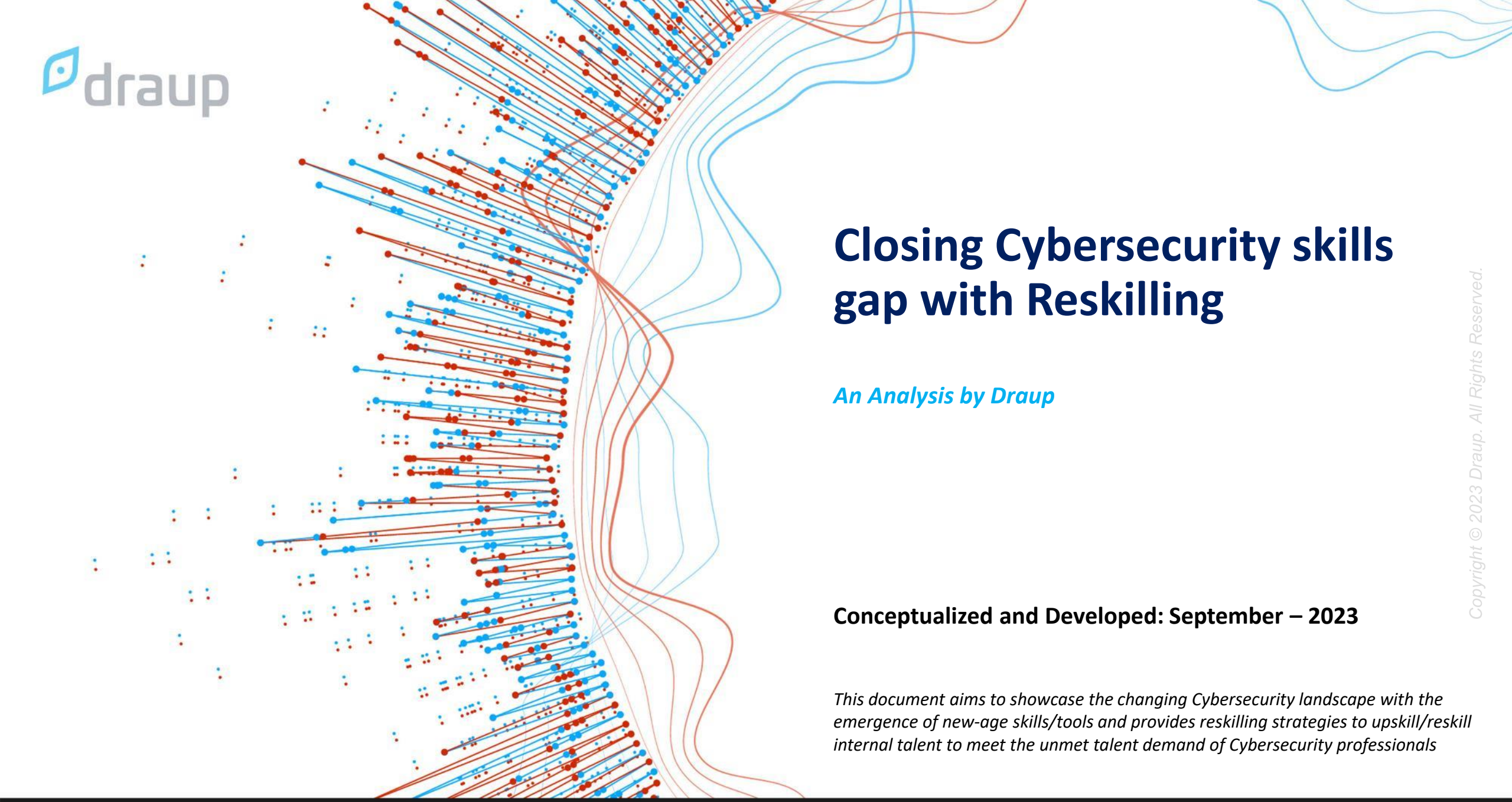


Closing Cybersecurity skills gap with Reskilling

An Analysis by Draup

Conceptualized and Developed: September – 2023

This document aims to showcase the changing Cybersecurity landscape with the emergence of new-age skills/tools and provides reskilling strategies to upskill/reskill internal talent to meet the unmet talent demand of Cybersecurity professionals

Challenging Cybersecurity Talent Landscape

Top Cybersecurity Priorities of Companies

Data Security and **Privacy** are the key priorities to protect from data breaches caused by sophisticated cyber attacks

New Age Skills Taxonomy

New-age skills like **Cryptographic Security, Privacy Engineering** are emerging

Hiring Challenges

Shortage of qualified Cybersecurity Talent, inflated talent cost, High Talent competition are key challenges

Reskilling to meet the unmet talent demand

Suitable role assessment

Internal roles such as **System Engineer** have a high skills overlap with roles such as Cybersecurity Engineer

Bridging the skill gap

System Engineer can acquire skills such as **Identity and Access Management** and **Endpoint Security**

Reskilling duration

With targeted learning modules, System Engineer can Reskill into a Cybersecurity Engineer in **~3.5 months**

CONTENTS

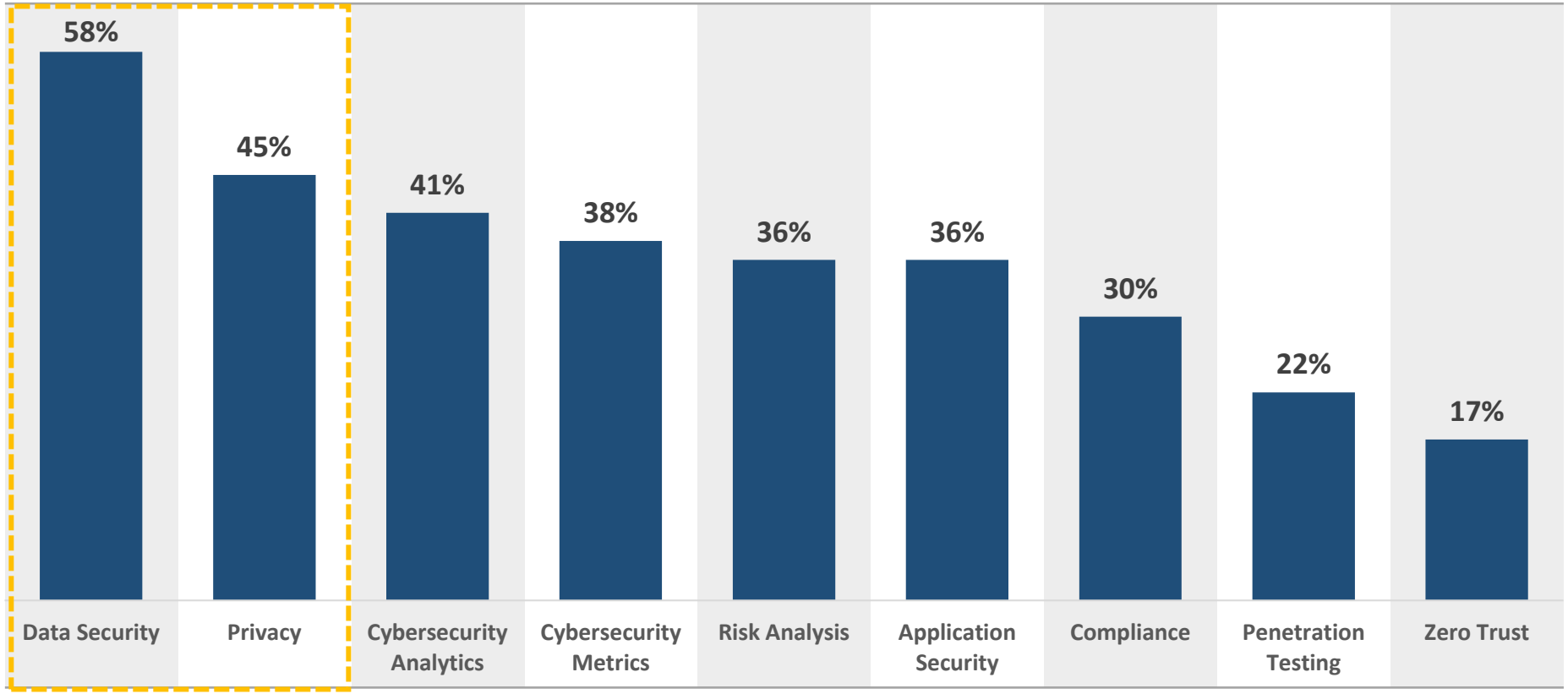
This section covers:

- Key Cybersecurity priorities for organizations
- Emerging skills in Cybersecurity
- HR Bottlenecks in Cybersecurity
- Reskilling as a solution

Rapid digital advancements are fueling the growth of Data theft. Organizations are focusing more on Data Security and Privacy to strengthen their frontline defense

Draup analyzed 300+ leading companies to understand the key Cybersecurity priorities for organizations

Top Priority Cybersecurity Areas for leading organizations



N[1]=1,125

TOP 5 Personal data breach was reported to be one of the **top 5 cyber crimes**

Average cost of a data breach to small business can range from **$120,000 to $1.24 million**[2]

Increasing frequency and sophistication of data breaches are leading to a growing focus on **Data Privacy & Security**

Note: 1. Total respondents Above analysis is based on Draup's research, insights from customer engagement, industry blogs, and whitepapers. Above mentioned areas are not exhaustive, and the impact level may vary across industries
Source: 1. Statista 2. Business.com

Expanding Cybersecurity Skills Taxonomy: Emerging Skills in Data Security and Identity Access Management are becoming critical for firms to combat advanced data theft

Draup leveraged its database of 30,000 skillsets to identify and map the core skill sets for Cybersecurity Talent

Clusters	Data Security	Security Governance & Assurance	Identity and Access Management (IAM)	Security Operations	Cloud & IoT Security	Offensive Security
Key Emerging Cybersecurity Skills	Data Protection Impact Assessment	Zero Trust Architecture (ZTA)	2FA solution	Incident Response Automation	Cloud Security Architecture	Vulnerability Assessment & Management
	Data Protect & Privacy (DPP)	Network Auditing	Single-Sign-On (SSO)	Secure DevOps (DevSecOps)	Cloud-Native Application Security	Security Assessment
	General Data Protection Regulations (GDPR)	Privacy Engineering	Privileged Access Management (PAM)	Endpoint Security	Secure IoT Device Management	Penetration Testing
	Network Security	Security Frameworks - ISO 27001, NIST 800-53	Cryptographic Security	Security Operations Center (SOC) Automation	Serverless Security	Malware Analysis
	Intrusion Detection Systems (IDS)	Threat Intelligence	Role-Based Access Control	SIEM (Security Information & Event Management)	Cloud Analytics Platform - Alteryx	Application Security
Emerging Cybersecurity Tools Tech Stack	Checkmarx	Securonix	SpectralOps	Cyclance	Vectra	Recon-ng
	Trustwave DBprotect	ManageEngine Log360	OneLogin	Snort 3, Suricata	Claroty	Parrot Security OS
	Kenna Security	NordLayer	Ping Identity	Sysmon	Imperva	Veracode
	Satori Data Security	Mandiant	SentinelOne	Zeek (formerly Bro)	Istio	Metasploit

Source: Draup leverages its database of 380 Million+ JDs, and 800 Million+ profiles to understand the skills required of Cybersecurity Job roles.
Note: Skillsets/Tools considered here are not exhaustive. The skillsets in the individual column might overlap in some cases; the individual columns are not Mutually Exclusive and Collectively Exhaustive

Hiring complexity of Cybersecurity roles: Relevant roles for Data Security and Privacy are difficult to acquire. Inflated talent cost, Skilled professional shortage, and Hiring competition are the top bottlenecks

Sample location analysis - US

Draup analyzed 100+ companies to understand the Cybersecurity Talent ecosystem and trends of global companies

Relevant Cybersecurity Roles	Talent Size	Median Base Pay (100K – 200K (in USD))	Demand Growth[1]	Top Talent Competitors (with high job postings)
Cyber Security Analyst	44,700	$1,10,560	42.40%	Bank of America, IBM, Fidelity, Dell
Cyber Security Engineer	24,700	$1,47,590	48.22%	Honeywell, Visa, Microsoft, AT&T, Comcast
Cyber Security Manager	13,300	$1,75,800	28.48%	JPMorgan Chase & Co., Capital One, Target, The Home Depot, Walmart
Cyber Security Consultant	12,200	$1,35,900	35.43%	Oracle, ebay, verizon, fiserv., Wells Fargo
Penetration Tester	6,900	$1,41,900	58.49%	leidos, Google, amazon, hackerone, hp

$112K (Median Base Pay for Tech & IT Roles)

K = Thousand

Key Challenges faced by HR Leaders

- Lack of Specialized Cyber Security skills
- High Talent Demand
- Growing Competition
- Budget Constraints

Source: Cybersecurity Talent workforce was calculated using Draup's 80+ ML Models that analyze 800 Million+ professional profiles and 380 Million+ JDs across 4,500 job roles. The above analysis is based on Draup's research, insights from customer engagement, industry blogs, and whitepapers. 1. Demand is calculated by comparing the Job Openings in September 2023 to openings between July and September 2023

Reskilling talent to meet the unmet demand: Internal talent with overlapping security skills can be reskilled to meet the entry-level requirement of critical Cybersecurity roles.

Favourable roles for Reskilling

Existing roles with skill overlapping skills	Reskilling Favorability
System Engineer	High
Network Engineer	High
Systems Administrator	High
Database Administrator	Medium
Network Administrator	Low
Linux Administrator	Medium
Server Administrator	Medium
Service Engineer	Low
QA Test Engineer	Low
Technical Support Engineer	Medium
Field Engineer	Low

Increasing order of Disruption

Reskilling Favorability: High | Medium | Low

(Critical Cybersecurity Skills Addition)

- Identity and Access Management
- Network Security & Auditing
- Threat Intelligence
- Endpoint Security
- Privileged Access Management
- Intrusion Detection Systems (IDS)

= (Reskilling)

Cybersecurity Engineer
(sample Reskilling case study analyzed further)

Strategies for Faster Reskilling

A Identifying internal roles suitable for Reskilling transition

B Assess the Reskilling feasibility and duration with skill gap analysis

C Map the relevant courses based on skill gaps for faster learning

Note: Draup analyses 16+ Million data attributes every day to help global HR leaders in Planning and Reskilling their Future-Ready Workforce.
Source: 1. McKinsey. Draup's internal analysis, Press releases, customer surveys, and interviews

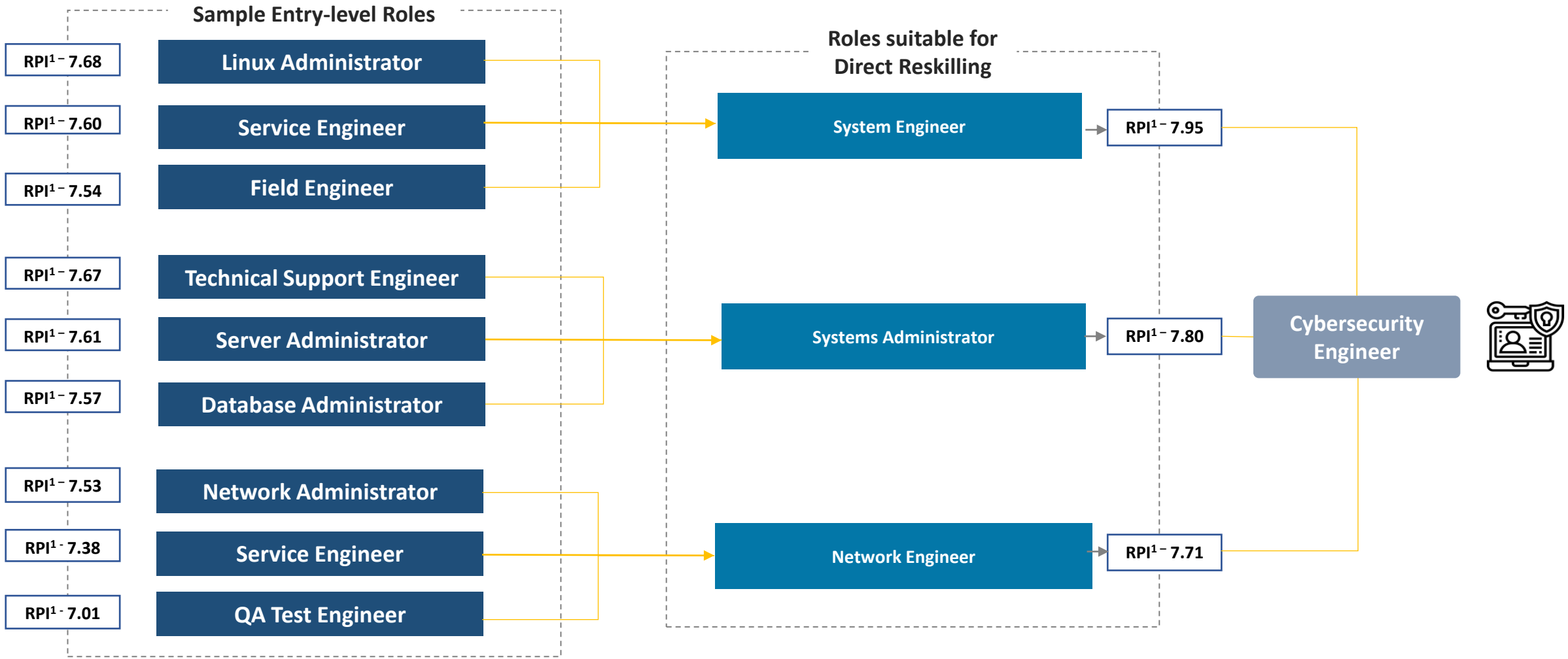
CONTENTS

This section covers:

- Reskilling Propensity Analysis for internal roles transitioning to In-demand Roles
- Skillset Analysis of a System Engineer
- Reskilling Journey of a System Engineer to a Cybersecurity Engineer
- Workload Analysis of a System Engineer
- Cost Savings with Reskilling

Job role identification for Reskilling (1/3): An effective Reskilling requires identifying suitable roles. Reskilling Talent in Disruption-prone Job roles could be mutually beneficial

Draup analyzed 1,500+ transitions of entry-level roles of leading firms to understand the transition feasibility for 'Cybersecurity Engineer' role



Note: The list of roles presented above is not exhaustive. **1**. The RPI or Reskilling Propensity Index Scores are derived from five parameters (path empirical data, compensation benchmarking, core skills overlap, soft skills overlap, and median experience)
Source: Draup tracks 4+ Million career paths using 75+ machine learning modules to draw feasible reskilling journeys. Draup analyses reskilling possibilities using Draup's Proprietary Reskilling Module and Reskilling Propensity Index

Reskilling feasibility analysis (2/3): Roles such as System Engineers demonstrate foundational proficiency in Security Governance and Data Security; ideal for Reskilling within 3-4 months

Draup analyzed 1,000+ JDs (using 75+ ML models) to understand the skill gap between traditional roles and Cybersecurity Engineer

Major skill gaps to be filled to reskill adjacent roles towards **Cybersecurity Engineer** role with in-demand emerging skills

Sample adjacent Job Roles to Reskill	Skill Domains						Tentative Reskilling Duration
	Programming Languages and Algorithms	Security Operations	Endpoint Security	Security Governance & Assurance	Data Analytics & Security	Identity and Access Management	
System Engineer							12-13 weeks
Systems Administrator							13-14 weeks
Network Engineer							14-15 weeks

Top reasons to choose such a role:

- High Overlapping skillsets
- Low talent cost
- High talent availability
- Low talent demand due to automation
- High-cost ROI compared to hiring

Sample role for Course Sequencing

Skill overlap	High	Moderate	Low

Note: Skill-level data has been extracted from Draup's Reskill Navigator.
Source: The represented data has been derived using Draup's Proprietary Talent Database, Draup tracks and analyses 4,500+ job roles and 380M+ Job descriptions across functions to understand the disruption in workflow due to tech advancements. Similar analysis can be performed for any job role.

Targeted skill-based course sequencing (3/3): A System Engineer can reskill to a Cybersecurity Engineer by acquiring required skills in Identity Access Management, Threat intelligence, etc.

Using 30+ AI models, Draup platform's Reskilling module can map targeted learning modules for Reskilling/Upskilling any job role

Skills Acquisition & Course Sequencing

System Engineer

Identity & Access Management (IAM)	Network Security	Threat Intelligence	Endpoint Security
IAM using Privileged Access Management (PAM) & Kerberos	Cisco NGFW Firepower Threat Defense (FTD) Training Part-1/2	Cyber Incident Response with Malware Analysis	Endpoint Security With Information Security
PAM and Kerberos	Cisco Firepower, Threat Defense, DNS	Malware Analysis	Threat and Vulnerability Management
Diploma in Identity and Access Management	Network Security with Intrusion detection	Incident Response and Forensics with Penetration Test	The Complete Cyber Security Course: End Point Protection
Network Security and Cybersecurity	Intrusion detection & Network auditing	Penetration Test, Computer Security Incident Management	Snort, Suricata and Endpoint Security

+Other Courses

Cybersecurity Engineer

(Entry Level Proficiency)

Skillsets Gained

Courses Learnt

Estimated Time for Course Completion

Job Ready Proficiency
3 Months – 3.5 Months
(147 hours with
2 hours/day)

Real-life Sample Case Study

Brian…

Indiana, USA

Experience : *15+ Years*

was working as

APTIV **System Engineer**

Aptiv *Dec 2021 – Jun 2023*

transitioned to

BW **Cybersecurity Engineer**

BorgWarner *Jun 2023 – Present*

Note: Draup performs complex assessments around various critical Reskilling parameters between existing and desired roles to understand the skill gap and match it with relevant learning modules. The path showcased is not absolute or exhaustive.
Source: Draup's dedicated Reskilling module 'Reskilling Navigator' intelligently prompts targeted courses for 4,500+ job roles from a corpus of 300K courses.

Reskilling benefits - Employee Satisfaction (1/2): Due to functional skills overlap, the Reskilled System Engineer can positively embrace the new Cybersecurity workloads/ skills

Draup analyzed 1,000+ JDs (using 75+ ML models) to understand the workflow of System Engineer before and after Reskilling

Workflow Analysis with overlapping workloads	Development & Installation	Configuration & Testing	Security Implementation & Maintenance	Risk Assessment and Management	Compliance and Regulations	Security Monitoring and Analysis	Threat Prevention
Traditional System Engineer	✓	✓	✓	✓	✓	✓	
System Engineer after acquiring Cybersecurity capabilities			✓	✓	✓	✓	✓

Enhanced Employee Satisfaction

Learning new skills and overcoming challenges can be **personally satisfying and boost self-esteem**

Faster adaptation to Changing Workloads

System Engineers are better prepared to adapt to changing workloads due to **functional overlap, allowing quick adjustment**

Existing skill utilization

System Engineer can make use of its existing skillsets like **Security Monitoring and Security Implementation**

Note: Draup's analysis. **Source:** The represented data has been derived using Draup's Proprietary Talent Database, Draup tracks and analyses 4,500+ job roles and 380M+ Job descriptions across functions to understand the workflow of sample roles. Similar analysis can be performed for any job role.

Reskilling benefits – Cost savings (2/2): Reskilling to Cybersecurity roles serve two major purposes; 'Providing viable career paths to Employees' and 'Saving Talent cost for Employers' (6-7% cost saving per FTE[1])

Draup's analysis of cost savings with 'Reskilling' over 'Lateral Hiring' of Cybersecurity talent

Benefits of Reskilling

Improves Retention

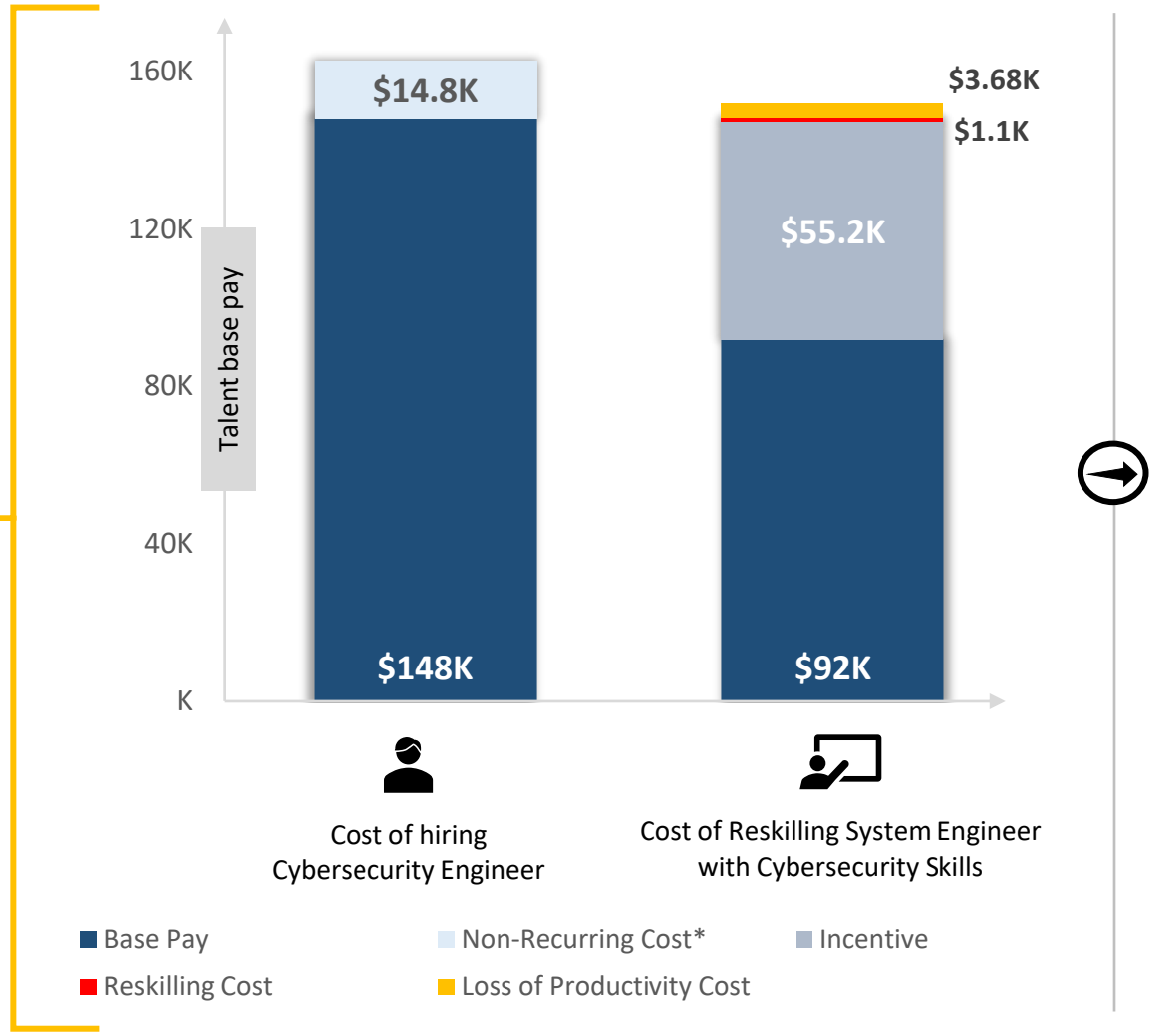
Reskilling reduces attrition rate by providing viable career paths to disrupted job roles to in-demand ones

Reduces Cost

Cost of Reskilling an existing employee allows 6-7% cost savings on the cost of hiring a new employee

Improves Efficiency

Reskilled employees identify and solve problems quickly due to familiarity with the company's infrastructure



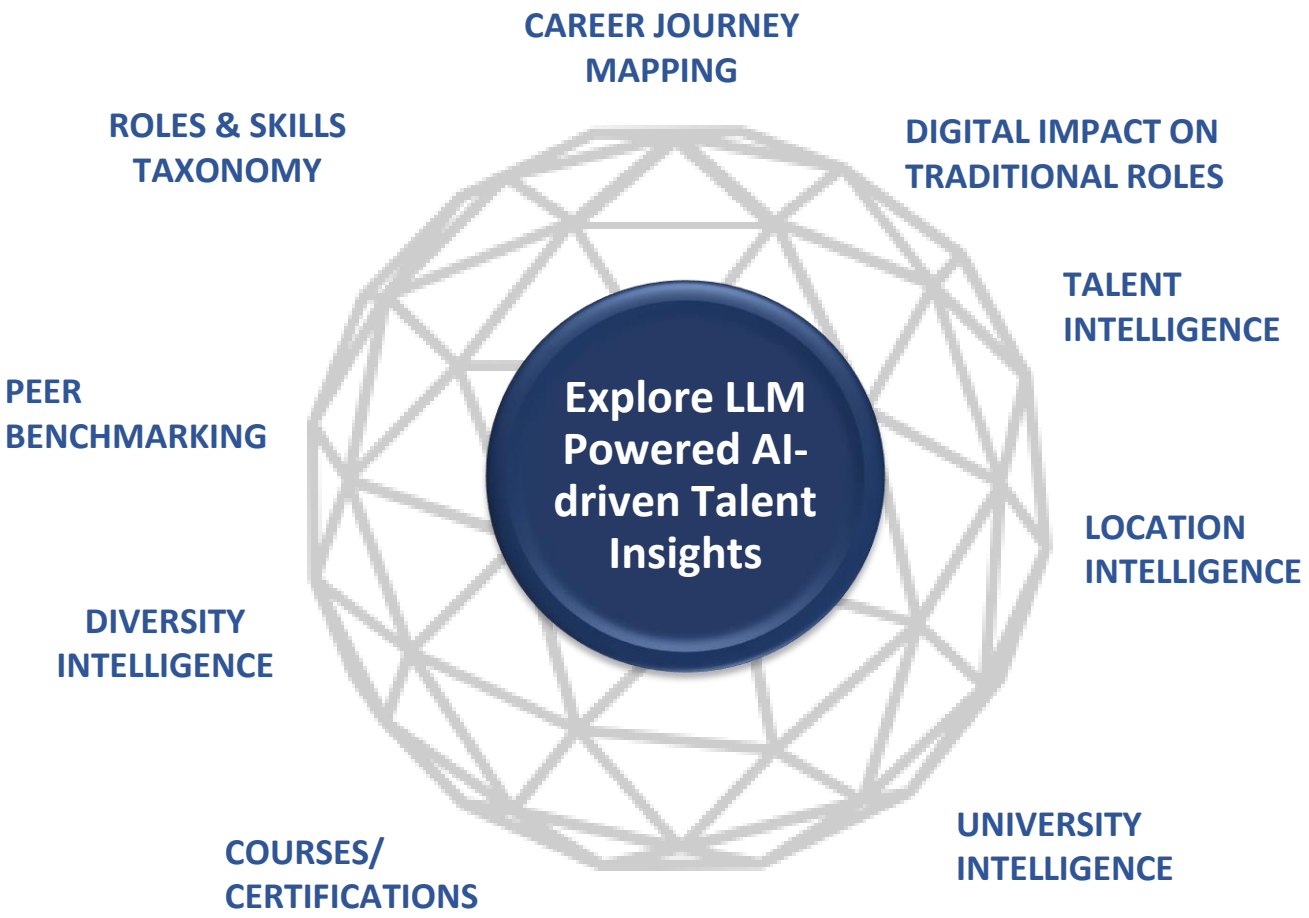
Overall cost saved by the company

~$10.82K

Note: 1. FTE is Full Time Employee *Non-Recurring Cost: one-time expense during the hiring process, including advertising costs, background check fees, travel expenses for interviews, sign-on bonuses, relocation expenses, etc. Analysis based on Draup's insights from customer engagement, industry blogs, and whitepapers.

Draup leverages Machine learning models to curate Reskilling insights provided in the report. Similar analysis can be performed for 4,500+ job roles and any Business function.

Draup Capabilities & Data Assets



EMPOWERS DECISION MAKING IN

- Reskilling/Upskilling
- Career Path Development
- Strategic Workforce Planning
- Talent Acquisition
- Peer Intelligence
- Diversity & Inclusion
- Global Locations Footprint
- Digital Transformation

and diverse other use cases…

Draup for Talent: Draup analyses 16+ Million data attributes every day to help global HR leaders in Planning, Hiring & Reskilling their Future-Ready Workforce

800M+
PROFESSIONALS

4,500+
JOB ROLES

1M+
PEER GROUP COMPANIES

33
INDUSTRIES

380M+
JOB DESCRIPTIONS

300,000+
COURSES

2,500+
LOCATIONS

53,000+
UNIVERSITIES

4M+
CAREER PATHS ANALYZED

30,000
SKILLS

47,000+
DIGITAL TOOLS & PLATFORMS

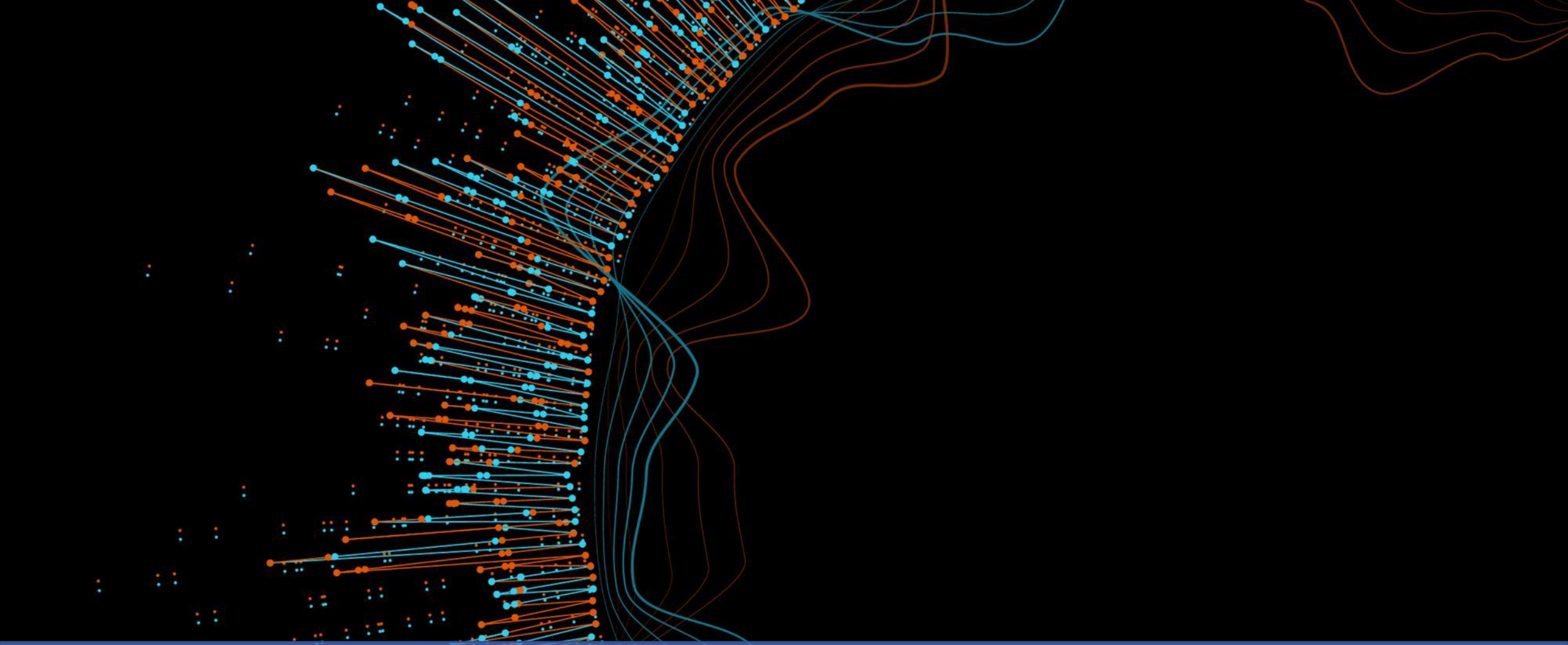
175,000+
UNIVERSITY PROFESSORS

75+
MACHINE LEARNING MODELS DEYELOPED

16M+
DAILY DATA POINTS ANALYZED

100+
LABOR STATISTIC DATABASE

1,000+
CUSTOM TALENT REPORTS



draup

www.draup.com

HOUSTON I BANGALORE