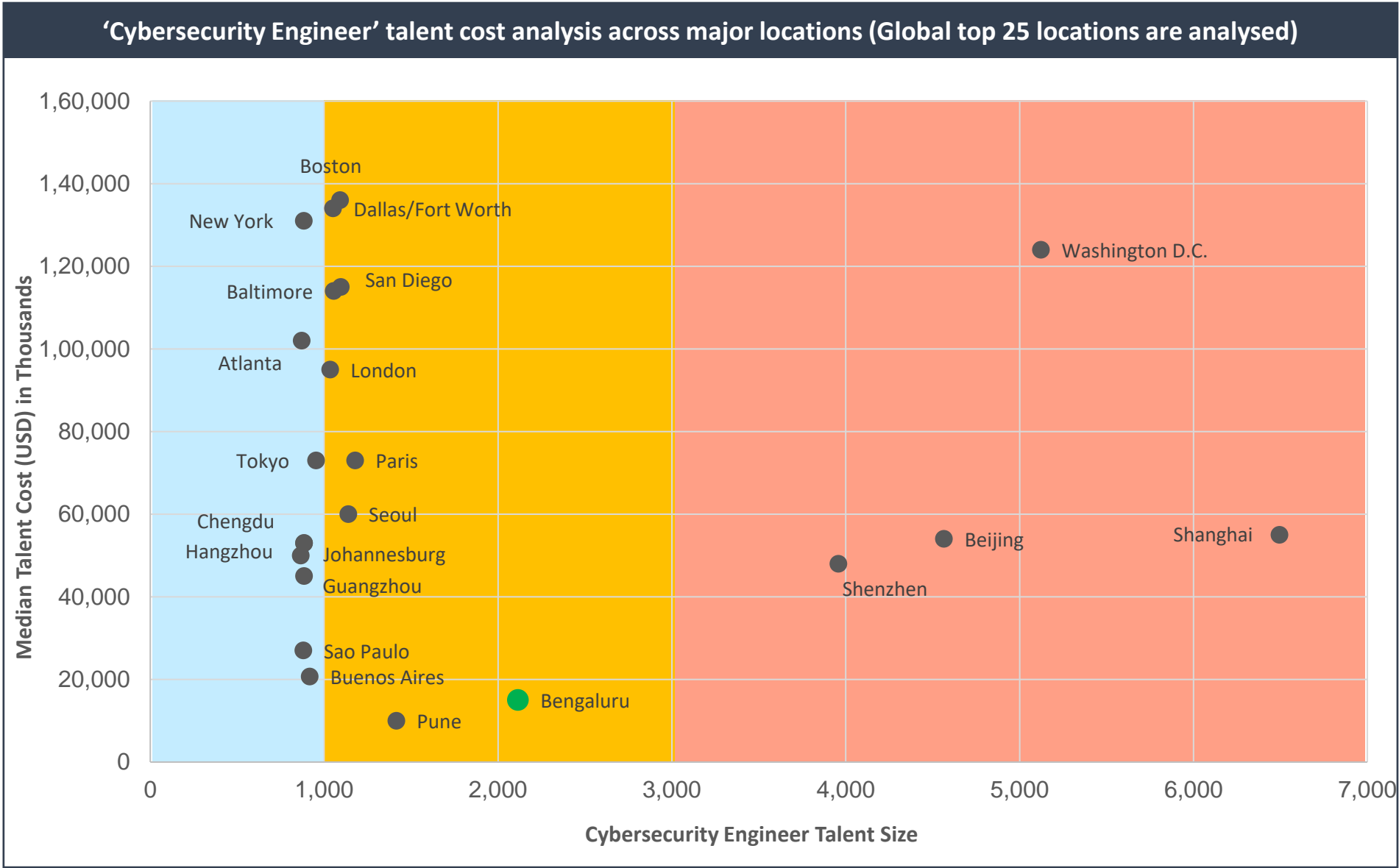


Draup analysed 400+ global locations and identified top hotspots with availability of ‘Cyber Security Engineer’ talent



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

Global Cost analysis for ‘Cybersecurity Engineer’ talent: Besides Washington D.C., all other high talent availability locations are based out of Asia; Bengaluru and Pune are the most cost-effective locations amongst them



~80% of Cyber Security Engineer talent is based out of top 12 location globally of which Asian locations are the highest

Bengaluru, with high Cyber Security engineer talent availability and low median talent cost is one of the best location to hire Cyber Security Engineer talent.

Copyright © 2022 DRAUP. All Rights Reserved.

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

Bengaluru Cyber Security Engineer talent landscape: With low talent cost and high talent availability, Bengaluru is the most desirable location to hire Cyber Security Engineer talent in India



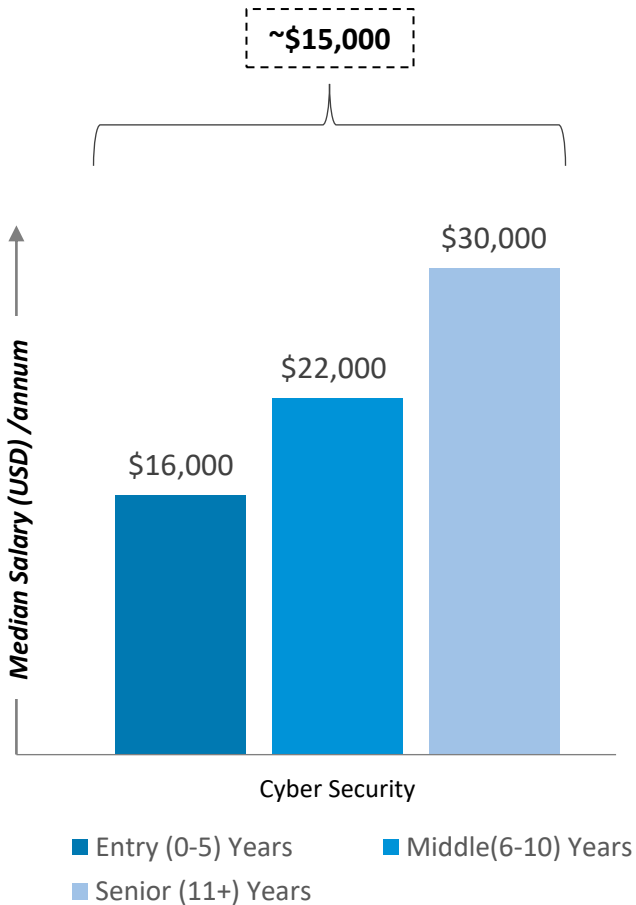
Bengaluru talent Overview:

Cybersecurity Engineer talent:
~2200

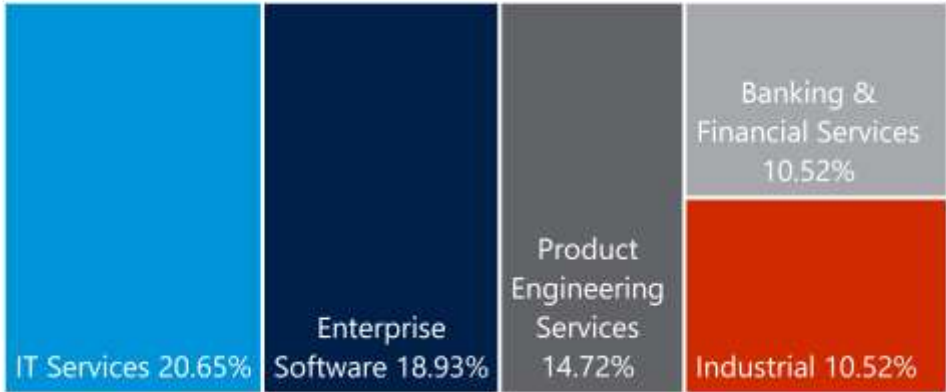
Overall Cybersecurity talent:
~30,000

Bengaluru is also leading destination for tech talent in India with ~20-25% of overall India’s tech talent

Median annual salary for Cyber Security Engineer talent in Bengaluru



Cybersecurity Engineer Talent distribution by vertical



























Top Employers for Cybersecurity Engineer talent



Note: All the salaries depicted are median base salaries and do not include additional compensation and benefits offered by individual companies. The data has been source from Draup cost simulator. Overview Insights have been extracted from Draup’s ML model which analyses 2M+ publications, Industry reports and news articles on a weekly basis; Draup’s Talent Module was used to extract top employers and talent size;

Draup’s Rolodex feature has been used to extract profiles based on different experience level that can be used by organisation to hire talent

	Name	Location	Current Designation	Current Company	Past Companies	Overall Experience	LinkedIn URL
High Experienced talent	Sunit Mahajan	Bengaluru	Lead Cybersecurity Engineer	 Target		13+ Years	 LinkedIn
	Mahesh Simson CEH, CHFI	Bengaluru	Sr. Cybersecurity Engineer	Synchronoss tech.		14+ Years	 LinkedIn
	Sandeep Mata	Bengaluru	Principal Cybersecurity Er	 Forcepoint		12+ Years	 LinkedIn
Mid Experience talent	Pankaj Sharma	Bengaluru	Sr. Cybersecurity Engineer	 Dell		7+ Years	 LinkedIn
	Girish Ameta	Bengaluru	Sr. Cybersecurity Engineer	 GE healthcare	-	7+ Years	 LinkedIn
	Varun Behera	Bengaluru	Cybersecurity Engineer	 Zensar		4+ Years	 LinkedIn
Entry level talent	Shivam Yadav	Bengaluru	Cybersecurity Engineer	 Siemens		3+ Years	 LinkedIn
	Sudha Gangai	Bengaluru	Cybersecurity Engineer	 Rapid Circle		2+ Years	 LinkedIn
	Ravikumar Pawar	Bengaluru	Cybersecurity Engineer	 Cognizant	-	2+ Years	 LinkedIn

CONTENTS

Pages

3-6

- Widening demand-supply gap of Cybersecurity talent

8-11

- Hiring insights and Location Intelligence for 'Cybersecurity Engineer' role

13-16

- **Reskilling/Upskilling strategies for Cybersecurity job roles**

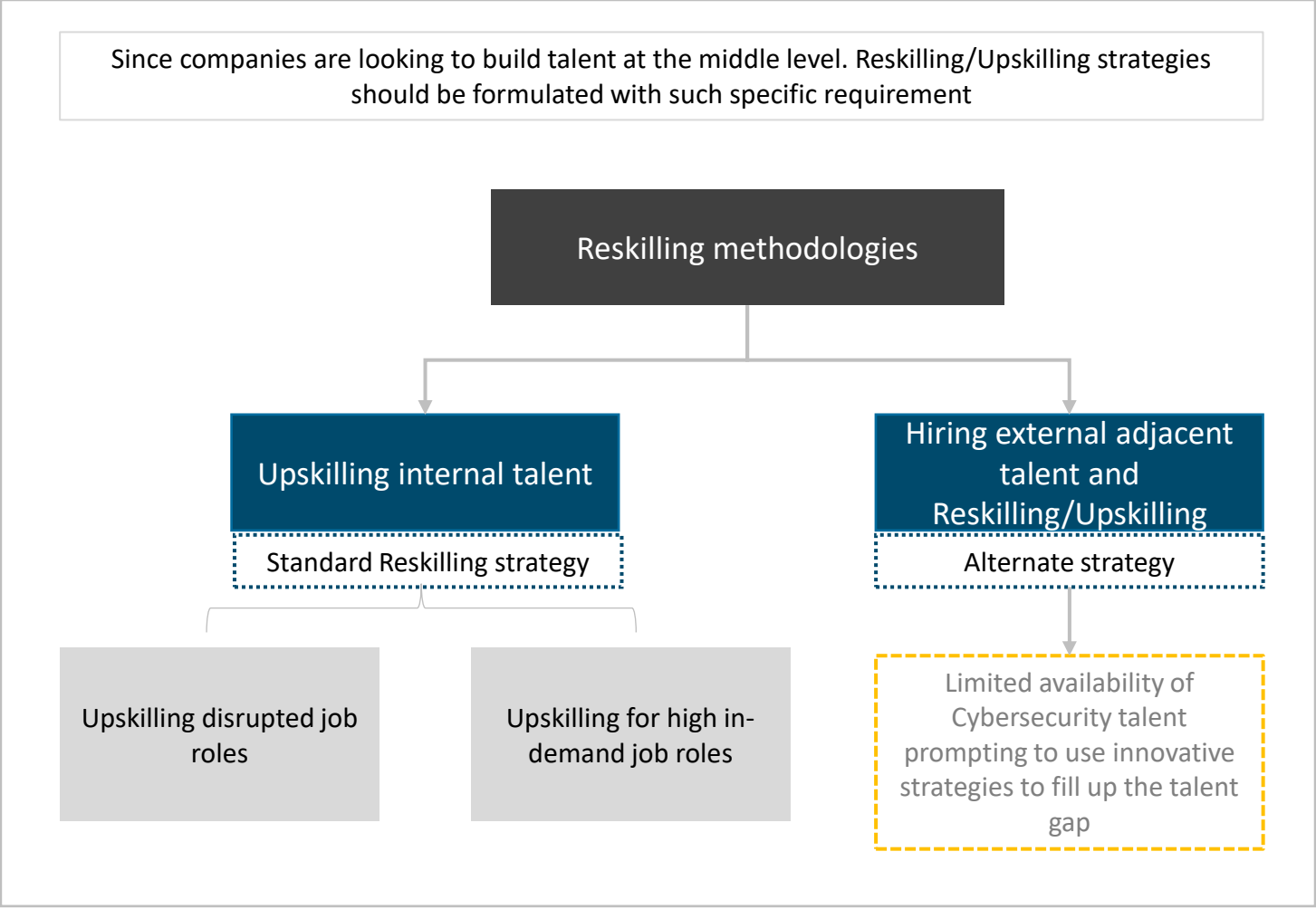
This section covers:

- Importance of reskilling/upskilling and formulating reskilling strategies
- Reskilling/Upskilling framework based on adjacent talent availability for specific location(Bengaluru)
- Case study showcasing transition of Network Engineer into Cybersecurity Engineer
- Sample profile showcasing upskilling/reskilling

The global cybersecurity workforce needs to grow 65% to effectively¹ defend organizations’ critical assets

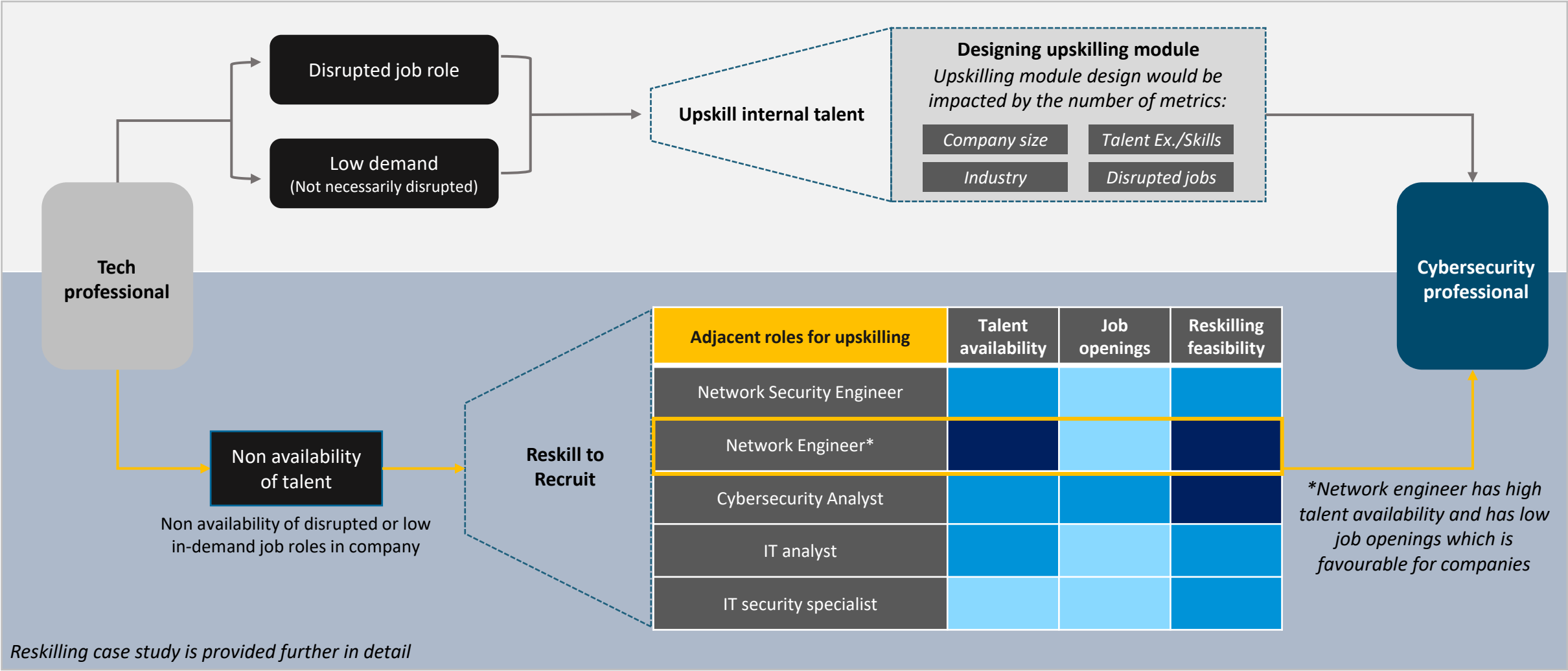


Reskilling/Upskilling strategy of every company would differ depending on the type of talent available, location, etc but framework can be broadly defined-



Reskilling/Upskilling framework (sample location Bengaluru): High availability of adjacent talent can be utilized to reskill and recruit to meet the unmet demand for Cybersecurity talent

Sample illustration of how Reskilling/Upskilling can provide an alternate career path of Cybersecurity to tech professionals in locations such as ‘Bengalure’

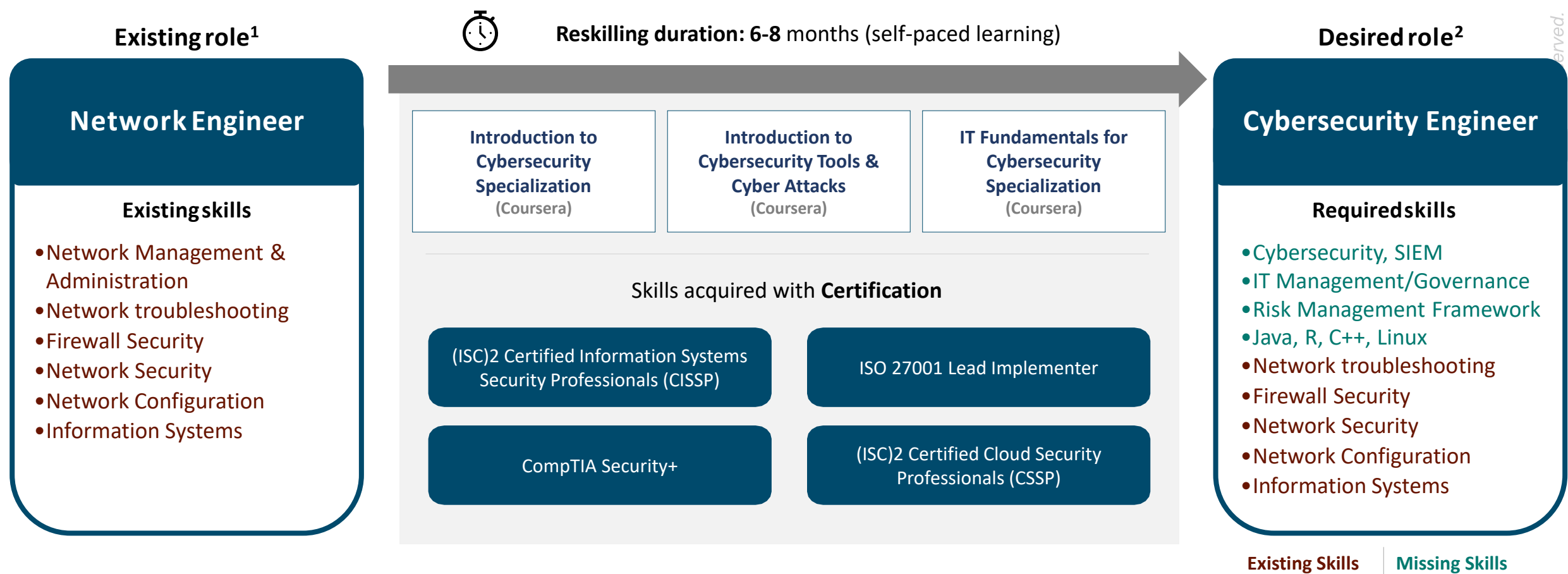


Copyright © 2022 DRAUP. All Rights Reserved.

Reskilling case study: Conventional job roles such as Network Engineer can be upskilled into ‘Cyber Security Engineer’ job role by providing Programming, Risk management framework, and Cybersecurity 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 Engineer’ role



1. Network Engineer considered here should have 4+ years experience with high overlapping skill sets of Cyber Security Engineer

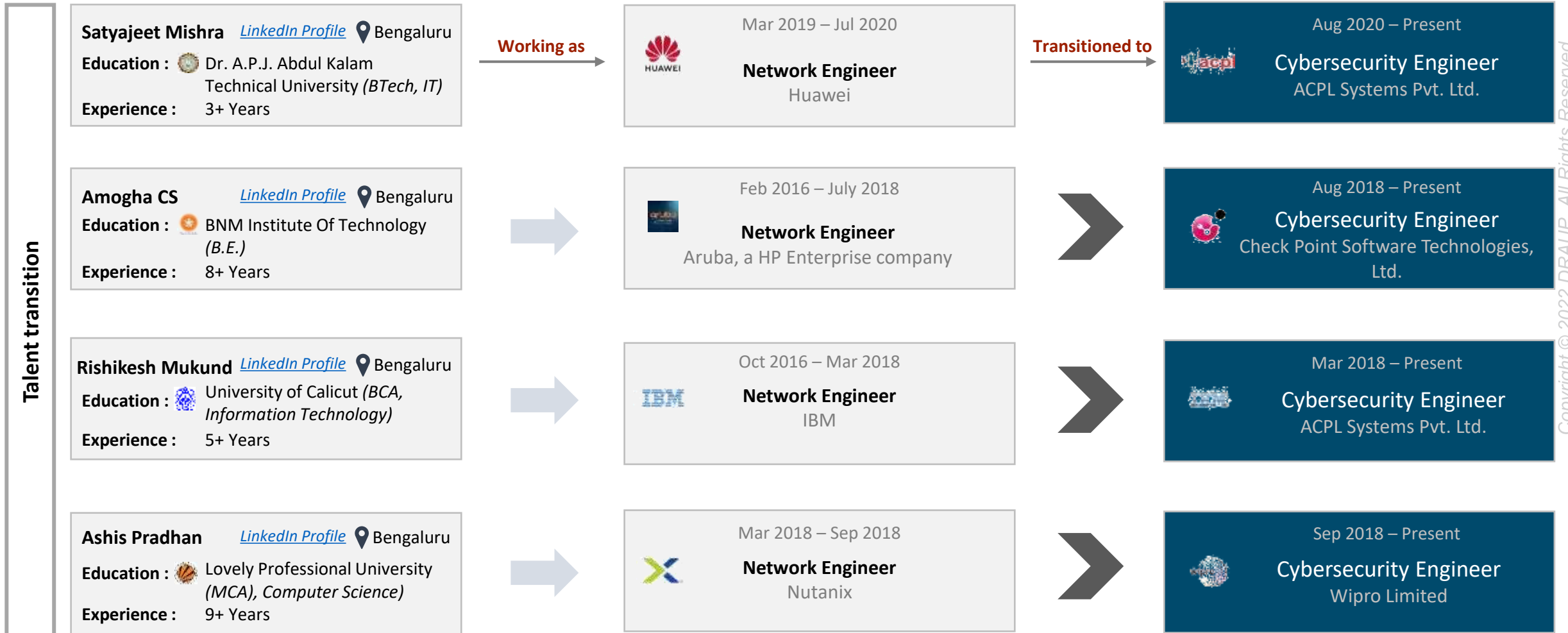
2. During transition time (6-8 months), Upskilled/Reskilled Network Engineer can be utilised to cater basic level Cyber Security Engineer workloads and can be trained simultaneously inhouse to gain advanced expertise

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

Source: Draup Reskill Navigator or Reskill stimulator

Sample 'Network Engineer' Talent profiles that successfully transitioned to Cyber Security Engineer roles

Presented case studies are among 1,000+ Career Transitions that Draup has Analyzed



Copyright © 2022 DRAUP. All Rights Reserved.

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



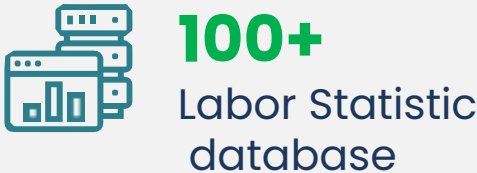
and diverse other use cases...

Copyright © 2022 DRAUP. All Rights Reserved.

Draup for Talent: Draup analyses 2,500+ global locations to help global HR leaders in understanding data-driven insights related to Talent/skill landscape, cost, demography and peer ecosystem



Every day, we analyze **10M+ data points** from over **8,000 data sources**



This data is strengthened by more than 70 Machine Learning models and over 12 Psychology models

Copyright © 2022 DRAUP. All Rights Reserved.



HOUSTON | BANGALORE

© 2022 DRAUP. All Rights Reserved.